# Polityka Certyfikacji i Kodeks Postępowania Certyfikacyjnego

# Niekwalifikowanych Usług EuroCert

# wersja 3.0

**Data wejścia w życie: 02.04.2024**

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

# Metryczka regulacji

| Podstawowe informacje | |
|---|---|
| Sygnatura | 0-PT-013-03 |
| 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 |
| 01.12.2017 | 1 | Wersja inicjalna. |
| 02.06.2020 | 2 | Zmiana częstotliwości publikacji CRL, wprowadzenie metod identyfikacji zdalnej osób fizycznych w sekcji 3.2.3. |
| 02.04.2024 | 3 | Całkowita zmiana treści. Dostosowanie do wymogów eIDAS, ETSI, CA/Browser Forum. |

# Spis treści

# 1. Wstęp

Niniejszy dokument stanowi Politykę Certyfikacji i Kodeks Postępowania Certyfikacyjnego, opracowane przez EuroCert Sp. z o.o. (zwaną dalej EuroCert lub Dostawcą Usług Zaufania - TSP), dotyczące wydawania następujących certyfikatów:

- Certyfikatów podpisywania kodu,
- Certyfikatów E-mail,
- Certyfikatów do uwierzytelniania stron internetowych,
- Certyfikatów do podpisów (pieczęci) elektronicznych

oraz certyfikatów niekwalifikowanych zgodnych z eIDAS (Usług Zaufania):

- Certyfikatów do podpisów (pieczęci) elektronicznych,
- Certyfikatów do uwierzytelniania stron internetowych,
- Innych certyfikatów.

PCKPC jest zgodny z wymaganiami eIDAS (1), a usługi dostarczane w ramach niniejszych przepisów są usługami zaufania UE.

TSP powiadomił Ministra właściwego ds. cyfryzacji o świadczeniu Usług Zaufania w dniu 6 grudnia 2017 roku.

TSP dostarcza swoim Klientom najważniejsze informacje również w formie Regulaminu Usług Zaufania. Regulamin jest publikowany zgodnie z wytycznymi zawartymi w sekcji 2.1.

TSP świadczy ww. usługi wyłącznie na podstawie umowy z Klientem.

PCKPC określa ramy świadczenia wyżej wymienionych usług i zawiera szczegółowe procedury i inne zasady działania. Zawiera również zalecenia dla Stron Ufających w zakresie weryfikacji podpisów (pieczęci) elektronicznych i Certyfikatów powiązanych z tymi usługami.

## 1.1. Wprowadzenie

Polityka Certyfikacji to zbiór zasad, które określają użyteczność Certyfikatu dla podmiotów i/lub określonej kategorii zastosowania, posiadających wspólne wymagania bezpieczeństwa. Zawartość i format dokumentu są zgodne z wymaganiami IETF RFC 3647 (2). Niniejszy dokument podzielony jest na 9 sekcji i zawiera wymagania bezpieczeństwa, procesy i praktyki określone przez TSP, przestrzegane przy świadczeniu usług. W celu przestrzegania struktury dokumentu wymaganej przez IETF RFC 3647 (2), nagłówki sekcji, w których PCKPC nie nakłada wymagań zostały opatrzone uwagą „Brak zastrzeżeń".

Niniejszy dokument zawiera wymagania dla wielu Polityk Certyfikacji. Większość tych wymagań dotyczy wszystkich Polityk Certyfikacji w takim samym stopniu i nie są specjalnie wyszczególniane. W przypadku, gdy dane 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 adekwatność i wiarygodność Certyfikatów w zależności od danego zastosowania. Polityki Certyfikacji określają podstawowe wymagania związane z certyfikatami, szczególnie w stosunku dla ich wystawcy, tj. Dostawcy Usług Zaufania. Sposób realizacji tych wymogów oraz szczegółowy opis procedur wymienionych w Polityce Certyfikacji zostały zawarte w PCKPS.

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

Celem niniejszego dokumentu jest podsumowanie wszystkich informacji, które powinien znać Klient zainteresowany usługami TSP, po to, aby pomóc Klientom (w tym potencjalnym):

- lepiej zapoznać się ze szczegółami i warunkami usług oraz praktycznymi aspektami świadczenia usług,
- zrozumieć działalność TSP i przez to łatwiej zdecydować czy (i które) usługi odpowiadają indywidualnym potrzebom czy oczekiwaniom.

Dodatkowo, niniejszy dokument ma na celu wsparcie użytkowników (w tym Stron Ufających) Certyfikatów, list CRL oraz odpowiedzi dotyczących statusu certyfikatów online wydawanych przez TSP 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.

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

Sekcja 1.6 niniejszego dokumentu określa znaczenia terminów, które nie są, lub nie są w pełni, użyte w tym samym znaczeniu co w innych fragmentach dokumentu. Terminy użyte w tym znaczeniu są w dokumencie pisane wielką literą, czcionką pochyłą.

## 1.2. Identyfikator i nazwa dokumentu

Główne dane identyfikacyjne PCKPC stanowią:

| | |
|---|---|
| Wydawca | EuroCert Sp. z o.o. |
| Nazwa dokumentu | Polityka Certyfikacji i Kodeks Postępowania Certyfikacyjnego Niekwalifikowalnych Usług EuroCert |
| Wersja dokumentu | 3.0 |
| Data obowiązywania | 02.04.2024 |

Lista i identyfikatory Polityk Certyfikacji, określonych w PCKPC są zawarte w sekcji 1.2.1.

### 1.2.1. Polityki Certyfikacji

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

Pierwsze pięć liczb 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 liczby zostały przypisane przez EuroCert wraz z poniższym znaczeniem:

| | |
|---|---|
| (1.2.616.1.113791) | EuroCert Sp. z o.o. |
| (2) | EuroCert Commercial |
| (1) | Dokumenty |
| (1) | Publiczne dokumenty |
| (x) | Unikalny identyfikator dokumentu |

Zgodnie z PCKPC, TSP wydaje Certyfikaty w oparciu o następujące Polityki Certyfikacji:

| OID | ZNACZENIE | SKRÓT |
|---|---|---|
| 1.2.616.1.113791.2.1.1.1 | Brak zgodności z eIDAS, klasa certyfikacji III., dla os. fiz., wydany na Urządzeniu Kryptograficznym. | AETHN |
| 1.2.616.1.113791.2.1.1.2 | Brak zgodności z eIDAS, klasa certyfikacji III., dla os. fiz., wydany bez Urządzenia Kryptograficznego. | AETSN |
| 1.2.616.1.113791.2.1.1.3 | Brak zgodności z eIDAS, klasa certyfikacji III., dla os. Prawnych, wydany bez Urządzenia Kryptograficznego. | AEJSN |
| 1.2.616.1.113791.2.1.1.4 | Brak zgodności z eIDAS, klasa certyfikacji III. | AExxN |
| 1.2.616.1.113791.2.1.1.5 | Brak zgodności z eIDAS, klasa certyfikacji II., dla os. fizycznych. | BETxN |
| 1.2.616.1.113791.2.1.1.6 | Brak zgodności z eIDAS, klasa certyfikacji II., dla os. prawnych. | BEJxN |
| 1.2.616.1.113791.2.1.1.8 | Brak zgodności z eIDAS, klasa certyfikacji II, wydany na Urządzeniu Kryptograficznym. | BExHN |
| 1.2.616.1.113791.2.1.1.7 | Brak zgodności z eIDAS, klasa certyfikacji II. | BExxN |
| 1.2.616.1.113791.2.1.1.9 | Brak zgodności z eIDAS, klasa certyfikacji III, do podpisywania kodu, wydany na Urządzeniu Kryptograficznym. | AKxHN |
| 1.2.616.1.113791.2.1.1.10 | Brak zgodności z eIDAS, klasa certyfikacji II, do podpisywania kodu, wydany na Urządzeniu Kryptograficznym. | BKxHN |
| 1.2.616.1.113791.2.1.1.11 | Polityka certyfikacji dla certyfikatów S/MIME. | xSxxN |
| 1.2.616.1.113791.2.1.1.12 | Niekwalifikowany do generowania i weryfikacji podpisów elektronicznych, klasa certyfikacji III., dla osób fizycznych, wydawany na Urządzeniu Kryptograficznym. | AATHN |
| 1.2.616.1.113791.2.1.1.13 | Niekwalifikowany do generowania i weryfikacji podpisów elektronicznych, klasa certyfikacji III., dla osób fizycznych, wydawany bez Urządzenia Kryptograficznego. | AATSN |
| 1.2.616.1.113791.2.1.1.14 | Niekwalifikowany do generowania i weryfikacji podpisów elektronicznych, klasa certyfikacji II., dla osób fizycznych. | BATxN |
| 1.2.616.1.113791.2.1.1.15 | Niekwalifikowany do generowania i weryfikacji pieczęci elektronicznych, klasa certyfikacji III., dla os. prawnych, wydawany na Urządzeniu Kryptograficznym. | ABJHN |
| 1.2.616.1.113791.2.1.1.16 | Niekwalifikowany do generowania i weryfikacji pieczęci elektronicznych, klasa certyfikacji III., dla os. prawnych, wydawany bez Urządzenia Kryptograficznego. | ABJSN |
| 1.2.616.1.113791.2.1.1.17 | Niekwalifikowany do generowania i weryfikacji pieczęci elektronicznych, klasa certyfikacji II., dla os. prawnych. | BBJxN |
| 1.2.616.1.113791.2.1.1.18 | Klasa certyfikacji III., certyfikaty do uwierzytelniania stron internetowych, dla os. prawnych. | AWJSN |

