Polityka Certyfikacji i Kodeks Postępowania Certyfikacyjnego

Kwalifikowanych Usług Zaufania EuroCert

wersja 5.0

Data wejścia w życie 02.04.2024

EuroCert Sp. z o.o.
ul. Puławska 474
02-884 Warszawa
https://eurocert.pl

Metryczka regulacji

Informacje ogólne		
Sygnatura		0-PT-025-05
Status		Zatwierdzona
Zatwierdzony przez		Łukasz Konikiewicz
Data zatwierdzenia		18.03.2024
Poufność, Integralność, Dostępność, Archiwizacja (PIDA)		
Klasa Poufności		0 - Jawne
Klasa Integralności		2 - Weryfikowalna
Dostępność	Klasa Uprawnień Dostępu	1 - Powszechnie Dostępne Zarządzane
	Klasa Krytyczności Czasu Dostępu	2 - Istotna
Wymóg archiwizacji		B20 - dwudziestoletni okres archiwizacji

Historia zmian		
Wejście w życie	Wersja	Dokonane zmiany
02.10.2018 r.	1	Wersja inicjalna powstała z połączenia dotychczasowych: Kodeksu postępowania certyfikacyjnego kwalifikowanych usług zaufania, Polityki certyfikacji dla kwalifikowanych certyfikatów, Polityki certyfikacji dla kwalifikowanych znaczników czasu.
19.06.2019	2	dodanie możliwości realizacji usługi podpisu/pieczęci w trybie zdalnym, wydłużenie czasu na unieważnienie certyfikatu do 24 godzin, umożliwienie samodzielnego generowania kluczy przez subskrybentów.
21.08.2019	3	Uwzględnienie nowej usługi: wydawania kwalifikowanych certyfikatów uwierzytelniania witryn internetowych.
22.04.2020	3.1	zmiana sposobu zawierania umowy poprzez akceptację warunków świadczenia usług, korekta definicji urządzenia QSCD, korekty językowe.
31.03.2021	4.0	Dodanie metody zdalnej weryfikacji tożsamości w rozdziale 3.2.
21.06.2023	4.1	Dodanie do profilu certyfikatu usługi OCSP.
02.04.2024	5.0	Całkowita zmiana treści, wprowadzenie certyfikatów email S/MIME oraz certyfikatów podpisu elektronicznego z pseudonimem.

Spis treści

1. Wstęp

Niniejszy dokument stanowi Politykę Certyfikacji i Kodeks Postępowania Certyfikacyjnego, należące do EuroCert Sp. z o.o. (zwaną dalej EuroCert lub Kwalifikowanym Dostawcą Usług Zaufania - QTSP), dotyczące wydawania zgodnych z eIDAS (1) kwalifikowanych:

1) Certyfikatów Podpisów Elektronicznych,
2) Certyfikatów Pieczęci Elektronicznych,
3) Certyfikatów Uwierzytelniania Witryn Internetowych,
4) Elektronicznych Znaczników Czasu.

PCKPC jest zgodny z wymaganiami eIDAS (1). Usługi dostarczane w ramach niniejszych przepisów są Kwalifikowanymi Usługami Zaufania UE.

QTSP powiadomił Ministra właściwego ds. cyfryzacji o świadczeniu Usług Zaufania w dniu 1 lipca 2016 roku.

Certyfikaty Uwierzytelniania Witryn Internetowych dla osób prawnych zgodnie z wymaganiami PCKPC spełniają wymagania certyfikatów EV (Extended Validation) określonych w CA/Browser Forum (2).

Audyt zgodności Kwalifikowanych Usług Zaufania został przeprowadzony przez niezależną jednostkę Tayllorcox PCEB (dalej jako: Tayllorcox).

Na podstawie pozytywnego wyniku audytu Organ Nadzoru zarejestrował Kwalifikowane Usługi Zaufania i opublikował stosowne informacje na polskiej Liście Zaufania (3) w dniu 30 czerwca 2017 r.

QTSP dostarcza swoim Klientom najważniejsze informacje również w formie Regulaminu (4). Regulamin jest publikowany zgodnie z wytycznymi zawartymi w sekcji 2.1.

QTSP świadczy usługi na podstawie umowy z Klientem.

PCKPC określa ramy świadczenia wyżej wymienionych usług, szczegółowe procedury i inne zasady działania. Zawiera również zalecenia dla Stron Ufających w zakresie weryfikacji Podpisów (Pieczęci) Elektronicznych, Elektronicznych Znaczników Czasu i Certyfikatów powiązanych z tymi usługami.

1.1. Wprowadzenie

Polityka Certyfikacji to zbiór zasad, które określają użyteczność Certyfikatu, Znacznika Czasu dla podmiotów i/lub określonej kategorii zastosowania, posiadających te same wymagania bezpieczeństwa.

Niniejszy dokument zawiera wymagania dla wielu Polityk Certyfikacji. Zdecydowana większość tych wymagań jest wspólna dla wszystkich Polityk Certyfikacji w takim samym zakresie i nie są specjalnie wyszczególniane. Tam, gdzie wymagania mają być traktowane inaczej, zostanie wyraźnie wskazane do której Polityki Certyfikacji odnoszą się dane wymagania.

Certyfikaty wydane zgodnie z niniejszym dokumentem zawierają identyfikator (OID) Polityki Certyfikacji, z którą są zgodne. Na podstawie tego identyfikatora Strony Ufające mogą sprawdzić stosowność i wiarygodność certyfikatów w kontekście konkretnego zastosowania.

Polityki Certyfikacji określają podstawowe wymagania w stosunku do Certyfikatów i Znaczników Czasu, przede wszystkim dla ich wystawcy, tj. QTSP. Sposób realizacji tych wymagań oraz szczegółowy opis procedur wymienionych w Polityce Certyfikacji zostały zawarte w PCKPC.

PCKPC jest jednym z wielu dokumentów wydanych przez QTSP, które wspólnie regulują zasady i warunki świadczenia usług. Inne istotne dokumenty to np. Regulamin oraz umowy z Klientami i partnerami.

Celem niniejszego dokumentu jest podsumowanie wszystkich informacji, które powinien znać Klient, który chciałby skorzystać z oferty QTSP, po to, aby pomóc Klientom (w tym potencjalnym):

1) lepiej zapoznać się ze szczegółami i warunkami usług oraz praktycznymi aspektami świadczenia usług,
2) zrozumieć działalność QTSP i przez to łatwiej zdecydować czy usługi są odpowiednie, i które usługi odpowiadają indywidualnym potrzebom czy oczekiwaniom.

Dodatkowo, niniejszy dokument ma na celu wsparcie użytkowników (w tym Stron Ufających) Certyfikatów, list CRL, odpowiedzi dotyczących statusu certyfikatów online oraz Znaczników Czasu wydawanych przez QTSP po to, aby mogli oni jednoznacznie zrozumieć sposób ich obsługi, poziom gwarantowanego przez nie bezpieczeństwa oraz odpowiednie techniczne, biznesowe i finansowe gwarancje i odpowiedzialność prawną z nimi związaną.

Zawartość i format dokumentu są zgodne z wymaganiami IETF RFC 3647 (5). Niniejszy dokument podzielony jest na 9 sekcji i zawiera wymagania bezpieczeństwa, procesy i praktyki określone przez QTSP, przestrzegane przy świadczeniu usług. W celu ścisłego przestrzegania struktury dokumentu wymaganej przez IETF RFC 3647 (5), dokument zawiera również te rozdziały, dla których PCKPC nie nakłada wymagań, które zostały opatrzone uwagą „Brak zastrzeżeń".

Poza niniejszym dokumentem działania użytkownika końcowego związane z wykorzystywaną usługą mogą podlegać innym wymogom znajdującym się w Regulaminie i umowach zawartych z dostawcą oraz w innych regulacjach i dokumentach niezależnych od QTSP.

Sekcja 1.6 niniejszego dokumentu określa znaczenia terminów, które nie są - lub nie są w pełni - użyte w innych obszarach w tym znaczeniu. Terminy użyte w tym znaczeniu są w dokumencie pisane wielką literą i kursywą.

1.2. Nazwa dokumentu i identyfikator

1.2.1. Dane identyfikacyjne dokumentu

Wydawca	EuroCert Sp. z o.o.
Nazwa dokumentu	Polityka Certyfikacji i Kodeks Postępowania Certyfikacyjnego Kwalifikowanych Usług Zaufania EuroCert
Wersja dokumentu	5.0
Data obowiązywania	02.04.2024

Lista i identyfikatory Polityk Certyfikacji, określonych w PCKPC są dostępne w sekcji 1.2.2.

Aktualna wersja PCKPC jest dostępna na stronie internetowej: https://eurocert.pl/category/documents/.

1.2.2. Polityki Certyfikacji

Wszystkie Certyfikaty wydane przez QTSP odnoszą się do tej Polityki Certyfikacji, na podstawie której zostały wydane.

Pierwsze pięć numerów OID, które identyfikują Politykę Certyfikacji stanowi unikalny identyfikator EuroCert:

(1)	International Organization for Standardization (ISO)
(2)	ISO Member Bodies
(616)	Poland
(1)	Organizations
(113791)	EuroCert Sp. z o.o.

Kolejne numery zostały przypisane przez EuroCert według własnego uznania wraz z poniższym znaczeniem:

(1.2.616.1.113791)	EuroCert Sp. z o.o.
(1)	Centrum Kwalifikowane EuroCert
(2)	Publiczne dokumenty
(x)	Unikalny identyfikator dokumentu

Zgodnie z PCKPC, QTSP wydaje Certyfikaty i Znaczniki Czasu na podstawie następujących Polityk Certyfikacji:

OID	PRZEZNACZENIE CERTYFIKATÓW	SKRÓT
1.2.616.1.113791.1.2.2	Polityka certyfikacji dla kwalifikowanych certyfikatów, do generowania i weryfikacji kwalifikowanych podpisów elektronicznych, dla osób fizycznych, wydawanych na Kwalifikowanym Urządzeniu do Składania Podpisu Elektronicznego.	QATBP
1.2.616.1.113791.1.2.4	Polityka certyfikacji dla kwalifikowanych certyfikatów, do generowania i weryfikacji zaawansowanych podpisów elektronicznych, dla osób fizycznych, wydawanych na Urządzeniu Kryptograficznym.	QATHP
1.2.616.1.113791.1.2.5	Polityka certyfikacji dla kwalifikowanych certyfikatów, do generowania i weryfikacji zaawansowanych podpisów elektronicznych, dla osób fizycznych, wydawanych bez urządzenia (do pliku).	QATSP
1.2.616.1.113791.1.2.3	Polityka certyfikacji dla kwalifikowanych certyfikatów, do generowania i weryfikacji kwalifikowanych pieczęci elektronicznych, dla os. prawnych, wydawanych na Kwalifikowanym Urządzeniu do Składania Pieczęci Elektronicznej, zakazująca używania pseudonimu.	QBJBN
1.2.616.1.113791.1.2.6	Polityka certyfikacji dla kwalifikowanych certyfikatów, do generowania i weryfikacji zaawansowanych pieczęci elektronicznych, dla os. prawnych, wydawanych na Urządzeniu Kryptograficznym, zakazująca używania pseudonimu.	QBJHN
1.2.616.1.113791.1.2.7	Polityka certyfikacji dla kwalifikowanych certyfikatów, do generowania i weryfikacji zaawansowanych pieczęci elektronicznych, wydawanych bez urządzenia (do pliku) dla os. prawnych, zakazująca używania pseudonimu.	QBJSN

1.2.616.1.113791.1.2.1	Polityka Certyfikacji dla kwalifikowanych certyfikatów uwierzytelniania witryn internetowych, dla os. prawnych, zakazująca używania pseudonimu.	QWJSN
1.2.616.1.113791.1.2.8	Polityka certyfikacji dla kwalifikowanych certyfikatów S/MIME, które mogą być również użyte do generowania i weryfikacji podpisów (pieczęci) elektronicznych, dla osób fizycznych lub prawnych, zakazująca używania pseudonimu.	QSxxN
1.2.616.1.113791.1.4	Kwalifikowana polityka znakowania czasem.	-

Zasady tworzenia i interpretacji skrótów nazw Polityk Certyfikacji można znaleźć w Załączniku A do niniejszego dokumentu.

W przypadku Polityk Certyfikacji dotyczących Certyfikatów przeznaczonych dla osób fizycznych, Podmiotem jest zawsze osoba fizyczna.

W przypadku Polityk Certyfikacji dotyczących Certyfikatów przeznaczonych dla innych osób niż osoby fizyczne, Podmiotem jest zawsze osoba prawna.

Na podstawie Polityki Certyfikacji [QWJSN], QTSP wydaje Certyfikaty Uwierzytelniania Witryn Internetowych.

W przypadku Certyfikatów Uwierzytelniania Witryn Internetowych w miejscu nazwy Podmiotu podana jest nazwa domeny.

Certyfikaty Uwierzytelniania Witryn Internetowych, Certyfikaty Email oraz Certyfikaty Pieczęci Elektronicznych nie mogą być wydane z pseudonimem.

QTSP stosuje się do aktualnej wersji dokumentu pt. „Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" (6), wydanego przez CA/Browser Forum dostępnego pod adresem https://cabforum.org/baseline-requirements-documents/.

W przypadku sprzeczności pomiędzy niniejszym dokumentem a powyższym, pierwszeństwo mają wymogi „Baseline Requirements".

QTSP stosuje się do aktualnej wersji dokumentu "CA/Browser Forum Guidelines for Issuance and Management of Extended Validation Certificates" (2), wydanego przez CA/Browser Forum dostępnego pod adresem https://cabforum.org/extended-validation/.

W przypadku sprzeczności pomiędzy niniejszym dokumentem a powyższym, pierwszeństwo mają wymagania "EV Guidelines".

Z wyjątkiem Certyfikatów Podpisu Elektronicznego, Certyfikaty mogą również zawierać nazwy systemów IT, aplikacji i mechanizmu automatyzacji, za pomocą których Certyfikat jest używany (Certyfikaty dla automatyzacji).

W przypadku Polityk Certyfikacji [xxxBx], wymagających użycia Kwalifikowanego Urządzenia do Składania Podpisu (Pieczęci) Elektronicznego QTSP upewnia się, że klucz prywatny związany z Certyfikatem jest umieszczony w Kwalifikowanym Urządzeniu do Składania Podpisu (Pieczęci) Elektronicznego, posiadającego certyfikację wydaną przez uprawniony organ certyfikacyjny zarejestrowany w państwie członkowskim UE.

W przypadku Polityki Certyfikacji ([xxxHx]), która wymaga użycia Urządzenia Kryptograficznego QTSP gwarantuje, że klucz prywatny należący do Certyfikatu jest przechowywany jedynie na takim Urządzeniu Kryptograficznym, dla którego wydano przynajmniej jeden z poniższych certyfikatów:

1) Certyfikat wydany w dowolnym kraju członkowskim Unii Europejskiej stwierdzający, że sprzęt jest Kwalifikowanym Urządzeniem do Składania Podpisu Elektronicznego;
2) Certyfikat Common Criteria (7) zgodny z profilem CEN SSCD PP (8) na poziomie EAL-4 lub wyższym;
3) Certyfikat Common Criteria (7) zgodny z profilem CEN 419 221-5 (9) na poziomie EAL-4 lub wyższym;
4) FIPS 140-2 na poziomie 2 lub wyższym (10);
5) FIPS 140-3 na poziomie 2 lub wyższym (11).

Zaawansowane podpisy (pieczęci) elektroniczne oparte na Kwalifikowanym Certyfikacie mogą być tworzone automatycznie i bezpośrednio, bez osobistego nadzoru, przy użyciu narzędzi IT określonych w przepisach prawa.

Certyfikaty zgodne z Politykami Certyfikacji wymagającymi użycia Kwalifikowanego Urządzenia do Składania Podpisu Elektronicznego [xxxBx] lub Urządzenia Kryptograficznego [xxxHx] mogą być wydane w ramach Usługi Zdalnego Podpisu, jeśli:

1) Usługa taka jest świadczona przez Kwalifikowanego Dostawcę Usług Zaufania;
2) Klucz prywatny użytkownika jest zarządzany w Kwalifikowanym Urządzeniu do Składania Podpisu Elektronicznego lub Urządzeniu Kryptograficznym posiadającym odpowiednie certyfikaty (zob. sekcje 6.2.1, 6.2.11, 8);
3) Usługa jest certyfikowana na zgodność przez niezależnego akredytowanego audytora, raport z oceny zgodności dowodzi, że Usługa Zdalnego Podpisu spełnia odpowiednie wymagania;
4) Kwalifikowany Dostawca Usług Zaufania oświadcza na piśmie, że zarządza kluczem prywatnym należącym do klucza publicznego wskazanego w Certyfikacie, w Kwalifikowanym Urządzeniu do Składania Podpisu Elektronicznego lub Urządzeniu Kryptograficznym, odpowiednio, zgodnie z certyfikacją urządzenia.

Usługa Zdalnego Podpisu spełnia wymagania następującej polityki usługi zaufania określonej w ETSI TS 119 431-1 (12):

- EU SSASC Policy (EUSCP OID: 0.4.0.19431.1.1.3).

Klucz prywatny odpowiadający Certyfikatowi wydanemu na podstawie Polityki Certyfikacji [xxxBx] wymagającej użycia Kwalifikowanego Urządzenia do Składania Podpisu Elektronicznego [xxxBx] jest chroniony przez Kwalifikowane Urządzenie do Składania Podpisu Elektronicznego. Kwalifikowany Podpis Elektroniczny (Pieczęć) może być stworzony tylko na podstawie takiego Certyfikatu.

Jeśli kwalifikowana Polityka Certyfikacji, na podstawie której wydano kwalifikowany Certyfikat nie wymaga Kwalifikowanego Urządzenia do Składania Podpisu Elektronicznego, można złożyć jedynie zaawansowany podpis (pieczęć) przy użyciu takiego kwalifikowanego Certyfikatu.

W przypadku Certyfikatów Email (S/MIME) QTSP spełnia wymogi aktualnej wersji dokumentu “Baseline Requirements for the Issuance and Management of Publicly Trusted S/MIME Certificates" (13) na stronie https://cabforum.org/smime-br/.

W przypadku sprzeczności pomiędzy niniejszym dokumentem a powyższym, pierwszeństwo mają wymagania “Baseline Requirements…”.

Wśród wszystkich Polityk Certyfikacji:

1) Polityki Certyfikacji [QATBN], [QATHN], [QATSN] są zgodne z Polityką Certyfikacji [QCP-n]] określoną w normie ETSI EN 319 411-2 (14);
2) Polityka Certyfikacji [QATBN] jest zgodna z Polityką Certyfikacji [QCP-n-qscd] określoną w normie ETSI EN 319 411-2 (14);
3) Polityki Certyfikacji [QBJBN], [QBJHN], [QBJSN] są zgodne z Polityką Certyfikacji [QCP-l] określoną w normie ETSI EN 319 411-2 (14);
4) Polityki Certyfikacji [QATHN], [QBJHN] są zgodne z Polityką Certyfikacji [NCP+] określoną w normie ETSI EN 319 411-1 (15);
5) Polityka Certyfikacji [QBJBN] jest zgodna z Polityką Certyfikacji [QCP-l-qscd] określoną w normie ETSI EN 319 411-2 (14);
6) Polityka Certyfikacji [QSxxN] jest zgodna z Polityką Certyfikacji [QCP-n-qscd] określoną w normie ETSI EN 319 411-2 (14), gdy certyfikat jest wydany na QSCD;
7) Polityka Certyfikacji [QSxxN] jest zgodna z Polityką Certyfikacji [QCP-l-qscd] określoną w normie ETSI EN 319 411-2 (14), gdy certyfikat jest wydany na QSCD;
8) Polityka Certyfikacji [QWJSN] jest zgodna z Polityką Certyfikacji [QEVCP-w] określoną w normie ETSI EN 319 411-2 (14);
9) Polityka Certyfikacji [QWJSN] w związku z PSD2 jest zgodna z Polityką Certyfikacji [QCP-w-psd2] określoną w normie ETSI TS 119 495 (16).

Zgodność z Politykami Certyfikacji ETSI

1) Zgodność Znaczników Czasu

Znaczniki Czasu wydane zgodnie z PCKPC są zgodne z wymaganiami poniżej:

- ETSI EN 319 421 (17)
  BTSP: a best practices policy for time stamp
  OID: itu-t(0) identified-organization(4) etsi(0)time-stamp-policy(2023)policy-identifiers(1)best-practices-ts-policy (1)

QTSP umieszcza swój własny OID w swoich Znacznikach Czasu i przestrzega wyżej wspomnianej polityki znakowania czasem ETSI (BTSP).

2) Zgodność Certyfikatów

W przypadku, kiedy Polityka Certyfikacji ETSI opiera się na innej Polityce ETSI i już zawiera wszystkie jej wymagania, w wydanych Certyfikatach podaje się jedynie identyfikator Polityki Certyfikacji wyższego rzędu, która zawiera już wymagania tej drugiej.

	[QCP-n]	[QCP-n-qscd]	[QCP-l]	[QCP-l-qscd]	[NCP]	[NCP+]	OVCP	EVCP	QEVCP-w	QCP-w-psd2
QATBN	(x)	X								
QATHN	X					X				
QATSN	X									
QBJBN			(x)	X						
QBJHN			X			X				
QBJSN			X							
QSxxN	X		X							

	[QCP-n]	[QCP-n-qscd]	[QCP-l]	[QCP-l-qscd]	[NCP]	[NCP+]	OVCP	EVCP	QEVCP-w	QCP-w-psd2
QSxxN (QSCD)	(x)	X	(x)	X						
QWJSN (normal)					(x)		(x)	(x)	X	
QWJSN (Open Banking)					(x)		(x)	(x)	X	
QWJSN (PSD2)					(x)		(x)	(x)	(x)	X

1.2.3. Zakres obowiązywania

Zakres przedmiotowy

PCKPC dotyczy świadczenia i korzystania z usług opisanych w sekcji 1.3.1.

Zakres czasowy

Niniejszy dokument wchodzi w życie z dniem 02.04.2024 i obowiązuje do odwołania. Przestaje obowiązywać automatycznie w momencie wejścia w życie nowszej wersji PCKPC lub zakończenia działalności.

PCKPC jest przeglądany przynajmniej raz w roku i aktualizowany w razie konieczności, w celu odzwierciedlenia wszelkich zmian wymogów lub potrzeb.

Zakres osobowy

PCKPC dotyczy każdego uczestnika wymienionego w sekcji 1.3.

QTSP dostarcza usługi zaufania głównie obywatelom krajów Unii Europejskiej oraz organizacjom zarejestrowanym na obszarze Unii Europejskiej, co jednak nie wyklucza osób fizycznych czy prawnych z innych państw, o ile zaakceptują zasady QTSP i pod warunkiem, że niezbędne środki bezpieczeństwa konieczne do świadczenia usług będą mogły być wdrożone w wystarczająco bezpieczny i ekonomiczny sposób.

Osoby z niepełnosprawnościami

QTSP dokłada wszelkich starań, by zapewnić dla wszystkich usługi najwyższej jakości oraz równe szanse dostępu do usług.

W celu zapewnienia równego dostępu do usług QTSP stosuje wszystkie możliwe i rozsądne środki, by udostępnić swoje usługi również osobom niepełnosprawnym. Szczególnie ważne jest, aby usługi dostosowane do specjalnych potrzeb niepełnosprawnych gwarantowały tą samą jakość, jak w innych przypadkach.

QTSP współpracuje z Klientami w celu dostarczenia najbardziej odpowiedniej formy usługi w celu zaspokojenia ich osobistych potrzeb w ramach przewidzianych przez PCKPC.

Zasięg geograficzny

PCKPC jest opracowany w oparciu o wymogi Unii Europejskiej, ale może zawierać również specyficzne wymagania dla usług świadczonych w Polsce na gruncie prawa polskiego.

QTSP może rozszerzyć zasięg terytorialny świadczonych usług z utrzymaniem co najmniej tak surowych zasad jak te przedstawione w PCKPC. W przypadku usług świadczonych Klientom zagranicznym szczegółowe warunki różniące się od PCKPC mogą zostać umieszczone w poszczególnych umowach.

Usługa świadczona na podstawie PCKPC jest dostępna na całym świecie. Certyfikaty, listy CRL, odpowiedzi OCSP i Znaczniki Czasu wydane zgodnie z PCKPC są ważne niezależnie od miejsca, w którym zostały zamówione i w którym będą używane i walidowane.

Usługa świadczona zgodnie z PCKPC może być używana wyłącznie w zakresie opisanym w niniejszym dokumencie.

1.2.4. Poziomy bezpieczeństwa

QTSP wyznaczył poziomy bezpieczeństwa biorąc pod uwagę kryteria bezpieczeństwa w poniżej opisany sposób.

Klasyfikacja według siły uwierzytelnienia Podmiotu Certyfikatu w kolejności malejącej:

a) kwalifikowane Certyfikaty [Q****];
b) niekwalifikowane Certyfikaty, klasa certyfikacji III. [A****] wydane przez EuroCert;
c) niekwalifikowane Certyfikaty, klasa certyfikacji II. [B****] wydane przez EuroCert;
d) niekwalifikowane Certyfikaty wydane przez inny podmiot niż EuroCert.

Klasyfikacja według poziomu bezpieczeństwa użytego sprzętowego nośnika w malejącej kolejności:

a) certyfikaty wydane na Kwalifikowanym Urządzeniu do Składania Podpisu Elektronicznego [***B*];
b) certyfikaty wydane na Urządzeniu Kryptograficznym [***H*];
c) inne, na przykład Certyfikaty wydane do pliku, bez sprzętowej ochrony (bez urządzenia) [***S*].

Na podstawie powyższych dwóch kategorii QTSP stworzył poniższy zagregowany ranking bezpieczeństwa w kolejności malejącej:

a) certyfikaty kwalifikowane wydane na Kwalifikowanym Urządzeniu do Składania Podpisu Elektronicznego [Q**B*];
b) certyfikaty kwalifikowane wydane na Urządzeniu Kryptograficznym [Q**H*];
c) inne kwalifikowane, na przykład Certyfikaty wydane do pliku bez urządzenia [Q**S*];
d) certyfikaty niekwalifikowane, klasa certyfikacji III. wydane przez EuroCert [A**S*];
e) certyfikaty niekwalifikowane, klasa certyfikacji II. wydane przez EuroCert [B**S*];
f) certyfikaty niekwalifikowane wydane przez innego dostawcę niż EuroCert.

Podczas komunikacji z Klientami, QTSP używa elektronicznych kanałów komunikacji i umożliwia wykorzystanie podpisu (pieczęci) elektronicznego w większości przypadków.

Co do zasady, podczas załatwiania spraw administracyjnych związanych z Certyfikatami Klient może użyć swojego własnego Certyfikatu w celu uwierzytelnienia dokumentów elektronicznych, o ile ten Certyfikat posiada co najmniej taki sam poziom bezpieczeństwa (zgodnie z powyższą klasyfikacją) jak odpowiedni Certyfikat, będący przedmiotem sprawy.

W wyjątkowych przypadkach, rozpatrywanych indywidualnie, QTSP może odstąpić od ścisłego przestrzegania powyższej klasyfikacji dla określonych podzadań w określonych przypadkach (na przykład odstąpienie od fizycznej weryfikacji w przypadku wniosku o nowy kwalifikowany Certyfikat lub jego modyfikację, w przypadku posługiwania się we wniosku Certyfikatem III klasy, gdyż taki sam wymóg fizycznej weryfikacji obowiązuje dla Certyfikatów III klasy i kwalifikowanych Certyfikatów).

1.3. Uczestnicy PKI

Korzystającymi z usług świadczonych w ramach PCKPC są:

a) EuroCert,
b) Klienci EuroCert (Subskrybenci i Podmioty),
c) Strony Ufające,
d) Inni uczestnicy.

1.3.1. Urząd Certyfikacji

Urząd certyfikacji jest Dostawcą Usług Zaufania, który wydaje Certyfikaty i Znaczniki Czasu w ramach Usługi Zaufania oraz świadczy usługi z nimi związane. Identyfikuje on osobę ubiegającą się o Certyfikat, prowadzi ewidencję danych, akceptuje zmiany związane z Certyfikatami i publikuje regulacje dotyczące Certyfikatów, klucze publiczne i informacje na temat aktualnego statusu ważności Certyfikatu (w szczególności o jego możliwym unieważnieniu). Ta działalność jest również nazywana Usługą Certyfikacyjną.

Wymagania niniejszego dokumentu odnoszą się do każdego Urzędu Certyfikacji, który zapewnia w swoim Kodeksie Postępowania Certyfikacyjnego, zgodność z dowolną Polityką Certyfikacji opisaną w niniejszym dokumencie.

Dane Urzędu Certyfikacji

Nazwa:	EuroCert Sp. z o.o.
KRS:	0000408592 Krajowy Rejestr Sądowy prowadzony przez Sąd Rejonowy dla m. st. Warszawy, XIII Wydział Gospodarczy
Siedziba:	Polska, 02-884 Warszawa, ul. Puławska 472.
Telefon:	(+48) 22 390 59 95
Adres internetowy:	https://www.eurocert.pl, https://www.sklep.eurocert.pl

Biuro Obsługi Klienta

Nazwa jednostki:	EuroCert Sp. z o.o.
Obsługa Klienta:	Polska, 02-884 Warszawa, ul. Puławska 472.
Godziny otwarcia:	dni robocze 8:00-16:00
Telefon:	(+48) 22 390 59 95
Email:	handlowy@eurocert.pl
Wnioski o unieważnienie:	uniewaznienia@eurocert.pl
Informacje o usługach:	https://www.eurocert.pl
Miejsce składania reklamacji:	EuroCert Sp. z o.o. Polska, 02-884 Warszawa, ul. Puławska 472
Urząd Ochrony Danych Osobowych:	Prezes Urzędu Ochrony Danych Osobowych 00-193 Warszawa, ul. Stawki 2
Urząd Ochrony Konkurencji i Konsumentów	https://uokik.gov.pl

Prezentacja Dostawcy Usług Zaufania

EuroCert jest kwalifikowanym dostawcą usług zaufania na terenie UE w rozumieniu eIDAS (1) .

EuroCert rozpoczął świadczenie usług związanych z podpisem elektronicznym na podstawie Ustawy o Podpisie Elektronicznym z 2001 r. (18) (zwaną dalej: Ustawą o podpisie elektronicznym):

- Usługi certyfikacyjne związane z kwalifikowanymi podpisami elektronicznymi, zgodnie z Ustawą o podpisie elektronicznym od 23 grudnia 2013 r. (numer rejestracji podmiotu: 1/10573-13/13).

Wraz z wejściem w życie dnia 1 lipca 2016 r. Rozporządzenia eIDAS (1) oraz polskiej Ustawy implementującej z dnia 5 września 2016 o Usługach Zaufania oraz Identyfikacji Elektronicznej (19) cały system usług związanych z podpisami elektronicznymi został ujednolicony na poziomie europejskim.

EuroCert zaczął wydawać kwalifikowane certyfikaty eIDAS dla osób fizycznych z dniem 1 lipca 2016 r.

Od 20 września 2017 EuroCert zaczął dostarczać następujące kwalifikowane usługi zaufania zgodnie z eIDAS:

- Kwalifikowane znakowanie czasem.

Od 1 października 2018 EuroCert zaczął dostarczać następujące kwalifikowane usługi zaufania zgodnie z eIDAS:

- Kwalifikowane certyfikaty dla pieczęci elektronicznych.

Od 1 października 2019 EuroCert zaczął dostarczać następujące kwalifikowane usługi zaufania zgodnie z eIDAS:

- Kwalifikowane certyfikaty do uwierzytelniania witryn internetowych.

Od 7 maja 2020 EuroCert zaczął dostarczać następujący komponent kwalifikowanych usług zaufania zgodnie z eIDAS:

- Zdalną usługę zarządzania kluczem przeznaczoną do zdalnego składania kwalifikowanych podpisów i pieczęci elektronicznych (tzw. Zdalną Usługę Podpisu).

Jakość i bezpieczeństwo informacji

EuroCert posiada dwupoziomowy system analizy ryzyka, który pokrywa oprócz ryzyka IT również całą organizację i ryzyko biznesowe. Analiza ryzyka jest weryfikowana co najmniej raz w roku. W oparciu o wyniki tej analizy QTSP:

a) podejmuje działania służące wyeliminowaniu wykrytych podatności i/lub
b) akceptuje zidentyfikowane ryzyka rezydualne wraz z uzasadnieniem takiej decyzji.

QTSP nie ujawnia swojej wewnętrznej Polityki Bezpieczeństwa z powodu jej poufnego charakteru. QTSP informuje swoich wykonawców, podwykonawców i inne zainteresowane strony o zasadach bezpieczeństwa, które ich dotyczą, w zakresie niezbędnym podczas zawierania umowy.

Jednostka organizacyjna świadcząca usługi certyfikacyjne

Urząd Certyfikacji „Centrum Kwalifikowane EuroCert" działający w ramach organizacji EuroCert odpowiada za wystawianie i zarządzanie Certyfikatami, publikację repozytorium Certyfikatów i informacji o statusie unieważnienia Certyfikatów, zarządzanie i dostarczanie Urządzeń do Składania

Podpisu Elektronicznego, świadczenie usługi statusu Certyfikatu online i zarządzanie regulacjami. EuroCert posiada własny Urząd Rejestracji.

Usługi

W ramach PCKPC, QTSP dostarcza Subskrybentom następujące usługi zaufania:

a) Wydawanie Certyfikatów kwalifikowanych zgodnych z eIDAS;
b) Wydawanie kwalifikowanych Certyfikatów Podpisów Elektronicznych podlegających eIDAS;
c) Wydawanie kwalifikowanych Certyfikatów Pieczęci Elektronicznych podlegających eIDAS;
d) Wydawanie kwalifikowanych Certyfikatów Uwierzytelniania Witryn Internetowych podlegających eIDAS;
e) Wydawanie kwalifikowanych Elektronicznych Znaczników Czasu;
f) Usługę Zdalnego Podpisu.

QTSP świadczy swoje usługi w ramach PCKPC jako kwalifikowany dostawca usług zaufania.

W przypadku Certyfikatów Uwierzytelniania Witryn Internetowych Podmiotem jest serwer sieciowy, zidentyfikowany przez nazwę domeny wskazaną w Certyfikacie. Aplikującym jest ta osoba fizyczna, która występuje w procesie ubiegania się o Certyfikat.

W celu świadczenia usług QTSP podpisuje z Subskrybentem umowę na świadczenie usług, w ramach której generuje kwalifikowane Certyfikaty dla Podmiotów wyznaczonych przez Subskrybenta. Certyfikat zapewnia certyfikowane połączenie pomiędzy danymi Podmiotu i kluczem publicznym należącym do klucza prywatnego, należącego do Podmiotu. W ramach umowy można wygenerować wiele Certyfikatów dla wielu Podmiotów.

W przypadku użycia kwalifikowanego certyfikatu wydanego na podstawie PCKPC, jeśli podpis elektroniczny (pieczęć) został złożony przy użyciu Kwalifikowanego Urządzenia do Składania Podpisu Elektronicznego, ten podpis elektroniczny (pieczęć) jest kwalifikowanym podpisem elektronicznym (pieczęcią). Jeśli podpis elektroniczny (pieczęć) nie został złożony przy użyciu Kwalifikowanego Urządzenia do Składania Podpisu Elektronicznego, wtedy ten podpis elektroniczny (pieczęć) jest zaawansowanym podpisem elektronicznym (pieczęcią) opartym na kwalifikowanym certyfikacie.

W przypadku ważnej subskrypcji Aplikujący może zainicjować następujące czynności:

a) aplikować o Certyfikat (i dodatkowo Urządzenie do Składania Podpisu/Pieczęci Elektronicznej), wydanie Certyfikatu odbywa się zgodnie z Polityką Certyfikacji lub politykami;
b) wystąpić o unieważnienie swojego Certyfikatu;
c) wystąpić o zawieszenie lub uchylenie zawieszenia swojego Certyfikatu.

Subskrybent może również wystąpić o unieważnienie, zawieszenie lub uchylenie zawieszenia Certyfikatu należącego do Podmiotu. Czynności te mogą zostać podjęte przez Administratora Organizacji upoważnionego przez Subskrybenta i zarejestrowanego przez QTSP.

QTSP publicznie udostępnia Listę Certyfikatów Unieważnionych. Lista ta zawiera wydane Certyfikaty, które zostały unieważnione. QTSP upublicznia również Certyfikat po uprzedniej zgodzie Aplikującego. Zawieszone, unieważnione lub wygasłe Certyfikaty są nieważne. Elektroniczne pieczęcie lub podpisy utworzone z nieważnym Certyfikatem nie mają mocy prawnej.

W przypadku Certyfikatów do Uwierzytelniania Witryn Internetowych zawieszenie nie jest możliwe.

QTSP wydaje również certyfikaty w celu przetestowania swojego systemu. Certyfikaty testowe nie mają mocy prawnej.

Na specjalną prośbę klienta, w indywidualnych przypadkach, QTSP może wydać nieodpłatne Certyfikaty produkcyjne do celów testowych. Z Certyfikatami utworzonymi w ten sposób należy obchodzić się z ostrożnie, gdyż mają one taki sam skutek prawny jak normalne Certyfikaty.

Typy Certyfikatów

Stosowane Polityki Certyfikacji omówione zostały w sekcji 1.2.2. Identyfikator stosowanej Polityki Certyfikacji jest zawsze podany w polu „CertificatePolicies" danego Certyfikatu.

Urząd Certyfikacji dostarcza swoim Klientom różne rodzaje Certyfikatów, które różnią się właściwościami i danymi uwierzytelniającymi Podmiot:

1) Certyfikat Organizacyjny:

    a) oznacza Certyfikat, w którym Podmiot jest Organizacją, urządzeniem pod kontrolą Organizacji; lub
    b) Certyfikat, który zaświadcza o związku pomiędzy osobą fizyczną (Podmiotem) a Organizacją; lub
    c) Certyfikat, który zaświadcza, że zawarta w nim domena należy do Organizacji.

    W takim przypadku, nazwa Organizacji określona jest w polu „O" w Certyfikacie.

    Nazwa Organizacji może być wskazana w Certyfikacie do Uwierzytelniania Witryn tylko w przypadku, gdy Organizacja jest legalnym użytkownikiem, właścicielem domeny lub ma odpowiednie do niej upoważnienie. Certyfikat do Uwierzytelniania Witryn nie może być wydany dla pseudonimu.

2) Certyfikat Profesjonalny oznacza Certyfikat wydany dla osoby fizycznej, który nie jest Certyfikatem Organizacyjnym i który zawiera tytuł lub nazwę zawodu Podmiotu w polu „Title".

3) Certyfikat dla Automatyzacji oznacza Certyfikat, w którym nazwa narzędzia IT (aplikacji lub systemu) używanego przez Podmiot jest wskazana wśród danych Podmiotu w Certyfikacie.

4) Certyfikat dla Pseudonimu oznacza Certyfikat, w którym nie ma oficjalnej nazwy Podmiotu, zweryfikowanej przez QTSP. W takich Certyfikatach nazwa jest podana w polu „Pseudonym" a w polu „CN" zaznacza się, że Certyfikat zawiera pseudonim.

5) Certyfikaty wymagające użycia Kwalifikowanego urządzenia do składania podpisu elektronicznego: w tym przypadku certyfikat jest wydany dla klucza publicznego, dla którego odpowiadający klucz prywatny został wygenerowany na QSCD – co gwarantuje, że klucz prywatny nie może być wyeksportowany lub skopiowany – wtedy taka informacja jest wskazana w certyfikacie w polu „QCStatements". Kwalifikowany podpis elektroniczny (pieczęć) może być złożony wyłącznie na podstawie Certyfikatu tego typu.

6) Certyfikat Osobisty oznacza Certyfikat, który nie zawiera pola „O" ani „Title". Ten typ może być wydany jedynie dla osób fizycznych.

QTSP wydaje Certyfikaty dla osób fizycznych i prawnych. W imieniu osób prawnych musi działać osoba uprawniona do reprezentacji lub osoba upoważniona przez reprezentanta.

Certyfikaty Testowe

QTSP wydaje certyfikaty testowe na własne potrzeby do testowania swojego systemu oraz stronom trzecim, by mogły przetestować usługi. Takie certyfikaty nie mają skutku prawnego a QTSP nie ponosi odpowiedzialności za ich wydanie, użycie i dostępność usługi z nimi związanych.

QTSP nie wydaje certyfikatów testowych w ramach działalności produkcyjnej głównej Jednostki Certyfikacji (root).

Wydawanie certyfikatów testowych odbywa się w ramach testowej Jednostki Certyfikacji Root stworzonej i działającej specjalnie w tym celu.

QTSP oznacza certyfikaty testowe w polu „CertificatePolicies" w następujący sposób (zob. sekcję 7.1.2):

- W Certyfikacie jako Polityka Certyfikacji występuje OID 1.2.616.1.113791.2.1.1.100 lub nic.

Urządzenia do Podpisu

QTSP umieszcza dane do składania podpisu elektronicznego (klucz prywatny) Podmiotu związane z certyfikatem na Urządzeniu do Składania Podpisu (Pieczęci) Elektronicznego, które odpowiada wymogom Kwalifikowanego Urządzenia do Składania Podpisu (Pieczęci) Elektronicznego zdefiniowanym w eIDAS (1). Użycie tych Kwalifikowanych Urządzeń do Składania Podpisu (Pieczęci) Elektronicznego jest warunkiem koniecznym dla złożenia kwalifikowanego podpisu (pieczęci) elektronicznego.

Jednostki Certyfikacji

Poniżej przedstawiono Jednostki Certyfikacji występujące w systemie urzędu certyfikacji EuroCert, podlegające PCKPC.

Kompletna hierarchia CA, uwzględniająca root i podległe CA: https://eurocert.pl/en/certyfikaty-i-listy-crl/.

Aktywna hierarchia RSA, oparta o algorytm SHA-512

- "Narodowe Centrum Certyfikacji" – Główna Jednostka Certyfikacji (Root)

Wydaje Certyfikaty oparte o algorytm SHA-512 dla Jednostek Certyfikacji i Jednostek Znakowania Czasem QTSP. Ta Jednostka Certyfikacji posiada samo podpisany Certyfikat SHA-512, oparty na kluczu RSA 4096 bit.

- Centrum Kwalifikowane EuroCert

Ta Jednostka Certyfikacji wydaje kwalifikowane certyfikaty dla osób fizycznych i prawnych zgodnie z Politykami Certyfikacji:

a) [QATBN] OID: 1.2.616.1.113791.1.2.2
b) [QATHN] OID: 1.2.616.1.113791.1.2.4
c) [QATSN] OID: 1.2.616.1.113791.1.2.5
d) [QBJBN] OID: 1.2.616.1.113791.1.2.3
e) [QBJHN] OID: 1.2.616.1.113791.1.2.6
f) [QBJSN] OID: 1.2.616.1.113791.1.2.7
g) [QSxxN] OID: 1.2.616.1.113791.1.2.8
h) [QWJSN] OID: 1.2.616.1.113791.1.2.1

- responder OCSP

Każda Jednostka Certyfikacji z Certyfikatem poświadcza osobny dedykowany urząd statusu certyfikatu online (OCSP responder), który udziela odpowiedzi na temat statusu unieważnienia Certyfikatów wydanych przez daną jednostkę certyfikacji. Nazwa respondera OCSP zawiera tekst „OCSP Responder"

występujący po nazwie danej jednostki certyfikacji. W Certyfikatach urzędu statusu certyfikatu online (OCSP responder) występuje rozszerzone użycie klucza "OCSPSigning".

Wszystkie powyższe pośrednie jednostki certyfikacji posiadają certyfikaty SHA-512 i wydają Certyfikaty końcowe oraz odpowiedzi OCSP oparte na algorytmie SHA-256. W tej hierarchii wszystkie certyfikaty Dostawcy używają kluczy RSA z długością klucza 4096 bitów.

W tej hierarchii wszystkie Certyfikaty wydane użytkownikowi końcowemu używają kluczy RSA o długości przynajmniej 2048 bitów lub kluczy ECC o długości co najmniej 256 bitów.

Najnowsza hierarchia oparta na krzywych eliptycznych (ECC)

- Centrum Kwalifikowane EuroCert

Produkcyjna pośrednia kwalifikowana jednostka certyfikacji, poświadczona przez Narodowe Centrum Certyfikacji. Ta Jednostka Certyfikacji wydaje kwalifikowane certyfikaty dla osób fizycznych i prawnych zgodnie z Politykami Certyfikacji:

a) [QATBN] OID: 1.2.616.1.113791.1.2.2
b) [QATHN] OID: 1.2.616.1.113791.1.2.4
c) [QATSN] OID: 1.2.616.1.113791.1.2.5
d) [QBJBN] OID: 1.2.616.1.113791.1.2.3
e) [QBJHN] OID: 1.2.616.1.113791.1.2.6
f) [QBJSN] OID: 1.2.616.1.113791.1.2.7
g) [QSxxN] OID: 1.2.616.1.113791.1.2.8
h) [QWJSN] OID: 1.2.616.1.113791.1.2.1

- responder OCSP

Każda Jednostka Certyfikacji poświadcza urząd statusu certyfikatu online (OCSP responder), który udziela odpowiedzi na temat statusu unieważnienia Certyfikatów wydanych przez daną jednostkę certyfikacji. Nazwa respondera OCSP zawiera tekst „OCSP Responder” występujący po nazwie danej jednostki certyfikacji. W Certyfikatach urzędu statusu certyfikatu online (OCSP responder) występuje Rozszerzone użycie klucza "OCSPSigning".

Powyżej wspomniane jednostki mają Certyfikaty oparte na ECC, 384-bit.

W tej hierarchii, wszystkie wydane Certyfikaty końcowe używają kluczy RSA o długości przynajmniej 2048 bitów lub kluczy ECC o długości co najmniej 256 bitów.

Wycofana, hierarchia SHA-1, RSA

QTSP wydawał 2-letnie Certyfikaty SHA-1 końcowe do 30.06.2018 r. QTSP nie używa tej hierarchii od 30.06.2018 r. QTSP utrzymuje hierarchie SHA-1 w celu weryfikacji wcześniej złożonych podpisów i znaczników czasu. Następujące Jednostki certyfikacji są w tej hierarchii:

- Narodowe Centrum Certyfikacji

Ważny od 26.10.2009 do 27.10.2020.

Główna jednostka certyfikacji, która wydawała Certyfikaty SHA-1 dla Jednostek Certyfikacji należących do QTSP do 14.02.2017. Ta jednostka certyfikacji posiada auto-certyfikat (certyfikat podpisany przez samą siebie). Wygasła 27.10.2020 r.

- Centrum Kwalifikowane EuroCert

(ważna od 14.01.2014 do 15.01.2019).

Produkcyjna pośrednia kwalifikowana jednostka certyfikacji, poświadczona przez Narodowe Centrum Certyfikacji. Ta jednostka nie wydawała certyfikatów pseudonimowych.

- Centrum Kwalifikowane EuroCert

(ważna od 14.02.2017 to 27.10.2020).

Produkcyjna pośrednia kwalifikowana jednostka certyfikacji, poświadczona przez Narodowe Centrum Certyfikacji. Ta jednostka nie wydawała certyfikatów pseudonimowych.

Pośrednie jednostki certyfikacji w hierarchii SHA-1 wydały specjalne końcowe listy CRL. Ważność starych podpisów elektronicznych może zostać zweryfikowana przy użyciu tych list CRL.

Publikacja Certyfikatów Głównych (Root)

Wszystkie Certyfikaty Główne są dostępne na stronie internetowej Urzędu Certyfikacji.

- Odcisk SHA-1 wycofanego Certyfikatu Głównego “Narodowe Centrum Certyfikacji”: a9516fa811535e7345881571066c770cf97f6695
- Odcisk SHA-1 aktualnego Certyfikatu Głównego “Narodowe Centrum Certyfikacji”: 89cec4842faf401b48d0f21d8043e9a63e7c02d5

Inne Certyfikaty QTSP mogą być zweryfikowane na podstawie samo-podpisanych Certyfikatów Głównych zatem te Certyfikaty są wyłącznie publikowane przez QTSP na jego stronie. Jeśli ze względu na wymogi prawne lub wynikające z umowy pomiędzy dostawcami - inny dostawca usług wydaje certyfikaty dla Jednostek Certyfikujących QTSP, QTSP również musi opublikować te Certyfikaty na swojej stronie internetowej. QTSP gwarantuje, że w przypadku Certyfikatów wydanych w ten sposób spełnia on wymogi certyfikacji krzyżowej i uznaje informacje zawarte w Polityce Certyfikacji dostawcy wydającego certyfikat jako wiążące. Zgodnie z tą zasadą QTSP przestrzega Polityki Certyfikacji NCCert (3) i – w pierwszej kolejności – uznaje zawarte wymagania za wiążące.

Przed upływem daty wygaśnięcia Certyfikatu, QTSP generuje nowe klucze i rozpoczyna działanie nowej Jednostki Certyfikacji oraz podejmuje wszelkie niezbędne kroki po to, by wymiana Certyfikatu nie zagrażała ciągłości usług.

1.3.2. Urzędy Rejestracji

Zob. definicję w sekcji 1.6.

Urząd Rejestracji (RA) może działać jako część QTSP, ale może też być oddzielną, niezależną organizacją. Działalność Urzędu Rejestracji spełnia wymagania opisane w PCKPC oraz innych dokumentach. Bez względu na rodzaj RA, QTSP jest zawsze w pełni odpowiedzialny za właściwe działanie Urzędu Rejestracji.

W przypadku niezależnego Urzędu Rejestracji, QTSP zobowiązuje Urząd Rejestracji w umowie do przestrzegania odpowiednich wymagań.

QTSP nie powierza niezależnym Urzędom Rejestracji - walidacji domen FQDN zgodnie z sekcją 3.2.2. Walidacji dokonuje własny wewnętrzny Urząd Rejestracji QTSP.

Zadania wewnętrznego Urzędu Rejestracji:

a) Rejestracja Podmiotu wskazanego w Certyfikatach użytkownika końcowego,
b) Administracja i rejestracja wydanych Certyfikatów i Urządzeń do Składania Podpisów lub Pieczęci Elektronicznych,
c) Utrzymywanie kontaktu z Klientami (odbieranie zapytań, zgłoszeń, wniosków i skarg i rozpoczęcie ich przetwarzania),
d) Unieważnienie, zawieszenie, uchylenie zawieszenia, odnowienie, modyfikacja i wymiana kluczy certyfikatów.

Obsługa klienta przez QTSP obejmuje również odbieranie wniosków dotyczących certyfikatów oraz rozpoczynanie ich przetwarzania.

Urząd Rejestracji może dokonywać rejestracji w poniższych lokalizacjach:

a) w biurze obsługi klienta QTSP,
b) przedstawiciel Urzędu Rejestracji może dokonać rejestracji u Klienta według wewnętrznych wytycznych QTSP.

1.3.3. Subskrybenci

W przypadku usługi znakowania czasem, Subskrybentem nazywany jest podmiot użytkujący Znacznik Czasu. Subskrybentem znacznika czasu może być osoba fizyczna lub prawna.

Podmiot to osoba fizyczna lub prawna, której dane umieszczono w Certyfikacie.

W przypadku Certyfikatów do podpisów elektronicznych, Podmiot jest Podpisującym i Aplikującym.

W przypadku Certyfikatów do pieczęci elektronicznych, Podmiotem jest składający pieczęć elektroniczną.

Aplikujący to osoba fizyczna, która występuje podczas aplikacji o Certyfikat do Uwierzytelniania Witryn Internetowych oraz Certyfikat do pieczęci elektronicznych.

Klienci usług dostarczanych przez QTSP:

1) Subskrybent
   a) Podpisuje umowę na świadczenie usług z QTSP (jako „Contract Signer” w rozumieniu certyfikatów EV),
   b) Akceptuje Regulamin usług zaufania (jako „Applicant Representative” w rozumieniu certyfikatów EV),
   c) Wyznacza Aplikujących (Podmiotów w przypadku Certyfikatów dla osób fizycznych),
   d) Wyraża zgodę na umieszczenie danych organizacji w Certyfikacie,
   e) Może wyznaczyć Administratorów Organizacyjnych,
   f) Odpowiada za płatności wynikłe z korzystania z usług.

2) Podmiot
   a) QTSP wydaje Certyfikat Podmiotowi.

3) Podpisujący
   a) użytkownik usługi certyfikatu podpisu elektronicznego, który może składać podpis elektroniczny przy pomocy wydanego Certyfikatu.

4) Składający pieczęć elektroniczną
   a) użytkownik usługi certyfikatu pieczęci elektronicznej, który może składać pieczęć elektroniczną przy pomocy wydanego Certyfikatu.

5) Aplikujący
   a) Składa wniosek o Certyfikat do Uwierzytelniania Witryn Internetowych (jako „Certificate Requester" i „Approver" w rozumieniu certyfikatów EV) oraz Certyfikat do pieczęci elektronicznych.

1.3.4. Strony Ufające

Strony Ufające nie muszą być stroną umowy z QTSP. PCKPC w sekcjach: 4.5.2, 4.9.6, 9.6.4 i 9.9.3 oraz inne polityki tam wspomniane zawierają rekomendacje dotyczące postępowania Stron Ufających.

QTSP utrzymuje kontakt ze Stronami Ufającymi głownie przez swoją stronę internetową.

Strona ufająca waliduje i używa podpisów elektronicznych, pieczęci oraz znaczników czasu wydanych przez QTSP. Strona ufająca zwykle nie wie, że podpis elektroniczny lub pieczęć zostały złożone przy użyciu Usługi Zdalnego podpisu.

1.3.5. Inni Uczestnicy

Niezależny audytor, który przeprowadza audyt oceny zgodności.

Organ Nadzoru.

1.4. Użycie Certyfikatu i znacznika czasu

1.4.1. Właściwe użycie Certyfikatu

Klucze prywatne należące do Certyfikatów użytkowników końcowych wydanych przez QTSP w oparciu o niniejszy dokument mogą być użyte jedynie do celów określonych w treści Certyfikatu oraz PCKPC. Celem użycia może być podpis, pieczęć lub uwierzytelnienie.

Certyfikaty do podpisów elektronicznych mogą być użyte wyłącznie w celu składania podpisu elektronicznego. Dzięki Certyfikatowi Podpisujący może zweryfikować autentyczność dokumentów podpisanych przez niego.

Certyfikaty do pieczęci elektronicznych mogą być użyte wyłączne do składania pieczęci elektronicznej. Przy pomocy Certyfikatu Składający pieczęć elektroniczną może zweryfikować autentyczność dokumentów podpisanych przez niego.

W przypadku Polityki Certyfikacji [QATBN], która wymaga użycia Kwalifikowanego Urządzenia do Składania Podpisu Elektronicznego klucz prywatny odpowiadający kwalifikowanemu Certyfikatowi jest chroniony przez Kwalifikowane Urządzenie do Składania Podpisu Elektronicznego. Certyfikaty wydane zgodnie z tą polityką są odpowiednie do składania kwalifikowanego podpisu elektronicznego.

Jeśli Polityka Certyfikacji nie wymaga użycia Kwalifikowanego Urządzenia do Składania Podpisu Elektronicznego, wtedy podpis elektroniczny oparty na certyfikacie wydanym według tej polityki może być uznany za zaawansowany podpis elektroniczny oparty na certyfikacie kwalifikowanym.

Dokument z kwalifikowanym podpisem elektronicznym zgodnie z art. 78^1 Kodeksu cywilnego (20) wywołuje te same skutki prawne co dokument podpisany własnoręcznie.

Klucz publiczny w Certyfikacie do podpisu elektronicznego (pieczęci), sam Certyfikat, Lista Certyfikatów Unieważnionych, Znaczniki Czasu i odpowiedzi online o statusie unieważnienia Certyfikatu mogą być użyte do utworzenia podpisu elektronicznego (pieczęci).

Certyfikaty do Uwierzytelniania Witryn Internetowych mogą być użyte wyłącznie do uwierzytelniania stron internetowych lub – jeśli to umożliwia – uwierzytelnienia klienta.

1.4.2. Niedozwolone użycie Certyfikatów

Użycie Certyfikatów wydanych zgodnie z niniejszym dokumentem oraz kluczy prywatnych do nich należących w celach innych niż określone w wartościach atrybutów Certyfikatu i PCKPC tj.: uwierzytelniania witryn, podpisu, pieczęci jest niedozwolone.

Certyfikaty Dostawcy

Certyfikaty główne root i pośrednie oraz powiązane z nimi klucze prywatne nie powinny być używane do wydawania Certyfikatów przed upublicznieniem tych Certyfikatów.

Klucz prywatny Jednostki Znakowania Czasem może być użyty wyłącznie do podpisywania znaczników czasu i użycie go do innych celów jest zabronione.

Certyfikaty użytkownika końcowego

Użycie Certyfikatów do podpisów elektronicznych wydanych zgodnie z niniejszym dokumentem wraz z kluczami prywatnymi do nich należącymi w celach innych niż składanie i weryfikacja podpisu elektronicznego jest zabronione.

Użycie Certyfikatów do pieczęci elektronicznych wydanych zgodnie z niniejszym dokumentem wraz z kluczami prywatnymi do nich należącymi w celach innych niż składanie i weryfikacja pieczęci elektronicznej jest zabronione.

Użycie Certyfikatów do Uwierzytelniania Witryn Internetowych wydanych zgodnie z niniejszym dokumentem i kluczy prywatnych do nich należących do celów innych niż uwierzytelnianie stron internetowych jest zabronione.

Używanie certyfikatu QWAC do ukrytego przechwytywania przez strony trzecie jest zabronione, chyba że zostało to autoryzowane przez rejestrującego domenę.

1.4.3. Użycie znaczników czasu

Znacznik czasu wiarygodnie poświadcza, że dokument elektroniczny ze znacznikiem czasu już istniał w obecnym stanie przed czasem wskazanym w znaczniku czasu.

Użycie klucza publicznego i certyfikatu przez Stronę ufającą

W celu zachowania poziomu bezpieczeństwa gwarantowanego przez QTSP, podczas używania usługi Strona ufająca powinna postępować rozważnie, w szczególności:

1) Weryfikować ważność i status unieważnienia certyfikatu;
2) Weryfikacja certyfikatu powinna obejmować całą ścieżkę certyfikacji aż po zaufany root lub pośredni certyfikat dostawcy;
3) Weryfikować czy certyfikat został wydany zgodnie z odpowiednią Polityką Certyfikacji;
4) Wziąć pod uwagę wszelkie ograniczenia wskazane w certyfikacie lub regulacjach, do których odwołuje się certyfikat.

1.5. Zarządzanie Polityką

1.5.1. Organizacja zarządzająca dokumentem

Dane organizacji zarządzającej PCKPC przedstawiono poniżej:

Nazwa organizacji	EuroCert Sp. z o.o.
Adres organizacji	Poland, 02-884 Warszawa, Puławska str. 472
Numer telefonu	+48 22 390 59 95
Email	biuro@eurocert.pl

1.5.2. Osoba do kontaktu

Pytania dotyczące niniejszego dokumentu można kierować bezpośrednio do:

Osoba do kontaktu	Kierownik Wydziału Zarządzania Zgodnością
Nazwa organizacji	EuroCert Sp. z o.o.
Adres organizacji	Poland, 02-884 Warszawa, Puławska str. 472
Numer telefonu	+48 22 390 59 95
Email	biuro@eurocert.pl

Raportowanie priorytetowych problemów związanych z Certyfikatami

QTSP utrzymuje ciągłą, całodobową (24/7) zdolność do wewnętrznego reagowania na zgłoszenia problemów z Certyfikatami o wysokim priorytecie. Osobą odpowiedzialną za przetwarzanie zgłoszonych zgłoszeń jest:

Osoba do kontaktu	Kierownik Wydziału Zarządzania Zgodnością
Nazwa organizacji	EuroCert Sp. z o.o.
Adres organizacji	Poland, 02-884 Warszawa, Puławska str. 472
Email	wsparcie@eurocert.pl
Formularz zgłoszenia incydentów	https://repozytorium.eurocert.pl/

QTSP jest zobowiązany do przetwarzania wyłącznie powiadomień przesłanych w języku polskim lub angielskim, powiadomienia przesłane w innych językach są niepewne i mogą zostać odrzucone bez dalszego przetwarzania.

Zgłoszenia problemów są przetwarzane zgodnie z wytycznymi przedstawionymi w sekcji 4.9 PCKPC.

1.5.3. Osoba lub Organizacja odpowiedzialna za zgodność KPC z Polityką Certyfikacji

Dostawca usług, który wydał Kodeks Postępowania Certyfikacyjnego jest odpowiedzialny za jego zgodność z Polityką Certyfikacji, do której się on odnosi i za dostarczenie usługi zgodnie z przepisami zawartymi w tych dokumentach (KPC).