| | | |
|---|---|---|
| 1.2.616.1.113791.2.1.1.19 | Klasa certyfikacji II., certyfikaty do uwierzytelniania stron internetowych. | BWJSN, BWTSN |
| 1.2.616.1.113791.2.1.1.20 | Certyfikaty do uwierzytelniania strony internetowej, generowane automatycznie. | CWxSN |

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

TSP nie wydaje Certyfikatów z pseudonimem.

Zgodnie z Politykami Certyfikacji, TSP może wydawać Certyfikaty w celu różnego użycia (do szyfrowania, uwierzytelniania itd.), Certyfikaty, które odpowiadają zaawansowanym podpisom (pieczęciom) elektronicznym zgodnym z Rozporządzeniem eIDAS (1), Certyfikaty, których używa się do uwierzytelnienia serwerów sieciowych. Lista dostępnych użyć jest opisana w rozszerzeniu Certyfikatów w sekcji 7.1.2.

Wydanie Certyfikatu klasy certyfikacji III podlega wcześniejszej fizycznej identyfikacji podmiotu przeprowadzanej przez TSP. W przypadku klasy II, dopuszczalna jest rejestracja zdalna.

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

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

Na podstawie Polityki Certyfikacji [*W*SN], TSP wydaje Certyfikaty do uwierzytelnienia serwera.

W przypadku Certyfikatów Uwierzytelniania Stron Internetowych w miejscu nazwy Podmiotu podana jest nazwa domeny i adres IP.

Certyfikaty Uwierzytelniania Stron Internetowych, Certyfikaty Email, Certyfikaty Pieczęci nie mogą być wydane z pseudonimem.

TSP przestrzega aktualnej wersji dokumentu pt. Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates (3): https://cabforum.org/baseline-requirements-documents/

W przypadku sprzeczności pomiędzy PCKPC a powyższym, pierwszeństwo mają wymogi “Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates”.

TSP spełnia wymogi aktualnej wersji dokumentu “CA/Browser Forum Guidelines for Issuance and Management of Extended Validation Certificates” (4): https://cabforum.org/extended-validation/

W przypadku sprzeczności pomiędzy PCKPC a powyższym, pierwszeństwo mają wymagania “CA/Browser Forum Guidelines for Issuance and Management of Extended Validation Certificates”.

Z wyjątkiem Certyfikatów Podpisu Elektronicznego, Certyfikaty mogą również zawierać nazwy systemów IT, aplikacji i procesu automatyzacji, za pomocą których Certyfikat jest używany (Certyfikaty dla automatyzacji). Wszystkie Polityki Certyfikacyjne zakazują używania pseudonimów, każdorazowo należy podać prawdziwe nazwisko Podmiotu wskazanego w certyfikacie.

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

- Certyfikat wydany w dowolnym kraju członkowskim Unii Europejskiej stwierdzający, że sprzęt jest Kwalifikowanym Urządzeniem do Składania Podpisu Elektronicznego;
- Certyfikat Common Criteria (5) zgodny z profilem CEN SSCD PP (6) na poziomie EAL-4 lub wyższym;
- Certyfikat Common Criteria (5) zgodny z profilem CEN 419 221-5 (7) na poziomie EAL-4 lub wyższym;
- FIPS 140-2 na poziomie 2 lub wyższym (8);
- FIPS 140-3, na poziomie 2 lub wyższym (9).

W przypadku Certyfikatu do Podpisywania Kodu, TSP przestrzega aktualnej wersji dokumentu pt. “Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates" (10): https://cabforum.org/baseline-requirements-code-signing/.

W przypadku sprzeczności pomiędzy niniejszym dokumentem a powyższym, pierwszeństwo mają wymagania “Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates".

W przypadku Certyfikatów Email (S/MIME) TSP spełnia wymogi aktualnej wersji dokumentu “Baseline Requirements for the Issuance and Management of Publicly Trusted S/MIME Certificates" (11) na stronie https://cabforum.org/smime-br/

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

Wśród Polityk Certyfikacji:

- każda Polityka Certyfikacji jest zgodna z Polityką Certyfikacji [LCP] określoną w normie ETSI EN 319 411-1 (12);
- Polityki [AATHN], [AATSN], [ABJHN], [ABJSN], [AETHN], [AETSN], [AEJSN], [AExxN], [AKxHN] są zgodne z Polityką Certyfikacji NCP;
- Polityka Certyfikacji [CWxSN] jest zgodna z Polityką Certyfikacji [DVCP] określoną w normie ETSI EN 319 411-1 (12);
- Polityki Certyfikacji [AWJSN], [AWJSN (EVC)], [BWJSN] są zgodne z Polityką Certyfikacji [OVCP] określoną w normie ETSI EN 319 411-1 (12);
- Polityka Certyfikacji [BWTSN] jest zgodna z Polityką Certyfikacji [IVCP] określoną w normie ETSI EN 319 411-1 (12);
- Polityka Certyfikacji [AWJSN (EVC)] jest zgodna z Polityką Certyfikacji [EVCP] określoną w normie ETSI EN 319 411-1 (12);
- Polityka Certyfikacji [AATHB], [ABJHN], [AETHN] jest zgodna z Polityką Certyfikacji [NCP+].

**Zgodność z Politykami Certyfikacji ETSI**

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 już zawiera wymagania tej drugiej.

| | [LCP] | [NCP] | [NCP+] | [DVCP] | [OVCP] | [IVCP] | [EVCP] |
|---|---|---|---|---|---|---|---|
| AETHN | (x) | (x) | X | | | | |
| AETSN | (x) | X | | | | | |
| AEJSN | (x) | X | | | | | |
| AExxN | (x) | X | | | | | |
| BETxN | X | | | | | | |
| BEJxN | X | | | | | | |
| BExxN | X | | | | | | |
| BExHN | X | | | | | | |
| AKxHN | (x) | X | | | | | |
| BKxHN | X | | | | | | |
| xSxxN | X | | | | | | |
| AATHN | (x) | (x) | X | | | | |
| AATSN | (x) | X | | | | | |
| BATxN | X | | | | | | |
| ABJHN | (x) | (x) | X | | | | |
| ABJSN | (x) | X | | | | | |
| BBJxN | X | | | | | | |
| AWJSN | (x) | | | | X | | |
| AWJSN (EVC) | (x) | (x) | | | (x) | | X |
| BWJSN | (x) | | | | X | | |
| BWTSN | (x) | | | | | X | |
| CWxSN | (x) | | | X | | | |

### 1.2.2. Zakres obowiązywania

**Zakres przedmiotowy**

PCKPC dotyczy świadczenia i użycia usług opisanych w sekcji 1.3.1.