Osobą odpowiedzialną za zgodność KPC z Polityką Certyfikacji, o której mowa w KPC jest:

Osoba odpowiedzialna	Kierownik Wydziału Zarządzania Zgodnością
Nazwa organizacji	EuroCert Sp. z o.o.
Adres organizacji	Poland, 02-884 Warszawa, Puławska str. 472
Numer telefonu	+48 22 390 59 95
Fax	-
Email	biuro@eurocert.pl

KPC i świadczenie usług nadzoruje Organ Nadzoru. Organ Nadzoru prowadzi rejestr Polityk Certyfikacji i Dostawców Usług Zaufania stosujących te polityki.

Rejestr usług zaufania Organu Nadzoru jest dostępny pod linkiem: https://www.nccert.pl/indexE.htm

1.5.4. Procedury zatwierdzania KPC

Przygotowanie, modyfikacja, zatwierdzanie i wydawanie nowej wersji PCKPC odbywa się zgodnie z procesem opisanym szczegółowo w sekcji 9.12.1.

1.6. Definicje I skróty

1.6.1. Definicje

Centrum danych	Obiekt przeznaczony do umieszczenia i eksploatacji systemów komputerowych i powiązanych komponentów. Te komponenty zwykle zawierają systemy telekomunikacyjne i łącza komunikacyjne, zapasowe źródło zasilania, dyski, klimatyzację, system ochrony przeciwpożarowej i systemy bezpieczeństwa (np. kontroli dostępu).
Klasa certyfikacji II	Grupa niekwalifikowanych Polityk Certyfikacji, które umożliwiają wydawanie Certyfikatów w oparciu o zdalną rejestrację Aplikującego.
Klasa certyfikacji III	Grupa niekwalifikowanych Polityk Certyfikacji, które wymagają wydawanie Certyfikatów w oparciu o osobistą, fizyczną rejestrację Aplikującego.
Podmiot	Osoba fizyczna, Organizacja lub urządzenie, system lub jednostka IT zidentyfikowane w Certyfikacie. Podmiot może sam być Aplikującym lub występować jako urządzenie pod nadzorem Aplikującego. Osoba fizyczna z tożsamością lub atrybutami zweryfikowanymi w Certyfikacie przez Dostawcę Usług Zaufania, zazwyczaj jest to osoba Podpisująca zwłaszcza w przypadku certyfikatu podpisu elektronicznego. Osoba prawna z tożsamością lub atrybutami zweryfikowanymi w Certyfikacie przez Dostawcę Usług Zaufania. W przypadku Certyfikatu do Uwierzytelniania Witryn, Podmiotem jest serwer internetowy, zidentyfikowany przez nazwę domeny.
Podpisujący	"Osoba fizyczna która składa podpis elektroniczny." (eIDAS (1) artykuł 3. punkt 9.) Osoba, o tożsamości zweryfikowanej w certyfikacie podpisu elektronicznego przez Dostawcę Usług Zaufania.
Składający Pieczęć	"Osoba prawna która składa pieczęć elektroniczną." (eIDAS (1) artykuł 3. punkt 24.)
Unikalny Identyfikator Podmiotu	Globalnie unikalny identyfikator Podmiotu przydzielony przez QTSP. Identyfikator znajduje się w polu Certyfikatu "Subject DN Serial Number" Podmiotu", zgodnie z wymaganiami sekcji 3.1.1.
Uwierzytelnienie	Uwierzytelnienie z wykorzystaniem certyfikatu klucza publicznego jest procesem, w którym Strona Ufająca weryfikuje tożsamość Podmiotu Certyfikatu (osoba fizyczna, organizacja, aplikacja, witryna internetowa, usługa lub serwer) przy użyciu metody do tego celu, w której klucz prywatny Podmiotu służy do zidentyfikowania a tożsamość jest weryfikowana za pomocą Certyfikatu.
Certyfikat do automatyzacji	Certyfikat, który zawiera również nazwę urządzenia IT (aplikacji, systemu), za pośrednictwem którego Podmiot używa Certyfikatu.

Lista zaufana	Dla krajów członkowskich UE, lista wydana przez państwo członkowskie zgodnie z eIDAS zawierająca informacje o dostawcach usług zaufania będących pod nadzorem tego państwa członkowskiego. Może być zwalidowana na podstawie centralnej listy zaufania wydanej przez Komisję UE zgodnie z oficjalnym dziennikiem Ustaw UE 2019/C 276/01.
Organ Nadzoru	Minister właściwy ds. informatyzacji, organ nadzorujący i monitorujący Usługi Zaufania (Ustawa o usługach zaufania, artykuł 27.1 (19))
Usługa Zaufania	Usługa elektroniczna zazwyczaj świadczona za wynagrodzeniem i obejmująca: a/ tworzenie, weryfikację i walidację podpisów elektronicznych, pieczęci elektronicznych lub elektronicznych znaczników czasu, usług rejestrowanego doręczenia elektronicznego oraz certyfikatów powiązanych z tymi usługami; lub b/ tworzenie, weryfikację i walidację certyfikatów uwierzytelniania witryn internetowych; lub c/ konserwację elektronicznych podpisów, pieczęci lub certyfikatów powiązanych z tymi usługami (eIDAS (1) Artykuł 3, punkt 16).
Dostawca Usług Zaufania	"Osoba fizyczna lub prawna, która świadczy przynajmniej jedną Usługę Zaufania, jako kwalifikowany lub niekwalifikowany Dostawca Usług Zaufania." (eIDAS (1) Artykuł 3, punkt 19)
Podpis Elektroniczny	Dane w postaci elektronicznej, które są dołączone lub logicznie powiązane z innymi danymi w postaci elektronicznej, i które użyte są przez Podpisującego jako podpis (eIDAS (1) Artykuł 3, punkt 10)
Certyfikat Podpisu Elektronicznego	„Poświadczenie elektroniczne, które przyporządkowuje dane służące do walidacji podpisu elektronicznego do osoby fizycznej i potwierdza co najmniej imię i nazwisko lub pseudonim tej osoby." (eIDAS (1) Artykuł 3, punkt 14)
Kwalifikowany Certyfikat Podpisu Elektronicznego	certyfikat podpisu elektronicznego, który jest wydawany przez kwalifikowanego dostawcę usług zaufania i spełnia wymogi określone w załączniku I do eIDAS (1); art. 3 p. 15
Kwalifikowany Certyfikat Pieczęci Elektronicznej	certyfikat pieczęci elektronicznej, który jest wydawany przez kwalifikowanego dostawcę usług zaufania i spełnia wymogi określone w załączniku III eIDAS (1); art. 3 p. 30
Kwalifikowany Certyfikat Uwierzytelniania Witryn Internetowych	certyfikat uwierzytelniania witryn internetowych, który jest wydawany przez kwalifikowanego dostawcę usług zaufania i spełnia wymogi określone w załączniku IV eIDAS (1); art. 3 p. 39
Dane służące do składania podpisu elektronicznego	unikalne dane, których podpisujący używa do składania podpisu elektronicznego (eIDAS (1) art. 3 , pkt 13) Zwykle, klucz prywatny, dawniej zwany jako dane do składania podpisu elektronicznego.
Urządzenie do składania podpisu elektronicznego	"Skonfigurowane oprogramowanie lub skonfigurowany sprzęt, które wykorzystuje się do składania podpisu elektronicznego" (eIDAS (1) artykuł 3, punkt 22).

Pieczęć Elektroniczna	Dane w postaci elektronicznej dodane do innych danych w postaci elektronicznej lub logicznie z nimi powiązane, aby zapewnić autentyczność pochodzenia oraz integralność powiązanych danych (eIDAS (1) artykuł 3, punkt 25)
Certyfikat Pieczęci Elektronicznej	Poświadczenie elektroniczne, które łączy dane służące do walidacji pieczęci elektronicznej z osobą prawną i potwierdza nazwę tej osoby (eIDAS (1) artykuł 3, punkt 29.)
Certyfikat Email	Certyfikat spełniający wymogi standardu S/MIME, który może być użyty do szyfrowania email i zapewnienia integralności w systemach internetowych email.
Dane służące do składania pieczęci elektronicznej	„Niepowtarzalne dane, które podmiot składający pieczęć wykorzystuje do złożenia pieczęci elektronicznej." (eIDAS (1) Artykuł 3, punkt 28) Zazwyczaj kryptograficzny klucz prywatny.
Urządzenie do składania pieczęci elektronicznej	skonfigurowane oprogramowanie lub skonfigurowany sprzęt, które wykorzystuje się do składania pieczęci elektronicznej (eIDAS (1) art. 3 pkt 31)
Dokument elektroniczny	oznacza każdą treść przechowywaną w postaci elektronicznej, w szczególności tekst lub nagranie dźwiękowe, wizualne lub audiowizualne (eIDAS (1) art. 3, pkt 35)
Elektroniczny znacznik czasu	dane w postaci elektronicznej, które wiążą inne dane w postaci elektronicznej z określonym czasem, stanowiąc dowód na to, że te inne dane istniały w danym czasie (eIDAS (1) art. 3, pkt 33)
Subskrybent	Osoba lub organizacja podpisująca umowę na usługi z Dostawcą Usług w celu używania niektórych z usług.
Reprezentant Subskrybenta (QWAC) (Applicant's representative)	Osoba fizyczna która jest albo Subskrybentem, zatrudniona przez Subskrybenta lub upoważniona do reprezentowania Subskrybenta, która może zapoznać się i zaakceptować Regulamin usług zaufania w imieniu Subskrybenta.
Strona Ufająca	W przypadku szyfrowania, strona, która szyfruje dokument elektroniczny dla odbiorcy. W przypadku uwierzytelniania, strona która weryfikuje tożsamość strony, która chce być zidentyfikowana przy użyciu dedykowanej do tego procedury. Odbiorca dokumentu elektronicznego, który działa na podstawie podpisu elektronicznego (pieczęci) opartego na danym certyfikacie. Strona komunikacji, która identyfikuje serwer sieciowy podczas wejścia na stronę w oparciu o Certyfikat Uwierzytelniania Witryn, ponadto ci dostawcy oprogramowania, którzy produkują przeglądarki internetowe lub aplikacje, w których używają Certyfikatu Uwierzytelniania Witryn. Odbiorca znacznika czasu który polega na tym znaczniku czasu.
Walidacja	proces weryfikacji i potwierdzenia ważności podpisu elektronicznego lub pieczęci (eIDAS (1) art. 3, pkt 41)
Dane służące do walidacji	"dane używane do walidacji podpisu elektronicznego lub pieczęci elektronicznej" (eIDAS (1) art. 3, pkt 40)
Ścieżka Walidacji	Dokument elektroniczny lub jego skrót hash i informacje przypisane sobie nawzajem (zwłaszcza certyfikaty, informacje dotyczące certyfikatów, dane użyte do składania podpisu lub pieczęci, aktualny

	status certyfikatu, informacja o unieważnieniu oraz data ważności certyfikatu wystawcy i informacja o jego unieważnieniu), za pomocą których można stwierdzić, czy zaawansowany lub kwalifikowany podpis elektroniczny, pieczęć lub znacznik czasu umieszczony na elektronicznym dokumencie był ważny w momencie podpisywania lub znakowania pieczęcią/znacznikiem czasu.
Zawieszenie	Czasowe wstrzymanie ważności Certyfikatu dokonane przed upływem terminu ważności wskazanym w Certyfikacie. Zawieszenie Certyfikatu nie jest definitywne, można przywrócić jego ważność.
Zaawansowany Podpis Elektroniczny	Zaawansowany podpis elektroniczny musi spełniać następujące wymogi: a) jest unikalnie przyporządkowany podpisującemu; b) umożliwia ustalenie tożsamości podpisującego; c) jest składany przy użyciu danych służących do składania podpisu elektronicznego, których podpisujący może, z dużą dozą pewności, użyć pod wyłączną swoją kontrolą; oraz d) jest powiązany z danymi podpisanymi w taki sposób, że każda późniejsza zmiana danych jest rozpoznawalna. (eIDAS (1) art 3, pkt 11)
Zaawansowana Pieczęć Elektroniczna	"Zaawansowana pieczęć elektroniczna musi spełniać następujące wymogi: a) jest unikalnie przyporządkowana podmiotowi składającemu pieczęć; b) umożliwia ustalenie tożsamości podmiotu składającego pieczęć; c) jest składana przy użyciu danych służących do składania pieczęci elektronicznej, które podmiot składający pieczęć może, mając je z dużą dozą pewności pod swoją kontrolą, użyć do złożenia pieczęci elektronicznej; oraz d) jest powiązana z danymi, do których się odnosi, w taki sposób, że każda późniejsza zmiana danych jest rozpoznawalna." (eIDAS (1) artykuł 3, punkt 26)
Certyfikat Root	Również znany jako certyfikat najwyższego poziomu. Samo-podpisany Certyfikat, wydany przez konkretną Jednostkę Certyfikacji dla samej siebie, który jest podpisany jej własnym kluczem prywatnym i który może być zweryfikowany jej własnym kluczem publicznym, wskazanym w certyfikacie.
HSM: Sprzętowy Moduł Bezpieczeństwa	Sprzętowe urządzenie kryptograficzne, które generuje, przechowuje i chroni klucze kryptograficzne oraz zapewnia bezpieczne środowisko do implementacji funkcji kryptograficznych.
Urząd Certyfikacji	Dostawca Usług Zaufania, który identyfikuje wnioskodawcę w ramach usługi certyfikacyjnej, wydaje Certyfikat, prowadzi rejestry, przyjmuje zgłoszenia zmiany danych Certyfikatów i publikuje regulacje dotyczące Certyfikatów (polityki), klucze publiczne, dane do weryfikacji podpisu i informacje o aktualnym statusie Certyfikatu (zwłaszcza o jego ewentualnym unieważnieniu).
Jednostka Certyfikacji	Jednostka systemu Urzędu Certyfikacji, która podpisuje Certyfikaty. Tylko jeden klucz prywatny należy do Jednostki (klucz podpisujący,

	dane do składania podpisu). Urząd Certyfikacji może obsługiwać kilka Jednostek Certyfikacji równocześnie.
Jednostka znakowania czasem	Jednostka systemu Dostawcy Usług Zaufania, która wykonuje podpis lub pieczęć pod znacznikiem czasu. Jednostka zawsze posiada jedne dane do składania podpisu/pieczęci (klucz prywatny). Dostawca Usług Zaufania może prowadzić wiele Jednostek tego typu równocześnie.
Polityka Certyfikacji	zestaw reguł, określający zasady świadczenia usługi, odpowiedzialność stron, zasady postępowania z danymi i mający zastosowanie do określonego kręgu podmiotów lub zastosowań, o wspólnych dla tego kręgu wymaganiach bezpieczeństwa, opracowywany na podstawie norm lub standardów określających wymagania dla polityk świadczenia usług (Ustawa o usługach zaufania (19) § 19. Ust. 1, 2).
Polityka znakowania czasem	Polityka usługi zaufania w której Dostawca Usług Zaufania, strona ufająca lub inna osoba (organizacja) nakłada wymagania i warunki dla użycia znaczników czasu dla społeczności stron ufających i/lub określonej kategorii zastosowania, posiadających te same wymagania bezpieczeństwa.
Specjalista ds. Walidacji	Pracownik Urzędu Certyfikacji z przypisaną rolą zaufania „Inspektor Rejestracji", który weryfikuje informacje zgodnie z Wymaganiami CABF Baseline Requirements.
Aplikujący	Osoba fizyczna występująca o Certyfikat.
Podwójna kontrola	Proces który używa dwóch lub więcej oddzielnych jednostek (osób, procesów, lub narzędzi) w sposób skoordynowany w celu zwiększenia wiarygodności i niezawodności procesu.
Reprezentowana Organizacja	Organizacja reprezentowana przez Administratora Organizacji podczas procesu wydawania Certyfikatu dla tej Organizacji.
Certyfikat do Podpisywania Kodu	Certyfikat, który może być użyty do weryfikacji źródła pochodzenia i integralności aplikacji.
Ujawnienie klucza kryptograficznego	Ujawnienie klucza kryptograficznego zachodzi wówczas, gdy osoba nieupoważniona miała do niego dostęp lub zaistniało wysokie prawdopodobieństwo ujawnienia wartości prywatnego klucza kryptograficznego.
Narodowe Centrum Certyfikacji (Root CA)	Jednostka organizacyjna określona w Ustawie o Usługach Zaufania (19), § 10 i § 11.
Pośrednicząca Jednostka Certyfikacji	Jednostka Certyfikacji, której Certyfikat został wydany przez inną Jednostkę Certyfikacji.
Klucz Kryptograficzny	Unikalny ciąg danych cyfrowych odpowiadający transformacji kryptograficznej, wymagany do szyfrowania, odszyfrowania, składania i weryfikacji podpisów lub pieczęci elektronicznych.
Zarządzenie Kluczem	Generowanie kluczy kryptograficznych, ich dostarczenie użytkownikowi lub ich algorytmiczna implementacja jak również zapisywanie, rejestracja, przechowywanie, archiwizacja, unieważnienie i usuwanie kluczy, co jest ściśle związane z wykorzystanymi procedurami bezpieczeństwa.
HASH	Ciąg bitów określonej długości, przypisany dokumentowi elektronicznemu, utworzony przy pomocy funkcji skrótu spełniającej wymogi eIDAS (1). HASH to ciąg bitów stałej długości, zależny od

	dokumentu elektronicznego na podstawie którego powstał. Jest mało prawdopodobne, aby dwa różne dokumenty mogłyby mieć ten sam HASH i jest praktycznie niemożliwe, aby mając dany HASH, stworzyć dokument mający ten sam HASH.
Klucz Prywatny	W infrastrukturze klucza publicznego, element asymetrycznej pary kluczy kryptograficznych należący do właściciela pary kluczy, który Podmiot powinien zachować w ścisłej tajemnicy. W przypadku szyfrowania, odbiorca potrzebuje swojego klucza prywatnego do odszyfrowania dokumentu, który uprzednio został zaszyfrowany dla niego. W przypadku uwierzytelnienia, strona, która jest identyfikowana używa swojego prywatnego klucza podczas procesu weryfikacji. W przypadku uwierzytelnienia witryn, serwer sieciowy używa swojego prywatnego klucza podczas procesu jego uwierzytelniania. W przypadku podpisu elektronicznego Podpisujący generuje podpis przy pomocy klucza prywatnego. W przypadku pieczęci elektronicznych, Składający pieczęć generuje pieczęć przy pomocy klucza prywatnego. Podczas tworzenia Certyfikatu, Urząd Certyfikacji używa kluczy prywatnych Jednostki Certyfikacji do składania podpisu lub pieczęci elektronicznej na Certyfikacie w celu jego zabezpieczenia.
Kwalifikowana usługa zaufania	usługa zaufania, która spełnia stosowne wymogi określone w eIDAS (1); art. 3 p. 17
Kwalifikowany dostawca usług zaufania	dostawcę usług zaufania, który świadczy przynajmniej jedną kwalifikowaną usługę zaufania i któremu status kwalifikowany nadał organ nadzoru; art. 3 p. 20 eIDAS (1)
Kwalifikowana Pieczęć Elektroniczna	Zaawansowana pieczęć elektroniczna, która została złożona za pomocą kwalifikowanego urządzenia do składania pieczęci elektronicznej i która opiera się na kwalifikowanym certyfikacie pieczęci elektronicznej (eIDAS (1) artykuł 3. Punkt 27.)
Kwalifikowane urządzenie do składania pieczęci elektroniczne	"Urządzenie do składania pieczęci elektronicznej, które spełnia odpowiednio wymogi określone w załączniku II" (eIDAS (1) artykuł 3. punkt 32.)
Kwalifikowany Podpis Elektroniczny	Zaawansowany podpis elektroniczny, który jest składany za pomocą kwalifikowanego urządzenia do składania podpisu elektronicznego i który opiera się na kwalifikowanym certyfikacie podpisu elektronicznego. (eIDAS (1) artykuł 3. punkt 12.)
Kwalifikowane urządzenie do składania podpisu elektronicznego	"Urządzenie do składania podpisu elektronicznego, które spełnia wymogi określone w załączniku II do eIDAS (1)." (eIDAS (1) artykuł 3. punkt 23.) Poprzednio zwane Bezpiecznym Urządzeniem do Składania Podpisu.
Kwalifikowany elektroniczny znacznik czasu	elektroniczny znacznik czasu, który spełnia wymogi określone w art. 42 eIDAS (1) (art. 3 p. 34 eIDAS)
Usługa Zdalnego Podpisu	Usługa zaufania, gdzie dostawca zarządza kluczami prywatnymi klientów w bezpiecznych warunkach, zapewnia niezbędne techniczne i organizacyjne warunki aby umożliwić klientowi wykonanie zdalnych

	operacji z wykorzystaniem klucza przechowywanego u dostawcy, takich jak podpisywanie, pieczętowanie.
Klucz Publiczny	W infrastrukturze klucza publicznego, element asymetrycznej pary kluczy kryptograficznych należący do właściciela pary kluczy, który powinien zostać upubliczniony. Upublicznienia zazwyczaj dokonuje się w formie Certyfikatu, który łączy nazwę/nazwisko Podmiotu z kluczem publicznym. W przypadku szyfrowania, klucz publiczny odbiorcy jest wymagany do stworzenia zaszyfrowanego dokumentu. W przypadku uwierzytelnienia, wymagany jest klucz publiczny strony, która jest identyfikowana w celu zweryfikowania jej tożsamości. W przypadku uwierzytelnienia witryn, wymagany jest klucz publiczny serwera sieciowego do weryfikacji jego tożsamości. W przypadku podpisu elektronicznego (pieczęci), wymagany jest klucz publiczny strony Składającej podpis (pieczęć) w celu weryfikacji autentyczności podpisu (pieczęci) – są to Dane do Walidacji Certyfikatu. Autentyczność Certyfikatów może być zweryfikowana kluczem publicznym Jednostki Certyfikacji.
Infrastruktura Klucza Publicznego, PKI	Infrastruktura wykorzystująca kryptografię asymetryczną, w tym algorytmy kryptograficzne, klucze, certyfikaty, normy i przepisy prawne, bazowy system instytucjonalny, różnorodnych dostawców i urządzeń.
Wniosek o Rejestrację	Dane i oświadczenie złożone przez Klienta w celu przygotowania Wniosku o Certyfikat i umowy o świadczeniu usług, w których Klient upoważnia Dostawcę Usług do przetwarzania danych.
Urząd Rejestracji	Organizacja, która sprawdza autentyczność danych użytkownika Certyfikatu i weryfikuje, czy Wniosek o Certyfikat jest autentyczny i czy został złożony przez upoważnioną osobę.
Nadzwyczajna Sytuacja Operacyjna	Nadzwyczajna sytuacja powodująca zakłócenia w działalności Dostawcy Usług, kiedy kontynuacja normalnej działalności Dostawcy Usług jest niemożliwa tymczasowo lub trwale.
Organizacja	Osoba prawna
Certyfikat Organizacyjny	Certyfikat, którego Podmiot jest Organizacją lub osobą fizyczną, która należy do Organizacji. W takim przypadku nazwa Organizacji jest wskazana w polu „O” Certyfikatu. Każdy certyfikat pieczęci jest Certyfikatem Organizacyjnym.
Administrator Organizacyjny	Osoba fizyczna która działa w imieniu Subskrybenta i - w przypadku specjalnego upoważnienia, szczególnie dla certyfikatów uwierzytelniania witryn (EV) - jest upoważniona do składania wniosku o certyfikat, udzielania zgody na wydanie certyfikatu, żądania wydania, wymiany, zawieszenia, uchylenia zawieszenia i unieważnienia certyfikatu wydanego Subskrybentowi.
Podpisujący umowę (Contract Signer)	Osoba fizyczna która jest albo Subskrybentem, osobą zatrudnioną przez Subskrybenta lub upoważnioną do reprezentowania Subskrybenta, która jest upoważniona do podpisania umowy w imieniu Subskrybenta.

Wnioskodawca Certyfikatu (Certificate Requester)	Osoba fizyczna która jest albo Subskrybentem, osobą zatrudnioną przez Subskrybenta lub inną osobą upoważnioną do reprezentowania Subskrybenta, która uzupełnia i wysyła Wniosek o Certyfikat EV w imieniu Subskrybenta.
Akceptujący certyfikat (Certificate Approver)	Osoba fizyczna która jest albo Subskrybentem, osobą zatrudnioną przez Subskrybenta lub inną osobą upoważnioną do reprezentowania Subskrybenta, uprawnioną do: a/ działania jako Wnioskodawca Certyfikatu i do upoważniania innych pracowników lub osób trzecich do występowania jako Wnioskodawca Certyfikatu, i b/ akceptowania Wniosków o Certyfikat EV złożonych przez innych Wnioskodawców Certyfikatu.
Certyfikat Uwierzytelnienia Serwera	Certyfikat, który jest wykorzystywany do uwierzytelnienia serwera lub jednej z jego usług. Pole CN takich Certyfikatów zawsze zawiera FQDN lub adres IP. Takie Certyfikaty są wydawane np. dla serwera CISCO VPN, kontrolera domeny, serwera SCEP, serwera VPN.
Kodeks Postępowania Certyfikacyjnego	"Kodeks Dostawcy Usług Zaufania zawierający szczegółowy opis wymogów proceduralnych i innych wymagań operacyjnych wykorzystywanych w celu świadczenia poszczególnych Usług Zaufania".
Umowa na świadczenie usługi	"Umowa pomiędzy Dostawcą Usług Zaufania a jego klientem, która zawiera warunki świadczenia Usług Zaufania i korzystania z nich".
Certyfikat	"Certyfikat podpisu elektronicznego, certyfikat pieczęci elektronicznej i certyfikat uwierzytelniania witryny oraz wszystkie te elektroniczne certyfikaty wydane w ramach Usługi Zaufania przez dostawcę usług, które zawierają dane do walidacji certyfikatu i inne dane związane ze stosowaniem certyfikatu. Certyfikat jako dokument elektroniczny jest w sposób wiarygodny chroniony przed fałszerstwem w momencie wydawania i przez cały okres ważności".
Wniosek o wydanie Certyfikatu	Dane i oświadczenie przekazane przez osobę aplikującą o wydanie Certyfikatu, w którym osoba aplikująca potwierdza autentyczność danych, które pojawią się w Certyfikacie.
Repozytorium Certyfikatów	Repozytorium danych zawierające różne Certyfikaty. Urząd Certyfikacji prowadzi Repozytorium Certyfikatów, w którym ujawniono wydane Certyfikaty. Jednocześnie Repozytorium Certyfikatów to również system zawierający Certyfikaty dostępne do użycia (magazyn certyfikatów) na komputerze Podmiotu i Strony Ufającej.
Szyfrowanie	proces, w którym podmiot wysyłający szyfruje dokumenty wykorzystując klucz publiczny odbiorcy, który następnie można odszyfrować jedynie przy użyciu prywatnego klucza adresata.
Klient	Wspólna nazwa obejmująca Subskrybenta i wszystkie powiązane z nim osoby ubiegające się o wydanie certyfikatu (Podmiot i Aplikujący).
Unieważnienie	Zakończenie ważności Certyfikatu przed upływem okresu ważności wskazanym w Certyfikacie. Unieważnienie Certyfikatu jest trwałe, unieważniony Certyfikat nie może być ponownie wznowiony.

Rejestr statusów unieważnienia	Wewnętrzny rejestr zawieszonych i unieważnionych Certyfikatów, który zawiera informacje o zawieszeniu lub unieważnieniu wraz z czasem dokładnym co do sekundy, prowadzony przez Urząd Certyfikacji.
Certyfikat uwierzytelniania witryn internetowych	poświadczenie, które umożliwia uwierzytelnianie witryn internetowych i przyporządkowuje witrynę internetową do osoby fizycznej lub prawnej, której wydano certyfikat (eIDAS (1) Artykuł 3, punkt 38.) W polu nazwy Certyfikatu podaje się nazwę domeny serwera internetowego.
Globalna nazwa domeny (Internationalized Domain Name)	nazwa domeny internetowej, która zawiera co najmniej jedną etykietę (etykiety oddzielone są kropkami) wyświetlaną w aplikacjach - w całości lub w części - w specyficznym językowo skrypcie lub alfabecie, jak np. „żęąś.example.com”. Te nazwy domen są przechowywane w systemie nazw domen (DNS) jako ciągi ASCII przy użyciu transkrypcji Punycode.
Otwarta Bankowość	Uregulowane środowisko dla usług płatniczych odrębnych od dyrektywy UE PSD2 lecz działających na podstawie identycznych lub bardzo podobnych wymagań.
Nazwa domeny Wildcard	Ciąg znaków rozpoczynający się od „*.” (U+002A ASTERISK, U+002E FULL STOP) po którym następuje pełna kwalifikowana nazwa domeny (FQDN).
Certyfikat Wildcard	Certyfikat uwierzytelniania witryn internetowych zawierający przynajmniej jedną Nazwę Domeny Wildcard w polu Certyfikatu „Subject Alternative Names”.
LDH-Label	Ciąg składający się z liter (znaków) ASCII, cyfr i myślnika, przy czym łącznik nie może pojawić się na początku ani na końcu ciągu. Podobnie jak wszystkie etykiety DNS, jego całkowita długość nie może przekroczyć 63 oktetów.
P-Label	XN-Label (etykieta XN), która zawiera ważny wynik algorytmu Punycode (jak określono w RFC 3492, sekcja 6.3) z piątej i kolejnych pozycji.
XN-Label	Klasa etykiet (znaczników), które zaczynają się od przedrostka „xn-„ (niezależnie od wielkości liter), które poza tym są zgodne z regułami dla etykiet LDH labels.

1.6.2. Akronimy

PCKPC	niniejszy dokument,
CA	Urząd Certyfikacji (Certificate Authority),
CAA	Certification Authority Authorization,
PC	Polityka Certyfikacji,
KPC	Kodeks Postępowania Certyfikacyjnego,
CRL	Lista Certyfikatów Unieważnionych,
CSPRNG	Cryptographically Secure Pseudo-Random Number Generator,
DVC	Domain Validation Certificate,
DVCP	Domain Validation Certificate Policy,
eIDAS	ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) NR 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do

	transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE,
EUSCP	EU SSASC Policy,
GMT	Greenwich Mean Time,
IERS	International Earth Rotation and Reference System Service,
EVC	Extended Validation Certificate,
EVCP	Extended Validation Certificate Policy,
FQDN	Fully Qualified Domain Name (w pełni kwalifikowana nazwa domeny),
IDN	Internationalized Domain Name (domena zawierająca diakrytyczne znaki narodowe),
IVC	Individual Validation Certificate (Certyfikat walidacji osoby fizycznej),
IVCP	Individual Validation Certificate Policy (Polityka Certyfikacji dla Certyfikatów IVC),
NCCert	Narodowe Centrum Certyfikacji (jednostka certyfikacji root),
NSCP	Normalized SSASC Policy,
LDAP	Lightweight Directory Access Protocol,
LSCP	Lightweight SSASC Policy,
OCSP	Online Certificate Status Protocol (protokół statusu certyfikatów on-line),
OID	Object Identifier (Identyfikator Obiektu),
OVC	Organization Validation Certificate (Certyfikat walidacji organizacji),
OVCP	Organization Validation Certificate Policy (Polityka Certyfikacji dla Certyfikatów OVC),
PKI	Public Key Infrastructure (Infrastruktura Klucza Publicznego),
QCP	Kwalifikowana Polityka Certyfikacji,
RA	Registration Authority (Urząd Rejestracji),
SSASC	Server Signing Application Service Component,
SCP	SSASC Policy,
SCAL	Sole Control Assurance Level,
SCDev	Signature Creation Device (Urządzenie do Składania Podpisu),
TSP	Dostawca Usług Zaufania,
TAI	International Atomic Time,
TSA	Time Stamping Authority (Urząd Znakowania Czasem),
TSU	Time Stamping Unit (Jednostka Znakowania Czasem),
TDS	TSA Disclosure Statement,
TW4S	Trustworthy System Supporting Server Signing,
UTC	Coordinated Universal Time,
QSCD	Kwalifikowane Urządzenie do Składania Podpisu Elektronicznego,
QWAC	Kwalifikowany Certyfikat Uwierzytelniania Witryn
QTSP	Kwalifikowany Dostawca Usług Zaufania (Qualified Trust Service Provider)

2. Obowiązki związane z publikowaniem i repozytorium

2.1. Repozytorium

QTSP Usług ujawnia polityki i warunki umowne w formie elektronicznej na swojej stronie internetowej pod linkiem: https://eurocert.pl/repozytorium/.

Wersje robocze nowych dokumentów są publikowane na powyższej stronie internetowej przynajmniej 14 dni przed wejściem w życie.

Obowiązujące dokumenty są dostępne na stronie wraz ze wszystkimi wcześniejszymi wersjami.

Aktualne wersje regulacji i warunków umownych są dostępne w wersji drukowanej w biurze obsługi klienta QTSP.

Po zawarciu umowy, QTSP udostępnia Klientowi Regulamin świadczenia usług i PCKPC w formie pliku pdf podpisanego elektronicznie, który można pobrać ze strony. QTSP udostępnia Klientowi spersonalizowaną Umowę na świadczenie usług w wersji papierowej, zatwierdzoną podpisem odręcznym i pieczątką lub w formie elektronicznego dokumentu pdf podpisanego kwalifikowanym podpisem elektronicznym lub pieczęcią.

QTSP powiadamia Klienta o każdej zmianie Regulaminu świadczenia usług zaufania.

2.2. Publikacja informacji certyfikacyjnej

QTSP publikuje na swojej stronie (https://eurocert.pl/index.php/en-us/documents/certificates-and-crls):

a) certyfikaty Dostawcy Usług Zaufania;
b) wszystkie Certyfikaty Krzyżowe, które identyfikują QTSP jako Podmiot;
c) certyfikaty użytkownika końcowego w przypadku zgody Podmiotu.

Certyfikaty Dostawcy Usług

QTSP ujawnia Certyfikaty jednostek znakowania czasem, jednostek certyfikacji i urzędów statusu certyfikatów online, w następujący sposób:

a) nazwę głównych jednostek certyfikacji root i funkcję skrótu ich certyfikatów root w PCKPC (zob. sekcję 1.3.1). Informacje dotyczące zmiany ich statusu są dostępne na stronie internetowej QTSP.
b) zmiany statusu Certyfikatów pośrednich jednostek certyfikacji, jednostek znakowania czasem i jednostek podpisujących odpowiedzi OCSP są publikowane na Liście CRL, stronie internetowej i w ramach usługi informowania o statusie certyfikatu (OCSP).

Certyfikaty użytkowników końcowych

QTSP ujawnia informacje o statusie wydanych Certyfikatów dla użytkowników końcowych w następujący sposób:

a) na liście certyfikatów unieważnionych (CRL),
b) w ramach usługi informowania o statusie certyfikatu online OCSP.

Informacja o statusie unieważnienia Certyfikatu użytkownika końcowego jest udostępniana przez QTSP i zgoda Aplikującego nie jest wymagana. Z metodami ujawniania informacji o statusie zapoznać się można w sekcji 4.10.

QTSP zapewnia, że dostępność jego systemu publikującego Certyfikaty Dostawcy Usług Zaufania, Repozytorium Certyfikatów i informacje o statusie unieważnienia będzie wynosić co najmniej 99,9% w skali roku.

2.3. Czas i częstotliwość publikacji

2.3.1. Częstotliwość publikacji zasad i warunków

Najważniejsze zasady i warunki świadczenia usług są zawarte w umowie na świadczenie usług zawartej z Klientem lub w Regulaminie usług zaufania (4).

QTSP dokonuje rewizji Regulaminu usług zaufania raz do roku lub niezwłocznie w przypadku nadzwyczajnego wniosku o zmianę i dokonuje stosownych zmian. Dokument otrzymuje wtedy nowy numer wersji nawet w przypadku drobnych zmian i określona zostaje planowana data jego wprowadzenia w życie, biorcą pod uwagę czas potrzebny na uzgodnienia.

Zatwierdzony dokument jest publikowany na stronie internetowej QTSP co najmniej 14 dni przed planowanym wejściem w życie.

2.3.2. Częstotliwość ujawniania Certyfikatów

QTSP przestrzega następujących reguł w odniesieniu do ujawniania Certyfikatów:

a) Certyfikaty głównych jednostek certyfikacji są ujawniane przed ich uruchomieniem;
b) Certyfikaty pośrednich jednostek certyfikacji są ujawniane w ciągu 5 dni roboczych od wydania;
c) QTSP ujawnia Certyfikaty użytkowników końcowych w swoim Repozytorium Certyfikatów niezwłocznie po ich wydaniu.

2.3.3. Częstotliwość publikacji zmienionego statusu unieważnienia

Informacja o statusie Certyfikatu użytkownika końcowego i Certyfikatów dostawcy jest dostępna natychmiast za pomocą usługi informowania o statusie certyfikatu online.

Informacje dotyczące statusu Certyfikatów są ujawniane w Repozytorium Certyfikatów i na listach CRL. Praktyki związane z wydawaniem list CRL są omówione w sekcji 4.10.

2.4. Kontrole dostępu do Repozytorium

Informacje publikowane w Repozytorium są jawne i każdy może się z nimi zapoznać bezpłatnie.

Informacje ujawniane przez QTSP mogą być zmienione, uzupełnione lub usunięte tylko przez QTSP. Informacje umieszczone w repozytorium są zabezpieczone przed nieautoryzowanym zmienianiem, dodawaniem i usuwaniem.

3. Identyfikacja i uwierzytelnianie

3.1. Nadawanie nazw

Niniejszy rozdział zawiera wymagania dotyczące danych wskazanych w Certyfikatach wydanych użytkownikom końcowym zgodnie z odpowiednią Polityką Certyfikacji.

Podstawowe pola identyfikator Wystawcy (Issuer) i identyfikator Podmiotu (Subject), zawarte w Certyfikacie są zgodne ze specyfikacjami formatu unikalnej nazwy zgodnie z ITU X.520 (21), RCF 5280 (22) i IETF RFC 6818 (23). Ponadto, QTSP stosuje alternatywne nazwy w rozszerzeniach: Alternatywną Nazwę Podmiotu (Subject Alternative Names) i Alternatywną Nazwę Wystawcy (Issuer Alternative Names).

QTSP może skrócić zawartość pól Certyfikatu zgodnie z wymaganiami dotyczącymi formatu nazw lub może wskazać dany rodzaj nazwy, więcej niż jeden raz w Certyfikacie.

3.1.1. Typy nazw

Nazwa Podmiotu

Nazwa Podmiotu Certyfikatu (zawartość pola Podmiot) składa się z:

- **commonName (CN)** - **nazwa powszechna** – OID: 2.5.4.3
  Nazwa Podmiotu

W przypadku osób fizycznych, nazwa Podmiotu w tym polu jest w takiej samej formie jak została zweryfikowana przez QTSP według sekcji 3.2.3.

W przypadku Organizacji, pełna lub skrócona nazwa Organizacji w tym polu jest w takiej samej formie jak została zweryfikowana przez QTSP według sekcji 3.2.2.

W przypadku gdy żadna z nazw Organizacji – pełna ani skrócona – nie mieści się w Certyfikacie, wpisuje się jednoznaczny skrót Organizacji.

Na prośbę Aplikującego w tym polu może być wpisana nazwa mechanizmu automatyzacji, za pośrednictwem którego Certyfikat ma być używany (Certyfikat do Automatyzacji).

Zawsze wypełniane.

W przypadku Certyfikatu do Uwierzytelniania Witryn, to pole zawiera tylko jedną wartość odpowiadającą jednej z wartości znajdujących się w rozszerzeniu "Alternatywne Nazwy Podmiotu" (Subject Alternative Names) w Certyfikacie.

Wartość pola musi być zapisana jak poniżej:

Fully-Qualified Domain Name:
W przypadku FQDN wartość musi być zgodna z wartością „dNSName" w rozszerzeniu „subjectAltName". W szczególności wszystkie tagi domeny (Domain Label) FQDN powinny być zakodowane jako tagi LDH-Labels, a tagi P-Labels nie powinny być konwertowana do ich reprezentacji Unicode.

Można wpisać jedynie tę domenę, która istnieje i którą Aplikujący posługuje się zgodnie z prawem.

Certyfikat do Uwierzytelniania Witryn nie może być wydawany z pseudonimem.

Zawsze wypełniane.

- **Surname (SN) - nazwisko** – OID: 2.5.4.4
  Nazwisko osoby fizycznej

W przypadku osób fizycznych w tym polu znajduje się nazwisko Podmiotu, pochodzące z pełnej nazwy podanej w polu CN.

QTSP zawsze wypełnia to pole.

W przypadku Certyfikatów Uwierzytelniania Witryn pole pozostaje niewypełnione.

W przypadku gdy Podmiotem Certyfikatu jest Organizacja, pola nie wypełnia się.

- **GivenName (G) - imię** – OID: 2.5.4.42
  Imię osoby fizycznej.

W przypadku Podmiotu osoby fizycznej w tym polu podaje się imię Podmiotu.

QTSP zawsze wypełnia to pole.

Jeżeli Podmiotem Certyfikatu jest Organizacja, pola nie wypełnia się.

W przypadku Certyfikatów Uwierzytelniania Witryn pole pozostaje niewypełnione.

- **Pseudonim (PSEUDO)** – OID: 2.5.4.65
  Pseudonim Podmiotu

- **SerialNumber - numer seryjny** – OID: 2.5.4.5

Niepowtarzalny identyfikator Podmiotu. To pole jest częścią nazwy Podmiotu i to nie jest to samo co pole numer seryjny certyfikatu wskazany przez IETF RFC 5280 (22).

W Certyfikacie podaje się przynajmniej jeden Numer Seryjny.

Może istnieć wiele OID dla tego samego Podmiotu ale tylko jeden Podmiot może być przypisany do danego OID. Podmiot jest zawsze uprawniony do wystąpienia o nowy (nieprzypisany nikomu) OID. QTSP nadaje taki sam OID dla dwóch Certyfikatów jedynie w przypadku, gdy Podmiot w obydwu Certyfikatach jest ten sam.

W przypadku Certyfikatu do Uwierzytelniania Witryn ten OID identyfikuje jednocześnie właściciela podanego w polu „Podmiot DN" i nazwę domeny podaną w polu „Alternatywne Nazwy Podmiotu".

To obowiązkowe pole zawiera numer rejestracyjny Podmiotu:

a) dla Organizacji prywatnych – numer rejestracyjny nadany przez Urząd Rejestracyjny (KRS). Jeśli nie występuje nr rejestracyjny wtedy wskazana jest data rejestracji w formacie YYYY-MM-DD.
b) dla jednostek Publicznych które nie mają nr rejestracyjnego lub możliwej do łatwego zweryfikowania daty powstania, pole zawiera: Government Entity.

Identyfikator może być podany w formacie:

a) określonym w ETSI EN 319 412-1 sekcja 5.1.3 (na przykład: "PNOPL- 81234567901"),
b) [Nazwa: Wartość] (na przykład: "Numer dowodu osobistego: AAAAAA"),
c) w innym formacie wymaganym przez Klienta,
d) QTSP może sam nadać unikalny identyfikator w formacie 1.2.616.1.113791.2.x, gdzie x to zmienna unikalna dla każdego Podmiotu, a ciąg cyfr po lewej to identyfikator EuroCert.

W "Numerze Seryjnym" QTSP nie umieszcza akcentów.

- **Organization (O) - Organizacja** – OID: 2.5.4.10
  Nazwa Organizacji

W przypadku Certyfikatu Organizacyjnego lub Certyfikatu Uwierzytelniania Witryn w polu „O" podaje się pełną lub skróconą legalną nazwę Organizacji zgodnie z nazwą zweryfikowaną przez QTSP według sekcji 3.2.2.

W przypadku Certyfikatu Organizacyjnego i Uwierzytelniania Witryn to pole jest zawsze wypełniane.

W przypadku Certyfikatów Osobistych wydanych dla osób fizycznych (nie związanych z organizacją) tego pola nie wypełnia się.

Znak towarowy, nazwa handlowa lub określenie DBA „działający pod nazwą handlową" - używane zgodnie z prawem przez Aplikującego - mogą być zawarte w tym polu na żądanie Aplikującego, w cudzysłowie, na początku, przed pełną nazwą organizacji.

QTSP może skracać przedrostki i przyrostki w nazwie organizacji (np. formę prawną).

Jeżeli nazwa połączona lub nazwa samej organizacji przekracza 64 znaków QTSP może skrócić nazwę lub pominąć nieistotne słowa w taki sposób, żeby nie wprowadzać w błąd Stron Ufających. W przeciwnym wypadku nie wystawia certyfikatu.

W przypadku Certyfikatu dostawcy wydanego dla Dostawcy Usług Zaufania, pole „O" zawsze się wypełnia oraz podaje się prawdziwą nazwę organizacji usługodawcy.

- **Organization Identifier (OrgId) - Identyfikator Organizacji** – OID: 2.5.4.97
  Identyfikator danej Organizacji

W przypadku Certyfikatu Organizacyjnego lub Certyfikatu Uwierzytelniania Witryn w tym polu jest identyfikator Organizacji wskazanej w polu „O", zgodnie z 5.1.4 ETSI EN 319 412-1.

Można podać jedynie dane zweryfikowane przez QTSP.

Wypełnienie tego pola jest obowiązkowe jeśli Podmiotem jest osoba prawna.

W przypadku Certyfikatów Osobistych, nie związanych z Organizacją, tego pola nie wypełnia się.

W przypadku certyfikatu Email (S/MIME) Sponsor-Validated pole jest zawsze wypełniane.

W przypadku Certyfikatów Organizacyjnych dla osób fizycznych lub Certyfikatów Uwierzytelniania Witryn pole jest opcjonalne. Jest obowiązkowe tylko w przypadku Certyfikatów Open Banking lub PSD2.

Jeśli Podmiotem jest osoba prawna i Klient zażąda wpisania do Certyfikatu danych Podmiotu w związku z Open Banking lub Dyrektywą UE o usługach płatniczych (PSD2) (24), pole to zawiera identyfikator składający się z numeru autoryzacji Podmiotu wydanego przez odpowiedni organ nadzoru finansowego, który nadzoruje usługi płatnicze Podmiotu, skrót organu i kod kraju organu zgodny z ISO 3166, zbudowany według wytycznych ETSI TS 119 495 (16) lub inny identyfikator rejestracyjny uznawany przez organ nadzoru, zbudowany według specyfikacji ETSI EN 319 412-1 (25).

- **Organizational Unit (OU) - Jednostka Organizacyjna** – OID: 2.5.4.11
  Nazwa jednostki organizacyjnej

W przypadku Certyfikatu Organizacyjnego nazwa jednostki organizacyjnej związanej z organizacją określoną w polu „O", lub inna informacja może być wpisana w tym polu.

W tym polu można zawrzeć jedynie te dane, które zostały zweryfikowane przez QTSP i do których używania Organizacja jest uprawniona.

Pole "OU" może być wypełnione jedynie wtedy, gdy pola „O", „L" i „C" są wypełnione.

Pole opcjonalne.

W przypadku Certyfikatów osobistych, nie związanych z Organizacją oraz Certyfikatów Uwierzytelniania Witryn, tego pola nie wypełnia się.

- **Business Category** (rodzaj działalności) – OID 2.5.4.15

Zawiera rodzaj (charakter) organizacji wskazanej w polu „O":

a) organizacja prywatna,
b) instytucja publiczna.

Obowiązkowe w przypadku Certyfikatów Uwierzytelniania Witryn.

- **jurisdictionOfIncorporationLocalityName** – OID: 1.3.6.1.4.1.311.60.2.1.1

Pełna nazwa miejscowości odpowiedniej dla organu rejestracyjnego, jeśli jurysdykcja organu funkcjonuje w danej miejscowości. Jest zawarta tylko, jeśli zawiera istotne informacje.

- **jurisdictionOfIncorporationStateOrProvinceName** – OID: 1.3.6.1.4.1.311.60.2.1.2

Pełna nazwa odpowiedniej jurysdykcji, jeśli funkcjonuje w danym regionie lub województwie. Jest zawarta tylko, jeśli zawiera istotne informacje

- **jurisdictionOfIncorporationCountryName** – OID: 1.3.6.1.4.1.311.60.2.1.3

Kod kraju odpowiedniego organu rejestracyjnego, składający się z dwóch liter zgodnie z ISO 3166-1 (26).

Jest zawsze wypełniany.

- **CountryName (C) - Nazwa Kraju** – OID: 2.5.4.6
  Identyfikator kraju.

W przypadku Certyfikatu Organizacyjnego lub Certyfikatu Uwierzytelniania Witryn w tym polu wpisuje się kod kraju, w którym zarejestrowano Organizację, składający się z dwóch liter, zgodnie z ISO 3166-1 (26).

W przypadku osoby fizycznej (Podmiotu niepowiązanego z Organizacją), w polu podaje się dwuliterowy kod kraju (zgodnie z ISO 3166-1 (26)), który wydal dokument, którym posługuje się Podmiot w celu identyfikacji.

W przypadku Polski wartość pola “C” to “PL”.

Pole zawsze musi być wypełnione.

- **streetAddress (SA) - adres** – OID: 2.5.4.9
  Dane adresowe

Miejsce powstania Organizacji wskazanej w polu „O”. Jeśli jest wypełnione, wszystkie zawarte informacje powinny zweryfikowane przez QTSP.

- **Locality Name (L) - Nazwa lokalizacji** – OID: 2.5.4.7
  Miejscowość

W przypadku Certyfikatu Organizacyjnego i Certyfikatu Uwierzytelniania Witryn nazwa miejscowości rejestracji Organizacji.

W przypadku Certyfikatu niepowiązanego z Organizacją pola nie wypełnia się.

- **State or Province Name (Województwo)** – OID: 2.5.4.8
  Nazwa województwa

W przypadku Certyfikatu Organizacyjnego lub Certyfikatu Uwierzytelniania Witryn podaje się nazwę województwa lub pełną nazwę kraju z pola „C”, gdzie zarejestrowano Organizację wskazaną w polu „O”.

Pole opcjonalne.

W przypadku Certyfikatu niepowiązanego z Organizacją pola nie wypełnia się.

- **Postal Code** – **kod pocztowy** – OID: 2.5.4.17
  Kod pocztowy

W przypadku Certyfikatu Organizacyjnego lub Certyfikatu Uwierzytelniania Witryn podaje się kod pocztowy miejsca zarejestrowania Organizacji wskazanej w polu „O”.

Pole opcjonalne.

W przypadku Certyfikatu niepowiązanego z Organizacją pola nie wypełnia się.

W przypadku certyfikatu Email (S/MIME) Sponsor-Validated pole nie jest wypełniane.

- **Title (T) - tytuł** – OID: 2.5.4.12
  Tytuł Podmiotu

Funkcja, stanowisko, tytuł lub zawód Podmiotu (osoby fizycznej).

W przypadku Certyfikatu Organizacyjnego pole wypełnia się na podstawie oficjalnego dokumentu przedstawionego przez Reprezentowaną Organizację wskazaną w polu „O".

W przypadku Certyfikatu Profesjonalnego pole wypełnia się na podstawie oficjalnego dokumentu wydanego przez Organizację niezależną od Podmiotu.

Pole "Title" może zawierać dodatkowe informacje o roli Podmiotu w organizacji.

W wyjątkowych przypadkach QTSP może zawrzeć w Certyfikacie kilka pól „T".

W przypadku Certyfikatu Uwierzytelniania Witryn pole nie jest wypełniane.

- **e-mail Address (EMAIL)** – OID: 1.2.840.113549.1.9.1
  Adres e-mail Podmiotu

Wypełnienie pola jest opcjonalne.

Pole zawiera ten sam adres e-mail, który został wskazany w polu "RFC822name" rozszerzenia alternatywnych nazw Podmiotu („Subject Alternative Names").

W przypadku Certyfikatu do Uwierzytelniania Witryn pola nie wypełnia się.

Certyfikat wydany zgodnie z PCKPC może zawierać dodatkowe pola „Podmiot DN" w zależności od konkretnej polityki certyfikacji. W tych polach można wpisać jedynie zweryfikowane wartości (nie powinny one zawierać wartości tekstowych wskazujących na brak danych takich jak: kropka ".", myślnik "-" lub spacja " ").

Rozszerzenia Certyfikatu

- Subject Alternative Names (Alternatywne Nazwy Podmiotu)

Rozszerzenie "Alternatywne Nazwy Podmiotu" nie znajduje się na liście krytycznych rozszerzeń Certyfikatu. Zawartość uzupełnia się w następujący sposób.

a) W przypadku Podmiotu, którym jest osoba fizyczna, na prośbę Podmiotu, jego nazwa inna niż wpisana w polu „Podmiot DN/Nazwa powszechna" może być tu wpisana (zazwyczaj inna nazwa występuje w polu „CN"). Ta nazwa może być napisana ze znakami diakrytycznymi lub bez.
   QTSP jest upoważniony do wskazania charakteru podanej nazwy. QTSP weryfikuje nazwy/nazwiska, które mają pojawić się w polu „Alternatywne Nazwy Podmiotu" i rozpatruje indywidualnie każdy przypadek. Podejmuje decyzję na podstawie tego czy da się udowodnić, czy dana Organizacja używa danej nazwy zgodnie z prawem, czy nazwa/nazwisko wnioskowane przez Klienta jest w rzeczywistości nazwą Podmiotu i czy nie wprowadza innych w błąd. Jeśli Podmiot wykonując dany zawód używa innego nazwiska/nazwy niż w dokumencie tożsamości, może poprosić QTSP, by wskazał to alternatywne nazwisko/nazwę w tym polu.

b) W przypadku Certyfikatu do uwierzytelniania witryn pole Alternatywne Nazwy Podmiotu zawsze zawiera przynajmniej jeden wpis. Wypełnienie pola jest obowiązkowe.
Każdy wpis ma wartość:

"dNSName"
Wpis zawiera pełną kwalifikowaną nazwę domeny FQDN, zweryfikowaną zgodnie z sekcją 3.2.2.2. FQDN składa się wyłącznie z LDH-Labels oddzielonych znakiem U+002E FULL STOP ".". Tag Domeny (Domain Label) o zerowej długości (zero-length), reprezentującej strefę główną (root zone) systemu nazw domen internetowych (Internet Domain Name System) nie jest umieszczona (np. "example.com" powinna być zapisana jako "example.com" a nie jako "example.com."). FQDN składa się wyłącznie z Domain Labels: P-Labels lub Non-Reserved LDH-Labels.
Pole "Alternatywne Nazwy Podmiotu" nie może zawierać nazwy wewnętrznej (Internal Name).
Wartości w "dNSName" powinny być zapisane zgodnie z preferowaną składnią nazwy "preferred name syntax", jak opisano w RFC 5280 (22), stąd nie może zawierać nazwy domeny ze znakiem specjalnym: dolną spacją ("_").
Domeny Wildcard są zabronione.

c) Adres e-mail Podmiotu może być podany w rozszerzeniu „alternatywnych nazwach podmiotu" w polu "rfc822Name". Jeśli adres e-mail ma być podany na Certyfikacie, to pole należy wypełnić. QTSP weryfikuje ważność adresu email zgodnie z rozdziałem 3.2.8. W przypadku certyfikatów Email (S/MIME) pole jest zawsze wypełniane. Ten sam adres e-mail może być wpisany w polu "EMAIL" (DN) w Certyfikacie.

- **CA/Browser Forum Organization Identifier "cabfOrganizationIdentifier"** – OID: 2.23.140.3.1

Pole opcjonalne.

Jest wypełniane jeśli pole "subject:organizationIdentifier" jest wypełnione.

Jeśli jest wypełnione, zawiera tą samą wartość co w polu "subject:organizationIdentifier".

Nazwa wystawcy certyfikatu (Jednostki Certyfikacji)

Identyfikator wystawcy Certyfikatu (pole Wystawca) składa się z następujących pól:

- **Nazwa powszechna (CN)** – OID: 2.5.4.3

Nazwa jednostki certyfikacji - wystawcy Certyfikatu w języku angielskim (zobacz sekcję 1.3.1).

- **Organizacja (O)** – OID: 2.5.4.10 "EuroCert Sp. z o.o."

Nazwa QTSP w języku angielskim bez znaków diaktrytycznych.

- **Identyfikator Organizacji (OrgId)** – OID: 2.5.4.97 „VATPL-9512352379"

Numer identyfikacji podatkowej QTSP.

- **Jednostka organizacyjna (OU)** – OID: 2.5.4.11

Nazwa jednostki organizacyjnej QTSP bez znaków diaktrytycznych.

Wypełnienie jest opcjonalne.

- **Lokalizacja (L)** – OID: 2.5.4.7 "Warszawa"

Nazwa miasta siedziby QTSP bez znaków diaktrytycznych.

- **Nazwa Kraju (C)** – OID: 2.5.4.6 "PL"

Dwuliterowy kod kraju siedziby QTSP zgodny z ISO 3166-1 (26).

- **Adres e-mail (EMAIL)** – OID: 1.2.840.113549.1.9.1 „biuro@eurocert.pl”

Wypełnienie jest opcjonalne.

Te same dane co powyżej zawarte są w certyfikacie Jednostki Certyfikacyjnej w polu Subject.

Alternatywne Nazwy jednostki certyfikacji - wystawcy Certyfikatu

Pola „Issuer Alternative Names” nie wypełnia się w Certyfikatach użytkowników końcowych. W Certyfikatach wystawcy podaje się jedynie adres e-mail w polu nazwy „Subject Alternative Names” (rfc822Name).

Nazwa Jednostki Znakowania Czasem

- **Nazwa powszechna (CN)** – OID: 2.5.4.3

Nazwa Jednostki Znakowania Czasem.

- **Organizacja (O)** – OID: 2.5.4.10

Nazwa QTSP.

- **Identyfikator Organizacji (OrgId)** – OID: 2.5.4.97

Numer identyfikacji podatkowej QTSP.

- **Jednostka Organizacyjna (OU)** – OID: 2.5.4.11

Nazwa jednostki organizacyjnej QTSP.

Wypełnienie jest opcjonalne.

- **Lokalizacja (L)** – OID: 2.5.4.7

Nazwa miasta siedziby QTSP bez znaków diakrytycznych.

Wypełnienie jest opcjonalne.

- **Nazwa Kraju (C)** – OID: 2.5.4.6

Dwuliterowy kod kraju siedziby QTSP zgodny z ISO 3166-1 (26).

- **Adres e-mail (EMAIL)** – OID: 1.2.840.113549.1.9.1

Nie wypełnia się.

Nazwy Alternatywne Jednostki Znakowania Czasem

To pole nie jest zawarte w Certyfikatach wydawanych dla Jednostek Znakowania Czasem.

Nazwa OCSP Responder

- **Nazwa powszechna (CN)** – OID: 2.5.4.3

Pole zawiera nazwę Jednostki Certyfikacji świadczącej usługę odpowiedzi OCSP, zgodnie z jej nazwą „CN” z dopiskiem „OCSP Responder”.

- **Organizacja (O)** – OID: 2.5.4.10 "EuroCert Sp. z o.o."

Nazwa QTSP w języku angielskim bez znaków diakrytycznych.

- **Identyfikator Organizacji (OrgId)** – OID: 2.5.4.97 "VATPL-9512352379"

Numer identyfikacji podatkowej QTSP.

- **Jednostka Organizacyjna (OU)** – OID: 2.5.4.11

Nie wypełnia się.

- **Lokalizacja (L)** – OID: 2.5.4.7 "Warszawa"

Nazwa miasta siedziby QTSP bez znaków diakrytycznych.

Wypełnienie jest opcjonalne.

- **Nazwa kraju (C)** – OID: 2.5.4.6 "PL"

Dwuliterowy kod kraju siedziby QTSP zgodny z ISO 3166-1 (26).

- **Adres e-mail (EMAIL)** – OID: 1.2.840.113549.1.9.1

Pola nie wypełnia się.

Nazwy alternatywne OCSP Responder

To pole nie jest zawarte w Certyfikatach wydanych dla OCSP Responderów.

3.1.2. Znaczenie nazw

Poniższe zasady dotyczą pola "Subject":

a) identyfikator powinien być jednoznacznie rozumiany;
b) nazwa osoby fizycznej w Certyfikacie powinna być wpisana w taki sam sposób, jak ta zweryfikowana przez QTSP zgodnie z sekcją 3.2.3;
c) nazwa Organizacji w Certyfikacie powinna być wpisana w taki sam sposób, jak ta zweryfikowana przez QTSP zgodnie z sekcją 3.2.2.

3.1.3. Anonimowość i pseudonimy Subskrybentów

QTSP wydaje Certyfikaty Podpisu Elektronicznego z pseudonimem.

3.1.4. Zasady interpretacji różnych nazw i ich form

W celu interpretacji identyfikatorów zaleca się Stronom Ufającym, by działały zgodnie z wytycznymi przedstawionymi w niniejszym dokumencie. Jeśli Strona Ufająca potrzebuje pomocy w interpretacji identyfikatora lub jakichkolwiek innych danych podanych w Certyfikacie, może skontaktować się bezpośrednio z QTSP. W takiej sytuacji QTSP nie powinien podawać żadnych dodatkowych informacji o Kliencie (jeśli prawo tego nie nakazuje) niż te, które zostały podane w Certyfikacie, udostępnia on tylko takie informacje, które pomogą w interpretacji podanych danych.

3.1.5. Unikalne nazwy

Każdy Podmiot posiada unikalną nazwę w Repozytorium Certyfikatów QTSP. W celu zapewnienia unikalności QTSP nadaje każdemu Podmiotowi identyfikator (OID) – unikalny w rejestrze QTSP, który jest wskazany w polu identyfikatora Podmiotu "Subject DN Serial Number".

Unikalny identyfikator Podmiotu (OID) jest nadawany zgodnie z kolejnością zgłoszeń o certyfikat zapewniając unikalność danych w polu „Podmiot” w Certyfikacie.

QTSP jako identyfikator może również wskazać na przykład: numer dowodu osobistego, paszportu, numer NIP, identyfikator wewnątrz danej organizacji.

Procedury dotyczące rozwiązywania sporów dotyczących nazw

QTSP weryfikuje, czy Klient może używać wskazanej nazwy. QTSP może unieważnić dany Certyfikat z powodu użycia nazwy lub innych danych niezgodnie z prawem.

3.1.6. Uznawalność, uwierzytelnienie i rola znaków towarowych

QTSP nigdy nie umieszcza znaków towarowych w Certyfikatach.

QTSP w trakcie świadczenia usług posługuje się znakiem towarowym EuroCert. Ten znak towarowy jest własnością EuroCert.

3.2. Pierwsza weryfikacja tożsamości

QTSP może korzystać z dowolnego kanału komunikacji w ramach przewidzianych prawem w celu weryfikacji tożsamości osoby lub organizacji występujących o Certyfikat i w celu sprawdzenia autentyczności dostarczonych danych.

QTSP ma prawo odmówić wydania Certyfikatu według własnego uznania bez podania przyczyny.

3.2.1. Weryfikacja posiadania Klucza Prywatnego

Przed wydaniem Certyfikatu QTSP Usług sprawdza czy Aplikujący posiada i zarządza kluczem prywatnym należącym do klucza publicznego Certyfikatu.

Jeżeli QTSP sam wygeneruje klucz prywatny należący do Certyfikatu Podmiotu, zazwyczaj na Kwalifikowanym Urządzeniu do Składania Podpisu Elektronicznego lub Urządzeniu Kryptograficznym, nie musi on weryfikować, czy Aplikujący posiada klucz prywatny.

Jeśli Aplikujący wnioskuje o wydanie Certyfikatu dla klucza wygenerowanego przez niego samego, zazwyczaj w przypadku certyfikatów w formie pliku (bez urządzenia), QTSP akceptuje Wniosek o Certyfikat w formacie PKCS#10, jednocześnie, weryfikuje czy właściciel prywatnego klucza rzeczywiście występuje o Certyfikat.

QTSP za równoważny dowód uznaje, jeśli Podmiot złożył Wniosek o Certyfikat podpisany przy użyciu kwalifikowanego certyfikatu, którego klucz publiczny ma być umieszczony w żądanym certyfikacie.

Jeśli klucz prywatny Podmiotu został wygenerowany i jest zarządzany przez innego Dostawcę Usług Zaufania, wtedy QTSP weryfikuje, że ten Dostawca Usług Zaufania posiada ten klucz prywatny i jest on pod wyłączną kontrolą Podmiotu. QTSP może zaakceptować autentyczne oświadczenie w tej sprawie od tego Dostawcy, również w formie elektronicznej. QTSP weryfikuje autentyczność tego oświadczenia. Weryfikacja posiadania klucza następuje poprzez akceptację Wniosku Certyfikacyjnego w formacie PKCS#10.

3.2.2. Weryfikacja tożsamości organizacji lub domeny

3.2.2.1. Weryfikacja tożsamości organizacji

Tożsamość Organizacji jest weryfikowana w następujących przypadkach:

a) jeżeli Podmiotem Certyfikatu, który ma zostać wydany jest Organizacja;

b) jeżeli Podmiotem Certyfikatu, który ma zostać wydany jest urządzenie lub system zarządzany przez Organizację (w tym Certyfikat do Uwierzytelniania Witryn, o którego wydanie wystąpiła Organizacja);
c) jeżeli Certyfikat jest wydawany osobie fizycznej, ale nazwa Organizacji jest również wpisana do Certyfikatu.

Nazwa Organizacji powinna być wpisana w Certyfikacie Organizacyjnym według wytycznych w sekcji 3.1.1.

QTSP może wydać Certyfikaty Organizacyjne wyłącznie za zgodą tej Organizacji. Osoby fizyczne działające w imieniu Organizacji powinny mieć upoważnienie, a ich tożsamość powinna być weryfikowana według wytycznych z sekcji 3.2.3.

Odnosząc się do znaków towarowych wpisywanych do Certyfikatu zob. sekcje 3.1.6.

Przed wydaniem Certyfikatu Organizacyjnego QTSP weryfikuje dane Organizacji i ich autentyczność w oparciu o wiarygodne publiczne rejestry (Kwalifikowane urzędowe źródło informacji).

Pozostałe dokumenty

Podczas walidacji Organizacji Prywatnych QTSP weryfikuje, czy Organizacja:

a) faktycznie istnieje, figuruje w oficjalnym rejestrze organizacji i ma aktywny status rejestracji,
b) fizycznie istnieje, tzn. jej adres jest faktycznym adresem, gdzie prowadzi działalność,
c) jest aktywna, tzn. faktycznie prowadzi działalność.

Podczas walidacji Organizacji Publicznej QTSP weryfikuje, czy Organizacja:

a) jest legalnie zarejestrowaną instytucją publiczną,
b) jest aktywna,
c) nazwa podana w Wniosku o Certyfikat pokrywa się z nazwą oficjalnie zarejestrowaną,
d) posiada dokładną datę powołania Organizacji lub identyfikator aktu prawnego ustanawiającego Organizację.

Podczas walidacji Organizacji Publicznej QTSP otrzymuje informacje bezpośrednio z następujących źródeł:

a) wiarygodne źródło informacji publicznej z tego samego organu rządowego,
b) wiarygodne źródło z nadrzędnego organu rządowego,
c) sędzia, który jest aktywnym członkiem Krajowego Sądownictwa, w tej samej jurysdykcji co walidowana organizacja publiczna.

Ponadto w takich przypadkach weryfikacji podlega:

a) czy osoba fizyczna występująca w imieniu Organizacji jest do tego upoważniona;
b) czy Organizacja wyraziła zgodę na wydanie Certyfikatu.

W celu przeprowadzenia weryfikacji, Klient powinien przedstawić następujące dane:

a) oficjalną nazwę, siedzibę i stan prawny Organizacji;
b) oficjalny numer rejestracyjny Organizacji (np. NIP, KRS);
c) nazwę jednostki organizacyjnej w ramach danej Organizacji, o ile ma być wpisana do Certyfikatu;
d) w przypadku wydawania Certyfikatu Organizacyjnego osobie fizycznej, stanowisko/rolę Podmiotu w danej Organizacji, o ile wymagane jest wpisanie tych informacji do Certyfikatu;

e) jeśli Podmiotem jest osoba prawna i Klient występuje o umieszczenie w certyfikacie danych Podmiotu dotyczących Open Banking lub Dyrektywy UE o Usługach Płatniczych (PSD2) (24), Klient powinien przekazać numer autoryzacji Podmiotu wydany przez krajowy organ nadzoru (NCA) nadzorujący usługi płatnicze Podmiotu lub inny identyfikator uznany przez NCA, typ usług płatniczych i nazwę NCA.

Następujące zaświadczenia i dowody muszą być dołączone do wniosku o wydanie Certyfikatu:

a) oświadczenie Aplikującego, że dane podane w celu identyfikacji Organizacji są poprawne i prawdziwe;
b) zaświadczenie, że osoba składająca wniosek o Certyfikat dla Organizacji jest upoważniona do działania w jej imieniu[1];
c) w przypadku Certyfikatu Organizacyjnego wydawanego osobie fizycznej – zaświadczenie, że dana organizacja wyraża zgodę na umieszczenie jej nazwy w Certyfikacie wydanym osobie fizycznej[2];
d) w przypadku dokumentów w formie papierowej, próbka popisu osoby upoważnionej do reprezentowania Organizacji lub inny oficjalny dokument równorzędny takiej próbce podpisu[3], zawierający nazwiska i podpisy osób uprawnionych do reprezentowania organizacji;
e) dokument potwierdzający istnienie Organizacji, jej nazwę i status prawny[4].

QTSP jest zobowiązany do weryfikacji ważności i autentyczności przedstawionych dokumentów.

Walidacja tożsamości Organizacji zagranicznych

QTSP weryfikuje również Organizacje zarejestrowane za granicą, o ile możliwe jest potwierdzenie danych na podstawie odpowiednich rejestrów kraju pochodzenia lub certyfikatu wydanego przez zaufaną stronę trzecią.

Weryfikując dane, QTSP akceptuje:

a) informacje uzyskane bezpośrednio z rejestrów urzędowych kraju obcego lub pozyskane od podmiotu trzeciego lecz uwierzytelnione przez pierwotnego wystawcę danych;
b) zaświadczenie wydane przez ambasadę lub konsulat obcego państwa w Polsce, potwierdzające istnienie danej organizacji oraz poprawność podanych danych;
c) zaświadczenie wydane przez polską ambasadę lub konsulat w obcym państwie, potwierdzające istnienie danej organizacji oraz poprawność podanych danych.

QTSP może też zaakceptować inne dokumenty i dowody, o ile poziom ich bezpieczeństwa jest równy dokumentom wymienionym powyżej. Uzyskanie takich dokumentów i przekazanie ich do QTSP leży po stronie Klienta.

QTSP akceptuje jedynie aktualne dokumenty i dowody, nie starsze niż 3 miesiące.

QTSP nie wydaje Certyfikatu, jeśli nie jest w stanie dostatecznie zweryfikować zaświadczeń, danych lub innych dokumentów wydanych za granicą należących do organizacji zagranicznej.

[1] Sekcja 3.2.5. zawiera szczegóły dotyczące weryfikacji upoważnień i uprawnień.
[2] Sekcja 3.2.5. zawiera szczegóły dotyczące weryfikacji upoważnień i uprawnień.
[3] W przypadku firm zarejestrowanych w KRS dokumenty, o których mowa mogą być pozyskane przez Dostawcę Usług.
[4] W przypadku firm zarejestrowanych w KRS dokumenty, o których mowa mogą być pozyskane przez Dostawcę Usług.

Walidacja tożsamości organizacji na podstawie certyfikatu pieczęci elektronicznej

W tym przypadku:

a) Aplikujący składa Wniosek w formie elektronicznej podpisany kwalifikowaną pieczęcią elektroniczną;
b) certyfikat użyty do weryfikacji tożsamości został wydany dla tej samej organizacji, która aplikuje o certyfikat;
c) certyfikat użyty do weryfikacji tożsamości powinien zawierać dane potrzebne do jednoznacznej identyfikacji organizacji;
d) QTSP weryfikuje autentyczność i integralność Wniosku poprzez sprawdzenie całej ścieżki pełnomocnictw;
e) QTSP akceptuje tylko takie pieczęci elektroniczne, które zostały złożone przy użyciu certyfikatu wydanego przez dostawcę usług zaufania w ramach usługi zaufania, która znajduje się na krajowej liście zaufanej i podpis ten był ważny w momencie podpisywania;
f) QTSP może akceptować tylko takie pieczęci elektroniczne, które są oparte na takim certyfikacie, który został wydany na podstawie weryfikacji osoby fizycznej reprezentującej organizację zgodnie z art. 24.1 a) lub b) eIDAS (1).

3.2.2.2. Walidacja lub kontrola uwierzytelnienia domeny

W Certyfikatach do uwierzytelniania witryn internetowych powinna być co najmniej jedna nazwa domeny.

Przed wydaniem Certyfikatu do uwierzytelniania witryn internetowych QTSP sprawdza autentyczność nazwy domeny, która ma być wpisana do Certyfikatu, a Aplikujący powinien udowodnić w praktyce, że ma kontrolę nad daną domeną.

Jeśli w Certyfikacie jest więcej niż jedna nazwa domeny, weryfikacja wspomniana powyżej powinna odbyć się dla każdej z domen.

QTSP wydaje Certyfikaty wyłącznie dla publicznych nazw domen używanych w Internecie, nie dla nazw domen przeznaczonych do użytku wewnętrznego.

QTSP wydaje Certyfikaty wyłącznie dla tych domen najwyższego poziomu (TLDs), które są widoczne w aktualnym rejestrze TLD IANA (IANA Root Zone Database).

QTSP wspiera korzystanie z międzynarodowych nazw domen (Internationalized Domain Names) zgodnie z wymogami IDNA2003 (27).

QTSP nie wystawia Certyfikatów dla obszaru nazw domeny najwyższego poziomu specjalnego użytku, typu ".onion".

QTSP zapewnia, że przed wystawieniem Certyfikatu, QTSP zwalidował każdą pełną nazwę domenową (FQDN) wskazaną w Certyfikacie przy wykorzystaniu co najmniej jednej z metod omówionych poniżej zgodnie z wymogami najnowszej wersji CA/Browser Forum Baseline Requirements.

3.2.2.2.1. Walidacja wnioskodawcy jako kontaktu domeny (BR 3.2.2.4.1)

Ta metoda nie jest wykorzystywana.

3.2.2.2.2. Email do kontaktu domeny (BR 3.2.2.4.2)

Potwierdzenie kontroli wnioskodawcy nad domeną FQDN odbywa się poprzez wysłanie wartości losowej e-mailem, a następnie otrzymanie od wnioskodawcy odpowiedzi potwierdzającej otrzymanie

tej wartości losowej. QTSP wysyła wartość losową na adres e-mailowy zarejestrowany jako kontakt domeny.

Każdy email może być użyty do identyfikacji wielu nazw domen.

QTSP może wysłać taki email do kilku odbiorców pod warunkiem, że każdy odbiorca widnieje w rejestrze nazw domen jako reprezentant podmiotu rejestrującego domenę, dla każdej domeny FQDN, która jest weryfikowana przy użyciu emaila.

Wartość losowa jest unikalna w każdej z wiadomości e-mail.

QTSP może ponownie przesłać email w całości, wraz z taką samą wartością losową pod warunkiem, że cała zawartość komunikacji i odbiorcy pozostają bez zmian. Wartość losowa jest ważna przez 30 dni od daty jej stworzenia.

3.2.2.2.3. Kontakt telefoniczny z kontaktem domeny (BR 3.2.2.4.3)

Ta metoda nie jest wykorzystywana.

3.2.2.2.4. Email konstruowany do kontaktu domeny (BR 3.2.2.4.4)

Sprawdzenie kontroli wnioskodawcy nad domeną FQDN poprzez

a) wysłanie wiadomości e-mail na, co najmniej jeden adres e-mail utworzony z użyciem:
   - "admin",
   - "administrator",
   - "webmaster",
   - "hostmaster" lub
   - "postmaster"

   jako część lokalna, po której następuje znak ("@") i nazwy domeny do weryfikacji,

b) umieszczenie w wiadomości e-mail unikalnej wartości losowej i

c) otrzymanie odpowiedzi zwrotnej od wnioskodawcy zawierającej potwierdzenie otrzymania wartości losowej.

Każdy e-mail może służyć do potwierdzania kontroli nad wieloma FQDN, pod warunkiem, że nazwa domeny użyta w wiadomości e-mail jest nazwą domeny dla każdej FQDN, która ma zostać potwierdzona.

Wartość losowa jest unikalna dla każdej wiadomości e-mail.

QTSP może ponownie wysłać mail w całości, wraz z taką samą wartością losową pod warunkiem, że cała zawartość komunikacji i odbiorcy pozostają bez zmian. Wartość losowa jest ważna przez 30 dni od daty jej stworzenia.

3.2.2.2.5. Dokument autoryzacji domeny (BR 3.2.2.4.5)

Ta metoda nie jest wykorzystywana.

3.2.2.2.6. Uzgodniona zmiana witryny internetowej (BR 3.2.2.4.6)

Ta metoda nie jest wykorzystywana.

3.2.2.2.7. Zmiana DNS (BR 3.2.2.4.7)

Sprawdzenie kontroli wnioskodawcy nad domeną FQDN odbywa się poprzez potwierdzenie otrzymania tokena żądania zawierającego wartość losową w rekordzie DNS TXT dla nazwy domeny do autoryzacji.

QTSP wykorzystuje unikalny token żądania dla każdego wniosku o certyfikat, który jest ważny tylko przez 30 dni.

Po pomyślnej walidacji FQDN przy użyciu tej metody QTSP może również wystawić certyfikaty dla innych FQDN, które kończą się etykietami zwalidowanej domeny FQDN.

3.2.2.2.8. Adres IP (BR 3.2.2.4.8)

Ta metoda nie jest wykorzystywana.

3.2.2.2.9. Certyfikat testowy (BR 3.2.2.4.9)

Ta metoda nie jest wykorzystywana.

3.2.2.2.10. TLS wykorzystujący numer losowy (BR 3.2.2.4.10)

Ta metoda nie jest wykorzystywana.

3.2.2.2.11. Inne metody (BR 3.2.2.4.11)

Ta metoda nie jest wykorzystywana.

3.2.2.2.12. Walidacja wnioskodawcy jako kontaktu domeny (BR 3.2.2.4.12)

Ta metoda nie jest wykorzystywana.

3.2.2.2.13. Email to DNS CAA Contact (BR 3.2.2.4.13)

Kontrola wnioskodawcy nad domeną FQDN jest potwierdzana poprzez wysłanie wartości losowej e-mailem, a następnie otrzymanie od wnioskodawcy odpowiedzi potwierdzającej otrzymanie tej wartości losowej.

Wartość losowa jest wysyłana na kontaktowy adres e-mail widniejący w rekordzie DNS CAA Email Contact. Odpowiednie dane źródłowe CAA są wyszukiwane za pomocą algorytmu wyszukiwania określonego w IETF RFC 8659 (28) Sekcja 3.

Kontaktowy e-mail w zasobie CAA powinien być podany w parametrach CAA. Ten e-mail powinien być zapisany w formacie określonym w RFC 6532 (29) sekcja 3.2 bez dodatków lub formatowania.

Przykład:
$ORIGIN example.com
CAA 0 contactemail "domainowner@example.com"

Każdy e-mail może służyć do potwierdzania kontroli nad wieloma FQDN, pod warunkiem, że każdy adres e-mail jest kontaktowym e-mailem DNS CAA dla każdej Nazwy Domeny, która ma zostać potwierdzona. Ten sam e-mail może być wysłany do wielu odbiorców, jeśli wszyscy ci odbiorcy stanowią kontaktowy e-mail z DNS CAA dla każdej Nazwy Domeny, podlegającej weryfikacji. QTSP może ponownie wysłać e-mail w całości, wraz z taką samą wartością losową pod warunkiem, że cała zawartość komunikacji i odbiorcy pozostają bez zmian.

Wartość losowa jest unikalna dla każdej wiadomości e-mail.

Wartość losowa jest ważna przez 30 dni od daty jej stworzenia.

Po pomyślnej walidacji FQDN przy użyciu tej metody QTSP może również wystawić certyfikaty dla innych FQDN, które kończą się etykietami zwalidowanej domeny FQDN.

3.2.2.2.14. Email to DNS TXT Contact (BR 3.2.2.4.14)

Kontrola wnioskodawcy nad domeną FQDN jest potwierdzana przez wysłanie wartości losowej e-mailem, a następnie otrzymanie od wnioskodawcy odpowiedzi potwierdzającej otrzymanie tej

wartości losowej. Wartość losowa jest wysyłana na kontaktowy adres e-mail widniejący w rekordzie DNS TXT dla nazwy weryfikowanej domeny, która służy do potwierdzenia FQDN.

Rekord DNS TXT powinien być umieszczony w subdomenie "_validation-contactemail" domeny podlegającej weryfikacji. Całkowita wartość RDATA tego rekordu TXT musi zawierać prawidłowy adres email zgodnie z RFC 6532 (29) sekcja 3.2, bez dodatkowych uzupełnień lub formatowania, w przeciwnym razie nie można użyć adresu e-mail.

Każdy e-mail może służyć do potwierdzania kontroli nad wieloma FQDN, pod warunkiem, że każdy adres e-mail jest kontaktowym e-mailem DNS TXT dla każdej Nazwy Domeny, która ma zostać potwierdzona. Ten sam e-mail może być wysłany do wielu odbiorców, jeśli wszyscy ci odbiorcy stanowią kontaktowy e-mail DNS TXT dla każdej Nazwy Domeny, podlegającej weryfikacji. QTSP może ponownie wysłać e-mail w całości, wraz z taką samą wartością losową pod warunkiem, że cała zawartość komunikacji i odbiorcy pozostają bez zmian. Wartość losowa jest unikalna dla każdej wiadomości e-mail. Wartość losowa jest ważna przez 30 dni od daty jej stworzenia.

Po pomyślnej walidacji FQDN przy użyciu tej metody QTSP może również wystawić certyfikaty dla innych FQDN, które kończą się etykietami zwalidowanej domeny FQDN

3.2.2.2.15. Phone Contact with Domain Contact (BR 3.2.2.4.15)

Sprawdzenie kontroli wnioskodawcy nad domeną FQDN odbywa się poprzez wykonanie połączenia telefonicznego na numer telefonu Domeny i uzyskanie odpowiedzi potwierdzającej w celu walidacji domeny.

Każde połączenie telefoniczne może służyć do potwierdzania kontroli nad wieloma domenami, pod warunkiem, że ten sam kontaktowy numer telefonu domeny obowiązuje dla każdej weryfikowanej domeny ADN i zapewnia odpowiedź potwierdzającą dla każdej ADN. W przypadku gdy odpowiada ktoś inny niż Kontakt Domeny, QTSP może poprosić o przełączenie do Kontaktu Domeny.

W przypadku odebrania przez pocztę głosową, QTSP może zostawić Wartość Losową i nazwy ADN, podlegające weryfikacji. Wartość Losowa musi zostać zwrócona do QTSP, w celu potwierdzenia wniosku. Wartość losowa jest ważna przez 30 dni od daty jej stworzenia.

Po pomyślnej walidacji FQDN przy użyciu tej metody QTSP może również wystawić certyfikaty dla innych FQDN, które kończą się etykietami zwalidowanej domeny FQDN.

3.2.2.2.16. Phone Contact with DNS TXT Record Phone Contact (BR 3.2.2.4.16)

Sprawdzenie kontroli wnioskodawcy nad domeną FQDN odbywa się poprzez wykonanie połączenia telefonicznego na kontaktowy numer telefonu rekordu DNS TXT i uzyskanie odpowiedzi potwierdzającej w celu walidacji ADN.

Rekord DNS TXT powinien być umieszczony w subdomenie "_validation-contactemail" domeny podlegającej weryfikacji. Całkowita wartość RDATA tego rekordu TXT musi zawierać prawidłowy Globalny Numer zgodnie z RFC 3966 (30) sekcja 5.1.4, w przeciwnym razie nie można użyć tego numeru.

Każde połączenie telefoniczne może służyć do potwierdzania kontroli nad wieloma domenami ADN, pod warunkiem, że ten sam kontaktowy nr telefonu DNS TXT obowiązuje dla każdej weryfikowanej domeny ADN i zapewnia odpowiedź potwierdzającą dla każdej ADN. QTSP nie może być przekierowany ani zażądać przekierowania, gdyż numer został specjalnie przeznaczony do celu walidacji domeny.

W przypadku odebrania przez pocztę głosową, QTSP może zostawić Wartość Losową i nazwy ADN, podlegające weryfikacji. Wartość Losowa musi zostać zwrócona do QTSP, w celu potwierdzenia wniosku. Wartość losowa jest ważna przez 30 dni od daty jej stworzenia.

Po pomyślnej walidacji FQDN przy użyciu tej metody QTSP może również wystawić certyfikaty dla innych FQDN, które kończą się etykietami zwalidowanej FQDN.

3.2.2.2.17. Phone Contact with DNS CAA Phone Contact (BR 3.2.2.4.17)

Sprawdzenie kontroli wnioskodawcy nad domeną FQDN odbywa się poprzez wykonanie połączenia telefonicznego na kontaktowy numer telefonu rekordu DNS CAA i uzyskanie odpowiedzi potwierdzającej do walidacji każdej ADN.

Każde połączenie telefoniczne może służyć do potwierdzania kontroli nad wieloma domenami ADN, pod warunkiem, że ten sam nr telefonu w DNS CAA widnieje dla każdej weryfikowanej ADN i zapewnia odpowiedź potwierdzającą dla każdej ADN.

Odpowiednie dane źródłowe CAA są wyszukiwane za pomocą algorytmu wyszukiwania określonego w IETF RFC 8659 (28) Sekcja 3.

Numer telefonu powinien być podany w parametrach CAA (contactphone). Cała wartość parametru musi zawierać Globalny Numer w formacie zgodnym z RFC 3966 (30) sekcja 5.1.4, w przeciwnym razie nie można użyć tego numeru. Globalny Numer zawiera prefix + i nr kierunkowy kraju i może zawierać wizualne separatory.

Poniżej przykład, gdzie posiadacz domeny określił atrybut kontaktu podając numer telefonu.
$ORIGIN example.com.
CAA 0 contactphone "+48 (1) 123-4567"

QTSP nie może być przekierowany ani zażądać przekierowania, gdyż numer został specjalnie przeznaczony do celu walidacji domeny.

W przypadku odebrania przez pocztę głosową, QTSP może zostawić Wartość Losową i Nazwy Domeny ADN, podlegające weryfikacji. Wartość Losowa musi zostać zwrócona do QTSP, w celu weryfikacji domeny. Wartość losowa jest ważna przez 30 dni od daty jej stworzenia.

Po pomyślnej walidacji FQDN przy użyciu tej metody QTSP może również wystawić certyfikaty dla innych FQDN, które kończą się etykietami zwalidowanej FQDN.

3.2.2.2.18. Agreed-Upon Change to Website v2 (BR 3.2.2.4.18)

Sprawdzenie kontroli wnioskodawcy nad domeną FQDN odbywa się poprzez weryfikację, czy Token Żądania zawierający Wartość losową został umieszczony przez wnioskodawcę w pliku pod identyfikowaną nazwą domeny.

a) Całkowity Token żądania nie powinien pojawić się w żądaniu użytym do uzyskania pliku, i
b) QTSP musi otrzymać pozytywną odpowiedź HTTP na żądanie (kod statusu 2xx HTTP).

Plik zawierający Token Żądania:

a) powinien być umieszczony w Weryfikowanej Nazwie Domeny (ADN) i
b) powinien być umieszczony pod katalogiem "/.well-known/pki-validation" i
c) powinien być dostępny poprzez protokół "http" lub "https" i
d) powinien być dostępny poprzez Autoryzowany Port.

QTSP nie akceptuje przekierowań (kod statusu 3xx http).

Wartość Losowa zawarta w Tokenie Żądania:

a) jest unikalna dla każdego Wniosku o Certyfikat;
b) pozostaje ważna w celu walidacji do użycia w odpowiedzi zwrotnej przez 30 dni od daty jej stworzenia.

QTSP dokonuje odrębnej walidacji dla każdej FQDN przy użyciu tej metody, nawet jeśli FQDN kończą się tą samą zweryfikowaną pełną nazwą FQDN.

3.2.2.2.19. Agreed-Upon Change to Website - ACME (BR 3.2.2.4.19)

Ta metoda nie jest wykorzystywana.

3.2.2.2.20. TLS Using ALPN (BR 3.2.2.4.20)

Ta metoda nie jest wykorzystywana.

Certyfikaty uwierzytelniania witryn nie zawierają adresów IP.

3.2.2.3. Uwierzytelnienie adresu IP

Certyfikaty Uwierzytelniania Witryn nie zawierają adresu IP, stąd nie ma potrzeby walidacji adresu IP.

3.2.3. Uwierzytelnienie osoby fizycznej

Tożsamość osoby fizycznej musi być potwierdzona:

a) jeżeli Podmiotem Certyfikatu, który ma zostać wystawiony jest osoba fizyczna;
b) jeżeli osoba fizyczna działa w imieniu organizacji w celu uzyskania Certyfikatu Organizacyjnego lub Certyfikatu Uwierzytelniania Witryny Internetowej.

Podczas wystawiania certyfikatu, tożsamość osoby fizycznej powinna być weryfikowana zgodnie z art. 24 ust. 1 eIDAS (1) przez fizyczną obecność osoby fizycznej lub przy użyciu innych metod identyfikacji zapewniających równoważny poziom bezpieczeństwa. QTSP używa metod identyfikacji przedstawionych w art. 24 ust. 1.

QTSP sprawdza tożsamość osoby fizycznej stosując jedną z poniższych metod w zależności od warunków technicznych i innych.

1) Osobista weryfikacja tożsamości.

a) Osoba fizyczna powinna stawić się osobiście przed osobą, która dokonuje weryfikacji tożsamości, którą może być:
   - Inspektor Rejestracji,
   - Notariusz, jako zaufana osoba trzecia zgodnie z prawem polskim.
b) Tożsamość osoby fizycznej jest weryfikowana podczas osobistej identyfikacji na podstawie oficjalnego dokumentu tożsamości.
   Identyfikacja może być przeprowadzona z wykorzystaniem oficjalnych dokumentów:
   - w przypadku obywateli Rzeczypospolitej Polskiej – dowód osobisty lub inny oficjalny dokumentu uznawany na terenie Polski jako dokument tożsamości;
   - paszport;
   - w przypadku identyfikacji osób fizycznych, które nie posiadają żadnego z wyżej wymienionych dokumentów, QTSP stosuje osobistą weryfikację tożsamości w oparciu o dowód osobisty obywateli wyłącznie z krajów Unii Europejskiej. W takiej sytuacji, akceptowany jest dowód osobisty osoby fizycznej lub prawo jazdy opublikowane w publicznej bazie PRADO - Public Register of Authentic identity and travel Documents Online (31) wydany przez kraj Unii Europejskiej.

c) Osoba fizyczna powinna oświadczyć na piśmie, w formie elektronicznej lub dokumentowej, że dane osobiste użyte do identyfikacji są prawdziwe i prawidłowe. Oświadczenie takie powinno być złożone w obecności osoby dokonującej weryfikacji tożsamości.
d) W przypadku obywateli Rzeczypospolitej Polskiej, sprawdzenie prawdziwości danych na dowodzie osobistym użytym do identyfikacji osobistej i autentyczności samego dowodu osobistego jest przeprowadzone przez Punkt Rejestracji w oparciu o wiarygodny rejestr publiczny. W przypadku innych osób fizycznych QTSP nie musi potwierdzać prawdziwości danych na dowodzie osobistym ani ważności dowodu przy użyciu rejestru publicznego, jeśli taki rejestr nie jest dostępny lub koszt dostępu do niego i koszt weryfikacji jest nieproporcjonalnie wysoki.
e) Adres osoby fizycznej powinien być sprawdzony na podstawie karty pobytu.
f) Osoba dokonująca weryfikacji tożsamości sprawdza, czy dokument tożsamości nie został sfałszowany.

Podczas pierwszej weryfikacji tożsamości QTSP może zaakceptować identyfikację przeprowadzoną przez notariusza jako sposób potwierdzania tożsamości równoważny z tym dokonanym przez Punkt Rejestracji, jeśli z zaświadczenia notarialnego, dołączonego do wniosku o wydanie certyfikatu podpisanego w obecności notariusza wynika, że notariusz porównał dane osobowe wnioskodawcy, który się przed nim stawił z zawartością rejestru publicznego lub innej bazy centralnej.

Dodatkowe zasady weryfikacji tożsamości cudzoziemców

QTSP uznaje identyfikację przeprowadzoną przez notariusza za granicą jako równoważną z weryfikacją przeprowadzoną przez swój Punkt Rejestracji, jeżeli notariusz jest zarejestrowany w obcym państwie, które:

a) przystąpiło do międzynarodowej dwustronnej umowy z Rzeczpospolitą Polską w sprawie wzajemnego uznawania dokumentów urzędowych; lub
b) ratyfikowało Konwencję Haską z 1961 r. znoszącą wymóg legalizacji zagranicznych dokumentów urzędowych (apostille).

Dokument wydany przez notariusza powinien być zgodny z wymogami przedstawionymi w danym porozumieniu.

QTSP uznaje wniosek o wydanie certyfikatu podpisany przed notariuszem jeżeli z zaświadczenia notarialnego wynika, że

a) notariusz zweryfikował tożsamość wnioskodawcy na podstawie odpowiedniego oficjalnego dokumentu służącego do weryfikacji tożsamości (np. dowód osobisty, paszport, itd.);
b) wnioskodawca podpisał wniosek o wydanie certyfikatu w obecności notariusza.

QTSP uznaje tylko oryginalne dokumenty wydane w języku polskim lub angielskim. W przypadku dokumentów wydanych w innych językach QTSP może zażądać tłumaczenia przysięgłego.

QTSP może również zaakceptować inne dokumenty i dowody po upewnieniu się, że ich poziom bezpieczeństwa jest równoważny powyższym. Dostarczenie takich dowodów QTSP leży po stronie Klienta.

QTSP akceptuje wyłącznie ważne dokumenty i dowody nie starsze niż 3 miesiące.

QTSP nie wystawia certyfikatu, jeśli uzna, że w oparciu o wewnętrzne zasady nie jest w stanie dostatecznie zweryfikować zaświadczenia, dokumentu lub danych przedstawionych przez zagraniczny podmiot.

2) Identyfikacja na podstawie certyfikatu podpisu.

W tym przypadku:

a) Wnioskodawca składa wniosek o wydanie certyfikatu w formie elektronicznej opatrzony kwalifikowanym podpisem elektronicznym opartym o certyfikat kwalifikowany nie-anonimowy;
b) podpisany elektronicznie wniosek o wydanie certyfikatu powinien zawierać dane wymagane w celu jednoznacznej identyfikacji osoby fizycznej;
c) QTSP weryfikuje autentyczność i integralność wniosku o wydanie certyfikatu w całej ścieżce certyfikacji (pełnomocnictw);
d) QTSP akceptuje wyłącznie takie podpisy elektroniczne, które wykorzystują certyfikat wystawiony przez Dostawcę Usług Zaufania zarejestrowanego na krajowej liście zaufania opublikowanej na zaufanej liście UE i który był ważny podczas składania podpisu;
e) QTSP uznaje tylko podpisy elektroniczne oparte na certyfikacie wydanym zgodnie z art. 24, ust. 1, a) lub b) eIDAS (1);
f) w zależności od informacji o podmiocie zawartych w certyfikacie użytym do uwierzytelnienia żądania certyfikatu:
   - jeśli tożsamość podmiotu nie może być jednoznacznie ustalona na podstawie danych, QTSP może umieścić w nowym certyfikacie tylko dane podmiotu zgodne z danymi podmiotu zawartymi w certyfikacie użytym do uwierzytelnienia żądania certyfikatu;
   - jeśli dane jednoznacznie ustalają tożsamość Podmiotu (np. zawierają numer dowodu osobistego lub inny niepowtarzalny identyfikator Podmiotu), QTSP może umieścić w nowym certyfikacie dane inne niż dane Podmiotu zawarte w certyfikacie użytym do poświadczenia żądania certyfikatu.

3) Inne metody identyfikacji zapewniające poziom bezpieczeństwa równoważny fizycznej obecności

QTSP może również zweryfikować tożsamość osoby fizycznej zgodnie z art. 24.1 eIDAS (1) przy użyciu następujących metod:

a) identyfikacja przy użyciu narzędzi komunikacji elektronicznej dostarczających biometrycznej technologii video, uznana za równoważną w stosunku do fizycznej obecności (zwaną dalej: wideoweryfikacją), zgodnie z art. 24.1.d eIDAS;
b) identyfikacja za pomocą środka identyfikacji elektronicznej zgodnie z art. 24.1.b eIDAS (1).

W takim przypadku, QTSP postępuje tak samo jak w przypadku opisanej wcześniej osobistej weryfikacji tożsamości, z tą różnicą, że zamiast fizycznego spotkania odbywa się identyfikacja na odległość równoważna fizycznej obecności.

Wideoweryfikacja

a) QTSP rejestruje wizerunek Klienta (poprzez nagranie wideo) z transmisji audiowizualnej na żywo, a następnie porównuje wykonane zdjęcie z fotografią w dokumencie tożsamości użytym do identyfikacji (zwanym dalej: dokumentem tożsamości). Identyfikacja kończy się wynikiem pozytywnym, kiedy QTSP może jednoznacznie stwierdzić, że osoba na zdjęciu w dokumencie tożsamości jest tożsama z osobą z transmisji audiowizualnej.

b) W celu prawidłowej identyfikacji podczas transmisji audiowizualnej, należy spełnić następujące warunki:
   - dokument tożsamości powinien być w dobrym stanie;
   - dobrze oświetlone otoczenie;
   - otoczenie wyciszone i bez zakłóceń;
   - brak obecności osób postronnych;
   - dostęp do urządzenia z wejściem audio-video;
   - dostęp do kamery z rozdzielczością obrazu video co najmniej 2 megapiksele;
   - dostęp do stabilnego połączenia internetowego z prędkością co najmniej 1.5Mbps.
c) QTSP zapewnia, że Klient jest informowany wcześniej o warunkach identyfikacji zdalnej oraz PCKPC.
d) QTSP nagrywa i przechowuje zapis całej komunikacji pomiędzy nim a Klientem powstałej podczas identyfikacji video przez co najmniej 20 lat od daty nagrania, a także zgodę Klienta, w sposób umożliwiający dostęp do tych danych oraz zapobiegający pogorszeniu jakości nagrania audio i video.
e) Rozdzielczość i jasność obrazu w urządzeniu komunikacji elektronicznej musi umożliwić identyfikację płci, wieku i rysów twarzy Klienta, a Klient powinien:
   - patrzeć w kierunku kamery tak, aby jego wizerunek mógł zostać rozpoznany, przechwycony i porównany z jego zdjęciem w dowodzie tożsamości,
   - w sposób zrozumiały podać numer dokumentu tożsamości użytego podczas transmisji audiowizualnej,
   - pokazać swój dokument tożsamości w taki sposób, aby zabezpieczenia dowodu oraz dane na nim zawarte mogły być rozpoznane, zapisane i zweryfikowane i
   - dane zawarte w dokumencie tożsamości mogły być powiązane z danymi klienta w bazie QTSP, a Klient mógł zostać zidentyfikowany na podstawie zdjęcia przedstawionego w dokumencie tożsamości.
f) QTSP powinien sprawdzić, czy przedłożony dokument jest odpowiedni do przeprowadzenia identyfikacji audiowizualnej, co oznacza, że
   - dokument jest zgodny z wymogami organu wydającego,
   - elementy zabezpieczające, takie jak hologram, kinegram oraz inne równoważne zabezpieczenia są rozpoznawane i są niezniszczone,
   - identyfikator dokumentu tożsamości jest tożsamy z dostarczonym przez Klienta, jest niezniszczony i nadaje się do odczytu.
g) Podczas transmisji audiowizualnej QTSP sprawdza, czy:
   - wizerunek Klienta odpowiada jego wizerunkowi przedstawionemu przez w jego dokumencie tożsamości,
   - dane Klienta zawarte w dokumencie tożsamości odpowiadają danym, do których QTSP ma dostęp.
h) Klient jest w trybie online podczas całej identyfikacji.

QTSP wystawia certyfikat jedynie wtedy, gdy identyfikacja audiowizualna spełnia wszystkie powyższe warunki.

Elektroniczny dokument tożsamości

a) QTSP umożliwia Klientom identyfikację przy użyciu elektronicznego dowodu osobistego, którzy taki dokument posiadają.
b) QTSP uznaje elektroniczny dowód osobisty jako środek identyfikacji elektronicznej w rozumieniu art. 24.1.b eIDAS (1).

c) QTSP może użyć tej usługi uwierzytelnienia za pośrednictwem brokera lub samodzielnie.

QTSP może wykorzystać dane potwierdzone podczas wcześniejszej procedury identyfikacji osoby fizycznej jeśli wnioskodawca występuje o nowy certyfikat, w przypadku wygaśnięcia lub unieważnienia poprzedniego, lub jeśli występuje o nowy certyfikat mimo ważności poprzedniego certyfikatu. Autentyczność wniosku o wydanie certyfikatu, prawdziwość i ważność danych, które pojawią się w certyfikacie oraz tożsamość wnioskodawcy jest sprawdzana przez QTSP.

3.2.4. Identyfikacja użytkownika znacznika czasu

Subskrybenci mogą używać znacznika czasu tylko po pozytywnej identyfikacji. Identyfikacja może być wykonana za pomocą certyfikatu uwierzytelniania lub loginu i hasła przydzielonych Subskrybentowi.

Domyślny punkt dostępu kwalifikowanej usługi znakowania czasem: https://services.eurocert.pl/TSA/

Korzystając z tego adresu URL QTSP wydaje tylko kwalifikowane znaczniki czasu.

3.2.5. Informacje o subskrybentach niezweryfikowanych

W Certyfikacie mogą znaleźć się jedynie dane zweryfikowane przez QTSP.

3.2.6. Weryfikacja upoważnień

Przed wydaniem certyfikatu organizacyjnego tożsamość osoby fizycznej reprezentującej osobę prawną jest weryfikowana zgodnie z wymogami sekcji 3.2.3.

Należy zweryfikować uprawnienia osoby fizycznej do reprezentacji.

Osoby uprawnione do działania w imieniu organizacji:

a) osoba uprawniona do reprezentowania danej organizacji,
b) osoba, posiadająca upoważnienie do reprezentowania organizacji od osoby uprawnionej,
c) administrator organizacyjny powołany przez osobę upoważnioną do reprezentowania organizacji.

Administratora można wyznaczyć w trakcie aplikowania o certyfikat lub w dowolnym momencie później za pomocą odpowiedniego formularza. W formularzu należy podać dane identyfikacyjne wyznaczonej osoby. Formularz powinien być podpisany (odręcznie lub przy użyciu kwalifikowanego podpisu elektronicznego) przez przedstawiciela organizacji, którego tożsamość jest weryfikowana przez QTSP po przyjęciu ww. formularza.

Wyznaczenie administratora nie jest obowiązkowe, ale można też wyznaczyć wielu administratorów w tym samym czasie. Jeśli nie ma administratora, czynności wykonuje osoba upoważniona do reprezentowania organizacji.

QTSP prowadzi listę osób fizycznych uprawnionych do złożenia Wniosku o Certyfikat w imieniu organizacji.

Na pisemny wniosek organizacji, który jest weryfikowany, QTSP przekazuje organizacji aktualną listę jej upoważnionych Administratorów Organizacyjnych.

3.2.7. Kryteria interoperacyjności

QTSP nie współpracuje z innymi Dostawcami Usług Zaufania podczas dostarczania usług.

3.2.8. Weryfikacja adresu e-mail

Niniejsza sekcja określa użyte procesy i procedury do potwierdzania kontroli Aplikanta nad adresem skrzynki pocztowej do umieszczenia w certyfikacie.

QTSP weryfikuje, że Aplikant kontroluje skrzynki email powiązane ze wszystkimi polami email w certyfikacie lub został upoważniony przez właściciela skrzynki do działania w imieniu właściciela.

QTSP nigdy nie deleguje weryfikacji kontroli nad skrzynką lub weryfikacji upoważnienia do skrzynki.

QTSP utrzymuje rejestr metod walidacji użytych do walidacji każdej domeny lub adresu email zawartych w certyfikacie, zawierający odpowiednią wersję S/MIME Baseline Requirements (13) lub TLS Baseline Requirements (6).

Ukończone walidacje upoważnienia Aplikanta mogą służyć do wydawania wielu certyfikatów na przestrzeni czasu. W każdym przypadku, walidacja przed wydaniem certyfikatu musi być zainicjowana w czasie określonym w odpowiednich wymaganiach (takich jak w 4.2.1).

Walidacja dostępu do skrzynki pocztowej przy użyciu domeny.

QTSP może potwierdzić, że Aplikant został upoważniony przez właściciela konta skrzynki email do działania w imieniu właściciela poprzez weryfikację kontroli nad nazwą domeny zawartą w adresie email, który ma być umieszczony w certyfikacie.

QTSP używa wyłącznie następujących zatwierdzonych metod w sekcji 3.2.2.4 „TLS Baseline Requirements" do wykonywania powyższej weryfikacji:

- Email to Domain Contact (BR 3.2.2.4.2),
- Constructed Email to Domain Contact (BR 3.2.2.4.4),
- DNS Change (BR 3.2.2.4.7),
- Email to DNS CAA Contact (BR 3.2.2.4.13),
- Email to DNS TXT Contact (BR 3.2.2.4.14),
- Phone Contact with Domain Contact (BR 3.2.2.4.15),
- Phone Contact with DNS TXT Record Phone Contact (BR 3.2.2.4.16),
- Phone Contact with DNS CAA Phone Contact (BR 3.2.2.4.17),
- Agreed-Upon Change to Website v2 (BR 3.2.2.4.18).

Walidacja dostępu do skrzynki pocztowej przy użyciu wiadomości email.

W przypadku wniosków o wydanie certyfikatu złożonych poprzez stronę internetową QTSP, QTSP sprawdza podany adres e-mail przed wysłaniem wniosku o certyfikat. Przed wypełnieniem formularza wniosku Klient jest pytany jedynie o adres e-mail. Na podany adres e-mail QTSP wysyła unikalny czterocyfrowy losowy numer i unikalny adres URL z ograniczonym okresem ważności, zawierający unikalny losowy numer. Informacje niezbędne do walidacji są wysyłane wyłącznie na adres do walidacji, nie są wysyłane żadną inną drogą. Wnioskodawca może wypełnić formularz w całości jedynie po wprowadzeniu tego otrzymanego numeru do formularza lub otworzeniu unikalnego linku. W ten sposób każdy przychodzący wniosek o wydanie certyfikatu posiada e-mail, który został już zweryfikowany.

W przypadku wniosków o wydanie certyfikatu złożonych w inny sposób niż stronę www, QTSP wysyła wiadomość e-mail z unikalnym losowym numerem lub unikalnym adresem URL z ograniczonym okresem ważności, zawierającym unikalny losowy numer, na adres do weryfikacji.

Informacje niezbędne do walidacji są wysyłane wyłącznie na adres do walidacji i nie są wysyłane żadną inną drogą.

Wnioskujący odpowiada i potwierdza wniosek poprzez wprowadzenie tego numeru losowego lub otworzenie unikalnego linku. Numer losowy wygasa po 30 dniach.

W przypadku Certyfikatów Email (S/MIME) wartość losowa jest ważna przez 24h.

3.3. Identyfikacja i uwierzytelnienie dla wniosków o recertyfikację

Recertyfikacja jest procesem wymiany klucza, w którym QTSP wystawia podmiotowi certyfikat z podmienionym kluczem publicznym. O wymianę można wystąpić jedynie w okresie ważności umowy na usługę.

W przypadku wniosku o recertyfikację QTSP weryfikuje fakt istnienia pierwotnego certyfikatu i sprawdza jego ważność.

QTSP zatwierdza wniosek o recertyfikację zarówno w przypadku ważnych jak i nieważnych certyfikatów (zawieszonych, unieważnionych i wygasłych).

Szczegóły dotyczące recertyfikacji znajdują się w sekcji 4.7.

3.3.1. Identyfikacja i uwierzytelnienie dla ważnych Certyfikatów

Identyfikacja wnioskodawcy odbywa się zgodnie z zasadami opisanymi w sekcji 3.2.3.

Jeżeli data ważności nowego certyfikatu nie jest późniejsza niż certyfikat podlegający recertyfikacji, QTSP wykorzystuje wyniki i dowody pozyskane w trakcie pierwotnego procesu walidacji.

3.3.2. Identyfikacja i uwierzytelnianie dla nieważnych Certyfikatów

QTSP przyjmuje wniosek o recertyfikację – jedynie w okresie trwania ważności umowy – w przypadku certyfikatów zawieszonych, unieważnionych i wygasłych.

Identyfikacja wnioskodawcy odbywa się na zasadach opisanych w sekcji 3.2.3.

3.4. Identyfikacja i uwierzytelnianie w przypadku odnawiania Certyfikatów

Odnowienie certyfikatu jest procesem, w którym QTSP wystawia certyfikat temu samemu podmiotowi, bez zmiany danych, lecz ze zmienioną datą ważności. O odnowienie certyfikatu można wystąpić wyłącznie w okresie trwania umowy.

3.4.1. Identyfikacja i uwierzytelnienie ważnych Certyfikatów

Identyfikacja wnioskodawcy odbywa się na zasadach określonych w sekcji 3.2.3. Uwierzytelnienie wniosku następuje na podstawie aktualnego certyfikatu.

Jeśli QTSP inicjuje odnowienie certyfikatu, może wykorzystać dowody zebrane podczas pierwszej weryfikacji tożsamości (patrz sekcja 3.2) oraz wyniki tej weryfikacji, jeżeli data ważności nowego certyfikatu nie jest późniejsza niż certyfikat podlegający odnowieniu.

3.4.2. Identyfikacja i uwierzytelnienie nieważnych Certyfikatów

Identyfikacja wnioskodawcy odbywa się na zasadach określonych w sekcji 3.2.3. Uwierzytelnienie wniosku następuje na podstawie środka identyfikacji elektronicznej lub innego środka uwierzytelniającego przypisanego Aplikantowi podczas pierwszej weryfikacji tożsamości.

3.5. Identyfikacja i uwierzytelnienie dla modyfikacji certyfikatów

Modyfikacja certyfikatu to proces, w którym QTSP wystawia nowy certyfikat temu samemu podmiotowi z tym samym kluczem publicznym, lecz z innymi danymi identyfikacyjnymi podmiotu.

3.5.1. Identyfikacja i uwierzytelnienie dla ważnych Certyfikatów

Identyfikacja wnioskodawcy odbywa się na zasadach opisanych w sekcji 3.2.3.

Jeżeli data ważności zmodyfikowanego certyfikatu nie jest późniejsza niż certyfikatu poprzedniego QTSP może wykorzystać dowody zebrane podczas pierwotnego procesu walidacji.

3.5.2. Identyfikacja i uwierzytelnienie dla nieważnych Certyfikatów

Nieważny certyfikat nie może być zmodyfikowany.

3.6. Identyfikacja i uwierzytelnienie wniosków o unieważnienie

QTSP przyjmuje i przetwarza wnioski o zawieszenie i unieważnienie certyfikatów oraz zgłoszenia dotyczące unieważnienia certyfikatu (na przykład, związane z ujawnieniem klucza prywatnego lub z niewłaściwym użyciem certyfikatu).

QTSP rozpatruje wnioski niezwłocznie i akceptuje jedynie wnioski zgłaszane przez strony do tego upoważnione.

W każdym przypadku QTSP weryfikuje autentyczność otrzymanego wniosku i uprawnienia osoby składającej Wniosek.

Identyfikacja i uwierzytelnianie takich wniosków zostały opisane w sekcji 4.9.

W przypadku certyfikatu uwierzytelniania witryny internetowej zawieszenie nie jest możliwe.

3.7. Zweryfikowane metody komunikacji

By zapewnić bezpieczną komunikację z wnioskodawcą i potwierdzić, że jest świadomy i akceptuje wystawienie certyfikatu, QTSP weryfikuje jego numer telefonu, adres e-mail lub adres pocztowy jako zweryfikowane metody komunikacji z wnioskodawcą.

W celu sprawdzenia zweryfikowanej metody komunikacji z wnioskodawcą QTSP:

a) Sprawdza, czy zweryfikowana metoda komunikacji należy do wnioskodawcy w oparciu o:
   - Dane dostarczone przez stosowną firmę telekomunikacyjną (numer telefonu);
   - Kwalifikowane publiczne źródło informacji;
   - Dokument wystawiony przez notariusza;
   - Identyfikację tożsamości wnioskodawcy.

b) Potwierdza użyteczność zweryfikowanej metody komunikacji.
   Inspektor ds. Rejestracji QTSP kontaktuje się z wnioskodawcą za pomocą zweryfikowanej metody komunikacji. Wiarygodność Zweryfikowanej Metody Komunikacji jest potwierdzana poprzez fizyczną obecność wnioskodawcy lub poprzez użycie hasła do wybranego kanału komunikacji.

3.8. Weryfikacja podpisów na umowie i wnioskach o certyfikat EV

Umowa subskrybencka oraz wniosek o certyfikat EV muszą być podpisane. Umowa subskrybencka musi być podpisana przez upoważnionego przedstawiciela subskrybenta (Podpisujący Umowy – Contract Signer). Wniosek musi być podpisany przez Aplikującego (Certificate Requester). Jeśli Certificate Requester nie jest również Akceptującym Certyfikat (Certificate Approver), wtedy Akceptujący Certyfikat osobno akceptuje Wniosek. W każdym przypadku, stosowne podpisy muszą być ważne i skuteczne prawnie, wiążące Subskrybenta z treścią dokumentu:

a) dla dokumentów w formie papierowej – podpisy odręczne zgodne ze wzorcem podpisu i (opcjonalnie) pieczęć firmy, zgodnie z zasadami reprezentacji w firmie,
b) dla dokumentów w formie elektronicznej – kwalifikowane podpisy elektroniczne.

Podczas walidacji podpisu, QTSP uwierzytelnia każdy podpis w taki sposób, dzięki któremu uzyskuje pewność, że osoba widniejąca na dokumencie jako podpisująca jest tą osobą, która rzeczywiście podpisała dokument w imieniu Aplikującego.

Podpis można zweryfikować na następujące sposoby:

a) w przypadku dokumentów w formie papierowej Wnioskodawca składa odręczny podpis w obecności Inspektora Rejestracji, po wcześniejszej walidacji tożsamości dokonanej przez Inspektora Rejestracji;
b) pozytywna walidacja kwalifikowanych podpisów elektronicznych;
c) w przypadku podpisów odręcznych poświadczonych notarialnie, QTSP weryfikuje przy użyciu wiarygodnych źródeł, czy notariusz ma stosowne, ważne uprawnienia w jurysdykcji Podpisującego i kontaktuje się z notariuszem, aby potwierdzić, czy rzeczywiście wydał on ten dokument;
d) Inspektor Rejestracji kontaktuje się z Wnioskodawcą lub Subskrybentem przy użyciu zweryfikowanej metody komunikacji, po czym otrzymuje od osoby odpowiedź potwierdzającą, że podpisała dokument w imieniu Wnioskodawcy lub Subskrybenta.

4. Wymagania operacyjne dotyczące cyklu życia Certyfikatu

Wystawienie nowego certyfikatu nowemu podmiotowi powinno być poprzedzone zgłoszeniem wniosku o rejestrację u QTSP i podpisaniem przez Subskrybenta umowy na świadczenie usług oraz podpisaniem przez Aplikującego wniosku o wydanie certyfikatu.

Wymiana certyfikatu następuje, gdy uprzednio zarejestrowany i zidentyfikowany podmiot wnioskuje o wydanie nowego certyfikatu w miejsce już istniejącego, w okresie ważności umowy na świadczenie usług. Wymiana certyfikatu może mieć miejsce z następujących powodów:

a) odnowienie certyfikatu oznacza wystąpienie o wystawienie certyfikatu z takimi samymi danymi podmiotu, jak w poprzednim certyfikacie i obydwa certyfikaty są wydane dla tego samego klucza publicznego. Szczegóły dotyczące odnawiania certyfikatu są omówione w sekcji 4.6.
b) modyfikacja certyfikatu oznacza wystąpienie o zmianę danych certyfikatu dotyczącą danych podmiotu zawartych w certyfikacie. QTSP otrzymuje wniosek o modyfikację certyfikatu w trakcie okresu ważności certyfikatu. Podczas modyfikacji certyfikatu, nowy certyfikat jest wystawiany dla tego samego klucza publicznego. Szczegóły dotyczące modyfikacji certyfikatu są omówione w sekcji 4.8.
c) recertyfikacja oznacza wystawienie nowego certyfikatu dla nowego klucza publicznego na wniosek podmiotu w trakcie okresu ważności certyfikatu lub po jego wygaśnięciu. Szczegóły dotyczące recertyfikacji są omówione w sekcji 4.7.

Jeśli w ramach aktualnej umowy na świadczenie usług Klient występuje z wnioskiem o nowy certyfikat, konieczna jest zmiana umowy.

Status certyfikatu może być:

- ważny,
- zawieszony,
- unieważniony lub
- wygasły.

Przepisy dotyczące zmiany statusu omówiono w sekcji 4.9. Szczegóły dotyczące usługi statusu certyfikatu przedstawiono w sekcji 4.10.

QTSP zapewnia obsługę certyfikatu jedynie na mocy stosownej umowy na świadczenie usług. Zasady dotyczące zakończenia umowy na świadczenie usług przedstawiono w sekcji 4.11.

4.1. Wniosek o wystawienie certyfikatu

Do wystawienia nowego certyfikatu wymagane jest wystąpienie z wnioskiem o jego wydanie. Przed złożeniem pierwszego wniosku o certyfikat, wnioskujący powinien złożyć u QTSP wniosek o rejestrację, na przykład, na stronie internetowej QTSP. Wnioskodawca podaje dane, które mają być w certyfikacie i wskazuje na rodzaj certyfikatu. Wnioskodawca upoważnia QTSP do zarządzania danymi osobowymi zawartymi we wniosku o rejestrację.

QTSP nie uznaje danych podanych we wniosku o rejestrację za prawdziwe, dopóki wnioskujący nie potwierdzi ich we wniosku o wystawienie certyfikatu.

Jeżeli pojawi się konieczność zawarcia nowej umowy na świadczenie usług QTSP przygotowuje umowę dla subskrybenta w oparciu o informacje podane we wniosku o rejestrację.

Umowa na świadczenie usług powinna zawierać rodzaje certyfikatów przeznaczonych dla konkretnych podmiotów w ramach usług świadczonych na podstawie umowy.

Wnioskujący może wystąpić o nowy certyfikat w ramach poprzedniej umowy. Jeżeli certyfikat jest wystawiany jako wymiana certyfikatu wyszczególnionego w umowie na świadczenie usług, nie jest konieczne zmienianie samej umowy. Jeżeli Klient wnioskuje o nowy certyfikat jako dodatkowy do pozostałych certyfikatów, należy zmienić umowę na świadczenie usług.

QTSP informuje subskrybenta o warunkach użytkowania certyfikatu przed zawarciem umowy.

Jeżeli wnioskodawca i subskrybent to nie jedna i ta sama osoba, informacja, o której mowa powyżej jest również przekazywana wnioskodawcy.

QTSP publikuje dokumenty zawierające te informacje w zrozumiałej formie na swojej stronie internetowej, w formie elektronicznej.

We wniosku o wystawienie certyfikatu podmiot powinien zawrzeć co najmniej następujące dane:

a) dane do umieszczenia w certyfikacie (np. imię i nazwisko, tytuł, nazwa organizacji, nazwa jednostki organizacyjnej, nazwa domeny, miejscowość, kraj, adres e-mail),
b) identyfikacyjne dane osobowe podmiotu – w przypadku organizacji, dane osoby reprezentującej podmiot: pełne imię i nazwisko, numer dokumentu tożsamości, nazwisko panieńskie matki, data urodzenia,
c) dane kontaktowe podmiotu – w przypadku organizacji, dane osoby reprezentującej organizację: numer telefonu, adres e-mail,
d) w przypadku wniosku o certyfikat organizacyjny – dane tej organizacji: oficjalna nazwa, siedziba, identyfikator urzędowy, opcjonalnie: nazwa jednostki organizacyjnej,
e) dane Subskrybenta do faktury.

Wraz z wnioskiem o wystawienie certyfikatu QTSP wymaga co najmniej poniższych dokumentów, zaświadczeń i oświadczeń (w przypadku identyfikacji zdalnej kopie tychże):

a) dokumenty niezbędne do identyfikacji podmiotu – w przypadku organizacji, osoby ją reprezentującej – zgodnie z sekcją 3.2.3,
b) w przypadku certyfikatu organizacyjnego, dokumenty identyfikacyjne tej organizacji zgodnie z sekcją 3.2.2,
c) jeśli podmiot jest organizacją, zaświadczenie lub upoważnienie przekazane przez organizację, że wnioskodawca jest upoważniony do reprezentowania organizacji zgodnie z sekcją 3.2.5,
d) w przypadku certyfikatu organizacyjnego, dowody wydane przez organizację, że wnioskodawca jest uprawniony do reprezentowania organizacji zgodnie z sekcją 3.2.5,

e) jeśli podmiot jest osobą fizyczną wnioskującą o wskazanie przynależności do organizacji, dowód na zgodę danej organizacji według wytycznych sekcji 3.2.2.

4.1.1. Kto może złożyć wniosek o wystawienie certyfikatu

Wniosek o wydanie certyfikatu może być złożony jedynie przez osobę fizyczną w celu uzyskania certyfikatu dla siebie samej, pracowników danej organizacji lub samej organizacji, którą ta osoba reprezentuje.

W przypadku certyfikatu organizacyjnego przedstawicielem może być jedynie osoba fizyczna zgodnie z sekcją 3.2.5. W przeciwnym wypadku wniosek o certyfikat jest automatycznie odrzucany.

Warunkiem wstępnym wystawienia certyfikatu jest wiążąca i ważna umowa na świadczenie usług (podpisana przez subskrybenta i QTSP) dotycząca wystawienia certyfikatu i jego utrzymania.