**Zakres czasowy**

PCKPC 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 TSP.

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

**Zakres osobowy**

PCKPC obowiązuje każdego uczestnika wymienionego w sekcji 1.3.

TSP 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 TSP i pod warunkiem, że niezbędne środki bezpieczeństwa konieczne do świadczenia usług będą mogły być wdrożone w wystarczająco bezpieczny i ekonomiczny sposób.

**Osoby z niepełnosprawnościami**

TSP dokłada wszelkich starań, by zapewnić równy dostęp do usług dla wszystkich.

W celu zapewnienia równych szans dostępu do usług TSP stosuje wszystkie możliwe i rozsądne środki, aby udostępnić swoje usługi również osobom niepełnosprawnym. Szczególnie ważne jest, aby usługi dostosowane do specjalnych potrzeb niepełnosprawnych osób gwarantowały tą sama jakość, jak w innych przypadkach.

TSP współpracuje z Klientami w celu dostarczenia odpowiedniej formy obsługi 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.

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

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

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

### 1.2.3. Poziomy bezpieczeństwa

TSP wyznaczył poziomy bezpieczeństwa biorąc pod uwagę odpowiednie kryteria bezpieczeństwa, w poniżej opisany sposób.

Klasyfikacja według siły uwierzytelnienia Podmiotu Certyfikatu w kolejności malejącej:

- Kwalifikowane Certyfikaty [Q****];
- Niekwalifikowane Certyfikaty, klasa certyfikacji III. [A****] wydane przez EuroCert;
- Niekwalifikowane Certyfikaty, klasa certyfikacji II. [B****] wydane przez EuroCert;
- Niekwalifikowane Certyfikaty nie wydane przez EuroCert.

Klasyfikacja według poziomu bezpieczeństwa użytego nośnika w kolejności malejącej:

- Certyfikaty wydane na Kwalifikowanym Urządzeniu do Składania Podpisu Elektronicznego [***B*];
- Certyfikaty wydane na Urządzeniu Kryptograficznym [***H*];
- inne, na przykład Certyfikaty wydane do pliku (bez urządzenia) [***S*].

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

- Certyfikaty kwalifikowane wydane na Kwalifikowanym Urządzeniu do Składania Podpisu Elektronicznego [Q**B*];
- Certyfikaty kwalifikowane wydane na Urządzeniu Kryptograficznym [Q**H*];
- Inne kwalifikowane, na przykład Certyfikaty wydane do pliku (bez urządzenia) [Q**S*];

- Certyfikaty niekwalifikowane, klasa certyfikacji III. wydane przez EuroCert [A**S*];
- Certyfikaty niekwalifikowane, klasa certyfikacji II. wydane przez EuroCert [B**S*];
- Certyfikaty niekwalifikowane wydane przez innego dostawcę niż EuroCert.

Podczas komunikacji z klientami, TSP 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) co dany Certyfikat, będący przedmiotem sprawy.

W wyjątkowych przypadkach, rozpatrywanych indywidualnie, TSP może odstąpić od ścisłego przestrzegania powyższej klasyfikacji dla określonych podzadań w określonych przypadkach (np. odstąpienie od fizycznej weryfikacji w przypadku wniosku o nowy kwalifikowany certyfikatu lub jego modyfikację istniejącego, 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

Odbiorcami niniejszego PCKPC są:

- TSP,
- Klienci EuroCert (Subskrybenci i Podmioty),
- Strony Ufające,
- Inni uczestnicy.

### 1.3.1. Urząd Certyfikacji

Urząd certyfikacji jest Dostawcą Usług Zaufania, który wydaje Certyfikaty w ramach Usługi Zaufanej 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 KPC, zgodność z dowolną PC 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.<br>Polska, 02-884 Warszawa, ul. Puławska 472 |
| Urząd Ochrona Danych: | Urząd Ochrony Danych Osobowych<br>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 Rozporządzenia 910/2014/EU (1) (zwanym dalej: eIDAS).

EuroCert rozpoczął świadczenie usług związanych z podpisem elektronicznym na podstawie Ustawy o Podpisie Elektronicznym z 2001 r. (13) (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 oraz polskiej Ustawy implementującej z dnia 5 września 2016 o Usługach Zaufania oraz Identyfikacji Elektronicznej (14) 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. Usługa Zdalnego Podpisu).

**Jakość i bezpieczeństwo informacji**

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

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

TSP nie ujawnia swojej wewnętrznej Polityki Bezpieczeństwa z powodu jej poufnego charakteru. TSP 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 „EuroCert Commercial" 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 TSP dostarcza Subskrybentom następujące usługi:

- Wydawanie Certyfikatów niepodlegających eIDAS;
- Wydawanie Certyfikatów Podpisów Elektronicznych podlegających eIDAS;
- Wydawanie Certyfikatów Pieczęci Elektronicznych podlegających eIDAS;
- Wydawanie Certyfikatów Uwierzytelniania Witryn Internetowych podlegających eIDAS;
- Zdalny Podpis Elektroniczny.

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

**Usługa wydawania Certyfikatów**

W celu wydania Certyfikatu TSP podpisuje z Subskrybentem umowę na świadczenie usług, w ramach której generuje 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 ważnej subskrypcji Aplikujący może zainicjować następujące czynności:

- Aplikować o Certyfikat (i dodatkowo Urządzenie do Składania Podpisu/Pieczęci Elektronicznej), wydanie Certyfikatu odbywa się zgodnie z Polityką Certyfikacji lub politykami;

- Wystąpić o unieważnienie swojego Certyfikatu;
- 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 TSP.

TSP publicznie udostępnia Listę Certyfikatów Unieważnionych. Lista ta zawiera wydane Certyfikaty, które zostały unieważnione. TSP 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.

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

Na specjalną prośbę klienta, w indywidulanych przypadkach, TSP 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 1.2.1. 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 przypisanymi Podmiotowi.

- Certyfikat Organizacyjny oznacza:
  a) Certyfikat, w którym Podmiot jest Organizacją, urządzeniem pod kontrolą Organizacji; lub
  b) Certyfikat, w którym Podmiotem jest osoba fizyczna, zawierający nazwę organizacji w polu „O", z którą dana osoba fizyczna jest związana; ten typ Certyfikatu może być używany jedynie w sposób określony przez Organizację; w przypadku Certyfikatu Organizacyjnego wydanego dla osoby fizycznej dalsze ograniczenia w odniesieniu do celu użycia Certyfikatu mogą być wskazane w polu „Title"; lub
  c) Certyfikat, który zaświadcza o związku pomiędzy Organizacją a nazwą domeny lub adresem IP. W takim przypadku, nazwa Organizacji zawarta 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 adresu IP lub ma odpowiednie do nich upoważnienie.

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

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

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

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

Urząd Certyfikacji wydaje Certyfikaty dla osób fizycznych i prawnych. W przypadku Certyfikatów dla osób prawnych wymagane jest upoważnienie dla osób fizycznych działających imieniu osoby prawnej.

**Certyfikaty Testowe**

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

TSP 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.

TSP 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 żaden OID.

**Urządzenia do Podpisu**

TSP umieszcza dane do składania podpisu elektronicznego (klucz prywatny) Podmiotu związane z certyfikatem na Urządzeniu do Składania Podpisu (Pieczęci) Elektronicznego.

**Jednostki Certyfikacji**

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

Hierarchia Jednostek Certyfikacji, uwzględniająca Jednostki Root i Podległe: https://eurocert.pl/en/certyfikaty-i-listy-crl/.

**Aktywna hierarchia RSA, oparta o algorytm SHA-256**

- **"EuroCert Commercial"** – Główna Jednostka Certyfikacji
  Wydaje Certyfikaty oparte o algorytm SHA-256 dla Jednostek Certyfikacji TSP. Ta Jednostka Certyfikacji posiada samo-podpisany Certyfikat (oparty na algorytmie SHA-256, RSA 4096 bit). Ta jednostka Certyfikacji wydaje również certyfikaty użytkownika końcowego dla osób fizycznych i prawnych zgodnie z Politykami Certyfikacji wymienionymi w sekcji 1.2.1.
- **responder OCSP**
  Każda Jednostka Certyfikacji poświadcza osobny dedykowany urząd statusu certyfikatu online (OCSP responder), który udziela odpowiedzi na temat statusu unieważnienia Certyfikatów wydanych przez tą jednostkę certyfikacji. Nazwa respondera OCSP zawiera tekst „OCSP Responder” następujący po nazwie danej jednostki certyfikacji, która go wygenerowała. W certyfikatach dla OCSP responder występuje rozszerzone użycie klucza "OCSPSigning".