Podmiot – w przypadku organizacji, przedstawiciel organizacji – może złożyć wniosek o wystawienie certyfikatu w następujący sposób:

a) w formie papierowej, podpisany odręcznie w punkcie obsługi klienta QTSP lub w mobilnym punkcie rejestracji QTSP w dniu uprzednio uzgodnionym (w tym przypadku w tym samym czasie odbywa się osobista identyfikacja),
b) w formie papierowej, podpisany odręcznie i przesłany do punktu obsługi klienta QTSP (w tym przypadku identyfikacja osobista odbędzie się w późniejszym czasie),
c) w formie elektronicznej podpisany podpisem lub pieczęcią elektroniczną w oparciu o kwalifikowany certyfikat nieanonimowy, wysłany poprzez portal klienta lub pod adres e-mail QTSP podany we wniosku.

Subskrybent i podmiot – w przypadku organizacji, przedstawiciel organizacji – powinni dostarczyć informacje kontaktowe we wniosku o rejestrację.

4.1.2. Nabór i odpowiedzialność

QTSP potwierdza tożsamość osoby składającej wniosek o wystawienie certyfikatu (zob. sekcja 3.2.3).

QTSP sprawdza, czy wniosek o wystawienie certyfikatu rzeczywiście został wysłany przez osobę, której dane widnieją na wniosku, za pomocą innych, sprawdzonych kanałów komunikacji.

W przypadku certyfikatu organizacyjnego, QTSP identyfikuje tę organizację (zob. sekcja 3.2.2) i upewnia się, że wnioskodawca jest upoważniony do reprezentowania tej organizacji (zob. sekcja 3.2.5) i do występowania o certyfikat dla tej organizacji (zob. sekcja 3.2.2).

Subskrybent upoważnia Aplikantów do występowania z wnioskiem o certyfikat i określa rodzaj tego certyfikatu (Politykę Certyfikacji zgodnie z którą ma być wydany ten certyfikat).

Aplikant powinien dostarczyć wszelkie niezbędne informacje w celu przeprowadzenia procesu identyfikacji.

Jeżeli zajdzie taka potrzeba, QTSP porównuje dane z oficjalnymi i autentycznymi rejestrami publicznymi (QGIS) takimi jak rejestry danych osobowych i adresowych lub rejestry organizacji. Jeśli to możliwe, QTSP porównuje dane elektronicznie.

QTSP nadaje unikalną nazwę podmiotu i przypisuje mu unikalny numer ID (OID). Proces ten opisano w sekcji 3.1.

QTSP rejestruje wszelkie wymagane informacje dotyczące tożsamości wnioskodawcy i organizacji w celu świadczenia usług i w celu późniejszego kontaktowania się.

QTSP rejestruje umowę na świadczenie usług podpisaną uprzednio przez subskrybenta, która zawiera oświadczenie subskrybenta, że jest on świadomy swoich obowiązków i zobowiązuje się do ich przestrzegania.

QTSP rejestruje wniosek o wystawienie certyfikatu podpisany przez Aplikanta - w przypadku organizacji, osoby upoważnionej do reprezentowania Podmiotu - który powinien zawierać:

- Potwierdzenie, że dane podane we wniosku o wystawienie certyfikatu są prawidłowe.
- Wyrażenie zgody na utrwalenie i przetwarzanie przez QTSP danych podanych we wniosku.
- Wyrażenie zgody (lub nie) na ujawnienie certyfikatu.

QTSP przechowuje wymienione wyżej dokumenty i zgody przez okres wymagany prawem.

QTSP archiwizuje umowy, wnioski o wystawienie certyfikatu i wszelkie dokumenty, zaświadczenia przekazane przez organizację, wnioskodawcę lub subskrybenta.

Jeżeli tożsamość wnioskodawcy lub powiązanie podmiotu z reprezentowaną organizacją nie może być bezspornie zweryfikowana lub jeśli dane podane we wniosku są nieprawidłowe, procedura zostaje przerwana. Klient może poprawić i uzupełnić dane oraz brakujące dokumenty.

Jeżeli tożsamość podmiotu - w przypadku organizacji, jej przedstawiciela - lub - w przypadku certyfikatu organizacyjnego - tożsamość organizacji - lub - w przypadku certyfikatu organizacyjnego wystawionego na osobę fizyczną - powiązanie tej osoby z reprezentowaną organizacją nie mogą być bezspornie zweryfikowane lub dane wskazane we wniosku są niepoprawne, QTSP umożliwia Klientowi poprawę i uzupełnienie danych lub dostarczenie brakujących dokumentów w ciągu trzech miesięcy od daty złożenia wniosku.

4.2. Przetwarzanie wniosku o wystawienie certyfikatu

4.2.1. Funkcje identyfikacji i uwierzytelnienia

QTSP identyfikuje wnioskodawcę zgodnie z sekcją 3.2 oraz weryfikuje autentyczność wniosku. W przypadku wniosku o wystawienie certyfikatu organizacyjnego, również sama organizacja musi być zidentyfikowana i weryfikacja uprawnień do reprezentacji odbywa się zgodnie z sekcją 3.2. QTSP rejestruje wszelkie informacje użyte przez podmiot lub – w przypadku certyfikatu organizacyjnego – organizację, do poświadczenia swojej tożsamości, łącznie z numerami rejestracyjnymi dokumentów tożsamości i ich datą ważności.

QTSP może użyć oryginalnych autentycznych dokumentów będących w jego posiadaniu lub autentycznych elektronicznych kopii tych dokumentów wykonanych podczas walidacji, do wskazanego czasu ich ważności lub do czasu unieważnienie dokumentów z jakichkolwiek powodów.

QTSP może użyć dokumentów i danych wskazanych w sekcji 3.2 do zweryfikowania danych do certyfikatu lub może ponownie użyć wyników swoich poprzednio zrealizowanych walidacji nie starszych niż 3 miesiące.

Inna zasada obowiązuje dla okresu ważności wyników walidacji adresu email zawartego w certyfikacie Email (S/MIME):

a) 30 dni w przypadku walidacji za pomocą wiadomości email;
b) 398 dni w przypadku walidacji za pomocą domeny.

W przypadku certyfikatów uwierzytelniania witryn internetowych QTSP może użyć dokumentów i danych wskazanych w sekcji 3.2 w celu weryfikacji informacji w certyfikacie lub może użyć wyników swoich poprzednich walidacji nie starszych niż 398 dni.

QTSP weryfikuje czy:

a) Subskrybent lub Wnioskodawca jest na „czarnej” liście organów publicznych,
b) zarejestrowany adres organizacji lub miejsce prowadzenia działalność jest w jakimkolwiek kraju, z którym nawiązywanie współpracy biznesowej jest zakazane.

QTSP nie wydaje Certyfikatu w takim wypadku.

4.2.2. Zatwierdzenie lub odrzucenie wniosku o wystawienie certyfikatu

W celu uniknięcia konfliktu interesów, QTSP gwarantuje osobową i organizacyjną niezależność od subskrybentów. Nie stanowi naruszenia zasady braku konfliktu interesów sytuacja, kiedy QTSP wystawia certyfikaty swoim pracownikom i współpracownikom.

Przed wystawieniem certyfikatu, QTSP weryfikuje autentyczność informacji podanych we wniosku o wystawienie certyfikatu, które mają pojawić się w certyfikacie.

Jeżeli podmiot wnioskuje o certyfikat, który ma zawierać adres e-mail, QTSP weryfikuje dany adres e-mail. QTSP sprawdza czy ten adres jest prawdziwy i rzeczywiście należy do podmiotu.

QTSP sprawdza rekordy CAA dla każdej nazwy dNSName w rozszerzeniu certyfikatu subjectAltName zgodnie z procedurą opisaną w IETF RFC 8659 (28), postępując zgodnie z instrukcjami IETF RFC 8659 (28) dla każdego znalezionego rekordu.

QTSP wystawia certyfikat jedynie wtedy, gdy poniższe warunki są osobno spełnione dla każdego dNSNames w rozszerzeniu „SubjectAltName”:

a) w przypadku każdej dNSName, rekord CAA:
   - nie zawiera wpisu "issue", lub
   - zawiera wartość „issue”: eurocert.pl

Na krótko przed wydaniem certyfikatu QTSP ponownie sprawdza automatycznie rekordy CAA.

QTSP akceptuje lub odrzuca wniosek o wystawienie certyfikatu po jego przetworzeniu.

Jeżeli tożsamość osoby fizycznej lub organizacji lub - w przypadku certyfikatu organizacyjnego dla osoby fizycznej – powiązanie podmiotu z reprezentowaną organizacją nie mogą być bezspornie zweryfikowane lub dane wskazane we wniosku są niepoprawne, a Klient ich nie poprawił na wezwanie QTSP, QTSP odrzuca wniosek.

W przypadku odrzucenia wniosku, QTSP informuje o tym fakcie wnioskodawcę i subskrybenta, jednakże nie ma obowiązku uzasadniania swojej decyzji.

4.2.3. Czas przetwarzania wniosków o wystawienie certyfikatu

QTSP przetwarza wniosek o wystawienie certyfikatu w ciągu pięciu dni roboczych, jeżeli dostępne są wszystkie potrzebne dane i dokumenty.

4.3. Wystawianie certyfikatu

QTSP wystawia certyfikat podmiotowi jedynie po zatwierdzeniu wniosku o wystawienie certyfikatu.

Wystawiony certyfikat zawiera jedynie dane podmiotu, które zostały podane we wniosku o wystawienie certyfikatu i które zostały zweryfikowane przez QTSP.

Jeśli QTSP dostarcza Podmiotowi osobiste kwalifikowane urządzenie do składania podpisu (pieczęci) elektronicznego – QTSP w procesie personalizacji generuje dla wnioskodawcy parę kluczy, ale certyfikat nie jest jeszcze wystawiany. Przekazanie kwalifikowanego urządzenia zawierającego klucz

prywatny odbywa się w kontrolowanym środowisku zgodnie z przepisami bezpieczeństwa opisanymi w sekcji 6.1.2.

Jeśli weryfikacja tożsamości odbywa się podczas fizycznego spotkania, pracownik QTSP wręcza Podmiotowi QSCD zawierające klucz prywatny. Podmiot potwierdza odebranie QSCD podpisując oświadczenie.

W pozostałych przypadkach, po zakończeniu weryfikacji tożsamości, QTSP dostarcza Podmiotowi QSCD wraz z kluczem prywatnym za pośrednictwem Urzędu Rejestracji.

Podmiot może otrzymać swoje urządzenie po weryfikacji tożsamości na podstawie dokumentu tożsamości. Strona przekazująca sprawdza, czy wygląd wnioskodawcy zgadza się ze zdjęciem w dowodzie tożsamości i (opcjonalnie) czy podpis pasuje do tego na dowodzie. Podmiot potwierdza odebranie QSCD podpisując oświadczenie.

QTSP Usług wystawia certyfikaty wyłącznie po weryfikacji, że kwalifikowane urządzenie znajduje się już w posiadaniu wnioskodawcy.

Po wydaniu certyfikatu QTSP przekazuje kod do aktywacji QSCD, generowany zgodnie z sekcją 6.4, w zaszyfrowanej formie na koncie portalu Klienta. Podmiot może odszyfrować kod poprzez ponowne wprowadzenie hasła dostępu do Portalu Klienta.

Jeśli klucz prywatny Podmiotu jest zarządzany przez Dostawcę w Usłudze Zdalnego Podpisu, QTSP wysyła także wystawiony certyfikat bezpośrednio do dostawcy usług zaufania zarządzającego kluczem.

4.3.1. Czynności Urzędu Certyfikacji podczas wystawiania certyfikatu

Wystawienie certyfikatu przebiega według ściśle określonego i kontrolowanego procesu, szczegółowo opisanego w wewnętrznych regulacjach QTSP.

QTSP opracował swoje wewnętrzne procesy administracyjne na podstawie analizy ryzyka i stosuje zasadę „Dual Control" podczas zapisywania danych umieszczanych w certyfikacie i weryfikowania autentyczności danych. QTSP zapewnia, że zapisywanie danych umieszczanych w certyfikacie i weryfikacja autentyczności danych nie może być przeprowadzone przez tą samą osobę.

Wystawiony certyfikat jest natychmiast dodawany do wewnętrznego repozytorium certyfikatów. Od tego czasu może być on zawieszony lub unieważniony, status unieważnienia jest dostępny za pośrednictwem usług OCSP lub CRL.

Początek ważności certyfikatu nie może być wcześniejszy niż rzeczywista data wydania certyfikatu. QTSP nigdy nie antydatuje certyfikatów.

4.3.2. Powiadamianie subskrybenta o wystawieniu certyfikatu

QTSP informuje wnioskodawcę i subskrybenta o wystawieniu certyfikatu i umożliwia wnioskodawcy odebranie certyfikatu.

4.4. Akceptacja certyfikatu

4.4.1. Proces akceptacji certyfikatu

Podmiot lub - jeśli certyfikat ma być wystawiony dla organizacji - przedstawiciel Podmiotu, powinien zweryfikować poprawność danych zawartych w certyfikacie podczas odbierania certyfikatu.

Wnioskodawca akceptuje certyfikat poprzez jego użycie, nie jest zatem wymagane specjalne oświadczenie.

4.4.2. Publikacja certyfikatu przez Urząd Certyfikacji

QTSP ujawnia wystawiony certyfikat w swoim publicznym repozytorium certyfikatów po przekazaniu certyfikatu. Warunkiem ujawnienia jest zgoda danego podmiotu.

Po wydaniu certyfikatu – tylko za zgodą Podmiotu – QTSP ujawnia certyfikat we własnym publicznym repozytorium.

4.4.3. Powiadomienie o wystawieniu certyfikatu przez Urząd Certyfikacji innych osób

W przypadku certyfikatu Organizacyjnego, wystawionego dla osoby fizycznej (Podmiotu) do składania podpisu elektronicznego w imieniu Organizacji, QTSP niezwłocznie powiadamia osobę kontaktową reprezentowanej organizacji o wystawieniu certyfikatu.

QTSP niezwłocznie powiadamia osobę upoważnioną do reprezentowania podmiotu o wystawieniu certyfikatu.

4.5. Para kluczy i użycie certyfikatu

4.5.1. Prywatny klucz subskrybenta i użycie certyfikatu

Klucz prywatny odpowiadający certyfikatowi podmiotu może być użyty jedynie w zgodzie z użyciem zapisanym w certyfikacie „keyUsage" (sekcja 6.1.7), a każde inne użycie jest zabronione.

Podmiot może używać swój klucz prywatny odpowiadający certyfikatowi podpisu elektronicznego jedynie do składania podpisu elektronicznego, a każde inne użycie (na przykład: autoryzacja lub szyfrowanie) jest zabronione.

Podmiot może używać swój klucz prywatny odpowiadający certyfikatowi pieczęci jedynie do składania pieczęci elektronicznej, a każde inne użycie jest zabronione.

Klucz prywatny należący do certyfikatu do uwierzytelniania witryn internetowych może być użyty wyłącznie do uwierzytelnienia witryny internetowej lub uwierzytelnienia klienta, a każde inne użycie jest zabronione.

Zabronione jest użycie klucza prywatnego odpowiadającego wygasłemu, unieważnionemu lub zawieszonemu certyfikatowi.

Podmiot jest zobligowany do właściwej ochrony klucza prywatnego i danych aktywacyjnych.

Podczas użytkowania należy przestrzegać ograniczeń wyszczególnionych w sekcji 1.4.

QTSP zawsze sprawdza ważność certyfikatu przed użyciem zdalnego klucza prywatnego do złożenia podpisu zdalnego i odmawia użycia klucza dla certyfikatu wygasającego później niż długość życia zastosowanych dla niego algorytmów kryptograficznych. Użycie klucza prywatnego zawsze wymaga identyfikacji i zgody Podmiotu.

4.5.2. Klucz publiczny strony ufającej i użycie certyfikatu

W celu zachowania należytego poziomu bezpieczeństwa gwarantowanego przez QTSP, w trakcie wykonywania czynności (na przykład, identyfikacji zdalnej, szyfrowania dokumentu), uwierzytelniania witryny internetowej, weryfikacji pieczęci lub podpisu elektronicznego, strona ufająca musi zachować szczególną ostrożność:

a) strona ufająca musi zweryfikować status certyfikatu: ważny czy unieważniony;
b) certyfikaty do podpisów elektronicznych i odpowiadające im klucze publiczne powinny być użyte jedynie w celu walidacji podpisu elektronicznego;

c) certyfikaty do pieczęci elektronicznej i odpowiadające im klucze publiczne powinny być użyte jedynie w celu walidacji pieczęci elektronicznej;
d) klucze publiczne należące do certyfikatów uwierzytelnienia witryn internetowych mogą być użyte jedynie w celu uwierzytelnienia witryny internetowej lub klienta;
e) klucze publiczne mogą być zaakceptowane wyłącznie w zakresie zastosowania, który jest zgodny z zawartością pól „Użycie klucza" (Key Usage) i „Rozszerzone użycie klucza" (Extended Key Usage) w certyfikacie;
f) weryfikacja certyfikatu powinna zostać przeprowadzona dla całej ścieżki certyfikacyjnej aż do zaufanego root lub certyfikatu dostawcy pośredniego;
g) podczas budowania ścieżki certyfikacji, strona ufająca akceptuje certyfikat dostawcy usług zaufania jako zaufany, jeśli:
   - widnieje na krajowej zaufanej liście (która może być zwalidowana poprzez listę zaufanych list EU, jak np. polskiej Liście Zaufania (3)) jako dostawca usług zaufania uprawniony do wystawiania kwalifikowanych certyfikatów i
   - certyfikat dostawcy usług zaufania był ważny w czasie składania podpisu, pieczęci i w czasie wydawania certyfikatu końcowego podpisu elektronicznego (pieczęci);
h) weryfikacja podpisu elektronicznego lub pieczęci elektronicznej powinna zostać przeprowadzona w sprawdzonej aplikacji, która spełnia określone wymagania techniczne, może być trwale skonfigurowana, została prawidłowo przygotowana i jest wolna od wirusów;
i) w przypadku certyfikatów osobistych powiązanych z organizacją rekomenduje się sprawdzenie, czy tytuł osoby podpisującej (upoważniający do podpisania dokumentu w imieniu organizacji) można ustalić na podstawie certyfikatu (na przykład, w polu „Tytuł");
j) zaleca się sprawdzenie, czy certyfikat został wystawiony zgodnie z właściwą polityką certyfikacji;
k) przy akceptacji kwalifikowanego podpisu elektronicznego lub pieczęci zaleca się zweryfikować czy certyfikat był wydany na podstawie Polityki certyfikacji wymagającej Kwalifikowanego urządzenia do składania podpisu elektronicznego (QSCD);
l) rekomenduje się sprawdzenie, czy występuje w certyfikacie limit wartości zobowiązań jakie można zaciągnąć jednorazowo (limit ten oznacza, że QTSP nie ponosi odpowiedzialności za użycie podpisu lub pieczęci elektronicznej dla transakcji powyżej tej kwoty i szkody z tego wynikłe);
m) Strony Ufające powinny zwrócić uwagę na wszelkie ograniczenia zawarte w certyfikacie lub w regulacjach przywołanych w Certyfikacie.

QTSP świadczy usługi swoim klientom i stronom ufającym, które służą do weryfikacji wystawionych certyfikatów.

4.6. Odnowienie certyfikatu

Usługa wystawienia nowego certyfikatu przez QTSP na nowy okres ważności dla tego samego klucza publicznego i tego samego podmiotu (i na te same dane) nazywa się odnowieniem certyfikatu.

Jeżeli podmiot chciałby kontynuować używanie certyfikatu po dacie jego wygaśnięcia, powinien zainicjować procedurę jego odnowienia. Odnowienie certyfikatu oznacza wystawienie nowego certyfikatu z tymi samymi danymi identyfikacyjnymi danego podmiotu, ale na nowy okres. Inne dane mogą ulec zmianie w certyfikacie np. CRL, OCSP czy klucz dostawcy użyty do podpisania certyfikatu.

4.6.1. Uwarunkowania dla odnowienia certyfikatu

Odnowienie certyfikatu jest dopuszczalne jedynie wtedy, kiedy spełnione są następujące warunki:

a) wniosek o odnowienie certyfikatu został złożony w okresie ważności certyfikatu lub po jego upływie;
b) certyfikat, który ma być odnowiony nie jest zawieszony ani unieważniony;
c) nie zachodzą okoliczności wskazujące na możliwość ujawnienia klucza prywatnego odpowiadającego certyfikatowi;
d) informacje dotyczące tożsamości podmiotu wpisane w certyfikacie są nadal aktualne.

QTSP może zaakceptować wnioski o odnowienie certyfikatu jedynie w ramach obowiązującej umowy o świadczeniu usług.

Jeżeli poprzedni certyfikat podmiotu jest unieważniony, to o nowy certyfikat można wnioskować tylko w ramach usługi recertyfikacji (zob. Sekcja 4.7) lub poprzez złożenie wniosku o nowy certyfikat (zob. sekcja 4.1).

Jeżeli jakiekolwiek dane podmiotu wskazane w certyfikacie uległy zmianie, należy wnioskować o nowy certyfikat w ramach usługi modyfikacji certyfikatu (zob. sekcja 4.8).

W trakcie odnawiania certyfikatu wnioskodawca jest informowany o ewentualnej zmianie warunków usługi od czasu wystawienia poprzedniego certyfikatu.

Jeżeli wnioskodawca i subskrybent to dwie różne osoby, wspomniane wcześniej informacje są również przekazywane subskrybentowi.

Jeżeli odnowienie certyfikatu odbywa się w ramach wiążącej umowy na świadczenie usług, nie jest wymagana jej zmiana.

4.6.2. Kto może wnioskować o odnowienie certyfikatu

Odnowienie certyfikatu musi być zainicjowane w imieniu Subskrybenta przez osobę uprawnioną do złożenia wniosku o wydanie nowego certyfikatu tego samego typu.

Wnioskodawca oświadcza we wniosku, że dane identyfikacyjne podmiotu podane w certyfikacie są nadal ważne.

QTSP jest uprawniony do zainicjowania odnowienia certyfikatu, jeśli wymagane jest to ze względu na zmiany w wewnętrznych lub zewnętrznych warunkach świadczenia usługi odnowienia, na przykład w poniższych sytuacjach:

a) z powodu zmian wymagań zewnętrznych, certyfikat nie może być już dalej używany w swojej obecnej formie;
b) QTSP pozyskał wiedzę, że dany certyfikat nie jest zgodny z PCKPC;
c) klucz podpisujący (klucz prywatny) dostawcy usług użyty do wystawienia certyfikatu musi być wymieniony.

Wniosek o odnowienie można złożyć w następujący sposób:

a) pisemnie, w formie papierowej, podpisany odręcznie w biurze obsługi klienta QTSP lub u mobilnego partnera ds. rejestracji QTSP w ustalonym wcześniej terminie (w takiej sytuacji następuje równocześnie osobista weryfikacja tożsamości);
b) w formie elektronicznej za pomocą podpisu elektronicznego lub pieczęci elektronicznej opartych o kwalifikowany certyfikat nieanonimowy - na adres email QTSP wskazany we wniosku lub przy użyciu aplikacji desktop do składania podpisu (pieczęci);

c) używając osobistego konta klienta na portalu internetowym, używając unikalnych danych uwierzytelniających do konta;
d) pisemnie, podpisany odręcznie i przesłany do biura obsługi klienta QTSP (w tym przypadku osobista identyfikacja tożsamości następuje w innym terminie).

4.6.3. Przetwarzanie wniosków o odnowienie certyfikatu

W trakcie weryfikacji wniosku o odnowienie certyfikatu QTSP sprawdza, czy:

a) złożony wniosek jest autentyczny;
b) wnioskodawca posiada stosowne uprawnienia i upoważnienie;
c) wnioskodawca oświadczył, że dane podmiotu, które mają zostać umieszczone w certyfikacie się nie zmieniły i są poprawne;
d) certyfikat podlegający odnowieniu nie jest zawieszony ani unieważniony;
e) na podstawie aktualnej wiedzy, algorytmy kryptograficzne będą wystarczająco odporne przez cały nowy okres ważności nowego certyfikatu.

Metoda użyta do identyfikacji i uwierzytelnienia w trakcie odnawiania certyfikatu została omówiona w sekcji 3.4.

4.6.4. Powiadomienie klienta o wystawieniu nowego certyfikatu

QTSP informuje wnioskodawcę i subskrybenta o wystawieniu certyfikatu.

4.6.5. Akceptacja odnowionego certyfikatu

Odnowiony certyfikat może być odebrany (pobrany elektronicznie) bez konieczności osobistej wizyty.

W trakcie odnawiania certyfikatu nie generuje się klucza i dlatego nie ma potrzeby przekazania go podmiotowi.

Jeśli klucz prywatny Podmiotu znajduje się na kwalifikowanym urządzeniu do składania podpisu elektronicznego, który jest w posiadaniu podmiotu, podmiot instaluje certyfikat na urządzeniu. Najprostszym sposobem jest instalacja przy użyciu aplikacji do zarządzania kartą dostarczonej przez QTSP wraz z instrukcją obsługi, a jeśli jest to konieczne – z asystą telefoniczną.

Jeśli klucz prywatny Podmiotu jest zarządzany zdalnie przez QTSP, QTSP wysyła także wystawiony certyfikat bezpośrednio do dostawcy usług zaufania zarządzającego kluczem w imieniu Podmiotu.

Wnioskodawca akceptuje certyfikat poprzez jego użycie, nie jest wymagane osobne oświadczenie.

4.6.6. Publikacja odnowionego certyfikatu przez Urząd Certyfikacji

QTSP ujawnia odnowiony certyfikat w taki sam sposób jak pierwotny certyfikat.

4.6.7. Powiadomienie innych podmiotów o wystawieniu certyfikatu

W przypadku certyfikatu Organizacyjnego, QTSP niezwłocznie powiadamia osobę kontaktową reprezentowanej organizacji o wystawieniu certyfikatu.

4.7. Certyfikat Re-Key

Re-key oznacza proces, w którym QTSP wystawia nowy certyfikat dla podmiotu dla nowego klucza publicznego.

Pozostałe dane mogą opcjonalnie być zmienione w nowym certyfikacie, na przykład okres ważności, CRL i OCSP lub klucz dostawcy użyty do podpisania certyfikatu.

4.7.1. Okoliczności dla Re-Key

Ważność poprzedniego certyfikatu nie jest warunkiem koniecznym dla Re-key, jednak QTSP powinien zatwierdzać wnioski o Re-key jedynie w ramach dotychczasowej umowy na świadczenie usług.

Podczas wymiany klucza wnioskodawca zostaje poinformowany przez QTSP, jeśli warunki świadczenia usług uległy zmianie od czasu wystawienia poprzedniego certyfikatu. Jeżeli wnioskodawca i subskrybent to dwie różne osoby, ta informacja jest przekazywana również subskrybentowi.

Proces Re-key odbywa się w ramach bieżącej umowy na świadczenie usług, nie ma potrzeby jej zmiany.

4.7.2. Kto może wnioskować o certyfikację nowego klucza publicznego

Wymiana klucza musi być zainicjowana przez osobę, która jest do tego uprawniona.

Wnioskodawca musi potwierdzić we wniosku, że dane identyfikacyjne podmiotu wpisane do certyfikatu są nadal ważne lub podaje nowe aktualne dane.

Wniosek o wymianę klucza można złożyć w następujący sposób:

a) na piśmie, podpisany odręcznie w biurze obsługi klienta QTSP lub u mobilnego partnera ds. rejestracji QTSP w ustalonym wcześniej terminie (w takiej sytuacji następuje równocześnie osobista weryfikacja tożsamości);
b) w formie elektronicznej za pomocą podpisu elektronicznego lub pieczęci elektronicznej w oparciu o kwalifikowany certyfikat nieanonimowy - na adres email QTSP wskazany we wniosku;
c) pisemnie, podpisany odręcznie i przesłany do biura obsługi klienta QTSP (w tym przypadku osobista identyfikacja tożsamości następuje w innym terminie).

4.7.3. Przetwarzanie wniosków o Re-key

W trakcie weryfikacji wniosku QTSP sprawdza, czy:

a) złożony wniosek jest autentyczny;
b) osoba składająca wniosek posiada stosowne uprawnienia i upoważnienie;
c) dane wpisane we wniosku są poprawne;
d) na podstawie aktualnej wiedzy, algorytmy kryptograficzne będą wystarczająco odporne przez cały nowy okres ważności nowego certyfikatu.

Przed rozpatrzeniem wniosku, tożsamość osoby składającej wniosek musi być sprawdzona zgodnie z sekcją 3.3.

4.7.4. Powiadamianie klienta o wystawieniu nowego certyfikatu

QTSP informuje wnioskodawcę i subskrybenta o wystawieniu certyfikatu.

4.7.5. Akceptacja recertyfikowanego certyfikatu

QTSP przekazuje certyfikat wystawiony dla nowego klucza publicznego po zidentyfikowaniu wnioskodawcy.

Jeżeli kwalifikowane urządzenie do składania podpisu elektronicznego będące w posiadaniu wnioskodawcy wciąż posiada przydatny klucz prywatny, nie jest konieczne wystawienie nowego klucza lub kwalifikowanego urządzenia do składania podpisu elektronicznego. QTSP wystawia tylko certyfikat dla nowego klucza publicznego.

Jeżeli konieczne jest wydanie nowego kwalifikowanego urządzenia do składania podpisu elektronicznego, QTSP personalizuje nowe urządzenie i dostarcza je wnioskodawcy, tak jak opisano w

rozdziale 4.3. QTSP wystawia certyfikat wyłącznie po sprawdzeniu w sposób wiarygodny, że kwalifikowane urządzenie do składania podpisu elektronicznego znajduje się już w posiadaniu wnioskodawcy.

Jeśli klucz prywatny Podmiotu jest zarządzany zdalnie przez innego dostawcę, QTSP wysyła także wystawiony certyfikat bezpośrednio do dostawcy usług zaufania zarządzającego kluczem w imieniu Podmiotu.

Jeżeli nowy klucz publiczny został dostarczony przez Podmiot, nie jest konieczne przekazanie klucza i kwalifikowanego urządzenia do składania podpisu elektronicznego.

Nowy certyfikat może zostać pobrany online bez konieczności osobistej wizyty.

Wnioskodawca akceptuje certyfikat poprzez użycie go, nie jest wymagane osobne oświadczenie.

4.7.6. Publikacja certyfikatu re-key

QTSP ujawnia nowy certyfikat w ten sam sposób jak pierwotny certyfikat.

4.7.7. Powiadomienie innych podmiotów o wystawieniu certyfikatu

W przypadku certyfikatu Organizacyjnego, QTSP niezwłocznie powiadamia osobę kontaktową reprezentowanej organizacji o wystawieniu certyfikatu.

4.8. Modyfikacja certyfikatu

Modyfikacja certyfikatu oznacza proces, w którym QTSP wystawia nowy certyfikat dla podmiotu ze zmienionymi danymi identyfikacyjnymi dla tego podmiotu lecz z niezmienionym kluczem publicznym.

Pod względem technicznym, zmiana certyfikatu oznacza wystawienie nowego certyfikatu. QTSP jest zobowiązany unieważnić poprzedni certyfikat, który zawiera nieaktualne dane (zob. sekcja 4.9).

W nowym certyfikacie zmianie mogą także ulec m.in.: okres ważności, CRL i OCSP lub klucz QTSP użyty do podpisania certyfikatu.

4.8.1. Okoliczności zmiany certyfikatu

Modyfikacja certyfikatu jest konieczna w następujących przypadkach:

a) zmiana danych w Certyfikacie;
b) zmiana danych certyfikatu wystawiającego Urzędu Certyfikacji, wpisanych w polu „Podmiot DN”, lub wymiana klucza publicznego;
c) zmienił się profil certyfikatu określony przez QTSP.

Warunki modyfikacji certyfikatu:

a) wniosek o zmianę certyfikatu został złożony podczas okresu ważności danego certyfikatu;
b) certyfikat nie jest zawieszony ani unieważniony;
c) nie zachodzą okoliczności wskazujące na możliwość ujawnienia klucza prywatnego odpowiadającego certyfikatowi.

QTSP przyjmuje wnioski o modyfikację certyfikatu jedynie w ramach aktualnej umowy na świadczenie usług.

Jeżeli poprzedni certyfikat został unieważniony lub wygasł, można wnioskować tylko o nowy certyfikat w ramach procesu wymiany klucza (zob. sekcja 4.7) lub w ramach procedury o wydanie nowego certyfikatu (zob. sekcja 4.1).

W trakcie zmiany certyfikatu wnioskodawca zostaje poinformowany o ewentualnych zmianach w warunkach świadczenia usługi od czasu wydania poprzedniego certyfikatu.

Jeżeli wnioskodawca i subskrybent to dwie różne osoby, ta informacja jest przekazywana również subskrybentowi. Zmiana certyfikatu odbywa się w ramach aktualnej umowy na świadczenie usług, nie jest wymagana jej zmiana.

4.8.2. Kto może wnioskować o zmianę certyfikatu

Zmiana certyfikatu może zostać zainicjowana tylko przez osobę uprawnioną na dzień składania wniosku o zmianę certyfikatu.

We wniosku wnioskodawca podaje nowe dane i składa oświadczenie, że są poprawne i prawdziwe.

QTSP sam rozpoczyna proces zmiany certyfikatu jeśli posiada wiedzę, że dane podmiotu wpisane do certyfikatu się zmieniły.

Wniosek można złożyć w następujący sposób:

a) na piśmie, podpisany odręcznie w biurze obsługi klienta QTSP lub u mobilnego partnera ds. rejestracji QTSP w ustalonym wcześniej terminie (w tym samym czasie następuje osobista weryfikacja tożsamości);
b) w formie elektronicznej za pomocą podpisu elektronicznego lub pieczęci elektronicznej złożonych przy użyciu kwalifikowanego certyfikatu nieanonimowego. Taki wniosek wysyłany jest na adres email QTSP wskazany we wniosku lub złożony na Portalu Klienta;
c) Pisemnie, podpisany odręcznie i przesłany do biura obsługi klienta QTSP (w tym przypadku osobista identyfikacja tożsamości następuje w innym terminie).

4.8.3. Przetwarzanie wniosku o zmianę certyfikatu

W trakcie weryfikacji wniosku o zmianę certyfikatu QTSP sprawdza, czy:

a) złożony wniosek jest autentyczny;
b) osoba składająca wniosek posiada stosowne uprawnienia i upoważnienie;
c) dane podane we wniosku są poprawne;
d) wniosek został złożony w trakcie okresu ważności certyfikatu;
e) na podstawie aktualnej wiedzy, algorytmy kryptograficzne będą wystarczająco odporne przez cały nowy okres ważności wydanego certyfikatu.

Sprawdzając autentyczność danych podmiotu, QTSP postępuje w taki sam sposób jak przy pierwotnej weryfikacji przeprowadzonej przed wydaniem certyfikatu po raz pierwszy.

Przed realizacją wniosku o zmianę certyfikatu, tożsamość osoby składającej wniosek musi być sprawdzona zgodnie z sekcją 3.5.

4.8.4. Powiadomienie klienta o wystawieniu nowego certyfikatu

QTSP informuje wnioskodawcę i subskrybenta o wystawieniu certyfikatu.

4.8.5. Akceptacja zmienionego certyfikatu

W trakcie procesu zmiany certyfikatu nie generuje się klucza i dlatego nie ma potrzeby przekazania go podmiotowi. Zmieniony certyfikat może być pobrany online bez konieczności osobistej wizyty.

Jeśli klucz prywatny podmiotu znajduje się na QSCD, który jest w posiadaniu podmiotu, podmiot instaluje certyfikat na urządzeniu. W tym celu QTSP zapewnia aplikację do zarządzania kartą wraz z instrukcją obsługi, i jeśli jest to konieczne – asystę telefoniczną.

Jeśli klucz prywatny Podmiotu jest zarządzany zdalnie przez Dostawcę, QTSP wysyła także wystawiony certyfikat bezpośrednio do dostawcy usług zaufania zarządzającego kluczem.

Podmiot akceptuje certyfikat poprzez jego użycie, nie jest wymagane osobne oświadczenie.

4.8.6. Publikacja zmienionego certyfikatu przez Urząd Certyfikacji

QTSP ujawnia zmieniony certyfikat w taki sam sposób jak pierwotny certyfikat.

4.8.7. Powiadomienie innych podmiotów o wystawieniu certyfikatu przez Urząd

W przypadku certyfikatu Organizacyjnego, QTSP niezwłocznie powiadamia Administratora Organizacyjnego reprezentowanej organizacji o wystawieniu certyfikatu.

Osoba upoważniona do reprezentowania Podmiotu jest informowana przez QTSP niezwłocznie o wydaniu certyfikatu.

4.9. Unieważnienie i zawieszenie certyfikatu

Unieważnienie certyfikatu następuje wtedy, gdy QTSP unieważnia certyfikat przed jego wygaśnięciem. Unieważnienie certyfikatu skutkuje trwałą i nieodwracalną zmianą statusu certyfikatu, innymi słowy, unieważniony certyfikat już nigdy nie będzie ponownie ważny.

Zawieszenie certyfikatu następuje wtedy, gdy QTSP czasowo wstrzymuje ważność certyfikatu przed jego wygaśnięciem. Zawieszenie certyfikatu jest tymczasowe, zawieszony certyfikat może być unieważniony lub – jeśli nie upłynął okres ważności – przywrócony do stanu ważności. W przypadku wycofania zawieszenia certyfikat staje się wstecznie obowiązujący, tak jakby w ogóle nie był zawieszony. Innymi słowy, ważność jest przywracana z dniem zawieszenia Certyfikatu.

Powód unieważnienia

QTSP może przetrzymywać informacje o przyczynach unieważnienia w wewnętrznym rejestrze statusów unieważnienia certyfikatów, który jest ujawniany w publicznej usłudze informowania o statusie unieważnienia. Jeśli Klient inicjuje unieważnienie, powody unieważnienia mogą być następujące.

a) ujawnienie klucza (keyCompromise (1)),
b) zaprzestanie używania certyfikatu (cessationOfOperation (5)),
c) wygaśnięcie uprawnień (privilegeWithdrawn (9)).

Możliwości dostępne dla każdej usługi unieważnienia są opisane w opisie każdej usługi.

Jeśli QTSP inicjuje unieważnienie, przyczyny unieważnienia mogą być następujące:

a) nieokreślona (unspecified (0), w którym to przypadku rozszerzenie reasonCode nie jest zawarte w statusie unieważnienia),
b) ujawnienie klucza (keyCompromise (1)),
c) zmiana danych (affiliationChanged (3)),
d) wymiana klucza (superseded (4)),
e) wygaśnięcie uprawnień (privilegeWithdrawn (9)).

W przypadku wniosku o zawieszenie powody mogą być te same, lecz status wyświetlany w usłudze statusu unieważnienia jest następujący:

a) zawieszony (certificateHold (6)).

Jeśli klient zażąda unieważnienia w trakcie zawieszenia, może podać te same przyczyny unieważnienia co powyżej.

Jeśli QTSP inicjuje unieważnienie zawieszonego certyfikatu wpisuje przyczynę unieważnienia określoną we wniosku o zawieszenie.

Używanie klucza prywatnego unieważnionego certyfikatu

Użycie prywatnego klucza należącego do unieważnionego lub zawieszonego certyfikatu jest zabronione. Jeśli to możliwe, prywatny klucz należący do unieważnionego certyfikatu powinien być zniszczony natychmiast po unieważnieniu.

Certyfikat do uwierzytelniania witryn internetowych nie może być zawieszony.

Zasady odpowiedzialności dotyczące unieważnienia lub zawieszenia:

- Jeżeli QTSP opublikował już status unieważnienia certyfikatu, QTSP nie ponosi żadnej odpowiedzialności, jeśli Strony Ufające uznają certyfikat za ważny.

4.9.1. Okoliczności unieważnienia certyfikatu

Unieważnienie Certyfikatu Subskrybenta

Urząd Certyfikacji unieważnia certyfikat końcowy w następujących przypadkach:

a) na podstawie prawidłowego wniosku o unieważnienie złożonego przy użyciu formularza online (patrz 4.9.3);
b) wnioskodawca lub subskrybent występuje z pisemnym wnioskiem o unieważnienie certyfikatu (patrz 4.9.3);
c) wnioskodawca lub subskrybent powiadamia Urząd Certyfikacji o fakcie niezaakceptowania wniosku o wydanie certyfikatu i w konsekwencji braku zgody;
d) Urząd Certyfikacji dowiaduje się, że klucz prywatny odpowiadający kluczowi publicznemu został ujawniony;
e) Urząd Certyfikacji uzyskuje dowód na to, że uprawnienia do domeny lub kontrola nad FQDN są podważalne;
f) Urząd Certyfikacji dowiaduje się, że klucz publiczny w certyfikacie nie odpowiada wymaganiom opisanym w sekcji 6.1.5. i 6.1.6;
g) Urząd Certyfikacji dowiaduje się, że certyfikat został niewłaściwie (niezgodnie z prawem) użyty;
h) Urząd Certyfikacji dowiaduje się, że subskrybent naruszył kluczowe zobowiązania w umowie na świadczenie usług lub Regulaminie usług zaufania;
i) Urząd Certyfikacji dowiaduje się, że użycie kwalifikowanej pełnej nazwy domeny wskazanej w certyfikacie przestało być prawnie dozwolone (np. decyzją sądu odebrano prawo do posługiwania się daną domeną lub jej właściciel nie przedłużył rejestracji domeny);
j) Urząd Certyfikacji dowiaduje się, że zawarte w certyfikacie informacje istotnie się zmieniły;
k) w przypadku modyfikacji certyfikatu z powodu zmiany danych podmiotu;
l) Urząd Certyfikacji dowiaduje się, że certyfikat został wydany niezgodnie z wymaganiami CABF Baseline Requirements lub z Polityką Certyfikacji lub z Kodeksem Postępowania Certyfikacyjnego;
m) Urząd Certyfikacji dowiaduje się, że dane w certyfikacie są niepoprawne;
n) Urząd Certyfikacji przestał być podmiotem upoważnionym do wydawania certyfikatów i nie zapewnia utrzymania istniejących CRL i usług OCSP;
o) unieważnienie jest wymagane przez Politykę Certyfikacji lub Kodeks Postępowania Certyfikacyjnego z powodów innych niż określone w tym rozdziale;

p) Urząd Certyfikacji dowiaduje się o istnieniu metody, która może prowadzić do ujawnienia klucza prywatnego subskrybenta, metod, które mogą wyliczyć klucz prywatny wykorzystując klucz publiczny (np. słaby klucz Debian zob. http://wiki.debian.org/SSLkeys), lub jeśli istnieje niezbity dowód na to, że konkretna metoda wykorzystywana do wygenerowania klucza prywatnego jest wadliwa;
q) Urząd Certyfikacji wystawił certyfikat na podstawie dokumentu pochodzącego od strony trzeciej, a następnie strona ta pisemnie wycofała ten dokument;
r) format i techniczna zawartość certyfikatu stanowią ryzyko dla Stron Ufających (np. w przypadku kiedy algorytm kryptograficzny lub rozmiar klucza nie są już bezpieczne);
s) Urząd Certyfikacji dowiaduje się, że mogło dojść do ujawnienia prywatnego klucza jednostki certyfikującej (wystawcy);
t) Urząd Certyfikacji dowiaduje się, że subskrybent nie dopełnił finansowych zobowiązań wynikających z umowy na świadczenie usług;
u) Urząd Certyfikacji zostanie powiadomiony lub w inny sposób dowie się o okolicznościach wskazujących, że korzystanie z adresu e-mail w certyfikacie nie jest już dozwolone;
v) certyfikat został zawieszony i nie został przywrócony w przysługującym terminie (zob. sekcja 4.9.16.);
w) zakończyła się umowa na świadczenie usług;
x) Urząd Certyfikacji zakończył działalność;
y) Organ Nadzoru wydał wiążącą prawnie i skuteczną decyzję;
z) wymóg unieważnienia wynika z przepisów prawa.

Powody unieważnienia certyfikatu dostawcy usług zaufania

Urząd Certyfikacji jest zobowiązany do unieważnienia certyfikatu pośredniej jednostki certyfikacyjnej w następujących przypadkach:

a) urząd certyfikacji obsługujący pośrednią jednostkę certyfikacyjną zwraca się z pisemną prośbą o unieważnienie certyfikatu;
b) urząd certyfikacji obsługujący pośrednią jednostkę certyfikacyjną powiadamia wystawiający Urząd Certyfikacji, że pierwotny wniosek o wystawienie certyfikatu nie został zatwierdzony i nie przyznaje autoryzacji wstecznie;
c) Urząd Certyfikacji dowiaduje się, że klucz prywatny nie jest w jego wyłącznym posiadaniu;
d) Urząd Certyfikacji dowiaduje się, że klucz publiczny w certyfikacie nie spełnia już wymagań określonych w sekcjach 6.1.5 i 6.1.6;
e) Urząd Certyfikacji dowiaduje się, że certyfikat został wykorzystany niezgodnie z prawem;
f) Certyfikat nie został wystawiony zgodnie z Polityką Certyfikacji i Kodeksem Postępowania Certyfikacyjnego lub działania pośredniej jednostki certyfikacyjnej nie są zgodne z tymi dokumentami;
g) Urząd Certyfikacji stwierdza, że niektóre informacje znajdujące się w certyfikacie są fałszywe lub wprowadzające w błąd;
h) wystawiający lub pośredniczący Urząd Certyfikacji kończy działalność z jakichkolwiek powodów i nie upoważnił innego Urzędu do utrzymywania listy CRL i unieważniania certyfikatów;
i) Urząd Certyfikacji utracił uprawnienia do wydawania certyfikatów i nie zapewnia utrzymania CRL i OCSP dla certyfikatów;
j) wymóg unieważnienia wynika z Polityki Certyfikacji lub Kodeksu Postępowania Certyfikacyjnego wydającego Urzędu Certyfikacji;

k) nastąpiła modyfikacja certyfikatu z powodu zmiany danych jednostki certyfikującej lub Urzędu Certyfikacji;
l) format i techniczna zawartość certyfikatu stanowi niedopuszczalne ryzyko dla Stron Ufających (np. w przypadku kiedy algorytm kryptograficzny lub rozmiar klucza nie są bezpieczne);
m) Urząd Certyfikacji zakończył działalność;
n) wymóg unieważnienia wynika z przepisów prawa.

Przyczyny unieważnienia certyfikatu pośredniego Urzędu Certyfikacji (CA) obsługiwanego przez inny Urząd Certyfikacji

Urząd Certyfikacji jest zobligowany do unieważnienie certyfikatu pośredniej jednostki certyfikacyjnej nadzorowanej przez inny urząd certyfikacji w następujących przypadkach:

a) urząd certyfikacji obsługujący pośrednią jednostką certyfikacyjną zwraca się z pisemną prośbą o unieważnienie certyfikatu;
b) urząd certyfikacji obsługujący pośrednią jednostką certyfikacyjną powiadamia wystawiający Urząd Certyfikacji, że pierwotny wniosek o wystawienie certyfikatu nie został zatwierdzony i nie przyznaje autoryzacji wstecznie;
c) Wystawiający Urząd Certyfikacji dowiaduje się, że CA obsługujący pośrednią jednostkę certyfikacyjną nie jest już w wyłącznym posiadaniu klucza prywatnego;
d) Wystawiający Urząd Certyfikacji dowiaduje się, że klucz publiczny w certyfikacie nie spełnia już wymagań określonymi w sekcjach 6.1.5 i 6.1.6;
e) Wystawiający Urząd Certyfikacji dowiaduje się, że certyfikat został wykorzystany niezgodnie z prawem;
f) certyfikat nie został wystawiony zgodnie z Polityką Certyfikacji i Kodeksem Postępowania Certyfikacyjnego lub działania CA obsługującego pośrednią jednostkę certyfikacyjną nie są zgodne z tymi dokumentami;
g) Urząd Certyfikacji stwierdza, że niektóre informacje znajdujące się w certyfikacie są fałszywe lub wprowadzają w błąd;
h) Wystawiający lub pośredniczący Urząd Certyfikacji kończy działalność z jakichkolwiek powodów i nie upoważnił innego Urzędu do utrzymywania listy CRL i unieważniania certyfikatów;
i) Urząd Certyfikacji utracił uprawnienia do wydawania certyfikatów i nie zapewnia utrzymania CRL i OCSP dla certyfikatów;
j) wymóg unieważnienia wynika z Polityki Certyfikacji lub Kodeksu Postępowania Certyfikacyjnego wystawiającego Urzędu Certyfikacji;
k) nastąpiła modyfikacja certyfikatu z powodu zmiany danych jednostki certyfikującej lub obsługującego ją urzędu certyfikacji;
l) Urząd Certyfikacji wystawił certyfikat na podstawie dokumentu pochodzącego od strony trzeciej, a następnie strona ta pisemnie wycofała ten dokument;
m) format i techniczna zawartość certyfikatu stanowi niedopuszczalne ryzyko dla Stron Ufających (np. w przypadku kiedy algorytm kryptograficzny lub rozmiar klucza nie są bezpieczne);
n) urząd certyfikacji obsługujący jednostkę certyfikacyjną lub Urząd Certyfikacji (wystawca certyfikatu tej jednostki) zakończył działalność;
o) wymóg unieważnienia wynika z przepisów prawa.

4.9.2. Kto może wnioskować o unieważnienie certyfikatu

O unieważnienie certyfikatu drogą online może wystąpić każdy kto zna hasło do unieważnienia i dane identyfikacyjne.

O unieważnienie certyfikatu na piśmie może wystąpić:

a) Subskrybent;
b) wnioskodawca;
c) w przypadku certyfikatu organizacyjnego – osoba upoważniona do reprezentowania danej organizacji;
d) osoba do kontaktu wymieniona w umowie na świadczenie usług;
e) administrator organizacyjny powołany przez subskrybenta;
f) organ nadzoru, który wydał podmiotowi licencję na świadczenie usług finansowych, w przypadku certyfikatu zawierającego dane podmiotu dotyczące Dyrektywy PSD2 (24) lub Open Banking;
g) Urząd Certyfikacji.

Ponadto, subskrybenci, strony ufające, dostawcy aplikacji i inne strony trzecie mogą złożyć raporty o problemach wysokiego ryzyka dotyczące certyfikatów informujące QTSP o uzasadnionym powodzie unieważnienia certyfikatu, takim jak oszustwo, nadużycie czy ujawnienie klucza.

QTSP udostępnia przejrzyste instrukcje jak raportować podejrzenia ujawnienia klucza prywatnego, nadużycia certyfikatu lub inne rodzaje oszustw, ujawnienia, nadużycia, niewłaściwe użycie czy jakiejkolwiek inne kwestie związane z certyfikatami pod adresem: https://repozytorium.eurocert.pl/ w sposób opisany w sekcji 1.5.2 niniejszego dokumentu.

4.9.3. Procedura unieważnienia

Klienci mogą złożyć wniosek o unieważnienie certyfikatu w następujący sposób:

- **Na stronie internetowej Dostawcy Usług 24h/7: https://eurocert.pl/en/zawieszenie-lub-uniewaznienie-certyfikatu.**

W przypadku unieważniania przez stronę internetową Klient podaje następujące informacje:

a) hasło do unieważnienia, potwierdzające autentyczność wniosku,
b) ostatnie trzy sekwencje cyfr oddzielonych kropką identyfikatora Podmiotu (np. 2.2.123) lub datę urodzenia Podmiotu będącego osobą fizyczną.

Wnioski złożone w ten sposób są przetwarzane niezwłocznie przez system IT, a Klient jest informowany niezwłocznie o wyniku realizacji wniosku.

Po pozytywnym unieważnieniu, nowy status pojawia się natychmiast w wewnętrznym rejestrze unieważnień. Proces ten nie trwa dłużej niż 5 minut od przyjęcia zgłoszenia unieważnienia.

Wnioski złożone w ten sposób mają zawsze powód unieważnienia: key compromise (keyCompromise (1))

QTSP rejestruje każdy wniosek o unieważnienie. W przypadku decyzji o unieważnieniu QTSP powiadamia Podmiot i Subskrybenta o tym fakcie poprzez email.

- **Przez portal Klienta 24h/7: https://eurocert.portal.pl**

Na portalu klient wybiera certyfikat do unieważnienia oraz jedną spośród następujących przyczyn unieważnienia:

a) ujawnienie klucza (keyCompromise (1)),
b) zaprzestanie używania certyfikatu (cessationOfOperation (5)),
c) wygaśnięcie uprawnień (privilegeWithdrawn (9)).

Do uwierzytelnienia wniosku mogą służyć:

a) podpis elektroniczny lub pieczęć elektroniczna:

   Podpis złożony przy użyciu nieanonimowego certyfikatu kwalifikowanego Aplikanta na portalu. Wnioski są przetwarzane w trakcie godzin pracy określonych w rozdziale 4.9.5. Przy użyciu tej metody wiele certyfikatów może zostać unieważnionych w jednym wniosku.

b) Wprowadzenie hasła do zawieszenia dla danego certyfikatu:

   Wnioski złożone w ten sposób są przetwarzane niezwłocznie, a Klient jest informowany niezwłocznie o wyniku realizacji wniosku. Przy użyciu tej metody tylko te certyfikaty mogą być unieważnione w jednym wniosku, które posiadają to samo hasło unieważnienia.

- **Poprzez email, za pomocą podpisu elektronicznego lub pieczęci**

W formie elektronicznej za pomocą podpisu elektronicznego lub pieczęci złożonych przy użyciu nie-anonimowego certyfikatu kwalifikowanego, pod adres email QTSP uniewaznienia@eurocert.pl; we wniosku można podać jedną z poniższych przyczyn:

- ujawnienie klucza (keyCompromise (1)),
- zaprzestanie używania certyfikatu (cessationOfOperation (5)),
- wygaśnięcie uprawnień (privilegeWithdrawn (9)).

- **W formie papierowej**

Pisemnie, podpisany odręcznie złożony osobiście w biurze obsługi klienta QTSP w godzinach pracy biura lub wysłany pocztą na adres obsługi klienta podany w 1.3.1. We wniosku można podać jedną z poniższych przyczyn:

- ujawnienie klucza (keyCompromise (1)),
- zaprzestanie używania certyfikatu (cessationOfOperation (5)),
- wygaśnięcie uprawnień (privilegeWithdrawn (9)).

W przypadku wniosku złożonego na piśmie, QTSP weryfikuje jego autentyczność i uprawnienia wnioskodawcy.

W przypadku wniosku o unieważnienie podpisanego elektronicznie nie ma potrzeby dalszej weryfikacji tożsamości wnioskodawcy i autentyczności samego wniosku.

W przypadku pisemnego wniosku o unieważnienie w formie papierowej wysłanego na adres e-mail, QTSP weryfikuje podpis odręczny na tym wniosku.

Jeżeli o unieważnienie wystąpił klient, ale nie podał powodu unieważnienia, QTSP uznaje, że powodem unieważnienia jest fakt, że podmiot już nie chce dłużej korzystać z certyfikatu (cessationOfOperation (5)).

Jeżeli klient wystąpił z wnioskiem o unieważnienie z powodu ujawnienia klucza, QTSP zapewnia od razu możliwość wystąpienia z wnioskiem o nowy certyfikat w ramach procedury wymiany klucza. Zasady procedury Re-key są opisane w sekcji 4.7.

Jeżeli o unieważnienie wystąpiono pisemnie, QTSP umożliwia unieważnienie certyfikatu z odroczoną datą, tzn. datą późniejszą niż data złożenia wniosku.

Wniosek o unieważnienie certyfikatu musi zawierać dane niezbędne do zidentyfikowania certyfikatu.

Wnioskodawca musi dostarczyć w szczególności następujące informacje:

a) dokładną nazwę podmiotu;
b) jeśli certyfikat został wydany na Kwalifikowanym urządzeniu do składania podpisu elektronicznego, unikalny identyfikator urządzenia;
c) unikalny identyfikator certyfikatu;
d) wnioskowaną datę unieważnienia, w przypadku, gdy unieważnienie nie następuje natychmiastowo;
e) dane identyfikacyjne Klienta.

Jeśli wniosek o unieważnienie jest nieprawidłowy lub niepełny, QTSP odrzuca go. QTSP powiadamia podmiot i subskrybenta o tym fakcie i powodzie odrzucenia za pomocą wiadomości e-mail.

Jeśli wniosek o unieważnienie jest prawidłowy i pełny, QTSP akceptuje go. W zależności od zawartości wniosku QTSP unieważnia certyfikat natychmiastowo lub zgodnie z podaną datą unieważnienia.

Po pomyślnym unieważnieniu, QTSP powiadamia o tym podmiot i subskrybenta za pomocą wiadomości e-mail.

Dalsze informacje o zawieszeniu i unieważnieniu można znaleźć na stronie QTSP pod następującym linkiem: https://eurocert.pl/index.php/en-us/documents/suspend-or-revoke-of-the-certificate

Zgłaszanie priorytetowych problemów dotyczących certyfikatów

QTSP zapewnia ciągłą nieustanną 24/7 zdolność wewnętrznego reagowania na ważne zgłoszenia dotyczących certyfikatów.

QTSP jest zobowiązany do przetwarzania wyłącznie zgłoszeń przesłanych w języku polskim lub angielskim, zgłoszenia przesłane w innych językach są niepewne i mogą zostać odrzucone bez dalszego przetwarzania.

QTSP rozpoczyna dochodzenie w ciągu 24 godzin od otrzymania zgłoszenia i podejmuje decyzję w sprawie unieważnienia, biorąc pod uwagę:

a) charakter zgłoszonego problemu;
b) konsekwencje unieważnienia;
c) liczbę otrzymanych zgłoszeń dotyczących konkretnego certyfikatu lub subskrybenta;
d) Podmiot dokonujący zgłoszenia;
e) odpowiednie regulacje prawne.

QTSP przesyła zainteresowanej stronie wstępny raport o wynikach dochodzenia zarówno subskrybentowi jak i podmiotowi, który zgłosił problem.

Po dokładnym rozpatrzeniu wszystkich faktów i okoliczności, QTSP w porozumieniu z subskrybentem i wnioskodawcą, podejmuje decyzję czy i kiedy unieważnić certyfikat.

Okres od otrzymania zgłoszenia do opublikowania unieważnienia nie może przekroczyć limitów określonych w sekcji 4.9.5.

W uzasadnionych przypadkach QTSP przesyła również organowi nadzoru sprawozdanie zawierające wyniki postepowania wyjaśniającego (dochodzenia).

4.9.4. Dopuszczalny okres zwłoki w unieważnieniu

QTSP nie przewiduje zwłoki w trakcie realizacji wniosku o unieważnienie.

4.9.5. Czas przetwarzania wniosku o unieważnienie

QTSP przetwarza wniosek o unieważnienie złożony przez stronę internetową QTSP natychmiast 24 godziny na dobę.

QTSP przetwarza wniosek o unieważnienie złożony w inny sposób w ciągu 24 godzin od wpłynięcia wniosku.

QTSP ustala czas otrzymania wniosku w następujący sposób:

a) W przypadku wniosków złożonych za pośrednictwem dedykowanego adresu email uniewaznienia@eurocert.pl w trakcie godzin pracy obsługi klienta, oficjalny czas wpłynięcia jest wtedy gdy email przychodzi na skrzynkę na serwerze QTSP. Email przychodzące poza godzinami pracy traktowane są jako odebrane na początku kolejnego dnia roboczego.
b) W przypadku wniosków na portalu klienta złożonych podczas godzin roboczych obsługi klienta, oficjalny czas wpłynięcia to faktyczny czas złożenia wniosku zapisany przez serwer. Wnioski złożone poza godzinami pracy są traktowane jako odebrane z początkiem kolejnego dnia roboczego.
c) W przypadku wniosków złożonych osobiście, czas otrzymania wniosku jest wtedy, gdy pracownik biura obsługi klienta otrzymuje wniosek.
d) W przypadku wniosków wysłanych pocztą, czas otrzymania wniosku jest wtedy, gdy list zostanie otrzymany przez QTSP w trakcie godzin pracy.

QTSP przestrzega ww. zasad jedynie w przypadku wniosków o unieważnienie wysłanych pod adres wskazany w sekcji 1.3.1. Jeżeli wnioski zostaną przesłane pod inny adres (np. bezpośrednio do partnera lub pracownika QTSP) lub innymi kanałami, wnioski pozostaną bez rozpatrzenia.

Jeżeli klient chciałby pilnie unieważnić certyfikat lub jeśli nie może stawić się osobiście w biurze QTSP, QTSP rekomenduje klientowi zawieszenie certyfikatu do czasu unieważnienia (zob. sekcja 4.9.13). Zawieszony certyfikat można unieważnić później. QTSP automatycznie unieważnia zawieszony certyfikat po upłynięciu określonego terminu (zob. sekcja 4.9.16.).

QTSP rozpoczyna dochodzenie w sprawie problemu dotyczącego certyfikatu uwierzytelniania witryny internetowej w ciągu 24 godzin od otrzymania zgłoszenia.

QTSP przesyła wstępny raport o wynikach dochodzenia subskrybentowi i podmiotowi, który zgłosił problem.

QTSP unieważnia certyfikat uwierzytelnienia strony internetowej w ciągu 24 godzin po spełnieniu warunków opisanych w sekcji 4.9.1.

QTSP unieważnia certyfikaty pośredniej jednostki certyfikacyjnej (wystawcy certyfikatów uwierzytelniania witryny internetowej) w ciągu 7 dni po spełnieniu warunków opisanych w sekcji 4.9.1.

4.9.6. Wymóg sprawdzenia unieważnienia dla Stron Ufających

W celu zachowania wysokiego poziomu bezpieczeństwa gwarantowanego przez QTSP, przed akceptacją i użyciem informacji zawartych w certyfikacie, Strony Ufające muszą działać z należytą starannością. Zaleca się, by weryfikowały one wszystkie certyfikaty ulokowane w ścieżce

certyfikacyjnej zgodnie z odpowiednimi standardami technicznymi. Weryfikacja powinna obejmować sprawdzenie ważności certyfikatów, wymagań polityk i dozwolone użycie klucza oraz sprawdzenie informacji o unieważnieniu przy wykorzystaniu listy CRL i OCSP.

4.9.7. Częstotliwość publikacji list CRL

QTSP wystawia nową listę CRL dla certyfikatów użytkownika końcowego przynajmniej raz dziennie.

Ważność tych list to 25 godzin.

NCCert wystawia nową listę CRL dla pośrednich jednostek certyfikacyjnych przynajmniej raz w miesiącu i niezwłocznie po każdym unieważnieniu, najpóźniej w ciągu godziny. Ważność list CRL to 24 godzin.

4.9.8. Maksymalny czas opóźnienia dla list CRL

Dopuszczalne jest maksymalnie 5 minut różnicy pomiędzy wygenerowaniem i upublicznieniem listy CRL.

4.9.9. Unieważnienie online /sprawdzanie statusu

QTSP świadczy usługę sprawdzenia statusu certyfikatu online (OCSP).

4.9.10. Wymogi sprawdzania statusu unieważnienia online

Usługa statusu certyfikatu online jest zgodna z wymaganiami opisanymi w sekcji 4.10.

QTSP udostępnia usługę OCSP za pomocą metody GET.

4.9.11. Inne formy publikacji informacji o unieważnieniu

QTSP udostępnia w swoim publicznym repozytorium certyfikatów - unieważnione lub zawieszone certyfikaty i ich status. Przeszukując to repozytorium, Klienci i Strony Ufające mogą osobiście, manualnie, bez pomocy żadnej specjalnej aplikacji, zweryfikować status unieważnienia certyfikatu.

4.9.12. Specjalne wymagania w przypadku ujawnienia klucza

Każda zainteresowana osoba może zgłosić do QTSP ujawnienie klucza wystawionego przez QTSP, jeśli takie zdarzenie miało miejsce.

Najszybsza droga na zgłoszenie zdarzenia odbywa się na poniższej stronie: http://eurocert.pl/repozytorium/

Zgłaszający musi udowodnić, że klucz prywatny rzeczywiście został ujawniony. Zgłoszenie musi zawierać:

- ujawniony klucz prywatny, lub
- żądanie certyfikacji w formacie PKCS#10 podpisane przez ujawniony klucz prywatny i zawierające następujący tekst w polu CN: „Dowód ujawnienia klucza”.

W przypadku ujawnienia klucza prywatnego jednej z jednostek certyfikacyjnych QTSP dołoży należytych starań, by powiadomić Strony Ufające o zaistniałym zdarzeniu (incydencie). QTSP publikuje każdą zmianę statusu swoich certyfikatów dostawcy na swojej stronie internetowej. W przypadku ujawnienia klucza prywatnego odpowiadającego certyfikatowi użytkownika końcowego wystawionego przez QTSP, QTSP może unieważnić dany certyfikat użytkownika końcowego. W takim przypadku powód unieważnienia (reasonCode) ustawia się wtedy na wartość "keyCompromise (1)".

4.9.13. Okoliczności zawieszenie certyfikatu

Certyfikaty uwierzytelniania witryn internetowych nie mogą być zawieszone.

QTSP umożliwia klientom czasowe zawieszenie certyfikatu, gdy zaistnieją przesłanki do unieważnienia. QTSP może sam zawiesić certyfikat z następujących powodów:

a) Subskrybent nie zapłacił za certyfikat;
b) QTSP podejrzewa, że dane wskazane w certyfikacie są fałszywe, nieprawidłowe. W takim przypadku QTSP rozpoczyna procedurę zawieszenia lub unieważnienia certyfikatu.
c) QTSP podejrzewa, że klucz prywatny należący do certyfikatu nie znajduje się w posiadaniu podmiotu i ma na to twarde dowody. Jeżeli QTSP ma wiedzę, na temat tego, że SCDev znalazło się w posiadaniu osoby nieuprawnionej, QTSP zawiesza każdy certyfikat, który znajduje się na tym urządzeniu;
d) Organ Nadzoru wydaje prawnie wiążącą i skuteczną decyzję.

QTSP nie przyjmuje wniosków o zawieszenie certyfikatów nieważnych.

4.9.14. Kto może wnioskować o zawieszenie certyfikatu

O zawieszenie certyfikatu mogą wystąpić te same osoby, które są uprawnione do rozpoczęcia procesu unieważnienia certyfikatu (zob. sekcję 4.9.2.)

4.9.15. Procedura rozpatrywania wniosków o zawieszenie

QTSP zapewnia możliwość zainicjowania zawieszenia każdego dnia o dowolnej godzinie.

QTSP umożliwia składanie wniosków o zawieszenie w taki sam sposób jak wnioski o unieważnienie, zgodnie z wymaganiami sekcji 4.9.3, z taką różnicą, że do zatwierdzenia wniosku o zawieszenie używa się hasła do zawieszenia.

W przypadku akceptacji wniosku o zawieszenie, zmiana statusu jest niezwłocznie zapisywana w rejestrze statusów certyfikatów.

W przypadku wniosków o zawieszenie otrzymanych innymi kanałami komunikacji przy rozpatrywaniu stosuje się wymagania opisane w sekcjach 4.9.3 i 4.9.5 dotyczące unieważnienia certyfikatu.

- **Zawieszenie na stronie internetowej dostawcy 24h/7**: https://eurocert.pl/en/zawieszenie-lub-uniewaznienie-certyfikatu

Przy zawieszeniu poprzez stronę internetową QTSP Klient musi dostarczyć następujące informacje:

a) hasło do zawieszenia uwierzytelniające wniosek o zawieszenie,
b) trzy ostatnie znaki Numeru Seryjnego Podmiotu Certyfikatu (np. 123) lub w przypadku osób fizycznych datę urodzenia podmiotu.

Wnioski o zawieszenie poprzez stronę internetową QTSP są przetwarzane niezwłocznie przez system informatyczny QTSP, który natychmiast powiadamia wnioskodawcę o wyniku na stronie internetowej.

W przypadku pomyślnego unieważnienia, jest ono natychmiast odnotowywane w wewnętrznym Rejestrze Statusu Unieważnienia. Cały proces kończy się maksymalnie w ciągu 5 minut od momentu przyjęcia wniosku do wpisania statusu unieważnienia do rejestru.

Wnioski złożone w ten sposób mają zawsze powód unieważnienia: ujawnienie klucza (keyCompromise (1)).

QTSP rejestruje każdy wniosek o zawieszenie certyfikatu. W przypadku pomyślnego zawieszenia, QTSP powiadamia o tym fakcie podmiot i subskrybenta poprzez e-mail.

- **Przez portal Klienta 24h/7: https://eurocert.portal.pl**

Na portalu klient wybiera certyfikat do zawieszenia oraz jedną spośród następujących przyczyn unieważnienia:

a) ujawnienie klucza (keyCompromise (1))
b) zaprzestanie używania certyfikatu (cessationOfOperation (5))
c) wygaśnięcie uprawnień (privilegeWithdrawn (9))

Do uwierzytelnienia wniosku mogą służyć:

a) Podpis elektroniczny lub pieczęć elektroniczna

Podpis złożony przy użyciu nie-anonimowego certyfikatu kwalifikowanego Aplikanta na portalu. Wnioski są przetwarzane w trakcie godzin pracy określonych w rozdziale 4.9.5. przy użyciu tej metody wiele certyfikatów może zostać zawieszonych w jednym wniosku.

b) Wprowadzenie hasła do zawieszenia

Wnioski złożone w ten sposób są przetwarzane niezwłocznie, a Klient jest informowany niezwłocznie o wyniku realizacji wniosku. Przy użyciu tej metody tylko te certyfikaty mogą być zawieszone w jednym wniosku, które posiadają to samo hasło.

- **Zawieszanie w taki sam sposób jak unieważnianie**

QTSP umożliwia składanie wniosków o zawieszenie w taki sam sposób, jak wniosków o unieważnienie, zgodnie z wymaganiami opisanymi w sekcji 4.9.3. Z wniosku o zawieszenie musi jasno wynikać, o który certyfikat chodzi i na jakiej podstawie ma nastąpić zawieszenie. Podmiot i subskrybent otrzymuje mailowe powiadomienie.

Przy zawieszaniu wymagane jest podanie jego powodu. Jeśli to klient wnioskuje o zawieszenie, ale nie podaje powodu, QTSP uznaje, że klient już nie chce dłużej korzystać z certyfikatu (cessationOfOperation (5).

Jeżeli klient wnioskuje o zawieszenie z powodu ujawnienia klucza, QTSP umożliwia klientowi wystawienie nowego certyfikatu w ramach procedury Re-key, jeżeli certyfikat nie zostanie odwieszony w określonym terminie i w rezultacie ulegnie unieważnieniu. Zasady dotyczące tej procedury są zawarte w sekcji 4.7.

4.9.16. Ograniczenia dotyczące okresu zawieszenia

Jeżeli o zawieszenie certyfikatu wnioskuje Klient, może on poprosić o wznowienie certyfikatu w ciągu 7 dni po zawieszeniu. Jeśli wznowienie certyfikatu nie nastąpi w ciągu tego okresu QTSP unieważnia certyfikat bez powiadomienia o tym fakcie.

Wniosek o wznowienie może być złożony jedynie w następujących formach:

a) osobiście w punkcie obsługi klienta QTSP;
b) elektronicznie, podpisany elektronicznie przy użyciu kwalifikowanego certyfikatu niepseudonimowego.

Po wznowieniu certyfikatu, QTSP powiadamia o tym fakcie mailowo podmiot i subskrybenta.

4.10. Usługi statusu certyfikatu

QTSP świadczy następujące usługi informowania o statusie unieważnienia certyfikatu:

a) OCSP – usługa online sprawdzenia statusu unieważnienia certyfikatu,
b) CRL – Listy certyfikatów unieważnionych.

Unieważnione i zawieszone certyfikaty są umieszczane na listach certyfikatów unieważnionych CRL.

Certyfikaty zawieszone są usuwane z CRL w przypadku wznowienia (uchylenia zawieszenia).

QTSP prowadzi wewnętrzny Rejestr Statusu Unieważnienia, który zawiera informację na temat bieżącego statusu unieważnienia wszystkich certyfikatów wydanych przez QTSP, łącznie z ważnymi, unieważnionymi i zawieszonymi statusami.

Unieważnione certyfikaty nie są usuwane z CRL nawet po ich wygaśnięciu.

Po pomyślnym zawieszeniu, wznowieniu i unieważnieniu, nowy status certyfikatu – zob. sekcja 4.9 – pojawia się natychmiast w rejestrze unieważnień.

Rejestr Statusu Unieważnienia zawiera również informację o statusie unieważnienia wygasłych certyfikatów, które będą dostępne do czasu wygaśnięcia Urzędu Certyfikacji (wystawcy).

QTSP generuje listy CRL na podstawie aktualnych informacji uzyskanych z Rejestru Statusu Unieważnienia, a więc wszelkie zmiany statusów unieważnienia będą publikowane na pierwszej liście CRL wystawionej po wprowadzeniu zmian.

Odpowiedzi OCSP wygenerowane przez QTSP (OCSP Responder) zawsze opierają się na informacji o statusie unieważnienia pozyskanej z Rejestru Statusu Unieważnienia w czasie wskazanym w odpowiedzi OCSP.

Odpowiedź OCSP wydana przez QTSP (za pośrednictwem OCSP Responder) może zawierać status „dobry” tylko w przypadku certyfikatów wydanych przez daną konkretną jednostkę certyfikacji i przechowywanych w Repozytorium Certyfikatów QTSP (pozytywne OCSP).

4.10.1. Szczegóły operacyjne

Każda jednostka certyfikacji QTSP wystawia listę CRL z następującą częstotliwością:

a) jednostka certyfikacji typu Root "Narodowe Centrum Certyfikacji": raz na miesiąc;
b) jednostki certyfikacyjne (subordinate) wykorzystujące SHA-512 lub ECC działające w ramach systemu QTSP – w ciągu 60 minut po unieważnieniu każdego certyfikatu wystawionego przez daną jednostkę certyfikacji ale nie rzadziej niż raz na 24 godziny.

Okres ważności listy CRL to 25 godzin. Bieżące listy CRL dla konkretnych certyfikatów są dostępne pod adresem: https://eurocert.pl/index.php/en-us/documents/certificates-and-crls.

Data wejścia w życie listy CRL ("thisUpdate") oznacza również czas, w którym jednostka certyfikacji utworzyła i rozpoczęła podpisywać listę CRL. Od tego momentu, w przypadku długiej listy CRL publikacja listy może zająć nawet jedną lub dwie minuty. Pojawienie się kolejnej listy CRL ("nextUpdate") oznacza najpóźniejszą datę, od której lista jest publicznie dostępna. W związku z tym odstępy czasu pomiędzy datą wejścia w życie listy CRL a datą publikacji kolejnej listy CRL mogą być dłuższe niż podane powyżej, co jednak nie wpływa na odstęp pomiędzy publikacjami kolejnych list CRL który wynosi najwyżej 24 godziny.

Ważność certyfikatu może być ustalona w najszybszy i najłatwiejszy sposób przy pomocy OCSP. QTSP zaleca jego użycie.

Protokół Statusu Certyfikatu Online (OCSP)

QTSP publikuje status unieważnienia certyfikatów również przy użyciu usługi OCSP.

QTSP udostępnia usługę OCSP zgodnie z zasadą “authorized responder" IETF RFC 6960 (32), a zatem każda jednostka certyfikacji certyfikuje osobno responder OCSP, który dostarcza informacji na temat statusu unieważnienia certyfikatów wystawionych przez daną jednostkę (sekcja 1.3.1).

QTSP świadczy usługę OCSP na dwa różne sposoby. Poniżej przedstawiono szczegóły tych wersji.

Usługa OCSP dla Klientów

a) Z tej wersji usługi OCSP mogą skorzystać wyłącznie klienci, którzy posiadają ważną umowę na utrzymanie certyfikatu. QTSP może zidentyfikować Klienta na podstawie certyfikatu lub poprzez login i hasło użytkownika przy zapytaniu.
b) Ta wersja usługi OCSP jest dostępna dla wszystkich certyfikatów, odpowiedzi zawsze zawierają bieżący status unieważnienia zawarty w rejestrze QTSP.
c) Wystawiona odpowiedź OCSP jest zawsze tworzona na moment zapytania. Wartości czasu "thisUpdate" i "producedAt" w odpowiedzi OCSP odpowiadają dacie i godzinie zapytania.
d) Wartość "nextUpdate" widniejąca w odpowiedzi pozostaje niewypełniona lub zawiera wartość czasu nie późniejszą niż termin wygaśnięcia certyfikatu OCSP respondera.
e) Usługa OCSP, może być użyta do uzyskania dowodu, który może później posłużyć do weryfikacji statusu certyfikatu na czas zapytania.

Ogólnodostępna i darmowa usługa OCSP

a) Ta wersja usługi OCSP jest ogólnodostępna i darmowa i Strony Ufające mogą mieć do niej dostęp tak samo jak do list CRL. Nie ma wymogu uwierzytelnienia przy zapytaniu.
b) Ta wersja usługi OCSP jest dostępna przez adres URL wpisany w certyfikacie.
c) Usługa OCSP dostarczana dla certyfikatów poczty e-mail (S/MIME) jest zgodna z wymaganiami IETF RFC 5019 (33), wspierając w ten sposób systemy PKI o dużym obciążeniu, które wymagają lekkiego rozwiązania w celu zmniejszenia wymagań dotyczących komunikacji i przetwarzania po stronie klienta.
d) Odpowiedź OCSP wygenerowana na podstawie procesu “Response Pre-production” IETF RFC 6960 (32) może być stworzona przed zapytaniem i nie musi koniecznie zawierać elementu „nonce”. QTSP może przekazać tę samą odpowiedź dla wielu zapytań. Wartości czasu dla "thisUpdate" i "producedAt" zawarte w odpowiedzi są identyczne, ale mogą być utworzone przed zapytaniem.
e) W przypadku innych certyfikatów, pole "nextUpdate" wpisane w odpowiedzi nie jest wypełniane lub zawiera wartość czasu nie późniejszą niż termin wygaśnięcia certyfikatu OCSP respondera.
f) W przypadku S/MIME oraz QWACs: czas „nextUpdate” wskazany w odpowiedzi jest zawsze wypełniany i zawiera czas nie późniejszy niż data wygaśnięcia certyfikatu respondera.
g) Wartość "thisUpdate" w odpowiedzi OCSP nigdy nie może być starsza niż 24 godziny, gdyż QTSP tworzy nową odpowiedź OCSP przynajmniej co 24 godziny.
h) W przypadku S/MIME oraz QWACs: różnica czasu pomiędzy „nextUpdate” i „thisUpdate” w odpowiedzi OCSP nigdy nie jest mniejsza niż 8 godzin.

i) Dla pozostałych certyfikatów, różnica czasu pomiędzy wartościami "nextUpdate" i "thisUpdate" w wystawionej odpowiedzi OCSP nie może być dłuższa niż 10 dni.
j) Tylko dla QWACs: wartość w polu „nextUpdate” powinna być wcześniejsza lub taka sama jak najwyższa wartość „notAfter” we wszystkich certyfikatach zawartych w polu „BasicOCSPResponse.certs” lub – jeśli pole „certs” jest pominięte – wcześniejsza lub równa „notAfter” certyfikatu CA, który wydał certyfikat, dla którego wygenerowano odpowiedź „BasicOCSPResponse”.
k) Odpowiedzi OCSP zawsze zawierają bieżącą informację zawartą w rejestrze unieważnionych certyfikatów QTSP zgodnie z czasem „thisUpdate” w odpowiedzi OCSP, jednak, jeśli wartość "thisUpdate" odpowiedzi OCSP jest wcześniejsza niż czas, dla którego przeprowadzana jest weryfikacja (wcześniejsza lub pokrywa się z czasem zapytania), odpowiedź OCSP nie stanowi twardego dowodu dla strony trzeciej co do statusu unieważnienia certyfikatu.

Ze względu na różnice powyższych wersji usługi OCSP, darmowa usługa publiczna może być uznana za równoważną usłudze świadczonej dla Klientów, tylko w poniższych przypadkach:

a) Jeśli nie ma potrzeby przechowywania odpowiedzi OCSP na dowód ważności Certyfikatu, lecz jest ona tylko używana do podejmowania szybkich decyzji w danym momencie, to w takim przypadku, przyjmuje się, że, że OCSP nie stanowi dla Strony Ufającej twardego dowodu potwierdzającego ważność certyfikatu dokładnie na konkretny czas.
b) Jeśli okres czasu pomiędzy czasem zapytania, a czasem, na który jest dokonywana weryfikacja jest dłuższy niż różnica pomiędzy „nextUpdate” i „thisUpdate” (która może wynosić najwyżej okres ważności certyfikatu OCSP Respondera). W tym przypadku odpowiedzi OCSP generowane przez publiczną usługę mogą być również uznane jako twardy dowód dla osób trzecich, ponieważ czas „thisUpdate” jest późniejszy niż czas, na który jest dokonywana weryfikacja.
c) Jeśli weryfikator nie składa zapytania sam (lecz na przykład używa odpowiedzi dołączonej do archiwalnego podpisu), wtedy nie ma potrzeby sprawdzania z jakiego pierwotnie źródła pochodzi odpowiedź. Wystarczy zweryfikować tylko, że czas „thisUpdate” jest późniejszy niż czas, na który jest dokonywana weryfikacja.

QTSP zapewnia obie wersje usługi OCSP z tą samą dostępnością.

4.10.2. Dostępność usługi

QTSP zapewnia ciągłą dostępność do Repozytorium Certyfikatów i warunków użycia certyfikatów wystawionych przez QTSP na poziomie co najmniej 99,9% w skali roku.

QTSP zapewnia dostępność informacji o statusie unieważnienia, usługi unieważnienia i wewnętrznego rejestru unieważnień na poziomie co najmniej 99% w skali roku.

Czas odpowiedzi usługi statusu unieważnienia w przypadku zwyczajnych operacji wynosi mniej niż 10 sekund.

4.10.3. Usługi opcjonalne

QTSP udostępnia różne usługi (CRL i dwa typy OCSP) zgodnie z opisem w niniejszej sekcji, w ramach których można zweryfikować status certyfikatu. Oprócz tego, QTSP udostępnia w swoim publicznym Repozytorium Certyfikatów unieważnione i zawieszone certyfikaty, wraz z wskazanymi statusami, po to, aby podczas przeszukiwania Repozytorium Certyfikatów Klienci i Strony Ufające mogli samodzielnie bez użycia specjalnej aplikacji zweryfikować status unieważnienia certyfikatu.

4.11. Koniec subskrypcji

QTSP unieważnia certyfikaty użytkownika końcowego w przypadku wygaśnięcia umowy podpisanej z subskrybentem.

4.12. Deponowanie i odzyskiwanie klucza

QTSP nie świadczy usługi deponowania klucza w przypadku klucza prywatnego należącego do certyfikatów uwierzytelniania witryn internetowych i certyfikatów podpisu lub pieczęci elektronicznej.

4.12.1. Deponowanie klucza i polityka odzyskiwania klucza

Klucz prywatny należący do certyfikatów uwierzytelniania witryn internetowych i certyfikatów podpisu lub pieczęci elektronicznej nie podlega deponowaniu.

4.12.2. Enkapsulacja symetrycznego klucza szyfrującego i polityka jego odzyskiwania

Klucz prywatny należący do certyfikatu uwierzytelniania witryn internetowych, certyfikatu podpisu lub pieczęci nie może być zdeponowany, a zatem nie ma potrzeby zarządzania symetrycznymi kluczami szyfrującymi.

4.13. Weryfikacja danych na potrzeby identyfikacji tożsamości przy wykorzystaniu certyfikatów atrybutu

QTSP ma ustawowy obowiązek przechowywać i chronić zebrane i zweryfikowane dane osobowe w celu weryfikacji tożsamości Podmiotów.

Zakres danych zdefiniowanych przez podmiot jest weryfikowany przez certyfikat atrybutu zgodnie ze standardami RFC 5280 (22) i RFC 5755 (34).

Dane, które mogą zostać zweryfikowane przez QTSP:

a) numer seryjny podmiotu (OID),
b) imię podmiotu,
c) nazwisko podmiotu,
d) miejsce urodzenia,
e) data urodzenia,
f) nazwisko matki,
g) nazwa i identyfikator dokumentu tożsamości użytego podczas pierwszej weryfikacji tożsamości.

5. Urządzenia, zarządzanie i kontroling operacyjny

QTSP stosuje fizyczne, organizacyjne i personalne środki bezpieczeństwa zgodne z powszechnie uznanymi standardami i stosuje procedury administracyjne i zarządzania egzekwujące te środki.

QTSP prowadzi ewidencję elementów systemu i zasobów związanych ze świadczeniem usług oraz przeprowadza analizę ryzyka z nimi związanego. Stosuje zabezpieczenia adekwatne do poziomu ryzyka dla poszczególnych elementów i zasobów.

QTSP monitoruje wymagania dotyczące przepustowości i zapewnia odpowiednią moc obliczeniową i pamięć do prawidłowego świadczenia usług.

5.1. Fizyczne środki kontroli

QTSP zapewnia kontrolę fizycznego dostępu do usług o znaczeniu krytycznym i minimalizuje fizyczne ryzyko dla aktywów związanych z usługami o znaczeniu krytycznym.

Fizyczne środki ochrony mają zapobiec nieupoważnionemu dostępowi lub zniszczeniu informacji i nieuprawnionemu wstępowi do stref fizycznych.

Usługi, które przetwarzają krytyczne i wrażliwe informacje są realizowane w bezpiecznych lokalizacjach w systemie QTSP.

Stopień zapewnianej ochrony odpowiada poziomowi zidentyfikowanych zagrożeń w przeprowadzonej analizie ryzyka.

W celu zapewnienia odpowiedniego poziomu bezpieczeństwa:

a) Usługi krytyczne, które muszą być chronione bardziej rygorystycznie są realizowane w chronionym pomieszczeniu komputerowym serwerowni. Serwerownia została specjalnie zaprojektowana i skonstruowana w tym celu łącząc różne elementy bezpieczeństwa (położenie i struktura stanowiska, kontrola i nadzór dostępu fizycznego, źródło zasilania, systemy chłodzenia, ochrona przed zalaniem i przeciwpożarowa, przechowywanie nośniki danych itd.).
b) Biuro obsługi klienta zostało zaprojektowane w taki sposób, aby spełniało wymogi dla świadczenia usługi rejestracji, przy realistycznych kosztach.
c) Mobilne jednostki rejestracji, spełniają wymagania związane z usługami rejestracji.
d) QTSP realizuje wszystkie krytyczne usługi w oddzielnych strefach bezpieczeństwa, ze wszystkimi niezbędnymi do tego urządzeniami znajdującymi się w zabezpieczonej serwerowni, będącej częścią strefy bezpieczeństwa.

5.1.1. Lokalizacja i wymogi budowlane systemu

Systemy IT QTSP są umieszczone i eksploatowane we właściwie zabezpieczonym Centrum Danych, wyposażonym w ochronę fizyczną i logiczną, co uniemożliwia nieuprawniony dostęp. W skład wyposażenia wchodzą: całodobowa ochrona fizyczna, specjalne zamki, czujniki włamania, monitoring wideo, system kontroli dostępu. Te rozwiązania bezpieczeństwa są ze sobą powiązane, współzależne i wzajemnie wspierające się i wspólnie zapewniają silną ochronę dla systemów IT, biorących udział w świadczeniu usług i dla danych poufnych przechowywanych przez QTSP.

5.1.2. Dostęp fizyczny

QTSP chroni swoje urządzenia i sprzęt, który bierze udział w procesie świadczenia usług przed nieautoryzowanym dostępem fizycznym.

QTSP zapewnia, że:

a) Każde wejście do Centrum Danych jest rejestrowane.
b) Do środka Centrum Danych może wejść wyłącznie jednocześnie dwóch upoważnionych członków personelu pełniących role zaufane, w tym przynajmniej jeden administrator lub operator systemu.
c) Osoby bez oddzielnej autoryzacji mogą przebywać w Centrum Danych jedynie w uzasadnionych przypadkach, w towarzystwie uprawnionego personelu.
d) Logi wejścia są archiwizowane w sposób ciągły i poddawane cotygodniowej ocenie.

Dane aktywacyjne (hasła, kody PIN) urządzeń nie mogą być przechowywane w formie otwartej („na wierzchu”) nawet w Centrum Danych.

W obecności osób nieuprawnionych:

a) nośniki danych zawierające poufne dane są fizycznie zamknięte;
b) zalogowanych stanowisk nigdy nie pozostawia się bez nadzoru;
c) procesy, w trakcie których może dojść do ujawnienia poufnych informacji są wstrzymane.

Opuszczając serwerownię, administrator lub operator systemów sprawdza, czy:

a) wszystkie urządzenia w Centrum Danych pracują w odpowiednim trybie bezpieczeństwa;
b) żadne stanowisko nie jest zostawione w stanie zalogowania;
c) fizyczne nośniki danych są odpowiednio zamknięte;
d) systemy i urządzenia zapewniające ochronę fizyczną działają prawidłowo;
e) aktywowano system alarmowy.

Za przeprowadzanie regularnych kontroli bezpieczeństwa fizycznego odpowiada wyznaczony personel odpowiedzialny. Kontrole te są realizowane w trybie planowej kontroli wewnętrznej. Wyniki kontroli są odnotowywane w raportach i zapisywane w specjalnych dziennikach zdarzeń (rejestrach kontroli).

5.1.3. Zasilanie i systemy chłodzące

QTSP korzysta z nieprzerwanego źródła zasilania awaryjnego, które:

a) posiada odpowiednią moc, by dostarczyć zasilanie do systemów IT i pomocniczych systemów Centrum Danych;
b) chroni sprzęt IT przed wahaniami napięcia z sieci zewnętrznej, przed przerwami w dostawie prądu i innymi zakłóceniami;
c) na wypadek utrzymującej się przerwy w dostawie prądu posiada własny agregat prądotwórczy, zasilany paliwem, który jest w stanie zapewnić potrzebny prąd na dowolny okres czasu.

Powietrze z zewnątrz nie może bezpośrednio przedostawać się do Centrum Danych. Czystość powietrza w Centrum Danych jest zapewniona dzięki odpowiedniemu systemowi filtrów, wyłapującemu zanieczyszczenia z powietrza: kurz, zanieczyszczenia, substancje żrące, toksyczne i materiały łatwopalne. System wentylacji dostarcza świeże powietrze odpowiednio odfiltrowane.

Wilgotność jest ograniczona do poziomu wymaganego przez systemy IT.

QTSP stosuje odpowiednio wydajne systemy chłodzące zapewniające optymalną temperatury pracy, aby zapobiec przegrzaniu urządzeń IT.

5.1.4. Narażenie na wilgoć i zalanie

Centrum Danych jest odpowiednio zabezpieczone przed zalaniem i powodzią. Cały obszar strefy bezpieczeństwa nie posiada urządzeń sanitarnych, w pobliżu nie ma kanalizacji ani wodociągów. Cały obszar strefy bezpieczeństwa jest monitorowany przez system czujników zalania. W chronionych salach komputerowych dodatkowo zastosowano podwyższoną podłogę.

5.1.5. Ochrona przeciwpożarowa

W Centrum Danych działa system przeciwpożarowy zatwierdzony przez właściwą Straż Pożarną. Czujniki dymu i ognia automatycznie alarmują straż pożarną. Zainstalowano automatyczny parowy system gaśniczy, który nie stanowi zagrożenia dla życia ludzkiego i nie uszkadza sprzętu IT.

W pomieszczeniach znajdują się ręczne gaśnice odpowiadające (pod względem typu i ilości) przepisom i są one umieszczone w widocznych miejscach.

5.1.6. Przechowywanie nośników danych

QTSP chroni wszystkie swoje nośniki danych przed nieautoryzowanym dostępem i przypadkowym uszkodzeniem. Tworzone są co najmniej dwie kopie zapasowe danych audytowych i archiwalnych. Kopie są przechowywane fizycznie osobno w sejfach w różnych lokalizacjach (pomieszczeniach operatorskich serwerowni), z dala od siebie. Nośniki są zabezpieczone przed szkodliwym wpływem środowiska, jak np. niska/wysoka temperatura, brud, kurz, wilgoć, promieniowanie UV-światło słoneczne, silne pole magnetyczne, silne promieniowanie.

5.1.7. Utylizacja odpadów

QTSP przestrzega przepisów ochrony środowiska dotyczących niszczenia zbędnych urządzeń i nośników danych.

QTSP klasyfikuje informacje w zakresie poufności, integralności, dostępności oraz okresu archiwizacji i określa sposób postępowania z danymi i ich nośnikami dla całego cyklu ich życia stosowny do przyjętej klasyfikacji. QTSP stosuje rozwiązania techniczne i organizacyjne zapobiegające ujawnieniu danych osobom i instytucjom nieupoważnionym. Stosuje zasadę wiedzy koniecznej zgodnie z którą dane są udostępniane wyłącznie w celu i w zakresie niezbędnym do realizacji ściśle zdefiniowanych zadań. Zapewnia, że dane zostaną usunięte z nośników danych a nośniki danych zostaną zniszczone przed przekazaniem ich do utylizacji. Tryb usuwania danych z nośników i niszczenia nośników danych jest ściśle uregulowany i przestrzegany. Niszczenie i przekazywanie do utylizacji nośników danych odbywa się zgodnie z obowiązującymi przepisami prawa. QTSP zapewnia zachowanie poufności informacji które nie zostały zaklasyfikowano jako jawne.

5.1.8. Odzyskiwanie danych poza siedzibą

QTSP tworzy kopie zapasowe raz na dobę, dzięki czemu wszystkie usługi mogą zostać przywrócone w przypadku poważnej awarii. Kopie są przechowywane w dwóch różnych lokalizacjach nie podlegających tym samym czynnikom ryzyka, w warunkach zapewniających taki sam poziom ochrony fizycznej i operacyjnej jak lokalizacja podstawowa. QTSP zapewnia bezpieczeństwo przesyłania danych pomiędzy ośrodkami podstawowym a zapasowym.

Co najmniej raz na kwartał przeprowadzany jest test odzyskiwania danych z kopii zapasowych. Główne okoliczności i wyniki przeprowadzonego testu zapisywane są w raportach z planowych kontroli wewnętrznych i audytu oraz odnotowywane w rejestrze kontroli.

5.2. Organizacyjne środki kontroli

QTSP dokłada starań, aby systemy sprawnie działały i były obsługiwane bezpiecznie, a ryzyko wystąpienia awarii było minimalne.

Proceduralne środki bezpieczeństwa mają na celu uzupełnienie i zwiększenie skuteczności środowiska fizycznego i zabezpieczeń personelu poprzez wyznaczenie i rozdzielenie ról zaufanych, dokumentowanie zakresu obowiązków dla tych ról, określenie liczby personelu wymaganego do każdego zadania, określenie ról wykluczających się z wykonywania konkretnych zadań oraz wymóg identyfikacji i uwierzytelnienia dla każdej roli.

Wewnętrzny system zarządzania QTSP zapewnia, że działa on zgodnie z przepisami prawa i regulacjami wewnętrznymi. W systemie tym każdy element systemu i proces mają przydzieloną osobę odpowiedzialną.

Osoby odpowiedzialne za poszczególne elementy systemu lub procesy są jednoznacznie przypisane do każdego elementu systemu i procesu. Procesy związane z rozwojem i działalnością operacyjną są rozdzielone. Nad prawidłowym funkcjonowaniem systemu, w tym procesów bezpieczeństwa, czuwa niezależny audytor systemu. Procesy są poddane bieżącej oraz okresowej udokumentowanej planowej kontroli wewnętrznej. System kontroli wewnętrznej podlega udokumentowanym audytom wewnętrznym. Ustanowione są formalna procesy zarządzania incydentami i zarządzania ryzykiem.

5.2.1. Role Zaufane

QTSP powołuje role zaufane w celu realizacji swoich zadań. Uprawnienia i funkcje zostały rozdzielone pomiędzy różnymi rolami zaufanymi w taki sposób, że jeden użytkownik nie jest w stanie samodzielnie ominąć zabezpieczeń.

QTSP powołał następujące role zaufane i obowiązki w następujący sposób:

a) Kierownik z pełną odpowiedzialnością za system IT QTSP: osoba odpowiedzialna za system IT CA. Formalnie mianuje osoby pełniące role zaufane.
b) Inspektor ds. bezpieczeństwa: ekspert ds. bezpieczeństwa, osoba w pełni odpowiedzialna za ustanowienie, wdrożenie i nadzór procesów bezpieczeństwa obejmujących bezpieczeństwo usług. Odpowiada w tym zakresie przed Kierownikiem i z nim współdziała.
c) Administrator Systemu: administrator infrastruktury. Osoba, której zadaniem jest instalowanie, konfiguracja i utrzymanie systemów QTSP. Jest on odpowiedzialny za niezawodne i ciągłe działanie powierzonych mu do obsługi części systemu, monitorowanie rozwoju technologii w poszczególnych elementach systemu, wykrywanie luk, słabych punktów w zabezpieczeniach każdego komponentu systemu i opracowywanie rozwiązań. Odpowiada za sporządzanie kopii zapasowych, testowanie sporządzonych kopii i odtwarzanie systemu z kopii.
d) Operator: operator systemu, osoba odpowiedzialna za ciągłe działanie systemu IT, tworzenie kopii zapasowych.
e) Niezależny audytor systemu: osoba, odpowiedzialna za przegląd zarejestrowanych i zarchiwizowanych danych QTSP, jest odpowiedzialna za kontrolę przestrzegania środków kontroli wdrożonych przez QTSP niezbędnych do prawidłowego funkcjonowania QTSP i za bieżący przegląd i monitorowanie istniejących wdrożonych procesów i realizację procedur.

Role zaufane mogą piastować zarówno osoby zatrudnione przez QTSP w formie umowy o pracę jak również współpracownicy na umowach kontraktowych (cywilno-prawnych oraz zlecenia).

Rolom zaufanym przypisany jest dostęp do strefy wysokiego bezpieczeństwa serwerowni. Osoby nie pełniące ról zaufanych nie mają uprawnień dostępu do tej strefy.

QTSP powołał również między innymi obowiązki nie przypisane do ról zaufanych w następujący sposób:

a) Specjalista ds. rejestracji: osoba odpowiedzialna za weryfikację tożsamości oraz poprawność złożonego przez Aplikanta wniosku.
b) Specjalista ds. personalizacji: osoba, której zadaniem jest zarządzanie i personalizacja kart inteligentnych.

5.2.2. Minimalny skład osobowy

Zgodnie z przepisami operacyjnymi i przepisami dotyczącymi bezpieczeństwa QTSP następujące operacje mogą być wykonywane wyłącznie w bezpiecznym środowisku w jednoczesnej obecności dwóch osób pełniących role zaufane:

a) generowanie własnej pary kluczy dostawcy usług;
b) wykonanie kopii zapasowej klucza prywatnego dostawcy usług;
c) aktywacja prywatnego klucza dostawcy;
d) zniszczenie prywatnego klucza dostawcy.

Co najmniej jedna osoba wykonująca operacje wymienione wyżej jest administratorem systemu, a druga osoba nie może być niezależnym audytorem systemu.

Podczas wykonywania wymienionych wyżej operacji nieupoważnione osoby nie mogą przebywać w pomieszczeniu.

5.2.3. Identyfikacja i uwierzytelnienie każdej z ról

Użytkownicy i osoby zarządzające systemami IT QTSP posiadają unikalne dane identyfikacyjne, które umożliwiają ich bezpieczną identyfikację i uwierzytelnienie.

Użytkownicy mają dostęp do systemów IT, krytycznych z punktu widzenia świadczenia usług certyfikacyjnych wyłącznie po identyfikacji i uwierzytelnieniu.

Dane do identyfikacji i uwierzytelnienia są unieważniane niezwłocznie w przypadku ustania praw użytkownika.

Każdy użytkownik systemu IT i każdy podmiot biorący udział w procesie administracyjnym jest identyfikowany indywidualnie.

W celu weryfikacji dostępu fizycznego QTSP używa systemu kontroli dostępu opartego na karcie RFID, natomiast w celu kontroli dostępu logicznego – certyfikatów VPN wydanych na urządzeniu SSCD. Bez pomyślnego uwierzytelnienia nie można wykonać żadnego działania krytycznego pod względem bezpieczeństwa. Przestrzegana jest Zasada Wiedzy Koniecznej (Zasada Wiedzy Uzasadnionej). Według tej zasady każdemu pracownikowi lub współpracownikowi QTSP nadawane są prawa dostępu w zakresie absolutnie koniecznym do wykonywania jego obowiązków.

5.2.4. Wzajemnie wykluczające się role

Członkowie Personelu QTSP mogą jednocześnie sprawować wiele ról zaufanych równocześnie pod warunkiem, że:

- Inspektor bezpieczeństwa i inspektor ds. rejestracji nie mogą pełnić funkcji niezależnego audytora systemu;
- inspektor bezpieczeństwa i niezależny audytor systemu nie mogą pełnić roli Administratora systemu;
- kierownik ponoszący całą odpowiedzialność za system IT nie może pełnić roli inspektora bezpieczeństwa i niezależnego audytora systemu.

QTSP dąży do niełączenia żadnych ról zaufanych.

5.3. Kontrole personelu

QTSP wymaga, aby jego polityka dot. personelu i praktyki dotyczące zatrudniania wzmacniały i wspierały wiarygodność działalności QTSP. Celem środków bezpieczeństwa zastosowanych wobec personelu i przez personel jest zminimalizowanie ryzyka wystąpienia błędów ludzkich, kradzieży, oszustwa czy nadużyć.

QTSP zwraca uwagę na kwestie bezpieczeństwa personelu już na etapie rekrutacji, w tym podpisywania umowy o pracę i kontroli personelu już w trakcie zatrudnienia. Osoby ubiegające się o pełnienie ról zaufanych muszą posiadać ważne zaświadczenie o niekaralności. Każda osoba pełniąca rolę zaufaną oraz wykonawcy/dostawcy zewnętrzni powinny podpisać umowę o poufności.

Jednocześnie, QTSP zapewnia swojemu personelowi otrzymanie i rozwijanie ogólnej wiedzy zawodowej wymaganej dla wszystkich stanowisk oraz wiedzy specjalistycznej niezbędnej do pełnienia poszczególnych ról.

5.3.1. Kwalifikacje, doświadczenie i zezwolenia

Od Personelu QTSP wymaga przynajmniej wykształcenia średniego, ale QTSP zapewnia przeprowadzenie odpowiedniego szkolenia stanowiskowego. Zaraz po zatrudnieniu QTSP organizuje swojemu nowemu Personelowi szkolenie, w trakcie którego zdobywają wiedzę niezbędną do wykonywania swojej pracy. Inspektorem ds. rejestracji może być wyłącznie osoba, która ukończyła kurs

umożliwiający jej rozpoznawanie dokumentów tożsamości akceptowalnych przez QTSP (dowód tożsamości, paszport i prawo jazdy). QTSP wspiera zawodowy rozwój Personelu, ale również oczekuje od nich samodzielnego poszerzania wiedzy w swoich dziedzinach. Obowiązkiem niektórych osób jest odkrywanie, zbieranie i systematyzowanie nowinek technicznych i biznesowych oraz dzielenie się nimi ze współpracownikami.

Role zaufane mogą być pełnione wyłącznie przez osoby niezależne, które nie są pod żadnym wpływem z zewnątrz oraz które posiadają niezbędną wiedzę i umiejętności, które mogą zostać zweryfikowane przez QTSP. Personel pełniący role zaufane musi być wolny od konfliktu interesów, który mógłby negatywnie wpłynąć na bezstronność działalności QTSP.

Kierownikiem który ponosi całą odpowiedzialność za system IT może być wyłącznie osoba, która posiada:

a) wykształcenie wyższe w specjalistycznej dziedzinie (w zakresie matematyki, fizyki lub innej dziedziny technicznej, nauki ścisłej);
b) co najmniej trzyletnie doświadczenie zawodowe w dziedzinie bezpieczeństwa IT.

5.3.2. Procedury sprawdzania kandydatów

QTSP powołuje na stanowiska kierownicze i do pełnienia ról zaufanych wyłącznie osoby które:

a) nie są karani i nie toczy się wobec nich żadne postępowanie karne.
b) nie mają zakazu wykonywania zawodu związanego z podpisem elektronicznym/usługami zaufania.

W dniu powołania kandydat przedstawia zaświadczenie o niekaralności nie starsze niż 3 miesiące.

Podczas rekrutacji QTSP weryfikuje informacje podane przez kandydata w CV takie jak: poprzednie miejsce zatrudnienia, referencje, kwalifikacje zawodowe.

5.3.3. Szkolenia

QTSP przeprowadza szkolenie dla nowo zatrudnionych osób, podczas których zdobywają niezbędną wiedzę i umiejętności do wykonywania swojej pracy, takie jak:

a) podstawowa wiedza z PKI;
b) charakterystyka systemu IT QTSP i sposób zarządzania nim;
c) niezbędna specjalistyczna wiedza do wykonywania powierzonych zadań;
d) procesy i procedury określone w publicznych i wewnętrznych regulacjach QTSP;
e) konsekwencje prawne działań;
f) zasad bezpieczeństwa IT w zakresie niezbędnym do wykonywania konkretnych zadań;
g) zasad ochrony danych osobowych.

QTSP szkoli inspektorów ds. rejestracji w zakresie ryzyka i niebezpieczeństwa związanego z weryfikacją danych wskazanych w certyfikacie.

Specjaliści ds. rejestracji przed powołaniem muszą zdać egzamin ze znajomości odpowiednich wymagań i procedur dotyczących weryfikacji danych.

Dostęp do systemów IT QTSP otrzymują wyłącznie osoby, które pomyślnie przeszły wymagane szkolenia.

5.3.4. Częstotliwość szkoleń przypominających

QTSP zapewnia, że personel ma zawsze niezbędny poziom wiedzy wymaganej na poszczególnych stanowiskach i dlatego, w miarę potrzeby, udostępnia możliwość odbycia szkoleń odświeżających lub podnoszących wiedzę.

Szkolenie odbywa się także, jeśli nastąpi zmiana w procesach lub systemach IT QTSP.

Materiały szkoleniowe są uaktualnianie przynajmniej raz na 12 miesięcy i zawierają najnowsze zagrożenia, aktualne praktyki i rozwiązania w zakresie bezpieczeństwa.

Szkolenie jest odpowiednio udokumentowane, w sposób jasno określający zakres, tematykę i listy uczestników.

5.3.5. Rotacja obowiązków służbowych

QTSP nie stosuje obowiązkowej rotacji pomiędzy indywidualnymi planami (harmonogramami) pracy.

5.3.6. Konsekwencje karne niedozwolonych działań

QTSP w umowach z członkami Personelu przewidział możliwość pociągnięcia ich do odpowiedzialności za zaniechania, błędy, zaniedbania lub umyślne wykroczenie. Jeśli pracownik lub współpracownik - z powodu zaniedbania lub umyślnie - narusza swoje obowiązki, QTSP może wszcząć wobec niego postępowanie dyscyplinarne i/lub nałożyć na niego kary, których wysokość jest uzależniona od rodzaju wykroczenia i konsekwencji. Wśród nich są: wycofanie premii, postępowanie dyscyplinarne, zwolnienie z pracy, cofnięcie nagrody (nominacji), degradacja, wszczęcie postępowania karnego, rozwiązanie umowy. Każda osoba pełniąca rolę zaufaną w momencie powołania na stanowisko:

a) otrzymuje pisemną informację o swoich prawach i obowiązkach prawnych, oraz klasyfikacji jej danych osobowych i zasad ich przetwarzania,
b) otrzymuje opis stanowiska pracy obejmujący również obowiązki w zakresie bezpieczeństwa,
c) podpisuje umowę o zachowaniu poufności, zawierającą konsekwencje (sankcje karne) za nieprzestrzeganie środków bezpieczeństwa.

Wszystkie powyższe dokumenty zawierają konsekwencje prawne z zakresu prawa pracy lub inne sankcje, które mogą zostać zastosowane w przypadku nieprzestrzegania obowiązków.

W przypadku działań personelu naruszających przepisy Ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej przewidziane są kary wynikające z rozdziału 6 tej Ustawy.

5.3.7. Wymagania dotyczące zleceniobiorców

Osoby pełniące role zaufane nie muszą być zatrudnione na umowę o pracę, lecz również w ramach umów cywilnoprawnych - w takim wypadku podlegają takim samym zasadom i wymogom (opisanym w rozdziale 5), jak pracownicy zatrudnieni na umowę o pracę.

W przypadku pełnienia innych zadań niż role zaufane, QTSP w miarę możliwości wybiera podwykonawców i wykonawców z listy wcześniej zakwalifikowanych dostawców. QTSP zawiera z takim wykonawcą pisemną umowę przed przystąpieniem do pracy.

Wszyscy wykonawcy, przed przystąpieniem do prac podpisują klauzulę poufności, w której zobowiązują się nie ujawniać ani w inny sposób nie wykorzystywać żadnych tajemnic handlowych/firmowych poznanych w trakcie wykonywania prac i że wiedza ta nie będzie wykorzystana w innym celu niż wykonanie umowy. Klauzula poufności zawiera kary za naruszenie. Zewnętrzni wykonawcy zatrudnieni w ramach umowy muszą posiadać odpowiednie umiejętności techniczne i QTSP nie przeprowadza dla nich żadnych szkoleń.

5.3.8. Dokumentacja udostępniana personelowi

QTSP zawsze udostępnia pracownikom i współpracownikom aktualną dokumentację i regulacje niezbędne do pełnienia przez nich wyznaczonych funkcji.

Każda osoba pełniąca rolę zaufaną otrzymuje następujące dokumenty na piśmie:

a) Polityka bezpieczeństwa QTSP,
b) Umowę o poufności do podpisania,
c) Opis stanowiska pracy,
d) Materiały szkoleniowe w przypadku planowanych lub nadzwyczajnych szkoleń, odpowiednie do danej formy kształcenia.

Wszyscy pracownicy i współpracownicy zostają poinformowani na piśmie o zmianach w polityce bezpieczeństwa organizacji QTSP.

5.4. Procedury rejestrowania

W celu zachowania bezpiecznego środowiska IT, QTSP wdraża i prowadzi kompleksowy system rejestrowania i monitorowania zdarzeń w całym swoim systemie IT.

5.4.1. Rodzaje zapisywanych zdarzeń

QTSP zapisuje każde zdarzenie związane z bezpieczeństwem, które może dostarczyć informacji o zdarzeniach, zmianach w systemie IT lub jego fizycznym środowisku zgodnie z powszechnie przyjętymi praktykami bezpieczeństwa IT. Dla każdego wpisu przechowuje następujące dane:

a) datę zdarzenia;
b) typ zdarzenia;
c) dane identyfikacyjne użytkownika lub systemu, który wywołał zdarzenie;
d) wynik danego zdarzenia (niepowodzenie, sukces).

Wszystkie nowe dzienniki zdarzeń, logi audytowe, są dodawane do wcześniejszych. Raz zapisane zapisy nie mogą być zmienione lub usunięte.

Dzienniki zdarzeń są dostępne dla niezależnych audytorów systemu, którzy sprawdzają zgodność funkcjonowania QTSP.

QTSP rejestruje zdarzenia co najmniej w następującym zakresie:

a) Zegar wewnętrzny:
   - synchronizacja zegara wewnętrznego z czasem UTC, w tym rekalibracje operacyjne;
   - utrata synchronizacji z UTC, w tym jakakolwiek utrata synchronizacji.
b) Znakowanie czasem:
   - zdarzenia związane z wydawaniem znaczników czasu.
c) Zdalne zarządzanie kluczem:
   - istotne zdarzenia środowiskowe związane z TW4S;
   - operacje podpisywania przez użytkownika (pomyślne podpisanie kluczem użytkownika i realizacje żądania DTBS/R);
   - uwierzytelnienie użytkownika w SAP;
   - zarządzanie danymi SAD użytkownika przez TW4S.

   Operacje podpisywania przez użytkownika muszą zawierać powiązany certyfikat.
d) System logów:
   - zamknięcie, ponowne uruchomienie systemu logów lub niektórych jego elementów;
   - zmiana dowolnych ustawień logowania, takich jak częstotliwość, progi alertów i kontrolowane zdarzenie;
   - zmiana lub usunięcie zapisanych logów;
   - czynności podjęte z powodu błędu w systemie logowania.

e) Logowanie do systemu:
   - udane i nieudane próby logowania do ról zaufanych;
   - w przypadku uwierzytelnienia na podstawie hasła:
     - zmiany dopuszczalnej liczby nieudanych prób logowań;
     - osiągnięcie limitu dopuszczalnej liczby nieudanych logowań dla loginu użytkownika;
     - odblokowanie użytkownika, który przekroczył limit dopuszczalnych nieudanych logowań;
   - zmiana techniki uwierzytelniania (np. z hasła na PKI).

f) ZARZĄDZANIE KLUCZAMI:
   - wszystkie zdarzenia związane z kluczem CA w trakcie całego cyklu życia kluczy CA (generowanie kluczy, zapisanie, ładowanie, niszczenie, itd.);
   - zdarzenia związane z generowaniem i zarządzeniem kluczami użytkownika (generowanie, użycie, zniszczenie);
   - wszystkie zdarzenia związane z zarządzaniem kluczami prywatnymi przechowywanymi w dowolnym celu przez QTSP.

g) ZARZĄDZANIE CERTYFIKATEM:
   - wszelkie zdarzenia związane z wystawieniem i zmianą statusu Certyfikatów dostawcy;
   - wszystkie wnioski, w tym o wystawienie certyfikatu, wymianę kluczy, odnowienie, zawieszenie i unieważnienie;
   - zdarzenia związane z przetwarzaniem i realizacją wniosku;
   - wszelkie czynności weryfikacji dokonane w związku z wydaniem certyfikatu, łącznie z datą i godziną rozmowy telefonicznej związanej z weryfikacją, numerem telefonu, nazwiskiem osoby, do której dzwoniono i uzyskanymi informacjami;
   - akceptacja i odrzucenie wniosku o wystawienie certyfikatu;
   - wystawienie certyfikatu lub zmiana jego statusu.

h) PRZEPŁYWY DANYCH:
   - wszelkie dane krytyczne pod względem bezpieczeństwa ręcznie wprowadzone do systemu;
   - dane i komunikaty krytyczne z punktu widzenia bezpieczeństwa otrzymane przez system.

i) KONFIGURACJA CA:
   - reparametryzacja, każda zmiana ustawień dowolnego komponentu CA;
   - dodanie lub usunięcie użytkownika;
   - zmiana ról i uprawnień użytkownika;
   - zmiana profilu certyfikatu;
   - zmiana profilu CRL;
   - wygenerowanie nowej listy CRL;
   - wygenerowanie odpowiedzi OCSP;
   - wygenerowanie znacznika czasu;
   - przekroczenie wymaganego progu dokładności czasu.

j) HSM:
   - Instalacja HSM;
   - odinstalowanie HSM;
   - usuwanie lub niszczenie HSM;
   - dostawa HSM;
   - resetowanie HSM;
   - wgrywanie kluczy i certyfikatów na HSM.

k) Zdalne kwalifikowane urządzenie do składania podpisu elektronicznego
   - instalacja HSM;
   - usunięcie HSM;
   - niszczenie HSM;
   - dostawa HSM;
   - resetowanie HSM;
   - wgrywanie kluczy i certyfikatów na HSM.

l) ZMIANA KONFIGURACJI:
   - sprzęt;
   - oprogramowanie;
   - system operacyjny;
   - patch naprawczy;
   - instalacja, aktualizacja, usunięcie oprogramowania w systemie QTSP.

m) DOSTĘP FIZYCZNY, BEZPIECZEŃSTWO LOKALIZACJI:
   - wejście i wyjście osób ze strefy bezpieczeństwa, w której znajdują się elementy systemu do świadczenia usług zaufania;
   - dostęp do elementu systemu wykorzystywanego do świadczenia usług zaufanych;
   - naruszenie bezpieczeństwa fizycznego, w tym nawet samo podejrzenie;
   - ruch w zaporze sieciowej lub ruterze.

n) ANOMALIE OPERACYJNE:
   - awaria systemu lub urządzeń;
   - błędy, awarie oprogramowania;
   - błąd walidacji integralności oprogramowania;
   - nieprawidłowe lub źle zaadresowane wiadomości;
   - ataki na sieć lub próby ataków;
   - awarie sprzętu;
   - awarie lub przerwy w dostawie prądu;
   - awaria zasilania awaryjnego;
   - istotne błędy dostępu do podstawowych usług sieciowych;
   - naruszenie PCKPC;
   - usunięcie zegara systemu operacyjnego.

o) INNE ZDARZENIA:
   - wyznaczenie osoby do roli bezpieczeństwa;
   - instalacja systemu operacyjnego;
   - instalacja aplikacji PKI;
   - uruchomienie systemu;
   - próba wejścia do aplikacji PKI;
   - próba zmiany hasła lub ustawienia hasła;
   - zapisanie wewnętrznej bazy danych i przywrócenie jej z kopii zapasowej;
   - operacje na plikach (tworzenie, zmiana nazwy, przenoszenie);
   - dostęp do bazy danych.

5.4.2. Częstotliwość przetwarzania logów audytowych

Niezależni audytorzy systemu QTSP dokonują analizy wygenerowanych logów każdego dnia roboczego.

Podczas analizy weryfikuje się autentyczność i integralność weryfikowanych logów, sprawdza się komunikaty o błędach pojawiające się w logach jak również (w razie potrzeby) dokumentuje się rozbieżności i podejmuje działania w celu wyeliminowania przyczyn nieprawidłowości.

W celu monitorowania systemów IT, QTSP wykorzystuje również zautomatyzowane systemy kontroli, które w sposób ciągły umożliwiają monitorowanie generowanych wpisów dziennika według określonych kryteriów i powiadamiają personel, jeśli zajedzie taka konieczność. Powiadomienia przychodzące z automatycznych narzędzi monitorowania są przetwarzane i oceniane przez dział IT w ciągu 24 godzin.

Dochodzenie, jego wynik i środki podjęte w celu wyeliminowania stwierdzonych uchybień są dokładnie dokumentowane.

5.4.3. Okres przechowywania dziennika zdarzeń, logów audytowych

Przed usunięciem z systemu online wpisy dziennika są archiwizowane i są przechowywane bezpiecznie przez czas określony w sekcji 5.5.2 zgodnie z wymaganiami wynikającymi z przepisów prawa.

Przez ten okres QTSP zapewnia, że dane można odczytać i w tym celu utrzymuje niezbędne oprogramowanie i sprzęt.

5.4.4. Ochrona dziennika zdarzeń, logów audytu

QTSP chroni powstałe logi przez wymagany okres przechowywania. Podczas tego okresu zachowane są następujące wymagania bezpieczeństwa dla logów:

a) Poufność – ochrona przed nieuprawnionym ujawnieniem: tylko uprawniona osoba, przede wszystkim niezależny audytor systemu, ma dostęp do dziennika;
b) Dostępność: upoważnione osoby mają dostęp do dziennika;
c) Integralność: logi są opatrzone kwalifikowanym znacznikiem czasu, dzięki czemu każda zmiana danych, usunięcie danych, wstawienie danych w dzienniku czy zmiana w kolejności wpisów jest zablokowana (widoczna);
d) Archiwizacja – wymagania dotyczące archiwizacji wynikające z obowiązujących przepisów prawa.

QTSP pieczętuje wpisy dziennika kwalifikowalnym znacznikiem czasu i następnie są one przechowywane w sposób uniemożliwiający niewykrywalną modyfikację zapisów dziennika.

Pliki dziennika są chronione przed przypadkowym i celowym uszkodzeniem za pomocą tworzenia kopii zapasowych. W przypadku zapisów zawierających dane poufne (np. osobowe) QTSP zapewnia bezpieczne (poufne) przechowywanie takich danych. Dostęp do wpisów dziennika mają wyłącznie upoważnione osoby, które absolutnie potrzebują ich do poprawnego wykonania swoich obowiązków służbowych. QTSP kontroluje dostęp do zapisów dziennika w sposób bezpieczny. QTSP przechowuje pliki dziennika w bezpiecznym środowisku, a kopie plików – w innym miejscu niepodlegającym tym samym zagrożeniom środowiskowym.

5.4.5. Procedury tworzenia kopii zapasowej pliku dziennika

Dzienne pliki dziennika są tworzone ze stale generowanych wpisów dziennika logów podczas pracy systemu.

Dzienne pliki dziennika są archiwizowane w dwóch kopiach i są przechowywane w fizycznie oddzielnych miejscach przez wymagany okres.

Dokładny proces tworzenia kopii zapasowych jest opisany w regulacjach wewnętrznych dotyczących kopii zapasowych QTSP.

5.4.6. System zbierania danych audytu (wewnętrzny/zewnętrzny)

Każda aplikacja w sposób automatyczny zbiera i przesyła zapisy do systemu logów.

Funkcje zapisywania informacji w logach rozpoczynają się automatycznie w momencie uruchomienia systemu i są one prowadzone w sposób ciągły w trakcie całego okresu działania systemu.

W przypadku jakichkolwiek nieprawidłowości działania automatycznych systemów monitorowania i systemu logów, działanie danego obszaru zostaje wyłączone przez QTSP aż do momentu rozwiązania problemu.

5.4.7. Powiadomienie podmiotu powodującego zdarzenie

Osoby, organizacje i aplikacje, których dotyczy zdarzenie nie zawsze są powiadamiane, ale jeśli zajdzie taka konieczność, QTSP angażuje ich w dochodzenie dotyczące zdarzenia. W takim przypadku Klienci, którzy zostali dotknięci lub wywołali zdarzenie współpracują z QTSP w celu jego wyjaśnienia. QTSP wdrożył, utrzymuje i nadzoruje proces bezpieczeństwa zarządzania incydentami. Proces ten reguluje sposób reakcji na incydenty bezpieczeństwa informacji i ochrony danych osobowych, w tym podejmowanie działań informacyjnych.

5.4.8. Ocena podatności

Oprócz codziennego przetwarzania wpisów dziennika eksperci QTSP monitorują dostępne publicznie informacje na temat możliwych podatności i nowych łat programowych. Analizują zebrane informacje, klasyfikują podatności i w razie potrzeby, informują zarząd o wynikach oraz proponują plan wzmocnienia bezpieczeństwa systemu.