Wszystkie powyższe jednostki certyfikacji posiadają Certyfikaty SHA-256 i klucze o długości 4096 bit oraz wydają Certyfikaty końcowe oraz odpowiedzi OCSP oparte na algorytmie SHA-256.

W tej hierarchii wszystkie wydane użytkownikowi końcowemu Certyfikaty używają kluczy RSA o długości 4096 bitów lub kluczy ECC o długości co najmniej 256 bitów.

**Publikacja Certyfikatów Root**

Wszystkie Certyfikaty Root są dostępne na stronie stronę internetową: https://eurocert.pl/certyfikaty-i-listy-crl/.

Odcisk SHA-1 Certyfikatu Root "EuroCert Commercial": b271243aae8b64e2312a4d78e3ceb804b234d5dd

Inne Certyfikaty TSP mogą być zweryfikowane na podstawie samo-podpisanych Certyfikatów Root, zatem te Certyfikaty są wyłącznie publikowane przez TSP na jego stronie. Jeśli ze względu na wymogi prawne lub wynikające z umowy, inny Dostawca Usług wydaje certyfikaty dla Jednostek Certyfikacji TSP, TSP również musi opublikować te Certyfikaty na swojej stronie internetowej. TSP gwarantuje, że w przypadku Certyfikatów wydanych w ten sposób spełnia on wymogi certyfikacji krzyżowej i uznaje informacje zawarte w Polityce Certyfikacji dostawcy usług wydającego certyfikat jako wiążące.

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

### 1.3.2. Urzędy Rejestracji

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

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

TSP nie deleguje walidacji domen FQDN i adresu IP zgodnie z sekcją 3.2.2 do niezależnego Urzędu Rejestracji. Walidacji dokonuje wewnętrzny Urząd Rejestracji TSP.

Główny wewnętrzny Urząd Rejestracji dokonuje rejestracji i wykonuje inne czynności związane z wydawaniem Certyfikatów oraz ich dalszym zarządzaniem, w ramach biura obsługi klienta wewnątrz organizacji.

Zadania biura obsługi Klienta, pełniącego rolę Urzędu Rejestracji:

- Rejestracja Podmiotu wskazanego w Certyfikatach użytkownika końcowego,
- Zarządzanie i rejestracja wydanych Certyfikatów i Urządzeń do Składania Podpisów lub Pieczęci Elektronicznych,
- Utrzymywanie kontaktu z Klientami (odbieranie zapytań, zgłoszeń, wniosków, skarg i rozpoczęcie ich przetwarzania),
- Unieważnienie, zawieszenie, uchylenie zawieszenia, odnowienie, modyfikacja certyfikatu i wymiana kluczy (re-key).

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

Urząd Rejestracji może dokonywać rejestracji w poniższych lokalizacjach:

- W biurze obsługi klienta TSP lub biurze niezależnego RA,

- Przedstawiciel Urzędu Rejestracji może dokonać rejestracji u Klienta według wewnętrznych wytycznych TSP.

### 1.3.3. Subskrybenci

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

W przypadku Certyfikatów do podpisu elektronicznego, Podmiot jest osobą Podpisującą i Aplikującą.

W przypadku Certyfikatów do pieczęci elektronicznych, Podmiot jest składającym pieczęć elektroniczną.

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

Klienci usług dostarczanych przez TSP:

- Subskrybent
  - Podpisuje umowę na świadczenie usług z TSP (jako „Contract Signer" w rozumieniu certyfikatów EV),
  - Akceptuje Regulamin usług zaufania (jako „Applicant Representative" w rozumieniu certyfikatów EV),
  - Wyznacza Aplikujących (Podmiotów w przypadku Certyfikatów dla osób fizycznych),
  - Wyraża zgodę na umieszczenie danych organizacji w Certyfikacie,
  - Może wyznaczyć Administratorów Organizacyjnych,
  - Odpowiada za płatności wynikłe z korzystania z usług.
- Podmiot
  - TSP wydaje Certyfikat Podmiotowi.
- Podpisujący
  - użytkownik usługi certyfikatu podpisu elektronicznego, który może składać podpis elektroniczny przy pomocy wydanego Certyfikatu.
- Składający pieczęć elektroniczną
  - użytkownik usługi certyfikatu pieczęci elektronicznej, który może składać pieczęć elektroniczną przy pomocy wydanego Certyfikatu.
- Aplikujący
  - Składa wniosek o Certyfikat do Uwierzytelniania Witryn Internetowych (jako „Certificate Requester" i „Approver" w rozumieniu certyfikatów EV) i Certyfikat do pieczęci elektronicznych.

### 1.3.4. Strony Ufające

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

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

Strony Ufające walidują i używają podpisów i pieczęci elektronicznych. Zwykle nie wiedzą, że podpisy lub pieczęci 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

#### 1.4.1. Właściwe użycie Certyfikatu

Klucze prywatne należące do Certyfikatów użytkowników końcowych wydanych przez TSP w oparciu o niniejszy dokument mogą być użyte jedynie do celów określonych w treści Certyfikatu oraz PCKPC. Celem użycia może być podpis, pieczęć, szyfrowanie lub uwierzytelnienie, w zależności od danego zakresu użycia (zastosowania) przypisanego do Certyfikatu (zob. sekcja 6.1.7).

Certyfikaty do podpisów elektronicznych mogą być użyte wyłącznie w celu składania podpisu elektronicznego. Dzięki Certyfikatowi Podpisujący może zweryfikować autentyczność dokumentów, które podpisuje.

Klucz publiczny w Certyfikacie do podpisu elektronicznego lub pieczęci, sam Certyfikat, Lista CRL, Znaczniki Czasu i odpowiedzi online o statusie unieważnienia Certyfikatu mogą być użyte do złożenia podpisu elektronicznego i zawierać się w nim.

Certyfikat do podpisów elektronicznych wydany zgodnie z PCKPC jest odpowiedni do składania zaawansowanych podpisów elektronicznych.

Certyfikaty do pieczęci elektronicznych mogą być użyte wyłączne do składania pieczęci elektronicznej. Przy pomocy Certyfikatu Składający pieczęć elektroniczną może zweryfikować autentyczność dokumentów, które podpisuje.

Certyfikat do pieczęci elektronicznych wydany zgodnie z PCKPC jest odpowiedni do składania zaawansowanych pieczęci elektronicznych.

Certyfikaty do Uwierzytelniania Witryn Internetowych mogą być użyte wyłącznie do uwierzytelniania stron internetowych lub 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 (keyUsage, extKeyUsage) i PCKPC jest niedozwolone.

**Certyfikaty Dostawcy**

Certyfikaty root i pośrednie CA oraz powiązane z nimi klucze prywatne nie powinny być używane do wydawania Certyfikatów przed ujawnieniem Certyfikatów CA.