Eksperci QTSP przeprowadzają kompleksową analizę podatności w celu zidentyfikowania potencjalnych zagrożeń wewnętrznych i zewnętrznych, które mogą skutkować nieautoryzowanym dostępem, wpływać na proces wystawiania certyfikatów lub pozwalać na modyfikację danych zapisanych w certyfikacie - w ciągu 48 godzin od każdego wykrycia poważniejszych uchybień lub poważniejszych zagrożeń zewnętrznych, lecz przynajmniej raz w roku.

W oparciu o wyniki analizy QTSP:

a) tworzy i wdraża plan działania w celu wyeliminowania podatności, lub
b) dokumentuje faktyczne podstawy podjęcia decyzji, że istniejące ryzyko rezydualne jest akceptowalne i występująca podatność nie wymaga podjęcia interwencji.

W pierwszej kolejności instaluje się nowe wersje oprogramowania i patche w systemie testowym QTSP i wyłącznie po pomyślnie zakończonych testach instaluje się je w produkcyjnym systemie wykorzystywanym do świadczenia usług.

Nowe oprogramowanie oraz patche nie są instalowane w produkcyjnym systemie jeśli powodują one dodatkowe podatności lub niestabilność systemu, które przewyższają korzyści wynikające z ich zastosowania. Powody niezainstalowania nowego oprogramowania (łatek) dokumentuje się.

5.5. Archiwizacja zapisów

5.5.1. Rodzaje archiwizowanych danych

Dokumenty w formie papierowej i elektronicznej są odpowiednio przygotowane przez QTSP w celu bezpiecznego długoterminowego archiwizowania.

QTSP archiwizuje przynajmniej następujące rodzaje informacji:

a) dokumenty związane z akredytacją QTSP;
b) wszystkie wydane wersje Polityki Certyfikacji i Kodeksu Postępowania Certyfikacyjnego;
c) wszystkie wersje Warunków Świadczenia Usług Zaufania EuroCert;
d) umowy związane z działalnością QTSP;
e) wszelkie informacje związane z rejestracją, w tym:
   - wszystkie dokumenty złożone wraz z wnioskiem o wystawienie certyfikatu;
   - dane identyfikacyjne dokumentów okazanych podczas identyfikacji tożsamości;
   - umowy o świadczenie usług zaufania;
   - inne oświadczenia o prawach subskrybenta;
   - tożsamość inspektora rejestracji weryfikującego wniosek o rejestrację;
   - okoliczności i wyniki weryfikacji wniosku;
f) wszelkie informacje dotyczące certyfikatu w trakcie całego cyklu jego życia;
g) informacje dotyczące personalizacji urządzenia do składania podpisu elektronicznego lub pieczęci elektronicznej;
h) wszystkie wpisy do dziennika zdarzeń w formie elektronicznej lub papierowej.

5.5.2. Okres przechowywania archiwum

QTSP przechowuje zarchiwizowane dane przez następujące okresy (chyba że przepisy prawa stanowią inaczej):

a) Politykę Certyfikacji przez co najmniej 20 lat od daty uchylenia;
b) Kodeks Postępowania Certyfikacyjnego przez co najmniej 20 lat od daty uchylenia;
c) Warunki świadczenia usług zaufania przez co najmniej 20 lat od daty uchylenia;
d) w przypadku identyfikacji tożsamości z wykorzystaniem systemu video, cały jej przebieg (nagrany) przez co najmniej 20 lat od daty nagrania;
e) główne dane związane z wydawaniem znacznika czasu przez co najmniej 20 lat od wydania;
f) wszystkie elektroniczne i papierowe dokumenty związane z certyfikatami przez co najmniej:
   - 20 lat od daty wygaśnięcia certyfikatu;
   - do momentu prawomocnego zakończenia sporu prawnego dotyczącego elektronicznego podpisu lub pieczęci elektronicznej złożonych z użyciem certyfikatu;
g) wszelkie inne dokumenty podlegają archiwizacji przez co najmniej 20 lat od daty utworzenia.

5.5.3. Ochrona archiwum

Archiwalne kopie papierowe lub elektroniczne są tworzone zgodnie z obowiązującym prawem wyłącznie z oryginalnych papierowych egzemplarzy dokumentów.

Każda z dwóch lokalizacji archiwum spełnia wymogi bezpieczeństwa i inne wymogi dotyczące archiwizacji. Podczas przechowywania danych QTSP zapewnia, że:

a) spełnione są wymagania bezpieczeństwa w zakresie ich logicznej integralności, poufności i dostępności;
b) zabezpieczone jest bezpieczeństwo dostępności fizycznej;
c) zachowują autentyczność.

Zarchiwizowane dane elektroniczne są opatrzone co najmniej zaawansowanym podpisem elektronicznym lub pieczęcią i kwalifikowanym znacznikiem czasu.

5.5.4. Procedury tworzeni archiwum kopii zapasowej

QTSP sporządza archiwalną kopię elektroniczną na podstawie oryginalnego dokumentu w wersji papierowej zgodnie z obowiązującym prawem. Archiwalne kopie elektroniczne są przechowywane zgodnie z tymi samymi zasadami, jak inne chronione dokumenty elektroniczne.

Po dokonaniu archiwizacji kopii elektronicznych zgodnych z oryginałem, QTSP ma prawo zniszczyć oryginalne dokumenty papierowe które posłużyły do wytworzenia kopii archiwalnych.

5.5.5. Wymagania dotyczące znakowania czasem zapisów

Wszystkie zapisy w elektronicznym dzienniku logów są opatrzone znacznikiem czasu z dokładnością co do sekundy.

Wartość czasu jest podana przez wewnętrzny zegar QTSP, który jest zsynchronizowany z dwoma osobnymi źródłami czasu Stratum-1 UTC:

a) pierwsze źródło czasu wykorzystuje satelitarny system GNSS (GPS i Galileo);
b) drugie źródło opiera się na sygnale fal długich (DCF77).

QTSP synchronizuje swój wewnętrzny zegar z powyższymi niezależnymi źródłami Stratum-1 z dokładnością do 0.1 sekundy co najmniej cztery razy dziennie.

W ten sposób QTSP zapewnia, że odchylenie czasu wskazanego w znaczniku czasu w stosunku do czasu UTC wynosi co najwyżej jedną sekundę.

QTSP znakuje codzienne pliki dziennika logów kwalifikowanym znacznikiem czasu.

Podczas przechowywania zarchiwizowanych danych zawsze zapewniona jest autentyczność danych tam zgromadzonych (nawet w przypadku wygaśnięcia algorytmów znacznika).

5.5.6. System zbiorów archiwum (wewnętrzny lub zewnętrzny)

Wpisy dziennika są generowane w chronionym systemie komputerowym QTSP, udostępniane są jedynie kopie plików dziennika, które zostały elektronicznie podpisane kwalifikowalnym znacznikiem czasu.

Oryginalne dokumenty papierowe stworzone w trakcie świadczenia usług są zabezpieczone i przechowywane przez QTSP w wewnętrznym repozytorium.

5.5.7. Procedury uzyskania i weryfikacji dokumentacji z archiwum

QTSP codziennie generuje podpisane pliki dziennika automatycznie.

Pliki zarchiwizowane są chronione przed nieautoryzowanym dostępem i utraceniem.

QTSP zapewnia kontrolowany dostęp do archiwum wyłącznie dla osób uprawnionych:

a) klienci mają wgląd do przechowywanych na ich temat danych;
b) Sądy, prokuratury, a także organy publiczne upoważnione do odbioru danych na podstawie odpowiednich przepisów prawa.

5.6. Zmiana klucza CA

QTSP zapewnia, że Jednostki Certyfikacyjne posiadają zawsze ważny klucz i certyfikat do swojej działalności. W tym celu, odpowiednio przed wygaśnięciem ich certyfikatu lub kluczy, QTSP generuje

nową parę kluczy dla swoich jednostek certyfikacyjnych, o czym zawczasu informuje klientów. Nowy klucz dostawcy jest generowany i zarządzany zgodnie z niniejszym dokumentem.

Jeżeli QTSP zmieni klucze dowolnego certyfikatu dostawcy, stosuje się do następujących zaleceń:

a) ujawnia nowe certyfikaty i klucze publiczne zgodnie z wymaganiami opisanymi w sekcji 2.2;
b) po wymianie kluczy, nowe certyfikaty użytkownika końcowego i znaczniki czasu są podpisywane tylko nowymi kluczami dostawcy;
c) QTSP zachowuje swoje stare certyfikaty i klucze publiczne dzięki czemu umożliwia weryfikację ważności podpisu (pieczęci) do momentu wygaśnięcia wszystkich certyfikatów i znaczników czasu podpisanych starym kluczem dostawcy.

5.7. Środki naprawcze w przypadku kompromitacji i wypadków losowych

W przypadkach awarii, QTSP podejmuje wszelkie niezbędne środki w celu zminimalizowania szkód powstałych wskutek wstrzymania usług i przywraca je najszybciej jak to możliwe.

Na podstawie oceny powstałego incydentu, QTSP podejmuje niezbędne zmiany i działania naprawcze, aby zapobiec wystąpieniu podobnych incydentów w przyszłości.

QTSP zgłasza incydent w ciągu 24 godzin od wystąpienia – w zależności od rangi – do każdej instytucji, wobec której ma taki obowiązek, oraz do Organu Nadzoru.

5.7.1. Procedury postępowania z incydentami i kompromitacją

QTSP postępuje według planu ciągłości działania.

Plan ciągłości działania zawiera procedury na wypadek ujawnienia klucza, podejrzenia ujawnienia oraz awarii zegara Jednostki Znakowania Czasem. QTSP ujawnia informacje o wyżej wymienionych zdarzeniach. QTSP nie wystawia znacznika czasu w przypadku wystąpienia powyższych zdarzeń do czasu wyjaśnienia sytuacji.

QTSP ujawnia informacje niezbędne do zidentyfikowania dotkniętych znaczników czasu w przypadku wystąpienia powyższych zdarzeń.

QTSP ustanowił i nieprzerwanie utrzymuje w pełni funkcjonalny system zapasowy, który znajduje się w bezpiecznej odległości od ośrodka podstawowego, pod innym adresem i który jest w stanie samodzielnie świadczyć pełny zakres usług.

QTSP na okresowo testuje przełączenie na działanie systemu zapasowego według posiadanego planu odtwarzania usług i przeprowadza coroczny przegląd aktualności swojego planu ciągłości działania.

QTSP dysponuje narzędziami i systemami bezpieczeństwa w celu zminimalizowania przerw spowodowanych awarią sprzętu i oprogramowania i naruszeniami danych. Możliwość przywrócenia usług jest zagwarantowana wyłącznie dzięki własnym aktywom zapasowym.

QTSP zaprojektował swój system IT świadczący usługi zaufania w taki sposób, aby usługi zaufania mogły działać nieprzerwanie w przypadku awarii pojedynczego urządzenia lub łącza telekomunikacyjnego.

W przypadku jednoczesnej awarii kilku urządzeń QTSP, jest w stanie uruchomić ośrodek zapasowy w ciągu maksymalnie 3 godzin, który zapewnia funkcjonowanie repozytorium certyfikatów, usługi unieważnienia i zawieszania i publikacji statusu certyfikatu.

Wewnętrzne polityki QTSP szczegółowo określają obowiązki związane z obsługą incydentów bezpieczeństwa. Wszelkie odstępstwa od normalnych operacji są rejestrowane w wewnętrznym systemie zarządzania zadaniami po ich wykryciu. QTSP, po wykryciu odchylenia,

niezwłocznie rozpoczyna dochodzenie w sprawie odchylenia, usuwa wykryte odchylenie tak szybko, jak to możliwe i, jeśli to konieczne, podejmuje środki zapobiegawcze, aby zapobiec ponownemu wystąpieniu odchylenia. Działania są realizowane zgodnie z uregulowaniami procesu zarządzania incydentami wdrożonego przez QTSP.

We wszystkich przypadkach QTSP uznaje za incydent bezpieczeństwa każde odchylenie, które może mieć wpływ na dostępność, integralność lub poufność usług (np. powodując przerwy w świadczeniu usług) - i nadaje priorytet każdej rozbieżności.

QTSP formalnie powiadamia Organ Nadzoru o przerwie w świadczeniu usług i incydencie bezpieczeństwa uznanym za poważny - w ciągu 24 godzin od wystąpienia incydentu.

5.7.2. Postępowanie w przypadku zagrożenia systemu, oprogramowania i/lub danych

Systemy IT QTSP są zbudowane z niezawodnego sprzętu i oprogramowania. Krytyczne funkcje zostały zrealizowane z wykorzystaniem zapasowych elementów systemu po to, by w momencie awarii któregoś elementu mogły one funkcjonować dalej.

QTSP każdego dnia wykonuje pełny backup swoich baz danych i zarejestrowanych logów (zdarzeń).

QTSP wykonuje pełny backup systemu z taką częstotliwością, aby być w stanie przywrócić pełny zakres usług w przypadku krytycznego zdarzenia losowego.

Plan ciągłości QTSP zawiera dokładne specyfikacje zadań realizowanych w celu utrzymania ciągłości działania, Plan odtwarzania usług reguluje działania które należy wykonać w przypadku niedostępności usług, w wypadku awarii krytycznego elementu systemu lub w wypadku ujawnienia klucza kryptograficznego, tak aby naruszenie nie zagroziło realizacji zobowiązań przez QTSP.

Po usunięciu problemu i przywróceniu integralności systemu, QTSP wznawia swoje usługi najszybciej jak to możliwe.

Usługi publikacji informacji o statusie certyfikatu mają pierwszeństwo podczas przywracania usług.

5.7.3. Procedury w przypadku ujawnienia klucza prywatnego

W przypadku ujawnienia klucza lub podejrzenia ujawnienia klucza prywatnego QTSP, niezwłocznie wykonuje się następujące czynności:

a) wszystkie certyfikaty związane z ujawnionym kluczem zostają unieważnione;
b) generuje się nowy klucz prywatny w celu przywrócenia usług;
c) status unieważnionych certyfikatów dostawcy jest publikowany zgodnie z metodą opisaną w sekcji 2.2;
d) informacje o ujawnieniu są przekazywane każdemu subskrybentowi i stronom ufającym;
e) certyfikaty, które zostały podpisane ujawnionym kluczem prywatnym zostają unieważnione;
f) w miejsce unieważnionych certyfikatów wystawione zostają nowe certyfikaty przy użyciu nowych kluczy dostawcy.

Plan odzyskiwania po awarii zawiera plan działania na wypadek ujawnienia klucza prywatnego dostawcy. Oprócz unieważnienie certyfikatu i klucza publicznego, obejmuje on ujawnienie okoliczności ujawnienia, powiadomienie wszystkich poszkodowanych, konieczne działania w celu uniknięcia ponownego wystąpienia ujawnienia oraz – w razie potrzeby – dostarczenie nowego klucza jednostce certyfikacji i użytkownikom końcowym dotkniętym skutkami ujawnienia. QTSP natychmiast zaprzestaje używania klucza jednostki certyfikacyjnej który został ujawniony.

Jeśli inny urząd certyfikacji również wystawił certyfikat dla danej jednostki certyfikacyjnej – na mocy prawa lub umowy pomiędzy CA a daną jednostką certyfikacyjną QTSP - QTSP natychmiast informuje ten wydający urząd certyfikacji o wystąpieniu ujawnienia i rozpoczyna procedurę unieważnienia certyfikatu należącego do danego klucza.

QTSP publikuje komunikat o unieważnieniu publicznego klucza dostawcy zgodnie z sekcją 1.3.1.

5.7.4. Zachowanie ciągłości działań po wydarzeniu losowym

Czynności podejmowane w następstwie awarii usługi powstałej na skutek katastrofy naturalnej lub innych zdarzeń losowych są opisane w Planie Odtwarzania Usług. Plan Ciągłości Działania reguluje działania organizacyjne i rozwiązania techniczne niezbędne do wdrożenia Planu Odtwarzania Usług. Wymagane czasy odtwarzania usług są oceniane metodą oceny wpływu zdarzeń na usługi (BIA – Business Impact Analysis).

W przypadku klęski żywiołowej, katastrofy, awarii mediów, naruszeń bezpieczeństwa, ujawnienia klucza i innych zdarzeń które mogłyby zakłócić ciągłość działalności biznesowej, QTSP w oparciu o realizowany Plan Ciągłości Działania, wdraża Plan Odtwarzania Usług (DRP – Disaster Recovery Plan) – proces przywracania usług. Usługi są przywracane w pierwszym etapie na minimalnym akceptowalnym poziomie.

QTSP dla potrzeb wdrożenia Planu Odtwarzania Usług utrzymuje zgodnie z Planem Ciągłości Działania lokalizację zapasową z systemami zapasowymi. Lokalizacja zapasowa znajduje się w takiej odległości od lokalizacji podstawowej, aby prawdopodobna katastrofa nie mogła dosięgnąć obu lokalizacji w tym samym czasie (lokalizacje podstawowa i zapasowa nie podlegają tym samym zagrożeniom jednocześnie).

QTSP zobowiązany jest jak najszybciej powiadomić poszkodowanych użytkowników o wdrożeniu Planu Odtwarzania Systemów i (ewentualnie) o przyczynach jego wdrożenia.

Po przywróceniu usług, QTSP niezwłocznie powraca do trybu działania biznesowego z zachowaniem poziomu bezpieczeństwa akceptowanego dla usług przed zdarzeniem.

5.8. Zakończenie działalności CA lub RA

W przypadku planowanego zakończenia świadczenia usług, QTSP powiadamia użytkowników końcowych i Organ Nadzoru na co najmniej 60 dni przed planowanym zakończeniem świadczenia usług.

Wyłączenie usług certyfikacyjnych i usług publikacji statusu certyfikatu

Wraz z powiadomieniem o zakończeniu świadczenia usług, QTSP zaprzestaje świadczenia następujących usług:

a) podpisywanie nowych umów subskrybenckich dotyczących znaczników czasu,
b) rejestrację,
c) wydawanie certyfikatu,
d) odnawianie certyfikatu,
e) modyfikacja certyfikatu,
f) wymiana kluczy.

Przynajmniej 20 dni przed planowanym zakończeniem świadczenia usług i co najmniej 14 dni po powiadomieniu klientów, QTSP:

a) unieważnia wszystkie ważne certyfikaty użytkowników końcowych;

b) zatrzymuje usługę unieważnienia i zawieszenia certyfikatów;
c) zaprzestaje regularnego wystawiania list CRL;
d) wystawia końcową listę CRL, z wartością "99991231235959Z" w polu "nextUpdate";
e) zaprzestaje wydawania nowych znaczników czasu.

Wraz z zakończeniem świadczenia usług, QTSP zamyka następujące usługi:

a) publikowanie certyfikatów,
b) publikowanie statusu unieważnienia certyfikatów,
c) usługę statusu certyfikatu online OCSP,
d) zdalne użycie kluczy użytkowników,
e) wsparcie techniczne,
f) dostarczanie informacji.

QTSP unieważnia certyfikaty odpowiadające zdalnym kluczom prywatnym zarządzanym przez QTSP niezwłocznie po zamknięciu Usługi Zdalnego Podpisu/Pieczęci. QTSP niszczy wszystkie klucze prywatne zarządzane w imieniu Klientów, związane z usługą zdalnego podpisu/pieczęci, w tym wszelkie jego kopie zapasowe oraz sporządza raport ze zniszczenia.

Przed planowanym zakończeniem usług, QTSP przeprowadzi negocjacje z innym Kwalifikowanym Dostawcą Usług Zaufania w sprawie przejęcia usług. QTSP przekaże swoje zapisy, w tym dane osobowe użytkowników innemu Dostawcy Usług Zaufania zgodnie z sekcją 9.3 lub – w przypadku braku porozumienia - Organowi Nadzoru lub też zakończy działalność bez przekazywania w zależności od wyniku negocjacji.

QTSP podejmuje działania w zakresie unieważnienia certyfikatów dostawcy (i niszczy klucze prywatne) w ciągu 60 dni, w zależności od wyniku negocjacji.

QTSP informuje Organ Nadzoru i Klientów o ostatecznym wyniku negocjacji. QTSP informuje swoich klientów za pomocą e-maila a Strony Ufające poprzez publikację na stronie internetowej.

QTSP publikuje ogłoszenie o zamknięciu aktywnych jednostek certyfikacji przynajmniej 5 dni przed zamknięciem, zgodnie z sekcją 2.1.

QTSP niszczy klucze prywatne zlikwidowanych urzędów certyfikacji w ciągu 5 dni roboczych po likwidacji w sposób rejestrowany.

Po zakończeniu usług, QTSP generuje pełną kopię zapasową danych przechowywanych w swoim systemie IT i pieczętuje ją kwalifikowanym znacznikiem czasu.

QTSP umożliwia upoważnionym stronom pomoc w zrozumieniu danych znajdujących się w rejestrach unieważnionych i zawieszonych certyfikatów, jeśli zajdzie taka potrzeba.

W celu przekazania danych innemu Kwalifikowanemu Dostawcy Usług Zaufania, QTSP umieszcza dane na nośnikach w formacie, który nowy Kwalifikowany Dostawca Usług Zaufania może odczytać lub przekazuje dane w oryginalnym formacie i zapewnia narzędzie, dokumentację lub wiedzę w celu odczytania danych.

6. Kontrole bezpieczeństwa technicznego

QTSP do świadczenia swoich usług wykorzystuje systemy złożone z niezawodnego i bezpiecznego pod względem technicznym sprzętu. QTSP zarządza swoimi kryptograficznymi kluczami prywatnymi podczas całego cyklu ich życia w module HSM, który posiada odpowiednią certyfikację.

Zarówno QTSP jak i dostawca systemu oraz wykonawcy kontraktowi posiadają wiedzę i duże doświadczenie w budowaniu systemów PKI i usługach zaufania i korzystają z międzynarodowo uznanych technologii.

QTSP nieustannie monitoruje zapotrzebowanie na wydajność systemu (przepustowość) i na podstawie wyznaczenia trendu szacuje oczekiwane przyszłe zapotrzebowanie na wydajność. QTSP może zwiększyć wydajność w razie potrzeby, aby zapewnić niezbędną moc obliczeniową i ciągłą dostępność magazynu pamięci.

6.1. Generowanie i instalacja pary kluczy

QTSP gwarantuje, że generowanie i zarządzanie wszystkimi kluczami prywatnymi wydanymi dla podmiotu, dla siebie lub swoich jednostek (np. repozytorium certyfikatów, urząd rejestracji), jest bezpieczne i zgodne z aktualnymi wymaganiami i standardami technicznymi.

6.1.1. Generowanie pary kluczy

QTSP wykorzystuje algorytmy generowania pary kluczy, które spełniają wymagania przedstawione w następujących normach:

a) ETSI TS 119 312 (35);
b) Rekomendacje CABF.

Generowanie kluczy Dostawcy

Przy generowaniu własnej pary kluczy QTSP zapewnia, że:

1) para kluczy jest generowana na podstawie skryptu generowania klucza;
2) w przypadku generowania pary kluczy CA, Akredytowany Audytor jest obecny w charakterze świadka procesu lub QTSP rejestruje video z przebiegu całego procesu;
3) jeśli para kluczy CA jest generowana dla jednostki root CA lub pośredniej jednostki certyfikacji zarządzanej przez inną organizację, akredytowany audytor jest świadkiem procesu;
4) audytor sporządza raport stwierdzający, że QTSP przestrzegał swojej ceremonii generowania kluczy podczas procesu generowania klucza i zastosował środki bezpieczeństwa w celu zapewnienia integralności i poufności pary kluczy;
5) w przypadku generowania kluczy dostawcy typu root i certyfikatu pośredniego, QTSP zapisuje przebieg procedury generowania kluczy i sporządza protokół, że nie doszło do naruszenia poufności i integralności kluczy. Raport jest podpisywany przez:
   a) Dla root CA: przez zaufaną rolę odpowiedzialną za bezpieczeństwo ceremonii generowania kluczy (np. inspektor bezpieczeństwa) oraz zaufaną osobę niezależną od QTSP (np. notariusza lub audytora), będącą świadkiem, że raport prawidłowo odzwierciedla przebieg ceremonii;
   b) Dla SubCA: przez zaufaną rolę odpowiedzialną za bezpieczeństwo ceremonii generowania kluczy (np. inspektor bezpieczeństwa), potwierdzającą, że raport prawidłowo odzwierciedla przebieg ceremonii;
6) generowanie pary kluczy dostawcy odbywa się w bezpiecznym środowisku (zob. sekcja 5.1), w obecności co najmniej dwóch osób z przypisanymi rolami zaufanymi (zob. sekcja 5.2.1), z zachowaniem zasady wiedzy współdzielonej z wyłączeniem obecności innych nieuprawnionych osób;

7) generowanie prywatnego klucza dostawcy przeprowadzane jest na urządzeniu, które:
   a) Spełnia wymagania ISO/IEC 19790 (36), lub
   b) Spełnia wymagania FIPS 140-2 (10) poziom 3 lub wyższy, lub
   c) Spełnia wymagania FIPS 140-3 (11) poziom 3 lub wyższy, lub
   d) Spełnia wymagania CEN 419 221-5 (9), lub
   e) Jest bezpiecznym systemem zgodnym z ISO/IEC 15408 (37) lub innymi równoważnymi kryteriami bezpieczeństwa równoważnymi poziomowi 4 lub wyższemu (EAL4+). Ocena opiera się na konstrukcji systemu bezpieczeństwa lub regulacjach dotyczących bezpieczeństwa spełniających wymogi niniejszego dokumentu;
8) szczegółowy zapis logów jest wykonywany z procesu generowania klucza;
9) QTSP podejmuje niezbędne środki w celu zapewnienia, że klucz prywatny został wygenerowany i zabezpieczony zgodnie z określonymi procesami podczas generowania klucza.

Generowanie kluczy infrastruktury

W przypadku generowania tzw. kluczy infrastruktury używanych w celach własnych, w swoich własnych systemach IT, QTSP upewnia się, że:

   a) generowanie kluczy infrastruktury dostawcy usług odbywa się w fizycznie chronionym środowisku (zob. sekcja 5.1) przez upoważnioną osobę pełniącą rolę zaufaną (zob. sekcja 5.2.1), z wyłączeniem obecności innych nieautoryzowanych osób;
   b) generowanie klucza jest w pełni zgodne z instrukcją zawartą w dokumentacji urządzenia.

Generowanie kluczy Subskrybentów

W przypadku generowania pary kluczy dla podmiotu, QTSP zapewnia, że:

a) klucze są generowane w fizycznie chronionym środowisku wyłącznie w obecności osób pełniących role zaufane;
b) jeśli Polityka Certyfikacji wymaga użycia kwalifikowanego urządzenia do składania podpisu elektronicznego lub urządzenia kryptograficznego, QTSP generuje klucz prywatny na jednym z tych urządzeń Aplikanta, które uniemożliwia ujawnienie klucza prywatnego;
c) QTSP nigdy nie generuje pary kluczy dla podmiotu do pliku, nie chronionych żadnym urządzeniem;
d) QTSP gwarantuje, że wygenerowana para kluczy jest zgodna z wymaganiami opisanymi w sekcjach 6.1.5 i 6.1.6, i że klucz prywatny nie jest jednym ze znanych słabych kluczy;
e) wygenerowane klucze prywatne na urządzeniach są przechowywane przez QTSP aż do momentu udokumentowanego przekazania klucza Klientowi, w odpowiednim bezpiecznym środowisku w celu zapobieżenia ujawnieniu;
f) w przypadku Usługi Zdalnego Podpisu: klucze są generowane w fizycznie chronionym środowisku, automatycznie lub przy udziale wyłącznie ról zaufanych.

QTSP nigdy nie generuje par kluczy dla certyfikatów uwierzytelniania witryn internetowych.

W przypadku pary kluczy wygenerowanej przez Podmiot:

   a) klucze są generowane w bezpiecznym środowisku, znajdującym się pod kontrolą wnioskodawcy;
   b) Wnioskodawca zapewnia odpowiednią ochronę wygenerowanego klucza prywatnego;
   c) QTSP gwarantuje, że wygenerowana para kluczy jest zgodna z wymaganiami zdefiniowanymi w sekcjach 6.1.5 i 6.1.6, i że klucz publiczny nie jest jednym ze znanych słabych kluczy.

Podczas przetwarzania Wniosku o certyfikat QTSP sprawdza parę kluczy i odrzuca Wniosek, jeśli jeden lub więcej poniższych warunków zostaje spełnionych:

a) para kluczy nie spełnia wymogów ustanowionych w sekcji 6.1.5 i/lub 6.1.6;
b) istnieją twarde dowody, że konkretna metoda użyta do wygenerowania klucza prywatnego była wadliwa;
c) QTSP wie o zademonstrowanej lub udowodnionej metodzie, która może prowadzić do ujawnienia klucza prywatnego podmiotu;
d) QTSP dowiedział się, że klucz prywatny Podmiotu został ujawniony, zgodnie z postanowieniami w sekcji 4.9.1;
e) QTSP wie o zademonstrowanej lub udowodnionej metodzie służącej do łatwego wyliczenia klucza prywatnego Podmiotu na podstawie klucza publicznego (np. słaby klucz Debian, zobacz https://wiki.debian.org/SSLkeys).

6.1.2. Dostarczenie klucza prywatnego subskrybentowi

Kiedy certyfikat do podpisu elektronicznego (pieczęci elektronicznej) jest wystawiany dla kluczy przechowywanych w pliku, klient sam generuje klucz prywatny, zatem nie ma potrzeby jego dostarczania.

QTSP nigdy nie generuje par kluczy dla certyfikatów uwierzytelniania witryny internetowej.

Jeżeli QTSP wygenerował prywatny klucz podmiotu, spełnione muszą zostać następujące wymagania:

Jeżeli klucz prywatny jest przekazywany podmiotowi:

a) Do momentu przekazania klucza, QTSP przechowuje wygenerowane dla podmiotu klucze prywatne i dane aktywacyjne w bezpiecznym miejscu uniemożliwiającym ich ujawnienie, skopiowanie, zmianę, zniszczenie czy użycie przez osoby nieupoważnione.
b) QTSP gwarantuje, że klucze prywatne i ich dane aktywacyjne mogą być odebrane wyłącznie przez upoważnionego wnioskodawcę.
c) QTSP uzyskuje dowody przekazania klucza prywatnego wnioskodawcy i dokładny czas.
d) Po przekazaniu wnioskodawcy klucza prywatnego, QTSP nie zatrzymuje żadnej kopii klucza prywatnego.

W przypadku Polityk Certyfikacji wymagających użycia urządzenia kryptograficznego (w szczególności kwalifikowanego urządzenia do składania podpisu elektronicznego), prywatny klucz podmiotu wraz z urządzeniem kryptograficznym, które zapewnia bezpieczne przechowywanie i użycie klucza prywatnego jest przekazywany wnioskodawcy osobiście z zaklejoną kopertą zawierającą kod aktywacyjny.

QTSP może również dostarczyć wnioskodawcy urządzenie kryptograficzne za pośrednictwem strony trzeciej, gwarantując, że:

a) urządzenie kryptograficzne jest w trybie transportu aż do momentu dostarczenia wnioskodawcy;
b) kod aktywacyjny do urządzenia jest przekazywany wnioskodawcy innym osobnym kanałem;
c) certyfikat zostanie wystawiony wyłącznie po uprzednim potwierdzeniu dostarczenia urządzenia wnioskodawcy.

Po wygenerowaniu klucza, kwalifikowane urządzenie do składania podpisu elektronicznego zawierające klucz prywatny jest w trybie transportowym, który zapewnia, że klucz prywatny nie może być użyty do podpisu elektronicznego przed aktywacją urządzenia.

W przypadku Polityk Certyfikacji niewymagających użycia urządzenia kryptograficznego ani kwalifikowanego urządzenia do składania podpisu elektronicznego, klient sam generuje klucz prywatny, a zatem nie ma potrzeby dostarczania go do klienta.

W przypadku Usługi Zdalnego Podpisu:

a) W trakcie całej usługi QTSP przechowuje klucz prywatny i dane aktywacyjne wygenerowane przez QTSP dla Podmiotu w bezpieczny sposób w celu uniknięcia ujawnienia klucza, skopiowania, modyfikacji, zniszczenia i użycia przez nieupoważnione osoby.
b) QTSP stosuje procedurę identyfikacji, która zapewnia, że klucz prywatny może być użyty wyłącznie przez uprawniony Podmiot.
c) QTSP przechowuje wystarczające dowody na to, że przekazanie kontroli nad kluczem prywatnym Podmiotowi nastąpiło w konkretnym autentycznym czasie.
d) QTSP zapewnia zabezpieczenia, że po przekazaniu dostępu do klucza prywatnego tylko Podmiot może uruchomić proces identyfikacji konieczny do użycia klucza prywatnego.

6.1.3. Dostarczenie klucza publicznego do wystawcy certyfikatu

Jeżeli para kluczy jest generowana przez wnioskodawcę, muszą zostać spełnione następujące warunki:

a) klucz publiczny musi zostać wysłany do QTSP w taki sposób, aby można go było jednoznacznie przypisać do wnioskodawcy;
b) proces wnioskowania o certyfikat musi wyraźnie wykazać, że wnioskodawca rzeczywiście posiada klucz prywatny odpowiadający kluczowi publicznemu.

Kiedy klucze są generowane przez wnioskodawcę, wysyła on do QTSP wniosek o certyfikat w formacie PKCS#10, który podpisany jest kluczem prywatnym odpowiadającym kluczowi publicznemu. Wniosek o certyfikat PKCS#10 zawiera klucz publiczny wygenerowany przez wnioskodawcę i dane podmiotu, które mają się znaleźć w certyfikacie, a zatem obydwa powyższe warunki zostają spełnione.

Certyfikaty dostawcy usług niezbędne do świadczenia usług zaufania wystawiane są przez Organ Nadzoru, więc QTSP dostarcza klucze publiczne do certyfikacji Organowi Nadzoru. QTSP wysyła wystawcy wniosek o certyfikat PKCS#10, który jest podpisany kluczem prywatnym należącym do klucza publicznego, który ma się znaleźć w certyfikacie.

6.1.4. Publikowanie klucza publicznego CA

QTSP publikuje certyfikaty obsługiwanych jednostek certyfikacji oraz informacje o statusie tych certyfikatów stronom zainteresowanym w następujący sposób:

a) QTSP publikuje na swojej stronie pełną hierarchię certyfikatów dostawcy zawierającą certyfikaty typu root i certyfikaty pośrednie dostawcy, z której można pobrać wszystkie aktualne certyfikaty dostawcy (zob. punkt dot. certyfikatów dostawcy https://eurocert.pl/index.php/en-us/documents/certificates-and-crls).
b) Nazwy głównych i pośrednich jednostek certyfikacyjnych i hash certyfikatów głównych znajdują się w sekcji 1.3.1.
c) Certyfikaty pośrednich jednostek certyfikacyjnych są publikowane na polskiej zaufanej liście (3) zarządzanej i publikowanej przez Organ Nadzoru w ramach wspólnego rozporządzenia europejskiego (38). Lista zawiera wszystkie certyfikaty dostawcy (łącznie z certyfikatami wygasłymi i unieważnionymi).

QTSP ujawnia stronom zainteresowanym status certyfikatu obsługiwanych przez CA jednostek certyfikacyjnych za pomocą następujących metod:

a) Status certyfikatu głównych jednostek certyfikacyjnych typu root jest dostępny na stronie internetowej QTSP.
b) Status certyfikatu pośrednich jednostek certyfikacyjnych jest ujawniony na liście CRL, na stronie internetowej i w ramach usługi odpowiedzi statusu certyfikatu online.

Odnośnie metod publikowania informacji o statusie, zobacz również Sekcję 4.10.

6.1.5. Rozmiary kluczy

QTSP używa tylko algorytmów kryptograficznych i minimalnych rozmiarów kluczy, które są zgodne z wymogami przedstawionymi w poniższych normach:

a) ETSI TS 119 312 (35);
b) Rekomendacje CABF.

QTSP używa przynajmniej 4096 bitowych kluczy RSA lub co najmniej 384 bitowych kluczy ECC we wszystkich aktualnych certyfikatach root i pośrednich oraz certyfikatach jednostek znacznika czasu i urzędów podpisujących odpowiedzi OCSP.

QTSP wydaje certyfikaty użytkownika końcowego i znaczniki czasu wyłącznie dla kluczy RSA przynajmniej 2048 bitowych lub kluczy ECC co najmniej 256 bitowych.

Podczas świadczenia usługi zdalnego podpisu, QTSP używa wyłącznie następujących algorytmów:

1) algorytm kryptograficzny: RSA
   a) długość klucza: 2048/3072/4096 bit
   b) algorytm hash: SHA-256
   c) padding algorithm: PKCS#1 ver.1.5

2) algorytm kryptograficzny: ECC
   d) długość klucza: 256 bits
   e) algorytm hash: SHA-256
   f) krzywa:
      - ECC NIST P-256
      - ECC NIST P-384 (384 bit)
      - ECC NIST P-521 (521 bit)

6.1.6. Generowanie parametrów klucza publicznego i kontrola jakości

QTSP generuje klucze zgodnie z opisem zamieszczonym w Sekcji 6.1.1.

Weryfikacja zgodności parametrów

QTSP weryfikuje zgodność każdego klucza dostawcy i subskrybenta przed wydaniem certyfikatu, z następującymi parametrami:

a) w przypadku kluczy RSA
   - długość klucza RSA jest w zakresie wspieranych wartości,
   - publiczny wykładnik potęgi RSA jest nieparzysty,
   - wartość publicznego wykładnika potęgi RSA wynosi co najmniej „(2 exp 16)+1” i najwyżej „(2 exp 256)-1”,
   - modulus jest nieparzysty, nie jest potęgą liczby pierwszej i nie ma dzielnika mniejszego niż 752.

b) w przypadku kluczy ECC
   - klucz jest prawidłowym punktem na obsługiwanej krzywej ECC (ECC Full Public-Key Validation Routine as defined in section 5.6.2.3.3 of NIST Special Publication 800-56A Revision 3 (39))

6.1.7. Cel użycia klucza (pole X.509 v3)

Klucz prywatny jednostki certyfikacyjnej typu root QTSP może być wykorzystany wyłącznie do następujących celów:

a) wystawienie auto-certyfikatów dla siebie samej,
b) podpisanie certyfikatów pośrednich jednostek certyfikacyjnych,
c) podpisanie certyfikatu dla wystawców odpowiedzi OCSP,
d) podpisanie list CRL.

Klucz prywatny pośredniej jednostki certyfikacyjnej QTSP – oraz klucz prywatny wystawiony dla pośredniej jednostki certyfikacyjnej obcej organizacji – może być wykorzystany wyłącznie do następujących celów:

a) podpisanie certyfikatów pośrednich jednostek certyfikacyjnych,
b) podpisanie certyfikatu użytkownika końcowego,
c) podpisanie certyfikatu jednostki znacznika czasu,
d) podpisanie certyfikatu dla usługi OCSP,
e) podpisanie list CRL.

QTSP umieszcza w certyfikatach użytkowników końcowych rozszerzenia dotyczące użycia klucza (keyUsage), które określają zakres użycia certyfikatu i stanowią ograniczenie techniczne użyteczności kluczy w aplikacjach kompatybilnych z X.509v3 (40). Wymagania dotyczące wartości w tym polu wymieniono w Sekcji 7.1.2.

Klucz prywatny podmiotu może być użyty wyłącznie zgodnie z użyciem klucza w certyfikacie, każde inne użycie jest niedozwolone.

Klucz prywatny odpowiadający certyfikatowi uwierzytelniania witryn internetowych może być użyty wyłącznie w celu uwierzytelnienia serwera www lub klienta, każde inne użycie jest niedozwolone.

Klucz prywatny odpowiadający certyfikatowi do podpisu może być użyty wyłącznie w celu złożenia podpisu elektronicznego, każde inne użycie jest zabronione.

Klucz prywatny pieczęci może być użyty wyłącznie w celu złożenia pieczęci elektronicznej, każde inne użycie jest niedozwolone.

Klucze prywatne Jednostki znakowania czasem mogą być użyte wyłącznie do podpisywania znaczników czasu.

Klucze prywatne wystawców odpowiedzi OSCP mogą być użyte wyłącznie do podpisywania odpowiedzi OCSP.

6.2. Ochrona klucza prywatnego i kontrole modułu kryptograficznego

QTSP gwarantuje bezpieczne zarządzanie posiadanymi kluczami prywatnymi, zapobiega ich ujawnieniu, skopiowaniu, usunięciu, modyfikacji i nieautoryzowanemu użyciu. QTSP może przechowywać klucz prywatny tylko tak długo jak wymaga tego dana usługa.

QTSP przechowuje i korzysta z prywatnych kluczy Root CA fizycznie oddzielnie od zwykłych operacji, w taki sposób, że tylko uprawnione role zaufane mogą aktywować klucz prywatny.

Klucze prywatne QTSP wykorzystywane do wystawiania Certyfikatów są przechowywane w bezpiecznym miejscu w module HSM.

QTSP usuwa klucze prywatne przechowywane w wycofanym z użytku module HSM, zgodnie z instrukcją obsługi urządzenia w sposób uniemożliwiający przywrócenie kluczy.

Urządzenia do składania kwalifikowalnego podpisu elektronicznego wykorzystywane do wydawania Certyfikatów zgodnych z Polityką Certyfikacji wymagającą takiego urządzenia, są przechowywane w bezpiecznym miejscu ze szczególna troską, w celu zabezpieczenia przed nielegalnym użyciem kluczy prywatnych od momentu wygenerowania kluczy aż po ich przekazanie podmiotowi.

W przypadku certyfikatów wystawionych zgodnie z Politykami Certyfikacyjnymi, które nie wymagają użycia kwalifikowanego urządzenia do składania podpisów elektronicznych, QTSP nie wystawia podmiotowi wcześniej kluczy prywatnych, co eliminuje konieczność zabezpieczania kluczy prywatnych użytkownika końcowego.

W przypadku certyfikatów służących do uwierzytelniania witryn internetowych, QTSP nigdy nie generuje wnioskodawcy par kluczy, co eliminuje konieczność zabezpieczania kluczy prywatnych użytkownika końcowego.

6.2.1. Standardy dotyczące modułu kryptograficznego i kontroli

Systemy QTSP wystawiające certyfikaty, podpisujące odpowiedzi OCSP, listy CRL i znaczniki czasu przechowują klucze prywatne w bezpiecznych urządzeniach sprzętowych, które spełniają następujące wymagania:

a) ISO/IEC 19790 (36), lub
b) FIPS 140-2 (10) poziom 3 lub wyższy, lub
c) FIPS 140-3 (11) poziom 3 lub wyższy, lub
d) CEN 419 221-5 (9), lub
e) EAL 4+ ISO/IEC 15408 (37) lub równoważne kryteria oceny poziomu bezpieczeństwa produktów IT.

W usłudze Zdalnego Podpisu (Pieczęci) QTSP zarządza kluczami prywatnymi użytkowników końcowych w module kryptograficznym który:

- Posiada certyfikat zgodności z Common Criteria (7), który potwierdza zgodność z wymaganiami CEN 419 241-1 (41), EAL4+ i jest opublikowany na liście QSCD Komisji UE (42).

QTSP przechowuje klucze prywatne dostawcy i klucze zdalne użytkowników końcowych poza modułem HSM wyłącznie w formie zaszyfrowanej. Do szyfrowania używa się wyłącznie algorytmów i parametrów klucza, które odpowiadają wymogom w sekcji 6.1.1 i które będą odporne na ataki kryptograficzne w czasie całego okresu ważności kluczy.

Klucze prywatne QTSP są przechowywane w fizycznie bezpiecznym miejscu nawet będąc w formie zaszyfrowanej, w sejfie w serwerowni, gdzie są dostępne wyłącznie dla autoryzowanego personelu.

W przypadku osłabienia algorytmów kryptograficznych i parametrów klucza QTSP dokonuje zniszczenia zaszyfrowanych kluczy lub koduje je ponownie przy użyciu algorytmu i parametrów klucza, które zapewniają silniejszą ochronę.

6.2.2. Kontrola klucza prywatnego (N z M) należącego do kliku osób

QTSP stosuje weryfikację „n z m” zwaną również podziałem sekretu przy aktywacji klucza prywatnego. Parametry są określone w ten sposób, że wymagana jest jednoczesna obecność przynajmniej „n” spośród „m” pisemnie upoważnionych przez kierownictwo pracowników lub współpracowników do wykonania kluczowych operacji przy użyciu prywatnych kluczy dostawcy.

6.2.3. Deponowanie klucza prywatnego

QTSP nie deponuje swoich własnych kluczy prywatnych dostawcy ani użytkowników końcowych.

6.2.4. Odzyskiwanie klucza prywatnego

QTSP tworzy kopie bezpieczeństwa swoich kluczy prywatnych dostawcy przed ich użyciem oraz kopie zarządzanych kluczy prywatnych użytkowników końcowych (codziennie) zgodnie z opisem zamieszczonym w sekcji 6.2.1 w bezpiecznym środowisku, w jednoczesnej obecności przynajmniej dwóch osób z przypisanymi rolami zaufanymi, bez udziału osób trzecich. Podczas tworzenia kopii zapasowej klucz prywatny opuszcza moduł w formie zaszyfrowanej i taki zaszyfrowany klucz może być załadowany do innego modułu. Zarówno tworzenie kopii jak i ponowne ładowanie klucza mogą się odbywać wyłącznie przy użyciu mechanizmów zabezpieczających opisanych w sekcji 6.2.2.

QTSP przechowuje kopię zapasową w dwóch egzemplarzach, z których co najmniej jedna kopia jest przechowywana w innym miejscu niż miejsce świadczenia usługi.

Takie same surowe standardy bezpieczeństwa stosuje się przy zarządzaniu i przechowywaniu kopii zapasowych jak przy działaniu systemu produkcyjnego.

QTSP nie wykonuje kopii kluczy prywatnych użytkownika końcowego, z wyjątkiem Usługi Zdalnego Podpisu.

6.2.5. Archiwizacja klucza prywatnego

QTSP nie archiwizuje swoich kluczy prywatnych i kluczy prywatnych użytkowników końcowych.

6.2.6. Wprowadzenie klucza prywatnego do i eksportowanie z modułu kryptograficznego

Wszystkie własne klucze prywatne dostawcy usług QTSP oraz klucze prywatne użytkowników końcowych zarządzane przez QTSP są tworzone w module HSM, który spełnia ściśle określone wymagania bezpieczeństwa.

Klucze prywatne nigdy nie występują w formie jawnej poza modułem HSM.

QTSP eksportuje klucz prywatny z modułu HSM w postaci niejawnej wyłącznie w celu wykonania bezpiecznej kopii.

Migracja (transfer) kluczy prywatnych dostawcy pomiędzy HSM-ami jest dozwolony wyłącznie w formie niejawnej kopii zapasowej.

Eksport i ładowanie kluczy prywatnych dostawcy odbywa się zgodnie z sekcją 6.2.2.

6.2.7. Przechowywanie klucza prywatnego w module kryptograficznym

QTSP przechowuje swoje klucze prywatne używane do świadczenia usług i zdalne klucze Klientów zarządzane przez QTSP – w module HSM zgodnie z sekcją 6.2.1.

Klucze prywatne są przechowywane i używane w module HSM zgodnie z certyfikacją urządzenia oraz instrukcjami obsługi.

6.2.8. Sposoby aktywacji klucza prywatnego

QTSP przechowuje swoje klucze prywatne dostawcy w HSM w zgodzie z instrukcją obsługi oraz wymaganiami przedstawionych w dokumentach certyfikacyjnych. Moduł HSM może być aktywowany wyłącznie przy użyciu odpowiednich kart operatorskich. Klucze prywatne w module HSM nie mogą być użyte przed aktywacją modułu. QTSP przechowuje karty operatorskie należące do HSM w bezpiecznym środowisku. Dostęp do tych kart mają wyłącznie upoważnieni pracownicy QTSP.

QTSP gwarantuje, że podpisy mogą być złożone za pomocą klucza prywatnego jednostki certyfikacyjnej root wyłącznie w przypadku komendy wydanej bezpośrednio przez upoważnioną do tego osobę.

W przypadku kluczy prywatnych użytkownika końcowego wygenerowanych przez QTSP, gwarantuje on, iż klucze prywatne i dane aktywacyjne do klucza prywatnego są generowane i zarządzane w bezpieczny sposób, który wyklucza możliwość nieautoryzowanego użycia klucza prywatnego. W przypadku kluczy prywatnych przekazywanych wnioskodawcy przez QTSP na QSCD lub urządzeniu kryptograficznym (takim jak karta inteligentna lub token), urządzenie jest przygotowane dla Podmiotu, skonfigurowane i przekazane Podmiotowi przez QTSP w taki sposób, że:

a) można jednoznacznie stwierdzić, że urządzenie nie było używane przed przekazaniem,
b) przed użyciem klucza prywatnego wnioskodawca uwierzytelnia się w QSCD lub urządzeniu kryptograficznym.

W celu aktywacji zdalnego klucza prywatnego, Podmiot powinien przedstawić hasło i unikalny krótkoterminowy kod (TOTP).

W przypadku, gdy wnioskodawca generuje klucz prywatny, ochrona tego klucza leży wyłącznie po stronie wnioskodawcy.

6.2.9. Sposoby dezaktywacji klucza prywatnego

Prywatne klucze dostawcy

Klucz prywatny używany przez QTSP i zarządzany przez urządzenia kryptograficzne zostaje dezaktywowany jeśli urządzenie traci status aktywny. Ma to miejsce kiedy:

a) użytkownik dezaktywuje klucz;
b) zasilanie urządzeń zostaje przerwane (wyłączenie prądu lub problemy z dostawą prądu);
c) następuje błąd urządzenia.

Klucz prywatny dezaktywowany w ten sposób nie może być użyty aż do momentu ponownej aktywacji modułu.

Klucze prywatne użytkownika końcowego

Jeżeli Polityki Certyfikacyjne wymagają użycia urządzeń kryptograficznych, klucze prywatne muszą być użyte zgodnie z wymaganiami określonymi w instrukcji obsługi modułów kryptograficznych i w dokumentach certyfikacyjnych.

Sprzętowe urządzenie kryptograficzne przekazane podmiotowi gwarantuje, że klucze prywatne są dezaktywowane w następujących przypadkach:

a) zasilanie urządzenia zostaje przerwane z jakiegokolwiek powodu;
b) wnioskodawca wychodzi z aplikacji, używającej urządzenia zawierającego klucz prywatny;
c) wnioskodawca wydaje urządzeniu za pomocą aplikacji polecenie dezaktywacji.

Dezaktywowany klucz i QSCD lub urządzenie kryptograficzne mogą być użyte do złożenia podpisu elektronicznego (pieczęci) wyłącznie po ponownym uwierzytelnieniu wnioskodawcy.

W przypadku, gdy Polityki Certyfikacyjne nie wymagają użycia QSCD i urządzenia kryptograficznego, właściwe użycie klucza prywatnego leży wyłącznie po stronie wnioskodawcy.

Właściwe użycie kluczy prywatnych do uwierzytelniania witryn internetowych leży po stronie wnioskodawcy.

6.2.10. Sposoby niszczenia klucza prywatnego

Prywatne klucze dostawcy

Unieważnione, wycofane, wygasłe lub ujawnione klucze prywatne QTSP są niszczone w sposób, który uniemożliwia ich dalsze użycie.

QTSP niszczy klucze prywatne dostawcy przechowywane w bezpiecznym module HSM zgodnie z procedurami i wymaganiami opisanymi w instrukcji obsługi i w dokumentach certyfikacyjnych danego modułu HSM, w jednoczesnej obecności dwóch pracowników QTSP (administratora infrastruktury i inspektora ds. bezpieczeństwa) z wyłączeniem obecności osób trzecich.

QTSP niszczy w udokumentowany sposób wszystkie kopie zapasowe klucza prywatnego w taki sposób, że jego przywrócenie i ponowne użycie nie jest możliwe.

Prywatne klucze użytkownika końcowego

Zniszczenie nieużywanych kluczy prywatnych wydanych na QSCD jest możliwe poprzez fizyczne zniszczenie QSCD, co jest obowiązkiem Podmiotu.

Na żądanie Klienta w jego obecności, QTSP może bezpłatnie zniszczyć QSCD przekazane przez klienta osobiście.

Jeżeli Polityka certyfikacji wymaga użycia QSCD lub urządzenia kryptograficznego, niepotrzebne klucze prywatne muszą być zniszczone zgodnie z wymaganiami określonymi w instrukcji obsługi danego modułu kryptograficznego i dokumentacji certyfikacyjnej. Prawidłowe zniszczenie kluczy prywatnych leży po stronie wnioskodawcy.

W przypadku, gdy Polityki Certyfikacyjne nie wymagają użycia urządzenia kryptograficznego, właściwe zniszczenie klucza prywatnego leży po stronie wnioskodawcy.

Zaleca się zniszczenie nieużywanych kluczy prywatnych podpisu, pieczęci lub uwierzytelniania witryny internetowej należących do użytkownika końcowego.

6.2.11. Ocena modułu kryptograficznego

Zgodnie z wymogami sekcji 6.2.1 wszystkie klucze prywatne QTSP są przechowywane w module kryptograficznym, który:

a) posiada certyfikat zgodności z ISO/IEC 19790 (36), lub
b) posiada certyfikat zgodności z FIPS 140-2 Level 3 (10), lub
c) posiada certyfikat zgodności z FIPS 140-3 Level 3 (11), lub
d) posiada certyfikat zgodności z Common Criteria (7) EAL4+, który potwierdza zgodność z wymaganiami normy CEN 419 221-5 (9), lub
e) posiada certyfikat wystawiony przez niezależną organizację certyfikującą zdolną do przeprowadzenia oceny produktów umożliwiających składanie podpisów elektronicznych, zarejestrowaną przez Organ Nadzoru lub w kraju członkowskim Unii Europejskiej.

Zgodnie z sekcją 6.2.1 QTSP w ramach Usługi Zdalnego Podpisu zarządza kluczami prywatnymi użytkowników końcowych w module kryptograficznym, który spełnia wymogi CEN 419 241-1 i jest na liście QSCD Komisji UE (42).

6.3. Inne aspekty zarządzania parą kluczy

6.3.1. Archiwizacja klucza publicznego

QTSP archiwizuje wszystkie certyfikaty przez co najmniej 20 lat od upływu okresu ważności lub do czasu prawomocnego zakończenia zaistniałego sporu prawnego związanego z certyfikatem (lub podpisem elektronicznym opartym na Certyfikacie).

Przez ten sam okres QTSP zachowuje metody, które pozwolą na otwarcie zawartości certyfikatu.

6.3.2. Okresy operacyjne certyfikatów i okresy używania par kluczy

Klucze i certyfikaty jednostek certyfikujących typu root

Okres ważności certyfikatów jednostek certyfikujących typu root QTSP oraz należących do nich kluczy prywatnych nie może przekraczać okresu czasu, w ciągu którego wykorzystywane algorytmy kryptograficzne - zgodnie z normami - mogą być bezpiecznie używane.

Okres ważności certyfikatów jednostek certyfikujących typu root oraz kluczy prywatnych:

- Klucz jednostki certyfikującej typu root „Narodowe Centrum Certyfikacji” jest ważny do 2032-09-03.

Klucze i certyfikaty pośrednich jednostek certyfikacyjnych

Okres ważności certyfikatów pośrednich jednostek certyfikacyjnych QTSP oraz kluczy prywatnych do nich należących:

a) nie powinien przekroczyć okresu czasu, w ciągu którego wykorzystywane algorytmy kryptograficzne - zgodnie z normami - mogą być bezpiecznie używane;
b) nie powinien przekroczyć okresu ważności certyfikatu jednostki głównej root lub pośredniej, która wydała certyfikat pośredniej jednostce certyfikacyjnej.

Klucze jednostki pośredniej (nie root) QTSP są ważne do momentu wygaśnięcia odpowiadających im certyfikatów.

Certyfikaty użytkowników końcowych

Okres ważności certyfikatów użytkowników końcowych wystawionych przez QTSP:

a) wynosi maksimum
   - 398 dni (=˜13 miesięcy) od wystawienia – w przypadku certyfikatów uwierzytelniania witryn internetowych;
   - 824 dni (=˜27 miesięcy) od daty wystawienia w przypadku certyfikatów Email (S/MIME);
   - 3 lata od wystawienia, w przypadku innych certyfikatów;
b) nie powinien przekroczyć okresu czasu, w ciągu którego wykorzystywane algorytmy kryptograficzne - zgodnie z normami - mogą być bezpiecznie używane;
c) nie może przekroczyć daty wygaśnięcia certyfikatu dostawcy, który wystawił dany certyfikat.

Podczas odnawiania i modyfikacji certyfikatu QTSP może wystawić nowy certyfikat dla tego samego klucza prywatnego użytkownika końcowego.

Okres ważności klucza dostawcy oraz użytkownika końcowego jest zagrożony jeśli wydana zostanie nowa wersja normy zgodnie, z którą aktualne algorytmy kryptograficzne lub parametry klucza nie są bezpieczne do końca planowanego okresu ważności. Jeśli to wystąpi, QTSP unieważni te certyfikaty.

QTSP niszczy zdalny klucz prywatny użytkownika zarządzany przez QTSP odpowiadający unieważnionemu certyfikatowi.

Certyfikaty urzędów znacznika czasu

QTSP publikuje klucz publiczny jednostki znacznika czasu w formie certyfikatu dostawcy usług zaufania na swojej stronie internetowej. Certyfikat jednostki znacznika czasu, wydany przez NCCert, służy do świadczenia usług zaufania zgodnie z: ETSI EN 319 411-1 (15) i ETSI EN 319 411-2 (14) jako kwalifikowany dostawca usług zaufania.

Okres ważności certyfikatów jednostek znakowania czasem:

a) maksymalnie 12 lat od wystawienia;
b) nie powinien przekroczyć końca okresu ważności zastosowanych algorytmów kryptograficznych i parametrów klucza;
c) nie powinien przekroczyć daty ważności certyfikatu dostawcy, który wystawił dany certyfikat.

Cykl życia kluczy znacznika czasu

Poniższe wymagania stosuje się w przypadku kluczy prywatnych używanych do podpisywania znacznika czasu:

a) NCCert określa w swojej Polityce Certyfikacji okres ważności kluczy prywatnych dla urzędów znacznika czasu (11 lat);
b) koniec okresu ważności klucza nie może być późniejszy niż koniec okresu ważności certyfikatu;
c) koniec okresu ważności klucza prywatnego nie jest późniejszy niż koniec okresu ważności zastosowanych algorytmów kryptograficznych i parametrów klucza;
d) klucz prywatny jednostki znacznika czasu nie jest używany po upływie okresu ważności;
e) procedury organizacyjne zapewniają, że przed upływem okresu ważności klucza, nowy klucz prywatny jest dostępny;
f) po wygaśnięciu klucza, QTSP nieodwracalnie niszczy wszystkie kopie klucza prywatnego w taki sposób, że przywrócenie klucza jest praktycznie niemożliwe.

6.4. Dane aktywacyjne

6.4.1. Generowanie i instalacja danych aktywacyjnych

Klucze prywatne QTSP są chronione zgodnie z procedurami, wymaganiami określonymi w instrukcji obsługi używanego modułu HSM oraz dokumentach certyfikacyjnych.

W przypadku użycia danych aktywacyjnych w postaci haseł, hasła są wystarczająco złożone, aby zapewnić wymagany poziom ochrony.

W przypadku QSCD lub urządzenia kryptograficznego dostarczonego przez QTSP na rzecz wnioskodawcy, QTSP zapewnia, że:

a) dane aktywacyjne są tworzone i instalowane dla ww. urządzeń w fizycznie bezpiecznym środowisku przy użyciu odpowiedniej jakości generatora liczb losowych;
b) dane aktywacyjne są przekazywane wnioskodawcy przy użyciu bezpiecznej metody.

QTSP nigdy nie generuje kluczy prywatnych do pliku dla certyfikatów użytkowników końcowych.

Stworzenie i instalacja danych aktywacyjnych dla kluczy prywatnych wygenerowanych przez wnioskodawcę jest obowiązkiem wnioskodawcy.

6.4.2. Ochrona danych aktywacyjnych

Pracownicy QTSP bezpiecznie zarządzają urządzeniami do aktywowania klucza prywatnego oraz samymi danymi aktywacyjnymi, chronią je za pomocą środków technicznych i organizacyjnych, a hasła przechowywane są wyłącznie w formie zaszyfrowanej.

W przypadku QSCD lub urządzenia kryptograficznego wydawanego wnioskodawcom przez QTSP:

a) QTSP zapisuje dane aktywacyjne wyłącznie w celu przekazania ich wnioskodawcy;
b) QTSP przekazuje dane aktywacyjne Wnioskodawcom w bezpieczny sposób.

Ochrona danych aktywacyjnych dla kluczy prywatnych utworzonych przez wnioskodawcę, jest obowiązkiem i odpowiedzialnością wnioskodawcy.

6.4.3. Inne aspekty danych aktywacyjnych

Nie określono.