**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.

## 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**

TSP utrzymuje ciągłą, całodobową (24/7) zdolność do wewnętrznego reagowania na pilne problemy związane z Certyfikatami. Osobą odpowiedzialną za przetwarzanie zgłoszonych problemów 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 zgłaszania incydentów | https://repozytorium.eurocert.pl/ |

TSP 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 PC

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

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 |
| 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 adresem: 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.<br><br>Osoba prawna z tożsamością lub atrybutami zweryfikowanymi w Certyfikacie przez Dostawcę Usług Zaufania.<br><br>Osoba fizyczna z tożsamością lub atrybutami zweryfikowanymi w Certyfikacie przez Dostawcę Usług Zaufania, zazwyczaj jest to osoba Podpisująca zwłaszcza w przypadku certyfikatu podpisu elektronicznego.<br><br>W przypadku Certyfikatu do Uwierzytelniania Witryn, Podmiotem jest serwer internetowy, zidentyfikowany przez nazwę domeny lub adres IP. |
| Podpisujący | "Osoba fizyczna która składa podpis elektroniczny."<br>(eIDAS (1) artykuł 3. punkt 9.)<br>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 TSP. 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. |
| Organ Nadzoru | Minister właściwy ds. informatyzacji, organ nadzorujący i monitorujący Usługi Zaufane (Ustawa o usługach zaufania, artykuł 27.1 (14)) |
| Usługa Zaufania | Usługa elektroniczna zazwyczaj świadczona za wynagrodzeniem i obejmująca:<br>a/ tworzenie, weryfikację i walidację podpisów elektronicznych, pieczęci elektronicznych lub elektronicznych znaczników czasu, usług rejestrowanego doręczenia elektronicznego oraz certyfikatów powiązanych z tymi usługami; lub<br>b/ tworzenie, weryfikację i walidację certyfikatów uwierzytelniania witryn internetowych; lub<br>c/ konserwację elektronicznych podpisów, pieczęci lub certyfikatów powiązanych z tymi usługami.<br>(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) art. 3, punkt 14) |
| Dane służące do składania podpisu elektronicznego | unikalne dane, których podpisujący używa do składania podpisu elektronicznego (eIDAS (1) art. 3 pkt 13)<br>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)<br>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 i korzystająca z tych usług. |
| Reprezentant Subskrybenta (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.<br>Odbiorca dokumentu elektronicznego, który działa na podstawie podpisu elektronicznego (pieczęci) opartego na danym certyfikacie.<br>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. |
| 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:<br>a) jest unikalnie przyporządkowany podpisującemu;<br>b) umożliwia ustalenie tożsamości podpisującego;<br>c) jest składany przy użyciu danych służących do składania podpisu elektronicznego, których podpisujący może, z dużą dozą pewności, użyć pod wyłączną swoją kontrolą; oraz<br>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:<br>a/ jest unikalnie przyporządkowana podmiotowi składającemu pieczęć; |

| | |
|---|---|
| | b/ umożliwia ustalenie tożsamości podmiotu składającego pieczęć;<br>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<br>d/ jest powiązana z danymi, do których się odnosi, w taki sposób, że każda późniejsza zmiana danych jest rozpoznawalna."<br>(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 bezpieczeństwa, 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). Urzędowi Certyfikacji może podlegać kilka Jednostek Certyfikacji 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 (14) § 19. ust. 1, 2). |
| 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 | 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 (14), § 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.<br>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 ją przy pomocy klucza prywatnego.<br>Podczas tworzenia Certyfikatu, Urząd Certyfikacji używa kluczy prywatnych Jednostki Certyfikacji do składania podpisu lub pieczęci elektronicznej na Certyfikacie w celu jego zabezpieczenia. |
| 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.)<br>Poprzednio zwane Bezpiecznym Urządzeniem do Składania Podpisu. |
| Usługa Zdalnego Podpisu | Usługa zaufania w której dostawca usługi zarządza kluczem prywatnym Klienta w bezpiecznych warunkach, zapewnia niezbędne warunki |

| | |
|---|---|
| | techniczne i organizacyjne, aby umożliwić klientowi wykonanie zdalnych operacji z użyciem klucza przechowywanego u Dostawcy, takich jak składanie podpisu, pieczęci. |
| 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.<br>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.<br>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:<br>a/ działania jako Wnioskodawca Certyfikatu i do upoważniania innych pracowników lub osób trzecich do występowania jako Wnioskodawca Certyfikatu, i<br>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 procedur i innych wymagań operacyjnych wykorzystywanych w celu świadczenia Usług Zaufania". |
| Umowa na świadczenie usług | "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.)<br>W polu nazwy Certyfikatu podaje się nazwę domeny serwera internetowego lub adres IP. |

| | |
|---|---|
| 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. „żęgóś.example.com”. Te nazwy domen są przechowywane w systemie nazw domen (DNS) jako ciągi ASCII przy użyciu transkrypcji Punycode. |
| Open Banking | Uregulowane środowisko dla usług płatniczych odrębnych od dyrektywy UE PSD2 lecz działających na podstawie identycznych lub bardzo podobnych wymagań. |
| Nazwa domeny typu Wildcard | Ciąg znaków rozpoczynający się od „*.” (U+002A ASTERISK, U+002E FULL STOP) po którym następuje pełna kwalifikowana nazwa domeny (FQDN). |
| Certyfikat typu 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 |
| LSCP | Lightweight SSASC Policy |
| NSCP | Normalized 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

TSP 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 TSP.

Po zawarciu umowy, TSP udostępnia Klientowi Regulamin świadczenia usług i PCKPC w formie pliku pdf podpisanego elektronicznie, który można pobrać ze strony. TSP 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.

TSP powiadamia Klienta o każdej zmianie Regulaminu świadczenia usług zaufania.

## 2.2. Publikacja informacji certyfikacyjnej

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

- Certyfikaty Dostawcy Usług Zaufania;
- Wszystkie Certyfikaty Krzyżowe, które identyfikują TSP jako Podmiot;
- Certyfikaty użytkownika końcowego, w przypadku zgody Podmiotu.

**Certyfikaty Dostawcy Usług**

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

- Nazwę głównych jednostek certyfikacji root i funkcję skrótu certyfikatów root w PCKPC (zob. sekcję 1.3.1). Informacje dotyczące zmiany ich statusu są dostępne na stronie internetowej Urzędu TSP.
- 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**

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

- Na liście certyfikatów unieważnionych (CRL),
- W ramach usługi informowania o statusie certyfikatu online OCSP.

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

TSP 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, a pojedyncze przerwy w świadczeniu usług nie przekroczą 3 godzin.

## 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 (15).

TSP 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 TSP co najmniej 14 dni przed planowanym wejściem w życie.

### 2.3.2. Częstotliwość ujawniania Certyfikatów

TSP przestrzega następujących reguł w odniesieniu do ujawniania Certyfikatów:

- Certyfikaty głównych jednostek certyfikacji są ujawniane przed ich uruchomieniem;

- Certyfikaty pośrednich jednostek certyfikacji są ujawniane w ciągu 5 dni roboczych od ich wydania;
- TSP 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 TSP mogą być zmienione, uzupełnione lub usunięte tylko przez TSP. Informacje umieszczone w repozytorium są zabezpieczone przed nieautoryzowanym zmienianiem, dodawaniem i usuwaniem

## 3. Identyfikacja i uwierzytelnienie

### 3.1. Nadawanie nazw

Niniejsza sekcja 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 (16), RCF 5280 (17) i IETF RFC 6818 (18). Ponadto, TSP stosuje alternatywne nazwy w rozszerzeniach: Alternatywną Nazwę Podmiotu (Subject Alternative Names) i Alternatywną Nazwę Wystawcy (Issuer Alternative Names).

TSP 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:

- **Common name (CN)** – OID: 2.5.4.3
  Nazwa powszechna Podmiotu

W przypadku osób fizycznych, nazwa Podmiotu w tym polu jest w takiej samej formie jak została zweryfikowana przez TSP 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 TSP 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 pojedynczą FQDN lub adres IP, które są jedną z wartości znajdujących się w rozszerzeniu “Alternatywne Nazwy Podmiotu” w Certyfikacie.

Wartość pola CN jest kodowana w następujący sposób:

1) IPv4 address:

Wartość jest kodowana jako „IPv4Address" zgodnie z RFC 3986 (19), Sekcja 3.2.2.

2) IPv6 address:

Wartość jest kodowana w reprezentacji tekstowej zgodnie z RFC 5952 (20), Sekcja 4. str. 81

3) Pełna Kwalifikowana Nazwa Domeny (FQDN) lub Nazwa Domeny Wildcard:

Pole CN zawiera jedną z wartości w „dNSName” w rozszerzenia „subjectAltName”. W szczególności, wszystkie etykiety domeny (Domain Label) FQDN i FQDN w Domenie Wildcard są kodowane jako etykiety LDH-Labels, a etykiety P-Labels nie są konwertowane do ich reprezentacji Unicode.