6.5. Środki kontroli bezpieczeństwa komputerowego

6.5.1. Szczególne wymagania techniczne dotyczące bezpieczeństwa komputerowego

Podczas konfiguracji i działania systemu informatycznego QTSP zapewnia zgodność z następującymi wymaganiami:

a) przed przyznaniem dostępu do systemu lub aplikacji, tożsamość użytkownika jest weryfikowana za pomocą uwierzytelniania wieloskładnikowego z użyciem certyfikatów VPN przechowywanych na karcie;
b) przydziela role użytkownikom, co zapewnia, że użytkownicy mają uprawnienia odpowiadające wyłącznie ich rolom;
c) tworzy wpis dziennika dla każdej transakcji, a wpisy dziennika są archiwizowane;
d) dla procesów krytycznych dla bezpieczeństwa zapewnia się, że domeny sieci wewnętrznej QTSP są wystarczająco chronione przed nieautoryzowanym dostępem;
e) stosuje odpowiednie procedury w celu przywrócenia usługi po utracie klucza lub awarii systemu.

6.5.2. Ocena bezpieczeństwa komputerowego

EuroCert posiada dwupoziomową ocenę ryzyka, która obejmuje poza ryzykiem informatycznym również całą organizację, w tym ryzyko biznesowe. Proces zarządzania ryzykiem w ramach zarządzania bezpieczeństwem komunikuje się z procesami zarządzania incydentami, zarządzania aktywami, zarządzania procesami biznesowymi, zarządzania personelem oraz z procesami kontroli wewnętrznej i audytu. Ocena ryzyka jest aktualizowana co najmniej raz w roku. Na podstawie wyników oceny ryzyka QTSP:

a) podejmuje działania w celu wyeliminowania wykrytych podatności, lub/i
b) akceptuje zidentyfikowane ryzyka rezydualne, podając powód decyzji.

6.6. Techniczne kontrole cyklu życia

6.6.1. Kontrola rozwoju systemu

W swoim produkcyjnym systemie IT, QTSP korzysta wyłącznie z aplikacji i narzędzi, które są:

a) komercyjnym oprogramowaniem pudełkowym, zaprojektowanym i rozwijanym zgodnie z udokumentowaną metodologią projektowania, lub;

b) dopasowanymi rozwiązaniami sprzętowymi i programowymi opracowanymi przez samego QTSP, zaprojektowanymi przy zastosowaniu ustrukturyzowanych metod rozwoju i kontrolowanego środowiska programistycznego, lub;
c) dopasowanymi rozwiązaniami sprzętowymi i programowymi opracowanymi przez wiarygodną stronę trzecią dla QTSP, zaprojektowanymi przy zastosowaniu ustrukturyzowanych metod rozwoju i kontrolowanego środowiska programistycznego, lub;
d) oprogramowaniem open source, które spełnia wymagania bezpieczeństwa, którego zgodność jest zapewniona dzięki weryfikacji oprogramowania i ustrukturyzowanemu rozwojowi oraz zarządzaniu cyklem życia.

Zakup sprzętu i narzędzi IT odbywa się w sposób wykluczający zmiany w komponentach sprzętowych i programowych przy wykorzystaniu sprawdzonych, zaufanych i regularnie certyfikowanych dostawców.

Kluczowe aktywa (komponenty sprzętowe i programowe) wykorzystywane do świadczenia kluczowych usług nie są wykorzystywane przez QTSP do innych celów.

QTSP stosuje odpowiednie środki bezpieczeństwa, aby zapobiec przedostawaniu się złośliwego oprogramowania do urządzeń wykorzystywanych do świadczenia usług certyfikacyjnych.

Sprzęt i oprogramowanie są regularnie sprawdzane pod kątem złośliwego oprogramowania przed pierwszym użyciem oraz później.

QTSP zachowuje taką samą ostrożność przy zakupie lub tworzeniu aktualizacji oprogramowania, jak przy zakupie pierwszej wersji.

QTSP zatrudnia rzetelny, odpowiednio przeszkolony personel do obsługi i instalacji oprogramowania i sprzętu.

QTSP instaluje dla sprzętu informatycznego wyłącznie oprogramowanie niezbędne do świadczenia usług.

QTSP posiada system śledzenia zmian, w którym każda zmiana systemu informatycznego jest rejestrowana.

QTSP prowadzi automatyczny system monitoringu do wykrywania wszystkich nieautoryzowanych zmian, który rejestruje wszystkie zmiany w każdym pliku, a w przypadku zmian w monitorowanych plikach, generuje wpis dziennika lub wysyła alert do operatorów systemu.

6.6.2. Kontrola zarządzania bezpieczeństwem

QTSP stosuje system śledzenia zmian w celu dokumentowania, obsługi, kontroli, monitorowania i utrzymywania instalacji, konfiguracji, w tym modyfikacji i ulepszeń systemów do świadczenia usług. System śledzenia zmian wykrywa wszelkiego rodzaju nieautoryzowane zmiany w systemie, wprowadzenie danych, które wpływają na system, oraz zmiany zapory sieciowej, routerów, programów i innych komponentów do świadczenia usług.

Przed instalowaniem programu QTSP za każdym razem upewnia się, że instalowany program ma właściwą wersję i jest wolny od jakichkolwiek nieautoryzowanych modyfikacji. QTSP regularnie sprawdza integralność oprogramowania w swoim systemie wykorzystywanym do świadczenia usług.

Każdy moduł HSM używany przez QTSP został zweryfikowany, przetestowany i oceniony. QTSP weryfikuje integralność modułów:

a) po nabyciu urządzeń w trakcie odbioru,

b) bezpośrednio przed pierwszym użyciem,
c) regularnie podczas pracy.

QTSP usuwa klucze dostawcy z modułu HSM trwale lub czasowo wycofanego z użycia.

QTSP przechowuje nieużywane moduły HSM w fizycznie chronionym miejscu.

6.6.3. Kontrola cyklu życia zabezpieczeń

QTSP zapewnia ochronę używanych modułów HSM w trakcie całego cyklu ich życia.

Podczas eksploatacji sprzętu i systemów informatycznych wykorzystywanych do świadczenia usług QTSP bierze pod uwagę następujące aspekty bezpieczeństwa związane z cyklem życia sprzętu:

a) wykorzystuje w swoich systemach odpowiednio certyfikowane moduły HSM;
b) po otrzymaniu modułów HSM dokonuje kontroli jakości, sprawdza, czy podczas transportu zapewniono ochronę przed włamaniem do urządzenia;
c) moduły HSM są przechowywane w bezpiecznym miejscu i są chronione na czas przechowywania przed włamaniem;
d) podczas eksploatacji stale przestrzega wymagań bezpieczeństwa przedstawionych w dokumentacji modułu HSM: security target, instrukcji obsługi i raportu certyfikacyjnego;
e) usuwa klucze prywatne przechowywane w wycofanych modułach HSM w taki sposób, że praktycznie niemożliwe staje się przywrócenie kluczy;
f) zarządza i utylizuje wycofane z eksploatacji moduły HSM zgodnie z ich wymaganiami zawartymi w security target, instrukcji obsługi i raporcie certyfikacyjnym.

6.7. Kontrola bezpieczeństwa sieci

QTSP przestrzega najlepszych praktyk branżowych w celu zapewnienia bezpieczeństwa sieci. Stosuje się do wymagań CA/B Forum's Network and Certificate System Security Requirements (43).

QTSP utrzymuje konfigurację swojego systemu informatycznego pod ścisłą kontrolą i dokumentuje każdą zmianę, w tym nawet najmniejszą modyfikację, ulepszenie i aktualizację oprogramowania. QTSP stosuje odpowiednie procedury do wykrywania wszelkich zmian sprzętu lub oprogramowania, do instalacji systemu oraz konserwacji systemu informatycznego. QTSP sprawdza autentyczność i integralność każdego komponentu oprogramowania przy pierwszej instalacji.

QTSP stosuje odpowiednie środki bezpieczeństwa sieci na przykład:

a) dzieli swój system informatyczny na oddzielne strefy bezpieczeństwa;
b) oddziela swoje systemy wspierające działanie systemu informatycznego od systemów świadczących usługi na żywo, w tym zapewnia że systemy zaufania znajdują się w podsieci logicznej wysokiego bezpieczeństwa odseparowanej logicznie od wewnętrznej sieci bezpieczeństwa przeznaczonej dla systemów (usług) wspierających;
c) separuje systemy produkcyjne służące do usług TSP i usług wspierających od systemów wykorzystywanych do rozwoju i testowania poprzez umieszczenie ich w osobnych sieciach logicznych;
d) ustanawia niezawodną komunikację między odseparowanymi zaufanymi systemami wyłącznie za pośrednictwem zaufanych kanałów komunikacji, które są logicznie odseparowane od innych kanałów komunikacji i zapewniają zaufaną identyfikację punktów końcowych oraz ochronę danych transferowanych kanałem przed modyfikacją lub ujawnieniem;
e) produkcyjne systemy informatyczne usług działają w bezpiecznych strefach sieciowych;

f) dostęp i komunikacja między strefami są ograniczone wyłącznie do tych, które są niezbędne do działania usługi (z dokładnością do portów);
g) wyłącza nieużywane protokoły i konta użytkowników;
h) wyłącza nieużywane porty i usługi sieciowe;
i) uruchamia wyłącznie aplikacje sieciowe bezwarunkowo niezbędne do prawidłowego działania systemu informatycznego;
j) regularnie dokonuje przeglądu ustalonego zestawu reguł.

QTSP wykonuje testy podatności publicznych i prywatnych adresów IP:

a) w ciągu tygodnia od otrzymania żądania od CA/Browser Forum;
b) po jakichkolwiek istotnych zmianach w systemie lub sieci;
c) przynajmniej co trzy (3) miesiące.

QTSP sprawdza konfigurację urządzeń sieci lokalnej (np. routerów) na zgodność z wymaganiami określonymi przez QTSP co najmniej raz na trzy miesiące.

Po dokonaniu wszelkich istotnych zmian w systemie IT i przynajmniej co rok, QTSP zleca wykonanie testu penetracyjnego zewnętrznemu niezależnemu ekspertowi, który posiada niezbędne umiejętności, wiedzę, narzędzia, biegłość i kieruje się kodeksem etycznym, niezbędnymi do przeprowadzenia testu i wydania rzetelnego raportu.

6.8. Znakowanie czasem

W celu ochrony integralności plików dziennika i innych plików elektronicznych, podlegających archiwizacji, QTSP stosuje kwalifikowane elektroniczne znaczniki czasu wydane przez jednostkę znakowania czasem EuroCert QTSA.

Znacznik czasu wydany przez QTSP jest zgodny z normami: IETF RFC 3161 (44), IETF RFC 5816 (45) i ETSI EN 319 422 (46).

W związku z tym, cechy znacznika czasu są następujące:
a) zawiera hash otrzymany w żądaniu od wnioskodawcy,
b) zawiera OID Polityki Znakowania Czasem,
c) zawiera unikalny identyfikator.

Jednostka znacznika czasu działa w bezpiecznym centrum danych QTSP, które gwarantuje prawidłową wartość czasu podaną w znaczniku czasu (zob. sekcja 6).

Zegar wewnętrzny TSU używany do wydawania znacznika czasu odpowiada dokładnemu czasowi UTC (zob. sekcja 6.8.3).

Dokładność czasu wskazanego w znaczniku czasu spełnia wymogi polityki znakowania czasem (zob. sekcja 6.8.3). Zastosowana dokładność jest również wskazana w samym znaczniku czasu (zob. sekcja 6.8.2).

TSU nie wydaje znacznika czasu jeśli wykryje, że jej zegar wewnętrzny różni się od aktualnego czasu UTC o więcej niż dopuszczalna wartość (zob. 6.8.3).

Klucze prywatne TSU nie służą do celów innych niż podpisywanie znaczników czasu (zob. 6.1.5).

Po zakończeniu okresu życia kluczy, klucz prywatny jest usuwany zgodnie z sekcją 6.3.2.

6.8.1. Żądanie znacznika czasu

Żądania znacznika czasu są zgodne z sekcją 2.4.1 IETF RFC 3161 (44) i zawierają następujące pola:

1) "reqPolicy"
2) "nonce"
3) "certReq"
4) "extensions"

QTSP akceptuje algorytmy hash w żądaniach znacznika czasu określone w ETSI TS 119 312 (35). Przy wyborze algorytmów hash QTSP bierze pod uwagę planowany okres użycia znacznika i oczekiwany okres trwałości hash. Obecnie wspierane algorytmy hash:

a) sha256 { joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) hashAlgs(2) sha256(1) }

b) sha512 { joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) hashAlgs(2) sha512(3) }

Struktura żądania znacznika czasu

1) version

Format żądania znacznika czasu odpowiada wersji “v1” określonej w IETF RFC 3161 (44), więc to pole zawiera wartość “1”.

2) MessageImprint

Dane do opatrzenia znacznikiem czasu, które składają się z dwóch części:

a) Hashing algorithm (hashAlgorithm)
OID algorytmu hash przy użyciu, którego powstał hash.

b) Hash (hashedMessage)
Wartość hash która jest podpisywana znacznikiem czasu. Długość hash odpowiada zastosowanemu algorytmowi hash.

3) identyfikator polityki znakowania czasem (reqPolicy)

Pole opcjonalne.

Wskazuje na politykę zgodnie, z którą ma zostać wydany znacznik czasu.

4) Nonce (nonce)

Opcjonalne.

Maksymalnie 64 cyfrowa wartość, która służy zapewnieniu unikalności znacznika czasu. W przypadku umieszczenia tego pola w żądaniu, odpowiedź znacznika czasu musi zawierać tą samą wartość.

5) Certificate request (certReq)

domyślnie "FALSE"

Jeśli pole zawiera wartość “TRUE”, certyfikat TSU przywołany w atrybucie “SigningCertificate” musi być umieszczony w odpowiedzi.

6) Extensions (extensions)

Opcjonalne pole.

Wnioskodawca może podać dodatkowe informacje w tym polu. QTSP wspiera tylko użycie rozszerzenia "Qualified Certificate Statements".

Jeśli przychodzące żądanie zawiera inne niż to rozszerzenie, QTSP nie wydaje znacznika czasu, zamiast tego odpowiada komunikatem błędu "unacceptedExtension".

6.8.2. Odpowiedź znacznika czasu

Odpowiedź znacznika czasu zgodnie z IETF RFC 3161 (44), sekcja 2.4.2 zawiera następujące rozszerzenia:

a) "accuracy";
b) "nonce".

W przypadku umieszczenia pola „nonce” w żądaniu znacznika czasu, odpowiedź znacznika czasu zawiera tą samą wartość.

QTSP używa zestawów algorytmów kryptograficznych i długości klucza do podpisania znacznika czasu określonych w ETSI TS 119 312 (35). Przy wyborze algorytmów kryptograficznych i długości klucza QTSP bierze pod uwagę planowany okres użycia znacznika. Obecnie wspierane algorytmy:

a) sha256WithRSAEncryption { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1)sha256WithRSAEncryption(11) }
b) sha512WithRSAEncryption { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1)sha512WithRSAEncryption(13) }
c) ecdsa-with-SHA256 { iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA256(2) }

Identyfikator używanej polityki znacznika czasu ETSI: ETSI Time Stamping profile (BTSP):

itu-t(0) identified-organization(4) etsi(0) time-stamp-policy(2023) policy-identifiers(1) baseline-tspolicy(1).

Struktura odpowiedzi znacznika czasu

1) Status (PKIStatusInfo)

Informacja o statusie sukcesu wydania znacznika zgodnie z IETF RFC 3161 (44) sekcja 2.4.2.

2) Time Stamp token (TimeStampToken)

Opcjonalne pole

Zawiera wydany znacznik czasu w przypadku wartości pola “status”: “0” lub “1”, w przeciwnym przypadku to pole nie jest zawarte w odpowiedzi.

Struktura tokena znacznika czasu

Token znacznika czasu podpisany przez TSU zgodnie z IETF RFC 3161 (44) sekcja 2.4.2, zawiera pola:

1) Version (version)

Format tokena znacznika odpowiadający wersji “v1” określonej w IETF RFC 3161 (44), więc pole zawiera wartość "1".

2) identyfikator polityki znakowania czasem (policy)

Obowiązkowe.

Wskazuje na politykę zgodnie z którą ma zostać wydany znacznik czasu.

Jeśli w żądaniu jest zawarta polityka w polu "reqPolicy", znacznik jest wydawany tylko jeśli OID wskazany w żądaniu jest wspierany, w przeciwnym wypadku żądanie jest odrzucane wraz z komunikatem o błędzie "unacceptedpolicy".

3) Message hash (messageImprint)

Dane podpisane znacznikiem czasu, dane zawierające tą samą wartość jak w żądaniu.

4) numer seryjny (serialNumber)

Obowiązkowe pole.

Unikalny numer seryjny dla każdego znacznika wydanego przez TSU. Maksymalna długość to 160 bit.

5) Time (genTime)

Obowiązkowe pole.

Czas wydania znacznika podany w formacie UTC. „genTime” jest podany z dokładnością do 1 sekundy zgodnie z RFC 5280 (22).

6) dokładność (accuracy)

Opcjonalne pole.

To pole określa dopuszczalne odchylenie czasu wskazanego w tokenie znacznika od czasu UTC. QTSP zawsze uwzględnia to pole w swoich znacznikach.

7) Ordering (ordering)

Domyślnie wartość "FALSE".

8) Nonce (nonce)

Opcjonalne pole.

Maksymalnie 64 cyfrowa wartość która służy zapewnieniu unikalności znacznika czasu. W przypadku umieszczenia tego pola w żądaniu, odpowiedź znacznika czasu musi zawierać tą samą wartość.

9) Tsa (tsa)

Opcjonalne pole.

Nazwa TSU może być umieszczona tutaj. Wtedy podana nazwa musi być taka sama jak nazwa Podmiotu znajdująca się w certyfikacie TSU, który podpisał znacznik.

10) rozszerzenia (extensions)

QTSP używa tego rozszerzenia we wszystkich znacznikach czasu. QTSP używa poniższego rozszerzenia do wskazania kwalifikowanego charakteru znacznika czasu zgodnego z eIDAS:

Qualified Certificate Statements – niekrytyczne, OID: 1.3.6.1.5.5.7.1.3

Rozszerzenie zawiera jedno oświadczenie: "esi4-qtstStatement-1" (OID: 0.4.0.19422.1.1).

6.8.3. Dokładność znacznika czasu

QTSP gwarantuje, że odchylenie czasu wskazanego w znaczniku od UTC wynosi najwyżej 1 sekundę. Zegar QTSP znajduje się w ściśle chronionym Centrum Danych, które uniemożliwia niezauważalną modyfikację zegara. QTSP nieustannie monitoruje swoje wewnętrzne systemy czasu. Jeśli odchylenie czasu wewnętrznego od UTC przekroczy 0,1 sekundy, wtedy QTSP zawiesza wydanie znacznika.

Dokładność wewnętrznego zegara QTSP jest sprawdzana każdego roku przez komisję ds. bezpieczeństwa QTSP.

6.8.4. Synchronizacja znacznika czasu

Czas wskazany w znaczniku jest podany przez wewnętrzny zegar QTSP zsynchronizowany z dwoma osobnymi źródłami Stratum-1 UTC:

a) jedno źródło czasu używa sygnału satelitarnego GPS;
b) drugie jest oparte na sygnale fal długich (DCF77).

W celu zapewnienia dokładności, QTSP synchronizuje swój własny zegar wewnętrzny z powyższymi źródłami Stratum-1 z dokładnością do 0,1 sekundy i wykonuje synchronizację przynajmniej 4 razy dziennie.

W ten sposób QTSP gwarantuje, że odchylenie czasu wskazanego w znaczniku od UTC wynosi najwyżej 1 sekundę.

6.8.4.1. Obsługa sekund przestępnych

Kiedy wystąpią sekundy przestępne, QTSP wykonuje synchronizację zegara na dany czas na podstawie uprzedniego powiadomienia kompetentnego organu zgodnie z ETSI 319 421 (17) załącznik C oraz ITU-R TF.460-6 (47).

Dodatnia sekunda przestępna występuje po 23:59:59 UTC danego dnia, po czym pomiar czasu zatrzymuje się na 1 sekundę i zostaje wznowiony następnego dnia o godzinie 00:00:00 UTC. W przypadku ujemnej sekundy przestępnej, godzina 23:59:59 UTC jest pomijana po godzinie 23:59:58 UTC danego dnia i natychmiast przychodzi godzina 00:00:00 następnego dnia.

6.8.4.2. Zmiana czasu letni-zimowy

QTSP wpisuje czas UTC do znacznika. QTSP zwraca uwagę stronom ufającym, że niektóre aplikacje mogą wyświetlać użytkownikom czas podany w znaczniku w różny sposób i w różnym formacie, zwykle używając lokalnego czasu. Może to prowadzić do nieporozumień u stron ufających w różnych strefach czasowych, szczególnie w okolicach wiosennej i jesiennej zmiany czasu.

6.8.5. Walidacja znacznika czasu

Podczas weryfikacji ważności pieczęci elektronicznej na znaczniku czasu, strona ufająca postępuje jak opisano w ETSI EN 319 102-1 (48). Podczas weryfikacji znacznika:

a) należy sprawdzić powiązanie oznakowanego dokument z znacznikiem i certyfikatem TSU;
b) podpis na znaczniku czasu powinien być zweryfikowany;
c) sprawdzić, czy znacznik czasu jest odpowiedni do danego celu, czy jego dokładność, wiarygodność i odpowiedzialność wystawcy są odpowiednie.

6.8.6. Dostępność usługi znakowania

QTSP gwarantuje nieprzerwaną dostępność usługi oraz zasad i warunków użycia znaczników czasu na poziomie co najmniej 99,9% w skali roku.

6.8.7. Wydawanie niekwalifikowanych znaczników czasu

TSU wydająca kwalifikowane znaczniki czasu zgodnie z eIDAS nie może wydawać niekwalifikowanych znaczników czasu. QTSP wydaje tylko kwalifikowane znaczniki czasu.

6.8.8. Zarządzanie kluczem TSU

Poniższe wymogi stosuje się wobec TSU:

a) algorytmy i rozmiar klucza do podpisywania znacznika czasu spełniają wymogi ETSI TS 119 312 (35);
b) jeśli możliwe, klucz prywatny TSU nie powinien być zaimportowany do wielu HSM-ów w tym samym czasie;
c) jeśli wiele HSM-ów używa tego samego klucza prywatnego, wtedy te klucze muszą należeć do jednego i tego samego certyfikatu;
d) tylko jeden klucz prywatny powinien być aktywny w TSU w danym czasie;
e) jedna jednostka sprzętowo-programowa może obsługiwać kilka różnych TSU, pod warunkiem, że powyższe wymagania są spełnione.

6.8.9. Sposoby dostępu do usługi znacznika czasu

Usługa może być użyta wyłącznie przy pomocy protokołu HTTPS. Bezpieczny kanał składa się - w zależności od sposobu uwierzytelnienia subskrybenta - z:

a) w przypadku uwierzytelnienia przy użyciu loginu i hasła, na podstawie certyfikatu TSU;
b) w przypadku identyfikacji użytkownika na podstawie certyfikatu uwierzytelnienia, zgodnie z wzajemnym uwierzytelnieniem klienta i serwera na podstawie certyfikatu klienta i serwera.

7. Profile certyfikatu, CRL i OCSP

7.1. Profil certyfikatu

Certyfikaty użytkowników końcowych wystawione przez QTSP oraz wszystkie certyfikaty główne i pośrednie dostawcy (w tym certyfikaty TSU), które znajdują się w ścieżce certyfikacyjnej używanej do wystawiania certyfikatów, są zgodne z następującymi zaleceniami i wymaganiami:

a) ITU X.509 Information technology - Open Systems Interconnection - The Directory: Public- key and attribute certificate frameworks (40);
b) IETF RFC 3739 (49);
c) IETF RFC 5280 (22);
d) IETF RFC 6818 (23);
e) IETF RFC 6962 (50);
f) ETSI EN 319 412-1 (25);
g) ETSI EN 319 412-2 (51) w przypadku certyfikatów wydanych osobom fizycznym;
h) ETSI EN 319 412-3 (52) w przypadku certyfikatów wydanych osobom prawnym;
i) ETSI EN 319 412-4 (53) w przypadku QWACs;
j) ETSI EN 319 412-5 (54);
k) ETSI TS 119 411-6 (55);
l) CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates (6);
m) Guidelines for the Issuance and Management of Extended Validation Certificates (2);
n) CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates (13).

7.1.1. Numery wersji

Certyfikaty głównej i pośredniej jednostki certyfikacyjnej (w tym certyfikat TSU) używane przez QTSP oraz Certyfikaty użytkowników końcowych wydane przez QTSP są certyfikatami w wersji "v3" zgodnie ze specyfikacją X.509 (40).

Certyfikaty mają następujące podstawowe pola:

1) Version (Wersja)

Certyfikat jest zgodny z wersją "v3" zgodnie ze specyfikacją X.509, więc w tym polu znajduje się wartość "2" (22).

2) Serial Number (Numer seryjny)

Unikalny identyfikator wygenerowany przez jednostkę certyfikacyjną wystawiającą certyfikat.

W przypadku certyfikatów użytkownika końcowego pole "Numer seryjny" zawiera losową liczbę o entropii co najmniej 8 bajtów (64 bit), wygenerowaną przez HSM zgodny z CSPRNG.

3) Algorithm Identifier (Algorytm podpisu)

Identyfikator (OID) zestawu algorytmów kryptograficznych używanych do tworzenia pieczęci elektronicznej poświadczającej certyfikat.

QTSP używa następujących algorytmów kryptograficznych:

a) "sha256WithRSAEncryption" (1.2.840.113549.1.1.11)
b) "sha384WithRSAEncryption" (1.2.840.113549.1.1.12)
c) "sha512WithRSAEncryption" (1.2.840.113549.1.1.13)
d) "ecdsa-with-SHA256" (1.2.840.10045.4.3.2)
e) "ecdsaWithSHA384" (1.2.840.10045.4.3.3)
f) "ecdsaWithSHA512" (1.2.840.10045.4.3.4)

4) Signature (Podpis)

Pieczęć elektroniczna stworzona przez QTSP poświadczająca certyfikat, która została utworzona za pomocą zestawu algorytmów zdefiniowanych w polu "Algorytm podpisu".

5) Issuer (Wystawca)

Unikalna nazwa jednostki certyfikacyjnej wystawiającej certyfikat zgodnie z formatem nazwy ITU X.501 (patrz 3.1).

6) Validity not before/not after (Ważność (ważny od & ważny do))

Początek i koniec okresu ważności certyfikatu.

Początek okresu ważności powinien być:

a) W przypadku certyfikatów dostawcy:
   - najwcześniejszy: rzeczywista data wydania minus 24h;
   - najpóźniejszy: rzeczywista data wydania.

b) W przypadku certyfikatów subskrybenta:
   - najwcześniejszy: rzeczywista data wydania minus 48 h;
   - najpóźniejszy: rzeczywista data wydania plus 48 h (QWAC).

QTSP nie stosuje datowania wstecznego.

Czas jest rejestrowany zgodnie z UTC i jest zgodny z kodowaniem IETF RFC 5280 (22).

7) Podmiot (Subject)

Unikalna nazwa podmiotu zgodnie z formatem nazwy ITU X.501 (56) (patrz 3.1). Zawsze wypełniane.

8) Identyfikator algorytmu klucza publicznego podmiotu (Subject Public Key Algorithm Identifier)

QTSP obsługuje algorytmy RSA i ECC w certyfikatach użytkowników końcowych.

Wartość, która ma być podana w tym polu:

a) "rsaEncryption" (1.2.840.113549.1.1.1)
b) "ecPublicKey" (1.2.840.10045.2.1)

9) Wartość klucza publicznego podmiotu (Subject Public Key Value)

Klucz publiczny podmiotu.

10) Unikalny identyfikator wystawcy (Issuer Unique Identifier)

Nie wypełniane.

11) Unikalny identyfikator podmiotu (Subject Unique Identifier)

Nie wypełniane.

7.1.2. Zawartość certyfikatu i rozszerzenia

QTSP korzysta wyłącznie z następujących rozszerzeń certyfikatów zgodnie ze specyfikacją X.509 (40):

Certyfikat jednostki certyfikującej root

1) **Polityki certyfikacji (Certificate Policies) – niekrytyczne**
   OID: 2.5.29.32

To pole nie występuje.

2) **Identyfikator klucza urzędu – niekrytyczne**
   OID: 2.5.29.35

Niepowtarzalny identyfikator klucza dostawcy o długości 40 znaków używany do pieczęci elektronicznej poświadczającej certyfikat.

Wartość pola: skrót SHA-1 klucza publicznego dostawcy.

Wypełnienie jest obowiązkowe.

W przypadku certyfikatu głównej jednostki certyfikacyjnej root wartość ta jest identyczna z wartością pola Identyfikatora klucza podmiotu.

3) **Identyfikator klucza podmiotu – niekrytyczne**
   OID: 2.5.29.14

Niepowtarzalny identyfikator klucza publicznego podmiotu o długości 40 znaków. Wartość pola: skrót SHA-1 klucza publicznego Podmiotu.

Zawsze wypełnione.

4) **Alternatywne nazwy podmiotu – niekrytyczne**
   OID: 2.5.29.17

Wypełnienie jest opcjonalne.

Wypełnia się zgodnie z sekcją 3.1.1.

5) **Podstawowe ograniczenia – krytyczne**
   OID: 2.5.29.19

Określenie czy certyfikat został wydany jednostce certyfikacyjnej. Rozszerzenie jest wymagane, a jego wartość to: CA = "TRUE".

Pole "pathLenConstraint" nie jest obecne w certyfikacie typu root.

6) **Użycie klucza – krytyczne**
   OID: 2.5.29.15

Określenie dozwolonego zakresu użycia klucza. Pole jest obowiązkowe, a używane wartości to:
   a) "keyCertSign",
   b) "cRLSign".

7) **Rozszerzone użycie klucza – niekrytyczne**
   OID: 2.5.29.37

Dodatkowy zakres użycia klucza. Pole nie występuje.

Powyższe pola są zawsze wypełniane. Nie ma więcej rozszerzeń certyfikatu.

Certyfikat Pośredniej Jednostki Certyfikującej

1) **Polityki certyfikacji – niekrytyczne**
   OID: 2.5.29.32

To pole może ograniczyć Polityki Certyfikacji, które mogą być używane do wystawiania certyfikatów użytkownika końcowego.

Pośrednie jednostki certyfikacji mogą wystawiać tylko tego typu certyfikaty użytkowników końcowych, które pasują do co najmniej jednej z wymienionych tutaj polityk certyfikacji.

Zawsze wypełniane.

W przypadku Certyfikatów wydawanych pośrednim jednostkom certyfikacyjnym QTSP, w tym polu może znajdować się Identyfikator "anyPolicy".

W tym polu można podać odniesienie do KPC powiązanego z Polityką Certyfikacji na podstawie której wydano certyfikat. W przypadku certyfikatów jednostki certyfikacyjnej wydanych innemu urzędowi certyfikacji, w tym polu może znajdować się tylko ten identyfikator, który odnosi się do polityki certyfikacji wdrożonej przez ten wystawiający urząd certyfikacji i nie musi to być identyfikator "anyPolicy".

2) **Identyfikator klucza urzędu – niekrytyczne**
   OID: 2.5.29.35

Niepowtarzalny identyfikator klucza dostawcy o długości 40 znaków używany do pieczęci elektronicznej poświadczającej certyfikat. Pole zawsze wypełniane.

Wartość pola: skrót SHA-1 klucza publicznego dostawcy.

3) **Identyfikator klucza podmiotu – niekrytyczne**
   OID: 2.5.29.14

Unikalny identyfikator klucza publicznego podmiotu o długości 40 znaków.

Wartość pola: skrót SHA-1 klucza publicznego Podmiotu.

Zawsze wypełnione.

4) **Alternatywne nazwy podmiotu – niekrytyczne**
   OID: 2.5.29.17

Wypełnienie jest opcjonalne. Wypełnia się go zgodnie z sekcją 3.1.1.

5) **Podstawowe ograniczenia – krytyczne**
   OID: 2.5.29.19

Określenie czy certyfikat został wydany jednostce certyfikującej. Rozszerzenie jest wymagane, a jego wartość to: CA = "TRUE".

Pole "pathLenConstraint" nie jest obecne w Certyfikacie.

6) **Użycie klucza – krytyczne**
   OID: 2.5.29.15

Określenie dozwolonego zakresu użycia klucza.

Pole zawiera następujące wartości:

a) "keyCertSign",
b) "cRLSign".

7) **Rozszerzone użycie klucza – niekrytyczne**
   OID: 2.5.29.37

Dodatkowy zakres użycia klucza.

Certyfikaty pośrednich jednostek certyfikacyjnych nie zawierają pola "Rozszerzone użycie klucza".

Certyfikat TSU do wystawiania znaczników czasu zawiera wartość:

- Time stamping (1.3.6.1.5.5.7.3.8)

8) **Punkty dystrybucji list CRL – niekrytyczne**
   OID: 2.5.29.31

Pole zawiera dostępność list CRL za pośrednictwem protokołu http.

Zawsze wypełniane.

9) **Dostęp do informacji o urzędzie – niekrytyczne**
   OID: 1.3.6.1.5.5.7.1.1

Określenie pozostałych usług związanych z korzystaniem z certyfikatu.

Pole jest obowiązkowe i zawiera następujące dane:

a) W celu szybkiej i rzetelnej weryfikacji aktualnego statusu unieważnienia certyfikatu, QTSP świadczy usługę statusu certyfikatu online. Dostępność tej usługi jest wskazana tutaj.
b) Aby ułatwić budowanie ścieżki certyfikacyjnej, QTSP udostępnia ścieżkę dostępu poprzez protokół http do certyfikatu jednostki certyfikacyjnej wystawiającej certyfikat.

Powyższe pola są zawsze wypełniane. Nie występują inne rozszerzenia certyfikatów.

Certyfikat użytkownika końcowego

1) Polityki certyfikacji – niekrytyczne
OID: 2.5.29.32

To pole zawiera nazwę ważnej polityki certyfikacji (patrz sekcja 1.2.1) w momencie wystawiania certyfikatu oraz inne informacje na temat innych zastosowań certyfikatu.

W przypadku certyfikatów użytkowników końcowych, QTSP zawsze wstawia w tym polu następujące dane:

a) identyfikator polityki certyfikacji (OID zgodnie z sekcją 1.2.1);
b) dostępność KPC;
c) ostrzeżenie tekstowe w języku angielskim i polskim[5], na podstawie którego można ustalić, że:
   - certyfikat jest kwalifikowany;
   - klucz prywatny związany z certyfikatem jest chroniony przez QSCD (wyłącznie w przypadku polityki certyfikacji wymagającej QSCD);
   - okres archiwizacji danych związanych z certyfikatem.
d) Identyfikator (OID) polityki certyfikacji określony w ETSI EN 319 411-2 (14), z którą certyfikat jest zgodny, w następujący sposób:
   - QCP-n: polityka dla kwalifikowanych certyfikatów UE dla osób fizycznych, OID: 0.4.0.194112.1.0;
   - QCP-l: polityka dla kwalifikowanych certyfikatów UE dla osób prawnych, OID: 0.4.0.194112.1.1;
   - QCP-l-qscd: polityka dla kwalifikowanych certyfikatów UE dla osób prawnych, gdzie klucz prywatny i certyfikat znajdują się na QSCD, OID: 0.4.0.194112.1.3;
   - QCP-n-qscd: polityka dla kwalifikowanych certyfikatów UE dla osób fizycznych, gdzie klucz prywatny i certyfikat znajdują się na QSCD, OID: 0.4.0.194112.1.2;
   - NCP+ (OID 0.4.0.2042.1.2) w przypadku certyfikatów wydanych na niekwalifikowanym SCDev;
   - w przypadku zwykłego certyfikatu uwierzytelniania witryn: QEVCP-w: polityka dla kwalifikowanych certyfikatów UE uwierzytelniania witryn dla osób fizycznych i prawnych i przyporządkowująca daną witrynę do danej osoby OID 0.4.0.194112.1.4;
   - w przypadku certyfikatów Open Banking: QEVCP-w: polityka dla kwalifikowanych certyfikatów UE uwierzytelniania witryn dla osób fizycznych i prawnych i przyporządkowująca daną witrynę do danej osoby OID 0.4.0.194112.1.4;
   - w przypadku certyfikatów PSD2: QCP-w-psd2: polityka certyfikacji dla kwalifikowanych certyfikatów uwierzytelniania witryn PSD2; OID: 0.4.0.19495.3.1.
e) Polityka certyfikacyjna zdefiniowana przez CA/Browser Forum w następujący sposób:

[5] Ta sama informacja jest również zawarta w formacie odczytywanym maszynowo w rozszerzeniu Qualified Certificate Statements również umieszczonym w certyfikacie.

- w przypadku certyfikatu uwierzytelniania witryn: EVCP określona w CA/Browser Forum OID 2.23.140.1.1.
- w przypadku certyfikatów Email (S/MIME) polityka certyfikacji zdefiniowana przez CA/Browser Forum:
  - ✓ w przypadku certyfikatów Organization-validated OID 2.23.140.1.5.2.3
  - ✓ w przypadku certyfikatów Sponsor-validated OID 2.23.140.1.5.3.3

We wszystkich przypadkach certyfikatów użytkowników końcowych należy wskazać co najmniej jedną politykę certyfikacyjną zgodnie z którą został wystawiony certyfikat. Co najmniej jeden taki identyfikator polityki certyfikacji (OID) i związany z polityką KPC (URL) są wskazywane w certyfikatach wydanych przez QTSP.

Certyfikaty użytkowników końcowych, które nie zawierają pola "Polityki certyfikacji", uznaje się za certyfikaty testowe. Certyfikat testowy może być używany wyłącznie do celów testowych i zostanie odrzucony w przypadku rzeczywistych transakcji.

W tym polu można podać odniesienie do powiązanego KPC.

2) **Identyfikator klucza urzędu– niekrytyczne**
   OID: 2.5.29.35

Niepowtarzalny identyfikator klucza dostawcy o długości 40 znaków używany do pieczęci elektronicznej poświadczającej certyfikat.

Wypełnienie jest obowiązkowe.

Wartość pola: skrót SHA-1 klucza publicznego dostawcy.

3) **Identyfikator klucza podmiotu – niekrytyczne**
   OID: 2.5.29.14

Unikalny identyfikator klucza publicznego podmiotu o długości 40 znaków.

Wartość pola: skrót SHA-1 klucza publicznego Podmiotu.

Zawsze wypełnione.

4) **Alternatywne nazwy podmiotu – niekrytyczne**
   OID: 2.5.29.17

Zob. sekcja: 3.1.1.

5) **Podstawowe ograniczenia – krytyczne**
   OID: 2.5.29.19

Określenie, czy certyfikat został wydany jednostce certyfikującej. Domyślna wartość rozszerzenia to: CA = "FALSE", zatem to pole nie jest obecne w certyfikatach użytkownika końcowego.

Pole "pathLenConstraint" nie jest obecne.

6) **Użycie klucza – krytyczne**
   OID: 2.5.29.15

Wskazanie zakresu dozwolonego użycia klucza.

W przypadku certyfikatów użytkownika końcowego do podpisu elektronicznego (pieczęci) pole jest obowiązkowe, a wartość jest ustawiona wyłącznie na następujące wartości:

- "nonRepudiation".

Dla certyfikatu do uwierzytelniania witryny internetowej dozwolone są wyłącznie następujące wartości:

Obowiązkowe:

- "digitalSignature"

Opcjonalne:

- w przypadku RSA "keyEncipherment",
- w przypadku ECC "keyAgreement".

Te same wartości użycia klucza są używane w certyfikatach uwierzytelniania serwera, takich jak serwer VPN CISCO, kontroler domeny lub certyfikatach uwierzytelniania serwera sieci VPN.

W przypadku certyfikatów Email (S/MIME):

- "nonRepudiation"
- "digitalSignature"

7) **Rozszerzone użycie klucza – niekrytyczne**
   OID: 2.5.29.37

Dodatkowy zakres użycia klucza.

Opcjonalna wartość dla kwalifikowanych certyfikatów do podpisu lub pieczęci:

- "Document Signing (1.3.6.1.4.1.311.10.3.12)"

Dla certyfikatów Email (S/MIME) obowiązkowa wartość:

- "emailProtection (1.3.6.1.5.5.7.3.4)".

W certyfikatach uwierzytelniania witryn internetowych obowiązkową wartością jest:

- "serverAuth (1.3.6.1.5.5.7.3.1)".

W certyfikatach uwierzytelniania witryny domyślnie ustawiono następującą dodatkową wartość, ale można ją też pominąć na żądania Wnioskodawcy:

- "clientAuth (1.3.6.1.5.5.7.3.2)".

8) **Punkty dystrybucji list CRL – niekrytyczne**
   OID: 2.5.29.31

Pole zawiera dostępność list CRL związanych z certyfikatem, za pośrednictwem protokołu http. W tym polu znajduje się (w formie adresu URL) dostępność list CRL związanych z certyfikatem

Obowiązkowe w przypadku certyfikatów użytkownika końcowego.

9) **Dostęp do informacji o urzędzie – niekrytyczne**
OID: 1.3.6.1.5.5.7.1.1

Określenie pozostałych usług związanych z korzystaniem z certyfikatu.

W przypadku certyfikatu użytkownika końcowego pole zawiera następujące dane:

a) W celu szybkiej i rzetelnej weryfikacji aktualnego statusu unieważnienia certyfikatu, QTSP świadczy usługę statusu certyfikatu online, której dostępność jest wskazana w tym polu.
b) Aby ułatwić budowanie ścieżki certyfikacyjnej, QTSP udostępnia ścieżkę dostępu poprzez protokół http do certyfikatu jednostki certyfikacyjnej wystawiającej certyfikat.

QTSP może podać w tym polu dane więcej niż jednej usługi i certyfikatu jednostki certyfikującej wystawiającej certyfikat.

10) **Qualified Certificate Statements – niekrytyczne**
OID: 1.3.6.1.5.5.7.1.3

Pole jest przeznaczone do wskazywania oświadczeń związanych z certyfikatami kwalifikowanymi, ale może być użyte również w przypadku certyfikatu niekwalifikowanego.

Na życzenie Klienta certyfikat użytkownika końcowego może zawierać opcjonalne oświadczenie opisujące dane podmiotu dotyczące Open Banking lub Dyrektywy w sprawie Usług Płatniczych UE (PSD2) (24) (OID: 0.4.0.19495.2). W takim wypadku w polu umieszcza się: rodzaj usługi PSD2 podmiotu oraz nazwę i skrót organu nadzorczego nadzorującego usługę finansową podmiotu.

W każdym innym przypadku pole nie występuje.

Każdy certyfikat końcowy zawiera następujące oświadczenia:

a) certyfikat jest kwalifikowanym certyfikatem UE: ’id-etsi-qcs 1’ (0.4.0.1862.1.1);
b) limit transakcyjny z wykorzystaniem certyfikatu: ’id-etsi-qcs 2’ (0.4.0.1862.1.2), opcjonalne;
c) oświadczenie, że QTSP zatrzymuje dane rejestracyjne związane z certyfikatem przez 20 lat od wygaśnięcia certyfikatu: ’id-etsi-qcs 3’ (0.4.0.1862.1.3);
d) oświadczenie, że klucz prywatny związany z certyfikatem znajduje się na QSCD: ’id-etsi-qcs 4’ (0.4.0.1862.1.4), tylko w przypadku polityki certyfikacji wymagającej QSCD;
e) dostępność dokumentu zawierającego skróconą wersję KPC: ’id-etsi-qcs 5’ (0.4.0.1862.1.5);
f) wskazanie, że certyfikat służy do podpisu: ’id-etsi-qct-esign’ (0.4.0.1862.1.6.1);
g) wskazanie, że certyfikat służy do pieczęci: ’id-etsi-qct-eseal’ (0.4.0.1862.1.6.2);
h) wskazanie, że certyfikat służy do uwierzytelniania witryn: ’id-etsi-qct-web’ (0.4.0.1862.1.6.3).

Żadne inne rozszerzenia certyfikatów nie są wypełniane.

Certyfikat urzędu znacznika czasu

1) **Polityki certyfikacji – niekrytyczne**
OID: 2.5.29.32

To pole zawiera identyfikator aktualnej polityki certyfikacyjnej w momencie wystawiania i używania certyfikatu urzędu znacznika czasu oraz inne informacje na temat innych zastosowań certyfikatu.

Wypełnienie pola jest obowiązkowe i pole nie może być krytyczne.

Odniesienie do powiązanego KPC związanego z Polityką można podać w tym polu.

2) **Identyfikator klucza urzędu – niekrytyczne**
   OID: 2.5.29.35

Niepowtarzalny identyfikator klucza dostawcy o długości 40 znaków używany do pieczęci elektronicznej poświadczającej certyfikat.

Wartość pola: skrót SHA-1 klucza publicznego dostawcy.

3) **Identyfikator klucza podmiotu – niekrytyczne**
   OID: 2.5.29.14

Niepowtarzalny identyfikator klucza publicznego urzędu znacznika czasu o długości 40 znaków. Wartość pola: skrót SHA-1 klucza publicznego.

4) **Alternatywne nazwy podmiotu– niekrytyczne**
   OID: 2.5.29.17

Centralny adres e-mail QTSP usług znacznika czasu może znajdować się w tym polu.

5) **Podstawowe ograniczenia – krytyczne**
   OID: 2.5.29.19

Określenie czy certyfikat został wydany jednostce certyfikacyjnej.

Domyślna wartość rozszerzenia to: CA = "FALSE", więc to pole nie jest obecne w certyfikacie wystawionym dla urzędu znacznika czasu.

Pole "pathLenConstraint" nie jest obecne w Certyfikacie wystawionym dla urzędu znacznika czasu.

6) **Użycie klucza – krytyczne**
   OID: 2.5.29.15

Określenie dozwolonego zakresu użycia klucza.

W certyfikatach wystawionych dla urzędu znacznika czasu występują tylko następujące wartości:

- "nonRepudiation",
- "digitalSignature".

7) **Okres użycia klucza prywatnego– niekrytyczne**
   OID: 2.5.29.16

Określenie dozwolonego okresu użycia klucza prywatnego.

W certyfikatach wystawionych urzędowi znacznika czasu, urząd certyfikacji ogranicza czas użycia klucza prywatnego, ustawiając wartości "notBefore" i "notAfter".

8) **Rozszerzone użycie klucza – krytyczne**
   OID: 2.5.29.37

Dodatkowy zakres użycia klucza. W certyfikatach urzędu znacznika czasu występują tylko następujące wartości:

- "timeStamping (1.3.6.1.5.5.7.3.8)".

9) **Punkty dystrybucji list CRL – niekrytyczne**
   OID: 2.5.29.31

Pole zawiera dostępność list CRL związanych z certyfikatem za pośrednictwem protokołu http.

Obowiązkowe do wypełnienia.

10) **Dostęp do informacji o urzędzie – niekrytyczne**
    OID: 1.3.6.1.5.5.7.1.1

Określenie innych usług związanych z korzystaniem z certyfikatu urzędu znacznika czasu świadczonych przez QTSP. Obowiązkowe pole, zawiera następujące dane:

a) W celu szybkiej i rzetelnej weryfikacji aktualnego statusu unieważnienia certyfikatu, QTSP świadczy usługę statusu certyfikatu online. Dostępność tej usługi jest wskazana tutaj.
b) Aby ułatwić budowanie ścieżki certyfikacyjnej, QTSP udostępnia ścieżkę dostępu poprzez protokół http do certyfikatu jednostki certyfikacyjnej wystawiającej certyfikat.

Powyższe pola są zawsze wypełniane zgodnie z podanymi zasadami. Nie ma więcej rozszerzeń certyfikatów.

Certyfikaty wydane dla OCSP responder

1) **Polityki certyfikacji – niekrytyczne**
   OID: 2.5.29.32

To pole zawiera identyfikator aktualnej polityki certyfikacyjnej (patrz sekcja 1.2.2) w momencie wystawiania i używania certyfikatu OCSP Responder oraz inne informacje na temat innych zastosowań certyfikatu.

Wypełnienie pola jest opcjonalne i pole nie może być krytyczne.

W tym polu można podać odniesienie do powiązanego KPC.

2) **Identyfikator klucza urzędu – niekrytyczne**
   OID: 2.5.29.35

Niepowtarzalny identyfikator klucza dostawcy o długości 40 znaków używany do pieczęci elektronicznej poświadczającej certyfikat.

Wartość pola: skrót SHA-1 klucza publicznego dostawcy. Zawsze wypełniane.

3) **Identyfikator klucza podmiotu – niekrytyczne**
   OID: 2.5.29.14

Niepowtarzalny identyfikator klucza publicznego OCSP Responder o długości 40 znaków. Wartość pola: skrót SHA-1 klucza publicznego. Zawsze wypełniane.

4) **Alternatywne nazwy podmiotu – niekrytyczne**
   OID: 2.5.29.17

Nigdy niewypełniane.

5) **Podstawowe ograniczenia – krytyczne**
   OID: 2.5.29.19

Określenie czy certyfikat został wydany jednostce certyfikującej.

Domyślna wartość rozszerzenia to: CA = "FALSE", więc to pole nie jest obecne w certyfikacie wystawionym dla OCSP Responder.

Pole "pathLenConstraint" nie jest obecne w Certyfikacie wystawionym dla OCSP Responder.

6) **Użycie klucza – krytyczne**
   OID: 2.5.29.15

Określenie dozwolonego zakresu użycia klucza.

W certyfikatach wystawionych dla OCSP Responder występują wyłącznie następujące wartości:

- "digitalSignature".

7) **Okres użycia klucza prywatnego – niekrytyczne**
   OID: 2.5.29.16

Określenia dopuszczalnego okresu użycia klucza prywatnego.

Nie wypełnia się.

8) **Rozszerzone użycie klucza – krytyczne**
   OID: 2.5.29.37

Dodatkowy zakres użycia klucza. W certyfikatach wystawionych dla OCSP Responder występują tylko następujące wartości:

- "OCSP Signing (1.3.6.1.5.5.7.3.9)".

9) **Punkty dystrybucji list CRL – niekrytyczne**
   OID: 2.5.29.31

Pole zawiera dostępność list CRL związanych z certyfikatem za pośrednictwem protokołu http.

Obowiązkowe do wypełnienia.

10) **Dostęp do informacji o urzędzie – niekrytyczne**
    OID: 1.3.6.1.5.5.7.1.1

Określenie innych usług związanych z korzystaniem z certyfikatu OCSP Responder świadczonych przez TSP. Obowiązkowe pole, zawiera następujące dane:

- Aby ułatwić budowanie ścieżki certyfikacyjnej, QTSP udostępnia ścieżkę dostępu poprzez protokół http do certyfikatu jednostki certyfikacyjnej wystawiającej certyfikat;
- W celu szybkiej i wiarygodnej weryfikacji aktualnego statusu unieważnienia certyfikatu, Dostawca Usług świadczy usługę statusu certyfikatu online. Dostępność tej usługi jest wskazana tutaj.

Powyższe pola są zawsze wypełniane zgodnie z podanymi zasadami. Nie ma więcej rozszerzeń certyfikatów.

7.1.3. Identyfikatory algorytmów

Nazwa algorytmu kryptograficznego użytego do poświadczenia certyfikatu. QTSP używa następujących algorytmów kryptograficznych do pieczętowania certyfikatów użytkowników końcowych:

a) "sha256WithRSAEncryption" (1.2.840.113549.1.1.11)
b) "sha384WithRSAEncryption" (1.2.840.113549.1.1.12)
c) "sha512WithRSAEncryption" (1.2.840.113549.1.1.13)
d) "ecdsa-with-SHA256" (1.2.840.10045.4.3.2)
e) "ecdsaWithSHA384" (1.2.840.10045.4.3.3)
f) "ecdsaWithSHA512" (1.2.840.10045.4.3.4)

7.1.4. Formy nazw

QTSP posługuje się nazwą wyróżniającą „DN” – złożoną z atrybutów zdefiniowanych w standardach: IETF RFC 5280 (22), ETSI EN 319 412-2 (51), ETSI EN 319 412-3 (52) i ETSI EN 319 412-4 (53) – w celu identyfikacji Podmiotu w certyfikatach wydanych na podstawie niniejszego dokumentu.

Certyfikat zawiera globalnie niepowtarzalny identyfikator podmiotu (OID), wypełniony zgodnie z zasadami w sekcji 3.1.1.

Wartość w polu "Nazwa wyróżniająca wystawcy" ("Issuer DN") certyfikatu jest identyczna z wartością w polu "Nazwa wyróżniająca podmiotu" ("Subject DN") Certyfikatu wystawcy.

7.1.5. Ograniczenia dotyczące nazwy

QTSP nie stosuje ograniczeń nazwy z wykorzystaniem pola "nameConstraints".

7.1.6. Identyfikator polityki certyfikacyjnej

QTSP zawiera w Certyfikatach rozszerzenie niekrytyczne (CertificatePolicies) zgodnie z wymaganiami sekcji 7.1.2.

7.1.7. Stosowanie rozszerzenia określającego ograniczenia nakładane na politykę

Nie przewidziano

7.1.8. Składnia i semantyka kwalifikatorów polityki

QTSP może umieścić krótkie informacje związane z użyciem certyfikatu (kwalifikatory polityki certyfikacji) w polu certificatePolicies (policyInformation). Pole zawiera dostępność KPC on-line (URI).

7.1.9. Przetwarzanie semantyki krytycznych rozszerzeń polityki certyfikacyjnej

Nie przewidziano

7.2. Profil CRL

7.2.1. Numer(y) wersji

QTSP wystawia listy unieważnionych certyfikatów w wersji "v2" zgodnie ze specyfikacją IETF RFC 5280 (22).

7.2.2. Listy CRL i rozszerzenia wpisów list CRL

Listy unieważnionych certyfikatów wydane przez QTSP obowiązkowo zawierają następujące pola:

1) tbsCertList

Pole zawiera informacje o wystawcy, ważność i inne informacje, jak również listę unieważnionych certyfikatów.

Całe pole jest podpisane kluczem prywatnym dostawcy.

a) Wersja (Version)

Dla CRL w wersji “v2” zgodnie z IETF RFC 5280 (22), wartością pola jest obowiązkowo "1".

b) Podpis (Signature)

Identyfikator algorytmu podpisującego użytego przez jednostkę certyfikacyjną podczas wydawania certyfikatu. Ten sam co identyfikator algorytmu użyty do podpisania CRL (zob. signatureAlgorithm).

c) Wystawca

Niepowtarzalna nazwa wystawcy listy CRL (wartość pola DN certyfikatu wystawcy).

d) Data wprowadzenia (thisUpdate)

Data wejścia w życie listy CRL. Wartość UTC z kodowaniem „UTCTime” zgodnie z IETF RFC 5280 (22). W przypadku list CRL wystawionych przez QTSP jest to taki sam czas jak czas wystawienia.

e) Następna aktualizacja (nextUpdate)

Czas wystawienia następnej listy CRL (patrz sekcja 4.10). Wartość UTC zgodna z kodowaniem „UTCTime” zgodnie z IETF RFC 5280 (22).

f) Certyfikaty unieważnione

Lista zawieszonych lub unieważnionych certyfikatów uszeregowanych w rosnącej kolejności według numeru seryjnego certyfikatu. Jeśli nie ma żadnych certyfikatów unieważnionych lub zawieszonych, to pole nie jest zawarte w CRL.

Obowiązkowe pola dla wszystkich wpisów:

- Numer seryjny certyfikatu (CertificateSerialNumber)
  Unikalny identyfikator certyfikatu wygenerowany przez Urząd Certyfikacji (składający się z cyfr)
- Data unieważnienia (revocationDate)
  Wartość UTC zgodna z kodowaniem „UTCTime” zgodnie z IETF RFC 5280 (22).

Opcjonalne rozszerzenia list CRL (crlEntryExtensions), które mogą być używane przez QTSP:

- Powód unieważnienia (reasonCode) – niekrytyczne OID: 2.5.29.21
  W tym polu podaje się powód unieważnienia.
  Obowiązkowe w przypadku pośrednich jednostek certyfikacji.
  W przypadku certyfikatów zawieszonych to pole jest obowiązkowe, jego wartość to: "certificateHold (6)".

g) Rozszerzenia CRL

- Identyfikator klucza dostawcy (AuthorityKeyIdentifier) OID: 2.5.29.35
  Identyfikator klucza publicznego który należy do klucza prywatnego używanego do podpisywania CRL, w formie hash SHA1.
- Numer seryjny listy CRL (cRLNumber) – niekrytyczne OID: 2.5.29.20
  Zawiera kolejne numery seryjne list CRL.

Poniższe rozszerzenie może być (pod pewnymi warunkami) używane przez QTSP:

- Wygasłe certyfikaty na liście CRL (expiredCertsOnCRL) – niekrytyczne OID: 2.5.29.60
  Wskazanie, zgodnie ze specyfikacją X.509, że QTSP nie usuwa wygasłych certyfikatów z listy CRL. (Patrz punkt 4.10).

2) Identyfikator algorytmu podpisu (signatureAlgorithm)

Identyfikator (OID) zestawu algorytmów kryptograficznych używanego do tworzenia pieczęci elektronicznej poświadczającej listę CRL. Nazwa i OID algorytmów kryptograficznych stosowanych przez QTSP:

a) "sha256WithRSAEncryption" (1.2.840.113549.1.1.11)
b) "sha384WithRSAEncryption" (1.2.840.113549.1.1.12)
c) "sha512WithRSAEncryption" (1.2.840.113549.1.1.13)

d) "ecdsa-with-SHA256" (1.2.840.10045.4.3.2)
e) "ecdsaWithSHA384" (1.2.840.10045.4.3.3)
f) "ecdsaWithSHA512" (1.2.840.10045.4.3.4)

3) Podpis (signatureValue)

Pieczęć elektroniczna QTSP poświadczająca listę unieważnionych certyfikatów. Dana jednostka certyfikująca poświadcza CRL za pomocą klucza używanego do podpisywania certyfikatów.

QTSP nie jest zobowiązany do wypełniania rozszerzeń.

7.3. Profil OCSP

QTSP prowadzi usługę statusu certyfikatów online zgodnie ze standardem IETF RFC 6960 (32) i IETF RFC 8954 (57).

Odpowiedzi OCSP wystawione przez QTSP zawierają następujące pola:

1) Identyfikator algorytmu (signatureAlgorithm)

Identyfikator algorytmu kryptograficznego używanego do podpisywania odpowiedzi OCSP (OID). QTSP stosuje następujące algorytmy kryptograficzne:

a) "sha256WithRSAEncryption" (1.2.840.113549.1.1.11)
b) "sha384WithRSAEncryption" (1.2.840.113549.1.1.12)
c) "sha512WithRSAEncryption" (1.2.840.113549.1.1.13)
d) "ecdsa-with-SHA256" (1.2.840.10045.4.3.2)
e) "ecdsaWithSHA384" (1.2.840.10045.4.3.3)
f) "ecdsaWithSHA512" (1.2.840.10045.4.3.4)

2) Podpis (Signature)

Podpis elektroniczny lub pieczęć elektroniczna QTSP.

3) Identyfikator OCSP Respondera (responderID)

Niepowtarzalny identyfikator OCSP Respondera, który wystawia odpowiedzi OCSP.

4) Data wprowadzenia (thisUpdate)

Data wejścia w życie odpowiedzi OCSP. Wartość UTC z kodowaniem zgodnym z IETF RFC 5280 (22).

5) Następna aktualizacja (nextUpdate)

Najpóźniejszy czas wydania następnej odpowiedzi OCSP. Wartość UTC z kodowaniem zgodnym z IETF RFC 5280 (22). Opcjonalna wartość. W przypadku certyfikatów uwierzytelniania witryny - obowiązkowa. Wartość jest równa czasowi wystawienia + 12 godzin.

6) Odpowiedź dotycząca statusu certyfikatu (SingleResponse)

Pole zawiera identyfikator certyfikatu (CertID) i status unieważnienia certyfikatu (CertStatus).

QTSP wydaje pozytywną odpowiedź OCSP zgodnie z wymaganiami CABF BR. Odpowiedź zawiera wartość "good" tylko wtedy, gdy certyfikat znajduje się w Repozytorium Certyfikatów QTSP, a jego status nie jest zawieszony ani unieważniony.

7.3.1. Numer wersji

QTSP obsługuje żądania i odpowiedzi dotyczące statusu certyfikatu online zgodne z wersją "v1", zgodnie ze standardem IETF RFC 6960 (32). Domyślna wartość pola (Wersja) to "v1", zatem to pole nie jest uwzględniane w odpowiedzi OCSP.

7.3.2. Rozszerzenia OCSP

QTSP może opcjonalnie umieścić następujące rozszerzenie OCSP:

1) ArchiveCutoff – niekrytyczne

QTSP może wskazać za pomocą standardowej notacji zgodnie ze specyfikacją IETF RFC 6960 (32), że zachowuje informacje o unieważnieniu po wygaśnięciu certyfikatu. (Patrz punkt 4.10).

QTSP może opcjonalnie umieścić następujące rozszerzenie OCSP:

2) Kod przyczyny (reasonCode) – niekrytyczne

W tym polu należy wskazać powód unieważnienia.