Można wpisać jedynie tę domenę lub adres IP, które istnieją i którymi Aplikujący posługuje się zgodnie z prawem.

Certyfikat do Uwierzytelniania Witryn nie może być wydawany z pseudonimem.

**Zawsze wypełniane.**

- **Surname (SN)** – 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.

W przypadku Certyfikatów IVCP w tym polu widnieje nazwisko osoby fizycznej wskazanej w Certyfikacie.

TSP zawsze wypełnia to pole.

W przypadku Certyfikatów DVCP, OVCP i EVCP pole pozostaje niewypełnione.

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

- **Given name (G)** – OID: 2.5.4.42
  Imię osoby fizycznej.

W przypadku Podmiotu będącego osobą fizyczną w tym polu podaje się imię Podmiotu, pochodzące z pełnej nazwy podanej w polu CN.

W przypadku Certyfikatu do Uwierzytelniania Witryn IVCP w tym polu znajduje się imię osoby fizycznej wskazanej w Certyfikacie.

TSP zawsze wypełnia to pole.

Jeżeli Podmiotem Certyfikatu jest Organizacja, pola nie wypełnia się.

W przypadku Certyfikatów DVCP, OVCP i EVCP pole pozostaje niewypełnione.

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

TSP nie wypełnia tego pola.

- **Serial number** – OID: 2.5.4.5
  Niepowtarzalny identyfikator (numer seryjny) Podmiotu.

To pole jest częścią nazwy Podmiotu i to nie jest to samo co pole numer seryjny certyfikatu wskazany przez IETF RFC 5280 (17).

W Certyfikacie zawarty jest 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. TSP 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 pole może zawierać numer rejestracyjny Podmiotu:

- Dla Organizacji prywatnych – numer rejestracyjny nadany przez Urząd Rejestracyjny (np. KRS). Jeśli nie występuje nr rejestracyjny wtedy wskazana jest data rejestracji w formacie YYYY-MM-DD.
- 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:

1) Określonym w ETSI EN 319 412-1 sekcja 5.1.3 (na przykład: "PNOPL- 81234567901"),
2) [Nazwa: Wartość] (na przykład: "Numer dowodu osobistego: AAAAAA"),
3) W innym formacie wymaganym przez Klienta,
4) TSP może nadać własny 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" TSP nie umieszcza akcentów.

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

W przypadku Certyfikatu Organizacyjnego, Certyfikatu OVCP lub EVCP, w polu „O" podaje się pełną lub skróconą legalną nazwę Organizacji zgodnie z nazwą zweryfikowaną przez TSP według sekcji 3.2.2.

W przypadku Certyfikatu Organizacyjnego, OVCP lub EVCP to pole jest zawsze wypełniane.

W przypadku Certyfikatu Code Signing wydanych dla osób fizycznych to pole jest obowiązkowe, zawiera wtedy imię i nazwisko osoby fizycznej.

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

W przypadku Certyfikatów DVCP i IVCP pola nie wypełnia się.

Pole może być użyte tylko na żądanie Aplikującego (w takim przypadku taki Certyfikat nazywa się Certyfikatem Organizacyjnym). Nazwa Organizacji może być wskazana w Certyfikacie do Uwierzytelniania Witryn tylko jeśli ta Organizacja jest prawnym użytkownikiem, właścicielem domeny lub adresu IP lub ma do nich upoważnienie.

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

Jeżeli nazwa połączona lub nazwa samej organizacji przekracza 64 znaków TSP 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 świadczącej usługę.

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

W przypadku Certyfikatu Organizacyjnego, Certyfikatu OVCP lub EVCP, w tym polu podaje się identyfikator Organizacji wskazanej w polu „O", zgodnie z 5.1.4 ETSI EN 319 412-1.

Można podać jedynie dane zweryfikowane przez TSP.

W przypadku Certyfikatu Organizacyjnego dla os. fizycznej, Certyfikatu OVCP lub EVCP wypełnienie tego pola jest opcjonalne. Obowiązkowe jest tylko w przypadku Otwartej Bankowości lub Certyfikatów PSD2 i Certyfikatów Email S/MIME Sponsor-Validated.

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 DVCP lub IVCP pola nie wypełnia się.

Jeśli Podmiotem jest osoba prawna i Klient zażąda wpisania do Certyfikatu danych Podmiotu związanych z Otwartą Bankowością lub Dyrektywą UE o usługach płatniczych (PSD2) (21), pole to zawiera identyfikator składający się z numeru autoryzacyjnego 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 (22) lub inny identyfikator rejestracyjny uznawany przez organ nadzoru, zbudowany zgodnie z ETSI EN 319 412-1 (23).

- **Organizational unit (OU)** – 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 TSP 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 Internetowych, tego pola nie wypełnia się.

- **Business category** – OID 2.5.4.15

Rodzaj organizacji wskazanej w polu „O”, zawiera jeden z poniższych:

  - organizacja prywatna,
  - organizacja publiczna.

Obowiązkowe w przypadku certyfikatów EVCP.

- **jurisdictionOfIncorporationLocalityName** – OID: 1.3.6.1.4.1.311.60.2.1.1

Pełna nazwa odpowiedniej jurysdykcji, jeśli 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 odpowiedniej jurysdykcji, składający się z dwóch liter zgodnie z ISO 3166-1 (24).

Jest zawsze wypełniany.

- **Country name (C)** – OID: 2.5.4.6
  Identyfikator kraju.

W przypadku Certyfikatu Organizacyjnego, Certyfikatu OVCP lub EVCP w tym polu wpisuje się kod kraju, w którym zarejestrowano Organizację, składający się z dwóch liter, zgodnie z ISO 3166-1 (24)

W przypadku Certyfikatu DVCP dwucyfrowy kod kraju (zgodnie z ISO 3166-1 (24) ) domeny lub adresu IP lub - jeśli ciężko to ustalić - kraju Aplikującego.

W przypadku osoby fizycznej (Podmiotu niepowiązanego z Organizacją), w polu podaje się dwuliterowy kod kraju (zgodnie z ISO 3166-1 (24)), który wydal dokument, którym posługuje się Podmiot w celu identyfikacji.

W przypadku Certyfikatu IVCP podaje się dwu literowy kod kraju (zgodnie z ISO 3166-1 (24)), z adresu osoby fizycznej wskazanej w polach "SN" i "GN".

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

Pole zawsze musi być wypełnione.

- **Street Address (SA)** – OID: 2.5.4.9
  Adres organizacji

Adres rejestracji Organizacji wskazanej w polu “O”. Jeśli jest wypełnione, wszystkie dane muszą być zweryfikowane.

- **Locality name (L)** – OID: 2.5.4.7
  Miejscowość

W przypadku Certyfikatu Organizacyjnego, OVCP lub EVCP nazwa miejscowości rejestracji Organizacji wskazanej w polu „O”.

W przypadku Certyfikatu IVCP nazwa miasta z adresu osoby fizycznej wskazanej w polach "SN" i "GN".

W przypadku Certyfikatu DVCP pola nie wypełnia się.

W przypadku Certyfikatu niepowiązanego z Organizacją pola nie wypełnia się.

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

W przypadku Certyfikatu Organizacyjnego, OVCP i EVCP podaje się nazwę województwa lub pełną nazwę kraju z pola „C", gdzie zarejestrowano Organizację wskazaną w polu „O".

W przypadku Certyfikatu IVCP podaje się nazwę województwa lub pełną nazwę kraju z pola „C", które jest miejscem zamieszkania osoby fizycznej wskazanej w polach "SN" i "GN".

Pole opcjonalne.

W przypadku Certyfikatu niepowiązanego z Organizacją pola nie wypełnia się.

W przypadku Certyfikatu DVCP pola nie wypełnia się.

- **Postal code** – OID: 2.5.4.17
  Kod pocztowy

W przypadku Certyfikatu Organizacyjnego, OVCP i EVCP podaje się kod pocztowy miejsca zarejestrowania Organizacji wskazanej w polu „O".

W przypadku Certyfikatu IVCP podaje się kod pocztowy miejsca zamieszkania osoby fizycznej wskazanej w polach "SN" i "GN".

Pole opcjonalne.

W przypadku Certyfikatu niepowiązanego z Organizacją pola nie wypełnia się.

W przypadku Certyfikatu DVCP oraz Email (S/MIME) Sponsor-Validated pola nie jest wypełniane.

- **Title (T)** – 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 przedstawionego przez Organizację niezależną od Podmiotu.

Zawartość pola może się wiązać z dalszymi ograniczeniami użycia Certyfikatu.

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

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

W przypadku Certyfikatów Uwierzytelniania Witryn pole nie jest wypełniane.

- **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" w rozszerzeniu 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**

- Alternatywne Nazwy Podmiotu (Subject Alternative Names)

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. Ta nazwa może być napisana ze znakami diakrytycznymi lub bez.
   TSP jest upoważniony do wskazania charakteru podanej nazwy. TSP 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 wnioskowana 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 TSP, 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 może wystąpić w następującej postaci:
   **"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 (17), stąd nie może zawierać nazwy domeny ze znakiem specjalnym: dolną spacją ("_").
   Domeny Wildcard są zabronione.
   **"iPAddress"**
   Zawiera adres IPv4 lub IPv6, potwierdzony zgodnie z Sekcją 3.2.2.3. Nie zawiera zastrzeżonego adresu IP.

TSP potwierdza, że Aplikujący sprawuje nadzór nad pełną nazwą domeny lub adresem IP lub, że ma prawo do ich używania nadane odpowiednio przez „Domain Name Registrant" lub cesjonariusza.

c) Adres e-mail Podmiotu może być podany w rozszerzeniu „Alternatywne Nazwy Podmiotu" w polu "rfc822Name". Jeśli adres e-mail ma być podany na Certyfikacie, to pole należy wypełnić. TSP 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 wystawcy Certyfikatu (jednostki certyfikacji) w języku angielskim (zobacz sekcję 1.3.1).

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

Nazwa TSP w języku angielskim bez znaków diaktrytycznych.

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

Numer identyfikacji podatkowej wydawcy Certyfikatu.

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

Nazwa jednostki organizacyjnej TSP bez znaków diaktrytycznych.

Wypełnienie jest opcjonalne.

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

Nazwa miasta siedziby bez znaków diaktrytycznych.

Wypełnienie jest opcjonalne.

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

Dwuliterowy kod kraju siedziby TSP zgodny z ISO 3166-1 (24).

- **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 polu Subject Certyfikatu jednostki certyfikacyjnej (wystawcy Certyfikatu).

**Alternatywne Nazwy Jednostki Certyfikacji - wystawcy Certyfikatu**

Pola „Issuer Alternative Names” nie wypełnia się w Certyfikatach użytkowników końcowych. W Certyfikatach Jednostek Certyfikacyjnych (Wystawcy certyfikatów użytkowników końcowych) podaje się jedynie adres e-mail w rozszerzeniu „Subject Alternative Names” (rfc822Name).

**Nazwa Jednostki Znakowania Czasem**

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

Nazwa TSU.

- **Organizacja (O)** – OID: 2.5.4.10

Nazwa TSP.

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

Numer identyfikacji podatkowej TSP.

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

Nazwa jednostki organizacyjnej TSP.

Pole opcjonalne.

- **Lokalizacja (L)** – OID: 2.5.4.7

Nazwa miasta siedziby TSP bez znaków diakrytycznych.

Wypełnienie jest opcjonalne.

- **Nazwa Kraju (C)** – OID: 2.5.4.6

Dwuliterowy kod kraju siedziby TSP zgodny z ISO 3166-1 (24).

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

Nie wypełnia się.

**Nazwy Alternatywne TSU**

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 TSP w języku angielskim bez znaków diakrytycznych.

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

Numer identyfikacji podatkowej TSP.

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

Nie wypełnia się.

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

Nazwa miasta siedziby TSP bez znaków diakrytycznych.

Wypełnienie jest opcjonalne.

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

Dwuliterowy kod kraju siedziby TSP zgodny z ISO 3166-1 (24).

- **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":

- Identyfikator powinien być jednoznacznie rozumiany;
- Nazwa osoby fizycznej w Certyfikacie powinna być wpisana w taki sam sposób, jak ta zweryfikowana przez TSP zgodnie z sekcją 3.2.3;
- Nazwa Organizacji w Certyfikacie powinna być wpisana w taki sam sposób, jak ta zweryfikowana przez TSP zgodnie z sekcją 3.2.2.

### 3.1.3. Anonimowość i pseudonimy Subskrybentów

TSP nie wydaje Certyfikatów 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 TSP. W takiej sytuacji TSP 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 TSP. W celu zapewnienia unikalności TSP nadaje każdemu Podmiotowi identyfikator (OID) – unikalny w rejestrze TSP, który jest wskazany w polu identyfikatora Podmiotu "Subject DN Serial Number".

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

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

**Procedury dotyczące rozwiązywania sporów dotyczących nazw**

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

#### 3.1.6. Uznawalność, uwierzytelnienie i rola znaków towarowych

TSP nigdy nie umieszcza znaków towarowych w Certyfikatach.

TSP w trakcie świadczenia usług posługuje się znakiem towarowym „EuroCert" oraz „ECSigner", których jest właścicielem.

### 3.2. Pierwsza weryfikacja tożsamości

TSP 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.

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

#### 3.2.1. Weryfikacja posiadania Klucza Prywatnego

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

Jeżeli TSP sam wygeneruje klucz prywatny należący do Certyfikatu Podmiotu, zazwyczaj na 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 wydawanych do pliku (bez urządzenia), TSP akceptuje Wniosek o Certyfikat w formacie PKCS#10, który jednocześnie zaświadcza, że właściciel prywatnego klucza rzeczywiście występował o Certyfikat.

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

#### 3.2.2. Uwierzytelnienie tożsamości organizacji lub domeny

##### *3.2.2.1. Uwierzytelnienie tożsamości organizacji*

Tożsamość Organizacji jest weryfikowana w następujących przypadkach:

- Jeżeli Podmiotem Certyfikatu, który ma zostać wydany jest Organizacja;
- 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);
- 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.

TSP może wydać Certyfikat Organizacyjny 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, TSP weryfikuje dane Organizacji i ich autentyczność w oparciu o wiarygodne publiczne rejestry (Kwalifikowane Urzędowe Źródło Informacji).

**Pozostałe dokumenty**

Podczas walidacji Organizacji Prywatnej, TSP weryfikuje, czy Organizacja:

- Faktycznie istnieje, figuruje w oficjalnym rejestrze organizacji i ma aktywny status rejestracji,
- Fizycznie istnieje, tzn. jej adres jest faktycznym adresem, gdzie prowadzi działalność,
- Jest aktywna, tzn. faktycznie prowadzi działalność.

Podczas walidacji Organizacji Publicznej, TSP weryfikuje, czy Organizacja:

- Jest legalnie zarejestrowaną jednostką publiczną,
- Jest aktywna,
- Nazwa podana we Wniosku o Certyfikat pokrywa się z nazwą oficjalnie zarejestrowaną,
- Posiada dokładną datę powołania Organizacji lub identyfikator aktu prawnego ustanawiającego Organizację.

Podczas walidacji Organizacji Publicznej, TSP otrzymuje informacje bezpośrednio z następujących publicznych źródeł informacji:

- Wiarygodne źródło z tego samego organu rządowego,
- Wiarygodne źródło z nadrzędnego organu rządowego,
- Sędzia, który jest aktywnym członkiem Krajowego Sądownictwa, w tej samej jurysdykcji co walidowana organizacja publiczna.

Ponadto w takich przypadkach weryfikacji podlega:

- Czy osoba fizyczna występująca w imieniu Organizacji jest do tego upoważniona;
- Czy Organizacja wyraziła zgodę na wydanie Certyfikatu.