Obowiązkowe w przypadku pośrednich jednostek certyfikacji.

W przypadku certyfikatów zawieszonych to pole jest obowiązkowe, a jego wartość to: “certificateHold (6)”.

7.4. Profil znacznika czasu

Profil znacznika czasu spełnia wymogi IETF RFC 3161 (44) i IETF RFC 5816 (45). Profil znacznika opisano w sekcji 6.8.

8. Audyt zgodności i inne rodzaje oceny

QTSP zleca audyt swojej działalności zewnętrznemu audytorowi i przedkłada szczegółowy raport z oceny zgodności z audytem do Organu Nadzoru w ciągu trzech dni roboczych od jego otrzymania. Audytor przeprowadza kompleksową kontrolę na miejscu w siedzibie QTSP co najmniej raz w roku. Przegląd ma na celu ustalenie, czy działalność QTSP jest zgodna z wymogami określonymi w rozporządzeniu eIDAS, a także z wymogami odpowiednich Polityk Certyfikacji i Kodeksów Postępowania Certyfikacyjnego.

Zakres i metodologia oceny zgodności są zgodne z następującymi dokumentami normatywnymi:

1) ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO i RADY (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające Dyrektywę 1999/93/WE (1);
2) ETSI EN 319 403-1 Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 1: Requirements for conformity assessment bodies assessing Trust Service Providers (58);
3) ETSI EN 319 401; Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers (59);
4) ETSI EN 319 411-1; Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements (15);
5) ETSI EN 319 411-2 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates (15);

6) ETSI TS 119 411-6 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 6: Requirements for Trust Service Providers issuing publicly trusted S/MIME certificates; (55);
7) ETSI EN 319 421 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time Stamps (17);
8) ETSI TS 119 431-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev (12);
9) ETSI TS 119 461 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects (60).

Wynikiem kontroli jest poufny dokument dostępny tylko dla upoważnionych osób.

Certyfikat zgodności wydany zgodnie ze sprawozdaniem z oceny zgodności publikowany jest na stronie internetowej QTSP.

Przy świadczeniu usług, QTSP stosuje przetestowane i certyfikowane elementy (produkty podpisu elektronicznego, elementy systemu IT itd.).

Aktualna lista QSCD używanych przez QTSP i informacje dotyczące ich certyfikacji znajdują się na stronie: https://eurocert.pl/lista-bezpiecznych-urzadzen-qscd/.

Informacyjna pełna lista QSCD znajduje się na stronie Komisji UE[6].

Przed użyciem QSCD, QTSP upewnia się, czy posiada ono ważną certyfikację, która spełnia aktualne wymagania.

QTSP zarządza QSCD w ciągu ich całego cyklu życia zgodnie z wymaganiami dołączonymi do certyfikatu urządzenia.

QTSP oferuje usługę zdalnego podpisu przy użyciu następującego QSCD do zarządzania kluczami użytkowników:

- Produkt: Cryptomathic Signer, version 4.8
- Developer: Cryptomathic A/S, Jægergårdsgade 118, 8000 Aarhus C, Denmark
- Certifier: A-SIT
- Certificate reference: A-SIT-VIG-19-052
- web: https://www.a-sit.at/downloads/1164
- The Qualified Electronic Signature Creation Device is Common Criteria certified on assurance level EAL4+, augmented by AVA_VAN.5

QTSP monitoruje status certyfikacji używanych QSCD przynajmniej do końca okresu ważności ostatniego certyfikatu wydanego na tych QSCD i podejmuje odpowiednie środki w przypadku zmiany tego statusu.

W przypadku unieważnienia certyfikacji QSCD, QTSP unieważnia wszystkie ważne certyfikaty wydane na tych QSCD, które zawierają oświadczenie „id-etsi-qcs 4" (zob. 7.1.2).

QTSP ocenił każdy z elementów systemu wykorzystywanych do świadczenia usług według klas bezpieczeństwa na podstawie swojego systemu oceny ryzyka. QTSP prowadzi ewidencję elementów systemu oraz związanych z nimi klas bezpieczeństwa w ramach swojego systemu zarządzania ryzykiem.

[6] https://eidas.ec.europa.eu/efda/browse/notification/qscd-sscd

Oprócz audytu zewnętrznego QTSP posiada również własny system kontroli wewnętrznej, za pomocą którego regularnie sprawdza zgodność z poprzednimi audytami i podejmuje niezbędne kroki w przypadku nieprawidłowości.

8.1. Częstotliwość i okoliczności oceny

QTSP przeprowadza raz do roku zewnętrzny audyt oceny zgodności swojego systemu informatycznego świadczącego usługi.

QTSP regularnie monitoruje swoje procesy wewnętrzne, których szczegóły określają PCKPC i regulacje wewnętrzne. Co najmniej raz w roku przeprowadza kompleksowy audyt wewnętrzny w celu zweryfikowania adekwatności swoich działań.

QTSP przeprowadza co kwartał wyrywkową kontrolę co najmniej 3% certyfikatów uwierzytelniania witryn wydanych od czasu poprzedniej kontroli, czy są one zgodne z PCKPC.

W przypadku certyfikatu dostawcy wydanego jednostce certyfikującej obsługiwanej przez inną organizację, działanie zewnętrznej jednostki certyfikującej jest kontrolowane raz do roku.

8.2. Kwalifikacje osoby dokonującej oceny

QTSP regularnie przeprowadza audyty wewnętrzne za pomocą swoich pracowników, którzy pełnią rolę niezależnego audytora systemu.

Weryfikacja zgodności z wymaganiami eIDAS i ETSI jest przeprowadzana przez organizację, która posiada autoryzację wydaną przez krajową organizację akredytacyjną państwa członkowskiego UE.

8.3. Powiązania pomiędzy osobą dokonującą oceny a ocenianym podmiotem

Audyt zewnętrzny przeprowadza osoba, która:

a) jest niezależna od właścicieli, kierownictwa i działalności ocenianego QTSP;
b) jest niezależna od ocenianej organizacji, ani ta osoba, ani jej najbliżsi krewni nie mają żadnych stosunków pracy lub stosunków służbowych z QTSP.
c) wynagrodzenie nie jest uzależnione od wniosków z przeprowadzonego audytu.

8.4. Obszary podlegające ocenie

Przegląd obejmuje następujące obszary:

a) zgodność z obowiązującymi przepisami prawa;
b) zgodność z normami technicznymi;
c) zgodność z Polityką Certyfikacji i KPC;
d) adekwatność zastosowanych procesów;
e) dokumentacja;
f) bezpieczeństwo fizyczne;
g) odpowiedni personel;
h) bezpieczeństwo IT;
i) przestrzeganie zasad ochrony danych.

Audyt obejmuje wszystkie aktywne pośrednie jednostki certyfikacji, które wydała wciąż jeszcze ważny certyfikat lub są zdolne do wystawienia certyfikatu.

Jeśli QTSP wydał certyfikat dla jednostki certyfikującej obsługiwanej przez inną organizację, wówczas audyt obejmuje również działalność tych organizacji zewnętrznych.

8.5. Czynności podjęte w wyniku stwierdzenia nieprawidłowości

Niezależny audytor podsumowuje wynik oceny w szczegółowym raporcie, który obejmuje sprawdzane elementy systemu i procesy oraz zawiera dowody wykorzystane do oceny. Rozbieżności ujawnione podczas oceny oraz terminy na ich poprawienie są odnotowywane w osobnym rozdziale sprawozdania.

Na podstawie powagi wykrytych różnic i braków, niezależny audytor może:

a) zaproponować propozycje modyfikacji, które należy opcjonalnie uwzględnić;
b) wymienić odstępstwa, które należy obowiązkowo wyeliminować.

8.6. Przekazywanie informacji o wynikach

QTSP publikuje podsumowanie raportu z oceny na swojej stronie internetowej: https://eurocert.pl.

QTSP nie publikuje szczegółowych informacji na temat stwierdzonych uchybień, gdyż są one traktowane jako informacje poufne.

Certyfikaty oceny zgodności są publikowane na stronie QTSP: eurocert.pl

Polska Lista Zaufania w formacie XML jest dostępna na stronie: https://www.nccert.pl/tsl.htm

Rejestr usług zaufania Organu nadzoru znajduje się na stronie: https://www.nccert.pl/uslugi.htm

9. Pozostałe biznesowe i prawne kwestie

9.1. Opłaty

QTSP publikuje informacje o opłatach i cenach na swojej stronie internetowej oraz udostępnia je w formie papierowej w swoim biurze obsługi klienta.

QTSP może jednostronnie zmienić cennik. QTSP publikuje wszelkie zmiany w cenniku na 30 dni przed jego wejściem w życie. Korzystne dla Klienta zmiany mogą wejść w życie w terminie krótszym niż 30 dni. Modyfikacje nie wpłyną na cenę usług opłaconych z góry.

Postanowienia związane z uiszczaniem i zwrotem opłat zawarte są w umowie o świadczenie usług oraz załącznikach do niej, w szczególności w Regulaminie usług zaufania EuroCert.

9.1.1. Opłaty za wystawienie certyfikatu i odnowienie

Zob. Sekcja: 9.1.

9.1.2. Opłaty za dostęp do certyfikatu

QTSP udziela stronom ufającym bezpłatnego dostępu on-line do swojego repozytorium certyfikatów.

9.1.3. Opłaty za unieważnienie lub za dostęp do informacji o statusie

QTSP świadczy na rzecz stron ufających bezpłatną usługę CRL i OCSP on-line dotyczącą statusu wszystkich wydanych przez siebie certyfikatów użytkownika końcowego i pośrednich.

9.1.4. Opłaty za inne usługi

Zob. Sekcja: 9.1.

9.1.5. Polityka zwrotów

Zob. Sekcja: 9.1.

9.2. Odpowiedzialność finansowa

QTSP bierze na siebie odpowiedzialność finansową za wypełnienie wszystkich swoich obowiązków określonych w niniejszym dokumencie oraz umowie o świadczenie usług zawartej z Klientem.

9.2.1. Ubezpieczenie

QTSP posiada wystarczające środki finansowe na pokrycie swoich zobowiązań związanych ze świadczeniem usług oraz na pokrycie kosztów związanych z zakończeniem działalności.

9.2.2. Inne aktywa

Nie przewidziano.

9.2.3. Ubezpieczenie lub gwarancja dla podmiotów końcowych

QTSP posiada ubezpieczenie od odpowiedzialności cywilnej.

Polisa ubezpieczeniowa od odpowiedzialności cywilnej obejmuje następujące szkody wyrządzone przez QTSP w związku ze świadczeniem usług:

a) szkody spowodowane naruszeniem umowy o świadczenie usług na rzecz odbiorców usług zaufania;
b) szkody wyrządzone poza umową odbiorcom usług zaufania lub osobom trzecim;
c) koszty wyrządzone Organowi Nadzoru przez QTSP, wynikające z zakończenia świadczenia usług zaufania;
d) zgodnie z Rozporządzeniem eIDAS (1) paragraf 17, ustęp 4, lit. e, koszty jednostki przeprowadzającej ocenę zgodności na wniosek organu nadzoru.

Wartość ubezpieczenia w polisie ubezpieczeniowej od odpowiedzialności cywilnej wynosi co najmniej 250 000 euro za każde zdarzenie (przy czym maks. 1 000 000 euro za wszystkie zdarzenia). Szkody powstałe z tego samego powodu w podobnym czasie stanowią pojedyncze zdarzenie ubezpieczeniowe.

Ubezpieczenie OC zapewnia pokrycie całej szkody poszkodowanego – do limitu ubezpieczenia – powstałej w wyniku szkodliwego działania QTSP niezależnie od tego, czy szkoda została spowodowana naruszeniem umowy czy poza umową.

Jeżeli uzasadnione roszczenie kilku uprawnionych stron związane ze zdarzeniem ubezpieczeniowym przekracza limit odpowiedzialności określony dla danego zdarzenia w ubezpieczeniu od odpowiedzialności cywilnej, wówczas odszkodowania z tytułu roszczeń następują proporcjonalnie do łącznej kwoty roszczeń w stosunku do limitu odpowiedzialności określonego w polisie.

9.3. Poufne informacje biznesowe

QTSP przetwarza dane klientów zgodnie z przepisami prawa. QTSP posiada politykę bezpieczeństwa informacji która określa cele i ustanawia odpowiedzialności w obszarze bezpieczeństwa oraz określa system regulacji wewnętrznych dotyczących bezpieczeństwa, w tym politykę bezpieczeństwa danych osobowych (patrz punkt 9.4).

Składając wniosek o certyfikat i podpisując umowę o świadczenie usług, klienci wyrażają zgodę na przechowywanie i przetwarzanie przez QTSP ich danych osobowych (w sposób zgodny z przepisami o przetwarzaniu danych). Zgoda taka dotyczy przekazywania osobom trzecim informacji określonych prawem w przypadku zakończenia działalności QTSP. Ponadto zgoda dotyczy przekazywania informacji podwykonawcom QTSP – wyłącznie w celu realizacji zadań związanych ze świadczeniem usługi.

Wnioskodawcy mogą wyrazić zgodę na ujawnienie certyfikatu w formularzu wniosku o certyfikat.

QTSP wykorzystuje dane klientów wyłącznie w celu świadczenia usług. QTSP ujawnia dane podmiotów i reprezentowanych organizacji pojawiające się w certyfikacie wraz z certyfikatem.

QTSP przechowuje dane, które nie zostały wprowadzone do certyfikatu, w sposób bezpieczny, w celu weryfikacji tożsamości podmiotów i organizacji i w celu realizacja innych obowiązków w zakresie raportowania danych. QTSP przechowuje dane, zgodnie z wymogami ustawowymi, przez określony czas. W trakcie przechowywania danych QTSP zapewnia integralność, poufność i bezpieczeństwo informacji. Zezwala na dostęp do informacji jedynie osobom, których zadania służbowe to uzasadniają oraz posiadającym upoważnienie do przetwarzania danych osobowych, sądom, prokuraturze, a także organom publicznym upoważnionym do odbioru danych na podstawie odpowiednich przepisów prawa.

QTSP zapewnia poufność i integralność informacji niejawnych, podczas przekazywania danych klientów.

9.3.1. Zakres informacji poufnych

QTSP stosuje czterostopniowy system klasyfikacji poufności danych poczynając od (1) danych jawnych, poprzez (2) dane do użytku służbowego dostępne dla wszystkich pracowników i współpracowników, (3) dane zwane tu chronionymi dostępne dla ograniczonej liczby osób wchodzących w skład personelu, w tym dane osobowe oraz (4) poufne firmowe podlegające szczególnym zabezpieczeniom, dane których ujawnienie mogłoby narazić EuroCert na poważne straty mogące doprowadzić do utraty możliwości funkcjonowania spółki. Za poufne QTSP uznaje w tym dokumencie ogólnie dane które nie należą do jawnych, takie jak:

a) wszystkie dane klienta, z wyjątkiem tych, które kwalifikują się jako informacje niepoufne określonych w sekcji 9.3.2;
b) oprócz danych klienta:
   - klucze prywatne i kody aktywacyjne,
   - wnioski o certyfikaty i umowy o świadczenie usług,
   - dane związane z transakcjami i dane dziennika logów,
   - przepisy, regulacje wewnętrzne - niedostępne publicznie,
   - wszystkie dane, których publiczne ujawnienie miałoby niekorzystny wpływ na bezpieczeństwo usługi.

9.3.2. Informacje poza zakresem informacji poufnych

QTSP uznaje za publiczne (jawne) wszystkie dane, które można uzyskać ze źródła publicznego lub na których ujawnienie subskrybent wyraził uprzednio pisemną zgodę.

QTSP traktuje wszystkie dane, które umieszcza w certyfikacie, jako informacje niepoufne. Takie dane pojawiają się w formularzu wniosku o certyfikat będącego integralną częścią umowy o świadczenie usług w wyraźnie oznaczony sposób.

QTSP zarządza statusem unieważnienia i zawieszenia certyfikatów użytkownika końcowego i certyfikatów pośredniczących jako informacją publiczną i udostępnia ją bez ograniczeń stronom ufającym, publikując listę CRL i świadcząc usługę on-line OCSP. Ujawnione informacje zawierają numer seryjny certyfikatu, czas unieważnienia i opcjonalnie przyczynę unieważnienia. Więcej informacji – zob. sekcje 7.2. i 7.3.

9.3.3. Obowiązek ochrony informacji poufnych

QTSP jest odpowiedzialny za ochronę przetwarzanych danych poufnych.

QTSP zobowiązuje swoich pracowników, podwykonawców i kontrahentów do ochrony wszystkich poufnych danych poprzez podpisanie oświadczenia o zachowaniu poufności lub w drodze umowy.

QTSP przetwarza dane osobowe zgodnie z przepisami rozporządzenia RODO oraz ustawy o ochronie danych osobowych (61), i ujawnia je na podstawie przepisów prawa osobom/organizacjom tylko w następujących przypadkach:

a) obowiązkowe przekazywanie informacji organowi nadzorczemu, władzy,
b) udzielanie informacji w ramach procesu (postępowania) cywilnego,
c) ujawnienie na wniosek właściciela.

QTSP zapewnia, że przetwarza informacje poufne zgodnie z przyjętymi uregulowaniami wewnętrznymi, w tym klasyfikacją PIDA (poufności, integralności, dostępności i archiwizacji) zgodnymi z obowiązującymi przepisami prawa.

Udzielanie informacji publicznym organom władzy

W celu prowadzenia dochodzenia lub zapobiegania przestępstwom popełnionym przy użyciu usług zaufania, a także w interesie bezpieczeństwa narodowego, QTSP – jeżeli spełnione są ustawowe kryteria udostępnienia danych – nieodpłatnie ujawnia informacje dotyczące tożsamości oraz informacje zweryfikowane przez QTSP zgodnie z art. 15 ustawy o usługach zaufania (19) organom śledczym i krajowym służbom bezpieczeństwa.

QTSP rejestruje fakt przekazania danych, ale nie informuje o tym klientów, których dane dotyczą.

Dostarczanie informacji w sytuacji postępowania cywilnego

W toku postępowania cywilnego sądowego lub pozasądowego dotyczących ważności certyfikatu QTSP może przekazać informacje o tożsamości podmiotu oraz informacje zweryfikowane przez QTSP, na podstawie przepisów prawa stronom postepowania, organom i instytucjom do tego upoważnionym.

QTSP rejestruje fakt przekazania danych i informuje o tym klientów, których to dotyczy.

Ujawnienie na żądanie właściciela danych

Na osobisty wniosek klienta lub na podstawie udzielonego oficjalnie upoważnienia, w formie pisemnej, QTSP ujawnia osobom trzecim poufne informacje dotyczące klienta.

Inne okoliczności powodujące ujawnienie informacji

W przypadku zakończenia działalności QTSP jest zobowiązany do przekazania swoich zapisów wraz z poufnymi danymi osobowymi użytkownika innemu dostawcy usług zaufania, który przejmuje je zgodnie z art. 20 ustawy o usługach zaufania (19).

9.4. Ochrona danych osobowych

QTSP zapewnia ochronę danych osobowych, działalność i regulacje QTSP są zgodne z wymogami ustawy o ochronie danych osobowych (61) i Rozporządzenia UE 2016/679 (GDPR) (62).

QTSP zgodnie z wymaganiami prawnymi:

a) przechowuje,
b) usuwa z bazy danych po wygaśnięciu obowiązku przechowywania, o ile klient nie wskaże inaczej, zarejestrowane dane osobowe i informacje o kliencie, zgodnie z wymogami prawnymi.

QTSP przechowuje w swojej ewidencji dane identyfikacyjne, dane o podmiocie pojawiające się w certyfikacie, oraz informacje o subskrybencie wyłącznie w celu świadczenia usługi, identyfikacji, zawarcia umowy i czasu przedawnienia rozliczeń.

QTSP ujawnia dane klienta osobom trzecim wyłącznie w przypadkach, gdy jest to przewidziane przepisami prawa lub jeśli klient wyraził na to pisemną zgodę.

9.4.1. Plan prywatności

QTSP posiada Politykę Prywatności i klauzule informacyjne, które zawierają szczegółowe przepisy dotyczące postępowania z danymi osobowymi.

Polityka prywatności znajduje się na stronie internetowej QTSP pod następującym adresem: https://eurocert.pl/.

Klauzule informacyjne są publikowane na stronie QTSP: https://eurocert.pl/repozytorium/

9.4.2. Informacje traktowane jako prywatne

QTSP chroni wszelkie dane osobowe przetwarzane w celu realizacji usługi, w tym pozyskane ze źródła publicznie dostępnego (certyfikatu lub urzędowego rejestru).

9.4.3. Informacje traktowane jako nieprywatne

QTSP może ujawnić publicznie dane Podmiotów zawarte w certyfikacie na podstawie pisemnej zgody Podmiotu lub osoby reprezentującej Podmiot.

QTSP może wskazać w certyfikacie unikalny identyfikator dostawcy przypisany do Podmiotu.

9.4.4. Odpowiedzialność za ochronę informacji prywatnych

QTSP przechowuje w sposób bezpieczny i chroni dane osobowe związane z wydaniem certyfikatu, ale nie ujawnione w certyfikacie. Dane są chronione odpowiednimi środkami, w szczególności przed nieuprawnionym dostępem, zmianą i ujawnieniem.

QTSP czasu ponosi całkowitą odpowiedzialność za zgodność z prawem przetwarzanych danych osobowych, przyjętą Polityką zarządzania danymi, w tym za działania swoich podwykonawców.

9.4.5. Powiadomienie i zgoda na użycie informacji prywatnych

QTSP ujawnia dane osobowe wskazane w certyfikacie wyłącznie na podstawie pisemnej zgody klienta.

QTSP wykorzystuje dane osobowe Klienta wyłącznie w zakresie niezbędnym do świadczenia usługi oraz w celu komunikacji z Klientem.

9.4.6. Ujawnianie informacji w związku z procedurą sądową lub administracyjną

W przypadkach określonych w odpowiednich przepisach prawa QTSP może ujawnić przechowywane dane osobowe o kliencie bez powiadamiania Klienta.

9.4.7. Inne okoliczności ujawnienia informacji prywatnych

Nie przewidziano

9.5. Prawa własności intelektualnej

W trakcie swojej działalności gospodarczej QTSP nie może naruszać żadnych praw własności intelektualnej osoby trzeciej.

Właścicielem klucza prywatnego i publicznego wydawanego przez QTSP klientom jest subskrybent, a wyłącznym użytkownikiem jest wnioskodawca bez względu na to czy jest nośnik fizyczny, który zawiera i chroni klucze.

Właścicielem certyfikatu wydanego przez QTSP swoim klientom jest QTSP, a jego wyłącznym użytkownikiem jest wnioskodawca.

QTSP może publikować, powielać, unieważniać i w inny sposób zarządzać wydanymi certyfikatami użytkowników końcowych, wraz z zawartym w nich kluczem publicznym w sposób opisany w regulaminie usług zaufania.

Informacje o statusie unieważnienia certyfikatu są własnością QTSP, która jest ujawniana zgodnie z zasadami w punktach 7.2. oraz 7.3.

Unikalny identyfikator przydzielony klientom przez QTSP jest własnością QTSP, który jest ujawniany w ramach certyfikatu przez QTSP w Repozytorium Certyfikatów.

Podmiot jest uprawniony do użycia identyfikatora wskazanego w certyfikacie (który identyfikuje podmiot certyfikatu).

Niniejszy dokument jest wyłączną własnością QTSP. Klienci i inne strony ufające są uprawnione do korzystania z dokumentu wyłącznie zgodnie z jego wymogami, a jakiekolwiek inne wykorzystanie do celów komercyjnych lub innych jest surowo zabronione.

Niniejszy PCKPC może być swobodnie rozpowszechniany wyłącznie w niezmienionej formie, w całości i ze wskazaniem pochodzenia.

Zasady korzystania z oprogramowania udostępnionego przez QTSP w celu korzystania z usługi znajdują się instrukcji obsługi znajdującej się w opisie oprogramowania lub zawartej w samym oprogramowaniu.

9.6. Oświadczenia i gwarancje

9.6.1. Oświadczenia i gwarancje CA

Odpowiedzialność Dostawcy Usług Zaufania

Odpowiedzialność QTSP opisana jest w niniejszym dokumencie oraz umowie o świadczenie usług z klientem wraz z załącznikami, zgodnie z którymi:

a) QTSP przyjmuje na siebie odpowiedzialność za potwierdzenie, że wnioskodawca miał prawo do używania lub sprawował kontrolę nad Nazwami Domen wymienionymi w certyfikacie;
b) QTSP ponosi odpowiedzialność za przestrzeganie procedur opisanych w obsługiwanych przez siebie Politykach Certyfikacyjnych;
c) QTSP ponosi odpowiedzialność za szkody wyrządzone podczas świadczenia usługi przez jego podwykonawców;
d) QTSP ponosi odpowiedzialność na zasadach odpowiedzialności za naruszenie umowy w Kodeksie cywilnym w stosunku do klientów będących z nim w stosunku umownym;
e) QTSP ponosi odpowiedzialność za wyrządzenie szkody poza umową w rozumieniu Kodeksu cywilnego w stosunku do osób trzecich (takich jak strona ufająca), które nie są z nim w stosunku umownym.
f) QTSP wypłaci Klientom odszkodowanie za udowodnione szkody, które wystąpią w zakresie jego odpowiedzialności, ograniczone do kwoty określonej w polisie i umowie z Klientem (patrz punkt Ograniczenie Odpowiedzialności finansowej 9.8.).
g) Jeżeli uzasadnione roszczenie kilku uprawnionych stron związane ze zdarzeniem ubezpieczeniowym przekracza limit odpowiedzialności określony dla danego zdarzenia w ubezpieczeniu od odpowiedzialności cywilnej, wówczas odszkodowania z tytułu roszczeń następują proporcjonalnie do łącznej kwoty roszczeń w stosunku do limitu odpowiedzialności określonego w polisie.

QTSP nie odpowiada za:

a) działania podmiotu związane z kluczem prywatnym;
b) działania podmiotu związane z urządzeniem do składania podpisu elektronicznego;
c) weryfikację i użycie certyfikatów przez strony ufające;
d) regulacje wydane przez strony ufające lub inne podmioty.

Obowiązki Dostawcy Usług Zaufania

QTSP jest zobowiązany do przestrzegania wymogów określonych w art. 24 ust. 2 eIDAS (1).

Podstawowym obowiązkiem QTSP jest świadczenie usługi zgodnie z niniejszym dokumentem, Regulaminem, Polityką Bezpieczeństwa Informacji, wewnętrznymi regulacjami dotyczącymi bezpieczeństwa określonymi w tej Polityce, Regulaminem Organizacyjnym.

Podstawowe obowiązki obejmują:

a) ustanowienie ram prawnych, regulacyjnych, materialnych, umownych itp. odpowiednich dla usługi;
b) zapewnienie wysokiej jakości i bezpieczeństwa usług zgodnie z odpowiednimi regulacjami;
c) nieprzerwane działanie i kontrola organizacji związanych z usługami (jednostki certyfikacji, obsługa klienta itp.);
d) przestrzegania procedur określonych w regulacjach oraz unikania lub eliminowania wszelkich potencjalnie występujących nieprawidłowości w działaniu;
e) zapewnienia usług każdemu wnioskodawcy, który akceptuje warunki określone w regulacjach;
f) prowadzenie publicznych rejestrów i własnych polityk, a także udostępnianie ich w sposób ciągły każdemu przez Internet.

Obowiązki Dostawcy Usług Zaufania wobec Subskrybentów znacznika czasu

QTSP jest zobowiązany do:

a) wydawania znaczników czasu zgodnych z ETSI EN 319 422 (46) na żądanie subskrybenta, które odpowiadają wartości hash i unikalnemu identyfikatorowi zawartym w żądaniu;
b) przestrzegania dokładności znacznika do 1 sekundy (odchylenie od UTC maks. 1 sekunda);
c) zapewnienia niezawodności i bezpieczeństwa usług zgodnie z wymogami dotyczącymi kwalifikowanych dostawców znacznika czasu;
d) rejestrowania wszelkich ważnych zdarzeń związanych z usługami w dziennikach zdarzeń (logach) i przechowywania tych dzienników zgodnie z wymogami prawnymi.

Obowiązki organizacji certyfikującej

Organizacja certyfikująca ma za zadanie konfigurowanie i obsługę jednostek certyfikujących (patrz sekcja: 1.3.1), a także jednostek niezbędnych do usługi statusu certyfikatu online, dbanie o repozytorium certyfikatów i informacji o statusie unieważnienia, zarządzanie kartami inteligentnymi i udostępnianie ich, oraz zarządzanie regulacjami.

Wewnętrzne, operacyjne regulacje QTSP określają sposób funkcjonowania organizacji certyfikującej. Certyfikaty dostawcy wydane przez jednostki certyfikacji (dla członków personelu ds. rejestracji, dyżurujących itp.) są zarządzane zgodnie z przepisami regulacji operacyjnych. Niniejszy akapit zawiera jedynie postanowienia dotyczące publicznego certyfikatu dostawcy i certyfikatów użytkownika końcowego.

Lista zadań, które należy wykonać w zakresie zarządzania regulacjami:

a) określanie, zatwierdzanie i utrzymywanie stosowanych typów certyfikatów;
b) przygotowywanie publicznych regulacji usług i regulacji wewnętrznych (niepublicznych), sprawdzanie ich pod kątem zgodności z przepisami prawa i regulacjami wewnętrznymi (niepublicznymi), oraz ich aktualizacja;
c) rejestrowanie komentarzy do publicznych regulaminów usług i rozpatrywanie wniosków.

Urząd Certyfikacji jest odpowiedzialny za:

a) autentyczność i poprawność wydanych certyfikatów;
b) wydane przez siebie regulacje oraz za ich zgodność z przepisami ustawowymi;
c) zgodność wygenerowanych par kluczy oraz za komplementarność klucza prywatnego i publicznego oraz certyfikatu;
d) związek pomiędzy kodami aktywacyjnymi urządzenia do składania podpisu elektronicznego (pieczęci) a kluczami wgranymi na urządzenie;
e) przestrzeganie swoich obowiązków.

9.6.2. Oświadczenia i gwarancje urzędu rejestracji

Zadaniem obsługi klienta jest reprezentowanie QTSP przed użytkownikami końcowymi. Wykonuje następujące zadania:

a) uczestniczy w sprzedaży usług;
b) dokonuje rejestracji podmiotów;
c) otrzymuje wnioski dotyczące certyfikatów (zawieszenie, unieważnienie, uchylenie zawieszenia, wymiana certyfikatu);
d) otrzymuje i obsługuje zgłoszenia związane z modyfikacją danych;
e) uczestniczy w publikacji statusu unieważnienia;
f) udziela klientom i stronom ufającym niezbędnych informacji w związku z prowadzoną przez nich działalnością związaną z usługami świadczonymi przez QTSP.

Urząd Rejestracji jest odpowiedzialny za:

a) ustalenie tożsamości osobistej Podmiotów;
b) ustalenie tożsamości osoby upoważnionej do reprezentowania Podmiotów;
c) ustalenie tożsamości organizacyjnej reprezentowanych organizacji i za ustalenie prawa osoby fizycznej do reprezentacji organizacji, w tym potwierdzenie tożsamości tej osoby;
d) autentyczność zarejestrowanych danych rejestracyjnych;
e) udzielanie informacji osobom korzystających z usług o treści i dostępności PCKPC, a także warunkach korzystania z usługi przed zawarciem umowy o świadczenie usług;
f) pełne wywiązanie się ze swoich zobowiązań.

9.6.3. Oświadczenia i gwarancje subskrybenta

Odpowiedzialność subskrybenta

Odpowiedzialność subskrybenta określa umowa o świadczenie usług i załączniki do niej (w tym regulamin usług zaufania).

Obowiązki subskrybenta

Obowiązkiem subskrybenta jest działanie zgodnie z warunkami umownymi i regulacjami QTSP podczas korzystania z usługi, w tym składanie wniosku o certyfikat, stosowanie certyfikatu i kluczy prywatnych.

Obowiązki subskrybenta są określone przez niniejszy PCKPC, umowę o świadczenie usług i Regulamin.

W przypadku gdy subskrybent zostanie poinformowany o jakimkolwiek faktycznym lub podejrzewanym niewłaściwym użyciu lub ujawnieniu klucza prywatnego związanego z kluczem publicznym zawartym w certyfikacie należącym do subskrybenta, jest on zobowiązany do:

a) niezwłocznego zgłoszenia tego faktu QTSP,
b) niezwłocznego żądania unieważnienia lub zawieszenia certyfikatu,
c) niezwłocznego zaprzestania korzystania z certyfikatu i związanego z nim klucza prywatnego.

Subskrybent może zainstalować certyfikat i powiązany z nim klucz prywatny wyłącznie na serwerach, które są dostępne pod jedną z domen wymienionym w polu subjectAltName(s) w certyfikacie, oraz korzystać z certyfikatu wyłącznie zgodnie ze wszystkimi obowiązującymi przepisami prawa i umową o świadczenie usług oraz Regulaminem.

Prawa subskrybenta

a) Subskrybenci mają prawo do korzystania z usług zgodnie z niniejszym PCKPC.
b) Subskrybenci są uprawnieni do określenia na piśmie, które podmioty powinny mieć możliwość otrzymania certyfikatów.
c) Subskrybenci mają prawo zażądać zawieszenia i unieważnienia certyfikatów.
d) Subskrybenci są uprawnieni do wyznaczania Administratorów Organizacyjnych.

Odpowiedzialność wnioskodawcy

Wnioskodawca jest odpowiedzialny za:

a) uwierzytelnienie, poprawność i prawdziwość danych podanych podczas rejestracji;
b) weryfikację danych wskazanych w certyfikacie;
c) udzielanie natychmiastowej informacji o zmianach swoich danych oraz danych wskazanych w certyfikacie;
d) korzystanie z urządzenia do składania podpisu elektronicznego (pieczęci), klucza prywatnego i certyfikatu zgodnie z regulacjami;
e) bezpieczne zarządzanie kluczem prywatnym i kodem aktywacyjnym;
f) bezpieczne zarządzanie urządzeniem do składania podpisu elektronicznego (pieczęci);
g) natychmiastowe powiadomienie i pełne informowanie QTSP w przypadkach spornych;
h) ogólne wywiązywanie się ze swoich zobowiązań.

Obowiązki wnioskodawcy

Wnioskodawca powinien:

a) zapoznać się uważnie z niniejszym dokumentem przed skorzystaniem z usługi;
b) podać wszystkie i wyłącznie prawdziwe dane wymagane przez QTSP niezbędne do korzystania z usługi;
c) jeżeli wnioskodawca dowie się o tym, że dane niezbędne do korzystania z usługi, w szczególności dane wskazane w certyfikacie, uległy zmianie, zobowiązany jest niezwłocznie:
   - powiadomić QTSP na piśmie,
   - zażądać zawieszenia lub unieważnienia certyfikatu oraz
   - zakończyć korzystanie z certyfikatu;
d) niezwłocznie zakończyć korzystanie z klucza prywatnego należącego do certyfikatu jeżeli podmiot dowie się o tym, że jego certyfikat został unieważniony lub że naruszone zostało bezpieczeństwo urzędu certyfikacji wystawiającego;

e) korzystać z usługi wyłącznie w celach dozwolonych (lub nie zabronionych) przez przepisy prawa, zgodnie z określonymi regulacjami i dokumentami;
f) zainstalować certyfikat uwierzytelniania witryny tylko na tym serwerze, który jest dostępny pod nazwą domeny wskazaną w certyfikacie;
g) zapewnić, że żadne nieupoważnione osoby nie mają dostępu do danych i narzędzi (haseł, tajnych kodów, urządzeń do składania podpisów) niezbędnych do korzystania z usługi;
h) niezwłocznie powiadomić QTSP na piśmie w przypadku rozpoczęcia sporu prawnego w związku z jakimkolwiek podpisem elektronicznym (pieczęcią) lub certyfikatami związanymi z usługą;
i) współpracować z QTSP w celu walidacji danych niezbędnych do wydania certyfikatów oraz zrobić wszystko, co w ich mocy, aby umożliwić jak najszybsze zakończenie takiej weryfikacji;
j) w przypadku, gdy klucz prywatny podmiotu, urządzenie do składania podpisu elektronicznego lub tajne kody niezbędne do aktywacji urządzenia trafią w ręce osób nieupoważnionych lub zostaną zniszczone, podmiot zobowiązany jest do niezwłocznego i pisemnego zgłoszenia tego faktu QTSP, a także do zainicjowania unieważnienia i/lub zawieszenia certyfikatów oraz zakończenia korzystania z certyfikatu;
k) odpowiedzieć na żądania QTSP w terminie określonym przez QTSP w przypadku naruszenia bezpieczeństwa klucza (ujawnienia) lub podejrzenia nielegalnego użycia;
l) przyjąć do wiadomości, że subskrybenci są uprawnieni do żądania unieważnienia i/lub zawieszenia certyfikatu;
m) przyjąć do wiadomości, że QTSP wydaje certyfikaty w sposób określony w PCKPC, po ukończeniu opisanych w nim etapów walidacji;
n) przyjąć do wiadomości, że QTSP umieszcza w certyfikatach tylko te dane, które odpowiadają rzeczywistości. W związku z tym QTSP weryfikuje dane, które mają być wprowadzone w Certyfikatach zgodnie z PCKPC;
o) w przypadku wnioskowania o certyfikat organizacyjny, przyjąć do wiadomości, że QTSP wyda certyfikat wyłącznie w przypadku zgody reprezentowanej organizacji;
p) w przypadku wnioskowania o certyfikat organizacyjny, przyjąć do wiadomości, że reprezentowana organizacja ma prawo żądać unieważnienia certyfikatu;
q) przyjąć do wiadomości i zaakceptować, że QTSP ma prawo zawiesić i/lub unieważnić certyfikat niezwłocznie:
   - gdy dowie się, że dane w nim wskazane nie odpowiadają rzeczywistości lub klucz prywatny nie jest w wyłącznym posiadaniu lub użytkowaniu wnioskodawcy. W takim przypadku wnioskodawca jest zobowiązany do zakończenia korzystania z certyfikatu;
   - jeżeli subskrybent naruszy umowę o świadczenie usług lub regulamin;
   - Unieważnienie jest wymagane przez wymagania CABF (Baseline) lub PCKPC;
   - QTSP dowie się, że certyfikat został wykorzystany do nielegalnej działalności (np. phishingu, oszustwa, rozprzestrzeniania złośliwego oprogramowania).
   - subskrybent nie uiści opłat za usługi w terminie.

Prawa wnioskodawcy

a) Wnioskodawcy mają prawo ubiegać się o certyfikaty zgodnie z PCKPC.
b) W przypadku, gdy zezwala na to odpowiednia polityka certyfikacyjna, wnioskodawcy są uprawnieni do złożenia wniosku o zawieszenie i unieważnienie swoich certyfikatów, zgodnie z niniejszym PCKPC.

9.6.4. Gwarancje i oświadczenia strony ufającej

Strony ufające decydują o akceptacji i sposobie użycia certyfikatu i znacznika czasu wedle swojego uznania i/lub swoich polityk. Podczas weryfikacji ważności, w celu zachowania poziomu bezpieczeństwa gwarantowanego przez QTSP, konieczne jest, aby strona ufająca postępowała ostrożnie, dlatego zaleca się zwrócenie szczególnej uwagi na:

a) wymagania określone w niniejszym dokumencie;
b) korzystanie z niezawodnego środowiska i aplikacji IT;
c) sprawdzenie statusu unieważnienia certyfikatu, certyfikatu do podpisywania znacznika czasu na podstawie aktualnej listy CRL lub odpowiedzi OCSP;
d) uwzględnienie wszelkich ograniczeń korzystania z certyfikatu, znacznika czasu, zawartych w certyfikacie i niniejszym dokumencie.

9.6.5. Oświadczenia i gwarancje innych stron

Odpowiedzialność reprezentowanej organizacji

Reprezentowana organizacja ponosi wyłączną odpowiedzialność za dokumenty, które wydaje. W szczególności za dokumenty, w których poświadcza, że wnioskodawca jest uprawniony do korzystania z certyfikatu zawierającego nazwę Organizacji. Jeśli jakiekolwiek informacje w zaświadczeniu wydanym przez Podmiot Reprezentowany ulegną zmianie, obowiązkiem Podmiotu Reprezentowanego jest niezwłoczne zgłoszenie tego faktu do QTSP.

Prawa reprezentowanej organizacji

a) QTSP wystawia certyfikaty, w których wskazana jest nazwa reprezentowanej organizacji, wyłącznie za jej zgodą.
b) Reprezentowana organizacja jest uprawniona do zawieszenia i unieważnienia certyfikatów, w których wskazana została jej nazwa.

9.7. Wyłączenie odpowiedzialności z tytułu gwarancji

QTSP wyłącza swoją odpowiedzialność, jeżeli:

a) wnioskodawcy nie przestrzegają wymogów związanych z zarządzaniem urządzeniem do składania podpisu elektronicznego (pieczęci) i kluczem prywatnym i danymi aktywacyjnymi;
b) klient nie może uzyskać dostępu do Usługi Zdalnego Podpisu z powodu czynników za które nie odpowiada QTSP;
c) nie jest w stanie dostarczyć informacji lub wypełnić swoich innych obowiązków komunikacyjnych z powodu problemów z Internetem lub jego częścią;
d) szkoda wynika ze słabości lub z błędów algorytmów kryptograficznych przyjętych przez zalecenia międzynarodowych standardów i/lub organ nadzorczy.

9.8. Ograniczenie odpowiedzialności

Odpowiedzialność Dostawcy Usług za szkody

QTSP nie ponosi odpowiedzialności za jakiekolwiek szkody, które wynikają z tego, że strona ufająca nie postępuje zgodnie z obowiązującymi przepisami prawa i regulacjami QTSP w trakcie walidacji i korzystania z certyfikatów, oraz gdy strona ufająca nie postępuje zgodnie z wymaganiami w danej sytuacji.

QTSP ponosi odpowiedzialność wobec osób trzecich za szkody umowne i pozaumowne związane z jego usługami wyłącznie za możliwe do udowodnienia szkody wynikające z zawinionego naruszenia jego obowiązków.

QTSP nie ponosi odpowiedzialności za jakiekolwiek szkody wynikające z niewykonania swoich zobowiązań w zakresie dostarczania informacji i innych komunikatów z powodu zewnętrznego, nieuniknionego zdarzenia wynikającego z nieprawidłowego działania Internetu lub jakiejkolwiek jego części. Jeśli QTSP przeprowadza porównanie danych z autentyczną bazą danych przed wydaniem certyfikatu, polega na danych otrzymanych z autentycznej bazy danych. QTSP nie ponosi żadnej odpowiedzialności za szkody wynikające z niepoprawności informacji dostarczanych przez takie publiczne autoryzowane bazy danych.

QTSP ponosi wyłączną odpowiedzialność za świadczenie usług zgodnie z postanowieniami niniejszego dokumentu, a także dokumentami, w nim przywołanymi (Polityki Certyfikacyjne, standardy, rekomendacje), oraz z jego własnymi regulacjami wewnętrznymi.

Proces administracyjny

QTSP rejestruje swoje działania, chroni integralność i autentyczność wpisów dziennika zdarzeń (logi), oraz przechowuje (archiwizuje) logi przez długi okres w celu ustalenia, udokumentowania i udowodnienia własnej odpowiedzialności za wyrządzone szkody, a także odszkodowania należnego mu z tytułu takich szkód.

Odpowiedzialność finansowa

QTSP posiada depozyt zgodny z wymogami prawnymi na pokrycie swojej odpowiedzialności finansowej i kosztów jej rozwiązania.

QTSP posiada ubezpieczenie od odpowiedzialności cywilnej zgodnie z wymaganymi przepisami prawa w celu zapewnienia swojej wiarygodności.

Ograniczenie odpowiedzialności finansowej

QTSP ogranicza obowiązek odszkodowawczy związany z usługami do 250 000 EUR w odniesieniu do jednego zdarzenia i 1 000 000 EUR w odniesieniu do wszystkich zdarzeń.

Jeżeli uzasadnione roszczenie o odszkodowanie kilku uprawnionych stron związane ze zdarzeniem ubezpieczeniowym przekracza limit odpowiedzialności określony dla danego zdarzenia w ubezpieczeniu od odpowiedzialności cywilnej, wówczas odszkodowania z tytułu roszczeń następują proporcjonalnie do łącznej kwoty roszczeń w stosunku do limitu odpowiedzialności określonego w polisie.

9.9. Odszkodowanie

9.9.1. Odszkodowawcza odpowiedzialność Dostawcy Usług

Szczegółowe zasady odpowiedzialności odszkodowawczej QTSP określa niniejszy dokument (patrz punkt: 9.8.), umowa o świadczenie usług oraz umowy zawierane z Klientami.

9.9.2. Odszkodowanie ze strony subskrybenta

Subskrybent ponosi odpowiedzialność odszkodowawczą za szkody lub straty wyrządzone QTSP spowodowane nieprzestrzeganiem przez Subskrybenta jego obowiązków i odpowiednich zaleceń.

9.9.3. Odszkodowanie ze strony stron ufających

Zob. sekcja: 9.8.

9.10. Terminy i wygaśnięcie PC i KPC.

9.10.1. Data wejścia w życie

Data wejścia w życie PCKPC jest określona na stronie tytułowej dokumentu.

9.10.2. Wygaśnięcie

Niniejszy dokument obowiązuje przez czas nieokreślony tzn. do momentu jego uchylenia lub wydania nowej wersji.

Sekcja 9. niniejszego dokumentu pozostaje w mocy nawet po utracie ważności PCKPC (niezależnie od powodu wygaśnięcia dokumentu) w stosunku do wszystkich certyfikatów, które QTSP wydał w trakcie obowiązywania PCKPC.

9.10.3. Skutki rozwiązania umowy

W przypadku odstąpienia od PCKPC QTSP publikuje na swojej stronie internetowej szczegółowe zasady odstąpienia oraz prawa i obowiązki utrzymujące się po odstąpieniu.

QTSP gwarantuje, że nawet w przypadku uchylenia PCKPC, przepisy dotyczące ochrony poufnych danych pozostają w mocy.

9.11. Indywidualne powiadomienia i komunikacja z klientami

QTSP posiada biuro obsługi klienta w celu utrzymywania kontaktu ze swoimi klientami.

Klienci mogą składać QTSP swoje oświadczenia wyłącznie w formie pisemnej, podpisane. Reprezentacja organizacji jest ważna tylko wraz z dowodem prawa do reprezentacji.

Inne powiadomienia mogą być składane w formie pisemnej lub w formie poczty elektronicznej.

QTSP utrzymuje komunikację ze swoimi klientami poprzez swoją stronę internetową lub pocztę elektroniczną.

9.12. Zmiany

QTSP zastrzega sobie prawo do zmiany niniejszego dokumentu w przypadku zmiany przepisów normatywnych, wymogów bezpieczeństwa, warunków rynkowych lub innych okoliczności.

9.12.1. Procedura wprowadzania zmian

QTSP ujawnia w swoich regulacjach publicznych wyłącznie te procedury, których znajomość nie zagraża bezpieczeństwu usług. QTSP posiada szereg wewnętrznych regulacji bezpieczeństwa i innych regulacji oraz wymagań na poziomie operacyjnym, które są poufne (niniejszy PCKPC wymienia kilka z nich). Procedury opisane w punkcie 8.4. audytują również te dokumenty.

Wszystkie regulacje wewnętrzne (jawne i niejawne) są zatwierdzane zgodnie z Metodyką Zatwierdzania Regulacji przez Kierownika QTSP. QTSP dokonuje przeglądu PCKPC corocznie lub w przypadku potrzeby aktualizacji. Zaktualizowany dokument otrzymuje nowy numer wersji po każdej zmianie. Zostaje również ustalony termin wejścia w życie, uwzględniający czas potrzebny na zatwierdzenie dokumentu. Działania są realizowane zgodnie z obowiązującą u QTSP Metodyką Zatwierdzania Regulacji.

QTSP publikuje zatwierdzony PCKPC na swojej stronie internetowej co najmniej 14 dni przed planowanym wejściem w życie.

9.12.2. Mechanizm i okres powiadamiania

QTSP powiadamia strony ufające o wydaniu nowych wersji dokumentu zgodnie z opisem w sekcji 9.12.1.

9.12.3. Okoliczności, w których identyfikator OID musi zostać zmieniony

QTSP wydaje nową wersję z nowym numer wersji w przypadku każdej zmiany PCKPC. Nie wpływa to na zmianę OID dokumentu.

9.13. Rozwiązywanie sporów

QTSP dąży do polubownego rozstrzygnięcia w drodze negocjacji powstałych sporów w związku z usługami.

QTSP i klient wspólnie uzgadniają, że w przypadku jakichkolwiek sporów, reklamacji lub skarg, podejmą próbę polubownego rozwiązania w drodze negocjacji przed skierowaniem sprawy na drogę prawną. Strona inicjująca będzie zobowiązana do niezwłocznego powiadomienia każdej innej zainteresowanej strony i do pełnego poinformowania jej o wszystkich konsekwencjach sprawy.

Klient ma prawo skierować sprawę do Organu Arbitrażowego w Warszawie przed wszczęciem postępowania sądowego.

Pytania, zastrzeżenia i reklamacje związane z działalnością QTSP lub z korzystaniem z wydanych certyfikatów należy kierować do Centralnego Biura Obsługi Klienta w formie pisemnej. W ciągu 3 dni roboczych od otrzymania zgłoszenia, QTSP poinformuje stronę zgłaszającą na podany przez nią adres o otrzymaniu zgłoszenia i czasie potrzebnym na jego rozpatrzenie. QTSP jest zobowiązany do udzielenia pisemnej odpowiedzi zgłaszającemu w wyznaczonym terminie.

QTSP może zażądać od podmiotu podania informacji niezbędnych do udzielenia odpowiedzi podmiotowi. QTSP rozpatruje reklamacje/skargę w ciągu 30 dni i zawiadamia zgłaszających o ich wynikach.

Jeżeli zgłaszający uzna odpowiedź za niewystarczającą lub jeżeli spór nadal nie może zostać rozstrzygnięty, zgłaszający może zażądać konsultacji z QTSP oraz ze stronami zainteresowanymi.

Wszyscy uczestnicy takich konsultacji otrzymują pisemne powiadomienie o terminie konsultacji z 10-dniowym wyprzedzeniem. Zgłoszenie, odpowiedź QTSP, a także wszelkie inne dokumenty zawierające niezbędne informacje zostaną przesłane uczestnikom w formie pisemnej.

Jeżeli konsultacja nie przyniesie rezultatu w ciągu 30 dni roboczych liczonych od dnia złożenia reklamacji, zgłaszający może złożyć pozew sądowy w tej sprawie. Strony objęte postępowaniem podlegają wyłącznej jurysdykcji sądu właściwego dla siedziby QTSP.

9.14. Obowiązujące prawo

QTSP przez cały czas podlega obowiązującym przepisom prawa polskiego. Prawo polskie jest prawem właściwym dla umów, regulacji i ich egzekwowania.

9.15. Zgodność z obowiązującym prawem

Obowiązujące przepisy:

1) Rozporządzenie (EU) nr 910/2014 Parlamentu Europejskiego i Rady z dnia 23 lipca 2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylająca dyrektywę 1999/93/WE (1);
2) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE;
3) Ustawa o ochronie danych osobowych z dn. 10 maja 2018 r. (61);
4) Kodeks cywilny z 23 kwietnia 1964 (20);
5) Ustawa o usługach zaufania (19).

9.16. Postanowienia dodatkowe

9.16.1. Całość umowy

Nie przewidziano.

9.16.2. Cesja

Dostawcy działający zgodnie z niniejszym dokumentem mogą scedować swoje prawa i obowiązki na osobę trzecią wyłącznie za uprzednią pisemną zgodą QTSP.

9.16.3. Rozdzielność postanowień

Jeżeli jakiekolwiek postanowienia niniejszego dokumentu staną się nieważne z jakiegokolwiek powodu, pozostałe postanowienia pozostaną w mocy bez zmian.

W przypadku konfliktu między przepisami krajowymi lub Unii Europejskiej a obowiązkowymi wymogami CABF S/MIME BR (13), QTSP powiadamia CAB Forum o faktach, okolicznościach i przepisach prawa przed wydaniem certyfikatów S/MIME.

9.16.4. Egzekucja (honoraria i zrzeczenie się praw)

QTSP może dochodzić odszkodowania i zwrot kosztów obsługi prawnej w celu zrekompensowania szkód, strat, kosztów spowodowanych przez jego partnerów. Jeżeli w konkretnej sprawie QTSP nie skorzysta z roszczenia odszkodowawczego za szkody, nie oznacza to, że w podobnych sprawach w przyszłości lub w przypadku naruszenia innych postanowień niniejszego dokumentu, zrezygnuje z dochodzenia roszczeń odszkodowawczych.

9.16.5. Siła wyższa

QTSP nie ponosi odpowiedzialności za niewykonanie, nienależyte wykonanie, opóźnienie w wykonaniu jakichkolwiek zobowiązań określonych w PCKPC, jeżeli jest to spowodowane nieprzewidywalną i niemożliwą do przewidzenia przyczyną zewnętrzną pozostającą poza kontrolą QTSP.

9.17. Inne postanowienia

Nie ustalono.

A Interpretacja skrótów nazw polityk certyfikacji

W celu łatwiejszego zapanowania nad Politykami Certyfikacyjnymi, QTSP definiuje pięcioznakową krótką nazwę (identyfikator) dla każdej Polityki, gdzie każdy znak ma znaczenie i definiuje niektóre podstawowe cechy danej Polityki zgodnie z następującymi regułami:

- Pierwszy znak [?....]
  - Q: polityka certyfikacji dla kwalifikowanego certyfikatu
  - A: polityki certyfikacji dla niekwalifikowanych certyfikatów, III klasa certyfikacji
  - B: polityki certyfikacji dla niekwalifikowanych certyfikatów, II klasa certyfikacji
  - C: polityka certyfikacji dla niekwalifikowanych certyfikatów automatycznych
- Drugi znak [.?...]
  - A: polityka certyfikacji dla certyfikatu do podpisu
  - B: polityka certyfikacji dla certyfikatu do składania pieczęci
  - W: polityka certyfikacji dla certyfikatu uwierzytelniania witryn
  - K: polityka certyfikacji dla certyfikatu do podpisywania kodu
  - S: polityka certyfikacji dla certyfikatu dla Email (S/MIME)
  - E: polityka certyfikacyjna dla certyfikatów do innych celów
- Trzeci znak [..?..]
  - T: polityka certyfikacji dla certyfikatów wydanych osobie fizycznej
  - J: polityka certyfikacji dla certyfikatów wydanych osobie prawnej
  - x: nie określono, certyfikat może być wydany dla dowolnego podmiotu
- Czwarty znak [...?.]
  - B: polityka certyfikacji dla certyfikatów wydanych na kwalifikowanym urządzeniu do składania podpisów elektronicznych
  - H: polityka certyfikacji dla certyfikatów wydanych na jakimkolwiek urządzeniu kryptograficznym
  - S: polityka certyfikacji dla certyfikatów wydanych w postaci pliku
  - x: nie określono, certyfikat może być wydany na dowolnej platformie
- Piąty znak [....?]
  - P: polityka certyfikacji dla certyfikatów wydanych dla pseudonimu (anonimowych)
  - N: polityka certyfikacji dla certyfikatów wykluczających użycie pseudonimu

B Bibliografia

1. ***ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO i RADY (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające Dyrektywę 1999/93/WE.***

2. ***CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates, v. 1.8.1, https://cabforum.org/working-groups/server/extended-validation/documents/.***

3. ***https://www.nccert.pl.***

4. ***Regulamin Usług Zaufania EuroCert; https://eurocert.pl/repozytorium/Zasady_i_warunki_swiadczenia_uslug/aktualne/.***

5. ***IETF RFC 3647: Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework, November 2003.***

6. ***CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates, v.2.0.2., https://cabforum.org/working-groups/server/baseline-requirements/documents/.***

7. ***Common Criteria for Information Technology Security Evaluation, Part 1 - 3.***

8. ***CEN CWA 14169: Secure signature-creation devices "EAL 4+", March 2004.***

9. ***CEN 419 221-5; Protection Profiles for TSP Cryptographic Modules - Part 5: Cryptographic Module for Trust Services.***

10. ***FIPS PUB 140-2 (2001 May 25): Security Requirements for Cryptographic Modules.***

11. ***FIPS PUB 140-3 (2019 March 22): Security Requirements for Cryptographic Modules.***

12. ***ETSI TS 119 431-1; Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD /SCDev.***

13. ***CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly Trusted S/MIME Certificates, v.1.0.3., https://cabforum.org/working-groups/smime/documents/.***

14. ***ETSI EN 319 411-2; Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates.***

15. ***ETSI EN 319 411-1; Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.***

16. ***ETSI TS 119 495; Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive (EU) 2015/2366.***

17. ***ETSI EN 319 421; Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.***

18. ***USTAWA z dnia 18 września 2001 r. o podpisie elektronicznym (uchylony z dniem 1 lipca 2016 r. wraz z wejściem eIDAS).***

19. *Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej.*

20. *Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny.*

21. *ITU X.520 Information technology - Open Systems Interconnection - The Directory: Selected attribute types.*

22. *IETF RFC 5280: Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile, May 2008.*

23. *IETF RFC 6818: Updates to the Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile, January 2013.*

24. *DIRECTIVE (EU) 2015/2366 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2015 on payment services in the internal market.*

25. *ETSI EN 319 412-1; Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures.*

26. *ISO 3166-1:2013, Codes for the representation of names of countries and their subdivisions - Part 1: Country codes.*

27. *IETF RFC 3490: Internationalizing Domain Names in Applications (IDNA), March 2003.*

28. *IETF RFC 8659: DNS Certification Authority Authorization (CAA) Resource Record, November 2019.*

29. *IETF RFC 6532: Internationalized Email Headers, February 2012.*

30. *IETF RFC 3966: The tel URI for Telephone Numbers, December 2004.*

31. *PRADO - Public Register of Authentic identity and travel Documents Online, https://www.consilium.europa.eu/prado/en/prado-start-page.html.*

32. *IETF RFC 6960: X.509 Internet Public Key Infrastructure - Online Certificate Status Protocol (OCSP), June 2013.*

33. *IETF RFC 5019: The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environment, September 2007.*

34. *IETF RFC 5755: An Internet Attribute Certificate Profile for Authorization, January 2010.*

35. *ETSI TS 119 312; Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.*

36. *ISO/IEC 19790:2012: Information technology – Security techniques – Security requirements for cryptographic modules.*

37. *ISO/IEC 15408-2002, Information Technology - Methods and Means of a Security - Evaluation Criteria for IT Security.*

38. *EU Trusted Lists of Certification Service Providers, https://eidas.ec.europa.eu/efda/tl-browser/#/screen/home.*

39. *NIST Special Publication 800-56A Revision 3 (April 2018): Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography.*

40. ***ITU X.509 Information technology - Open Systems Interconnection - The Directory: Public- key and attribute certificate frameworks.***

41. ***CEN EN 419 241-1:2018 (July 2018); Trustworthy Systems Supporting Server Signing – Part 1: General System Security Requirements.***

42. ***Compilation of Member States notification on SSCDs and QSCDs; https://eidas.ec.europa.eu/efda/browse/notification/qscd-sscd.***

43. ***CA/Browser Forum Network and Certificate System Security Requirements, v.1.7, https://cabforum.org/working-groups/netsec/documents/.***

44. ***IETF RFC 3161: Internet X.509 Public Key Infrastructure - Time-Stamp Protocol (TSP), August 2001.***

45. ***IETF RFC 5816: ESSCertIDv2 Update for RFC 3161, April 2010.***

46. ***ETSI EN 319 422; Electronic Signatures and Infrastructures (ESI); Timestamping protocol and time-stamp token profiles.***

47. ***Recommendation ITU-R TF.460-6 (2002): Standard-frequency and time-signal emissions.***

48. ***ETSI EN 319 102-1; Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation.***

49. ***IETF RFC 3739: Internet X.509 Public Key Infrastructure - Qualified Certificates Profile, MARCH 2004.***

50. ***IETF RFC 6962: Certificate Transparency, June 2013.***

51. ***ETSI EN 319 412-2; Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons.***

52. ***ETSI EN 319 412-3; Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons.***

53. ***ETSI EN 319 412-4; Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates.***

54. ***ETSI EN 319 412-5; Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements.***

55. ***Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 6: Requirements for Trust Service Providers issuing publicly trusted S/MIME certificates.***

56. ***ITU X.501 Information technology - Open Systems Interconnection - The Directory: Models.***

57. ***IETF RFC 8954: Online Certificate Status Protocol (OCSP) Nonce Extension, November 2020.***

58. ***ETSI EN 319 403-1; Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 1: Requirements for conformity assessment bodies assessing Trust Service Providers.***

59. ***ETSI EN 319 401; Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.***

60. ***ETSI TS 119 461; Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects.***

61. ***Ustawa o ochronie danych osobowych z dn. 10 maja 2018 r. .***

62. ***REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.***