W celu przeprowadzenia weryfikacji, Klient powinien przedstawić następujące dane:

- Oficjalną nazwę, siedzibę i stan prawny Organizacji;
- Oficjalny numer rejestracyjny Organizacji (np. NIP, KRS);
- Nazwę jednostki organizacyjnej w ramach danej Organizacji, o ile ma być wpisana do Certyfikatu;
- W przypadku wydawania Certyfikatu Organizacyjnego osobie fizycznej, stanowisko/rolę Podmiotu w danej Organizacji, o ile wymagane jest wpisanie tych informacji do Certyfikatu;
- Jeśli Podmiotem jest osoba prawna i Klient występuje o umieszczenie w certyfikacie danych Podmiotu dotyczących Otwartej Bankowości lub Dyrektywy UE o Usługach Płatniczych (PSD2) (21), 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:

- Oświadczenie Aplikującego, potwierdzające, że dane podane w celu identyfikacji Organizacji są poprawne i prawdziwe;
- Zaświadczenie, że osoba składająca wniosek o Certyfikat dla Organizacji jest upoważniona do działania w jej imieniu[1];
- W przypadku Certyfikatu Organizacyjnego dla osoby fizycznej – zaświadczenie, że dana organizacja wyraża zgodę na umieszczenie jej nazwy w Certyfikacie[2];
- 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;
- Dokument potwierdzający istnienie Organizacji, jej nazwę i status prawny[4].

TSP jest zobowiązany do weryfikacji ważności i autentyczności przedstawionych dokumentów.

**Walidacja tożsamości Organizacji zagranicznych**

TSP 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, TSP akceptuje:

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

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

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

TSP 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:

- Wnioskodawca składa wniosek o wydanie certyfikatu w formie elektronicznej opatrzony pieczęcią elektroniczną opartą o certyfikat o klasie certyfikacji nie niższej niż wnioskowany certyfikat (zob. 1.2.3.);
- certyfikat użyty do weryfikacji tożsamości został wydany dla tej samej organizacji, która aplikuje o certyfikat;
- Dane organizacji odpowiadają danym zawartym w certyfikacie użytym do podpisania wniosku o certyfikat;
- certyfikat użyty do weryfikacji tożsamości powinien zawierać dane niezbędne w celu jednoznacznej identyfikacji organizacji;
- TSP weryfikuje autentyczność i integralność wniosku o wydanie certyfikatu poprzez sprawdzenie całej ścieżki pełnomocnictw.

#### *3.2.2.2. Walidacja upoważnienia lub kontroli nad domeną*

W Certyfikatach do uwierzytelniania witryn internetowych wymagana jest co najmniej jedna nazwa domeny lub adres IP.

Przed wydaniem Certyfikatu do uwierzytelniania witryn internetowych TSP sprawdza autentyczność nazwy domeny lub adresu IP, które mają być wpisane do Certyfikatu, a Aplikujący powinien udowodnić w praktyce, że ma kontrolę nad daną domeną lub adresem IP.

Jeśli w Certyfikacie wskazana jest więcej niż jedna nazwa domeny lub adres IP, weryfikacja wspomniana powyżej powinna odbyć się dla każdej z nazw.

Jeśli w Certyfikacie jest podana nazwa domeny zawierająca znak typu wildcard "*" (Certyfikat Wildcard), TSP upewnia się, że Aplikujący jest upoważnionym użytkownikiem całego zakresu nazw domeny objętego nazwą domeny typu wildcard. TSP nie wydaje Certyfikatu, w którym zakres nazw domeny odpowiadający nazwie domeny typu wildcard jest zarejestrowany jako gTLD lub ccTLD (na przykład: "*.com", "*.co.uk"), lub jako subdomena pod tymi domenami TLD, pod którymi jest możliwa bezpośrednia rejestracja publicznej nazwy domeny. TSP sprawdza publiczne nazwy domeny pod kątem bezpośredniej rejestracji w sekcji "ICANN DOMAINS" w "Public Suffix List" (https://publicsuffix.org/list/public_suffix_list.dat).

TSP wydaje Certyfikaty wyłącznie dla publicznych nazw domen i adresów IP używanych w Internecie, nie dla nazw domen i adresów IP przeznaczonych do użytku wewnętrznego.

TSP wydaje Certyfikaty wyłącznie dla tych domen najwyższego poziomu (TLDs), które są widoczne w aktualnej bazie TLD IANA (IANA Root Zone Database).

TSP wspiera korzystanie z międzynarodowych nazw domen IDN (Internationalized Domain Names) zgodnie z wymogami IDNA2003 (25).

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

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

TSP prowadzi rejestr na temat tego, które z poniższych metod walidacji domeny zostały użyte, zawierający odpowiednią wersję CA/BF BR.

#### *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. TSP wysyła wartość losową na adres e-mailowy zarejestrowany jako kontakt domeny.

Każdy email może być użyty do identyfikacji wielu nazw domen.

TSP 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.

TSP 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 do kontaktu domeny (BR 3.2.2.4.4)*

Sprawdzenie kontroli wnioskodawcy nad domeną FQDN poprzez

- 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 (ADN),
- umieszczenie w wiadomości e-mail unikalnej wartości losowej i
- 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 (ADN) użyta w wiadomości e-mail jest nazwą domeny (ADN) dla każdej FQDN, która ma zostać potwierdzona.

Wartość losowa jest unikalna dla każdej wiadomości e-mail.

TSP 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 uprawnień do 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 (ADN) do autoryzacji.

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

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

Ta metoda jest wskazana do walidacji nazwy domeny typu Wildcard.

#### *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 (26) 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 (27) 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 (ADN), 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 (ADN), podlegającej weryfikacji. TSP

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 aktywna przez 30 dni od daty jej stworzenia.

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

Ta metoda jest wskazana do walidacji nazwy domeny typu Wildcard.

#### *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 (27) 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. TSP 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 TSP może również wystawić certyfikaty dla innych FQDN, które kończą się etykietami zwalidowanej domeny FQDN

Ta metoda jest wskazana do walidacji nazwy domeny typu Wildcard.

#### *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 ADN.

Każde połączenie telefoniczne może służyć do potwierdzania kontroli nad wieloma domenami ADN, 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, TSP może poprosić o przełączenie do Kontaktu Domeny.

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

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

Ta metoda jest wskazana do walidacji nazwy domeny typu Wildcard.

#### *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 (28) 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. TSP nie może być przekierowany ani zażądać przekierowania, gdyż numer został specjalnie przeznaczony do celu walidacji domeny.

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

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

Ta metoda jest wskazana do walidacji nazwy domeny typu Wildcard.

#### *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 (26) Sekcja 3.

Numer telefonu powinien być podany w parametrach CAA (contactphone). Cała wartość parametru musi zawierać Globalny Numer w formacie zgodnym z RFC 3966 (28) 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"

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

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

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

Ta metoda jest wskazana do walidacji nazwy domeny typu Wildcard.

#### *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) TSP 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.

TSP 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.

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

Ta metoda jest nie wskazana do walidacji nazwy domeny typu Wildcard.

#### *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.

### *3.2.2.3. Uwierzytelnienie adresu IP*

Ta sekcja opisuje dozwolone procesy i procedury do walidacji własności lub kontroli adresu IP (zawartego w Certyfikacie) sprawowanej przez Aplikanta.

TSP przed wydaniem Certyfikatu waliduje każdy adres IP umieszczony w Certyfikacie używając przynajmniej jednej z metod opisanych w niniejszej sekcji.

Ukończona walidacja upoważnienia Aplikanta może być użyta do wydania wielu Certyfikatów na przestrzeni czasu. W każdym przypadku przed wydaniem Certyfikatu walidacja powinna być zapoczątkowana w terminie określonym w sekcji 4.2.1.

TSP prowadzi rejestr metod, które zostały użyte do walidacji poszczególnych adresów IP, biorąc pod uwagę odpowiednia wersję Baseline Requirements.

Certyfikaty EVCP nie mogą zawierać adresu IP.

#### *3.2.2.3.1. Agreed-Upon Change to Website (BR 3.2.2.5.1)*

Potwierdzenie kontroli wnioskodawcy nad adresem IP poprzez weryfikację, czy Wartość Losowa jest zawarta wewnątrz pliku w katalogu "/.well-known/pki-validation" pod adresem IP, który jest dostępny dla TSP poprzez protokół HTTP/HTTPS za pośrednictwem Autoryzowanego Portu.

Wartość Losowa nie powinna pojawić się w żądaniu.

TSP zapewnia Wartość Losową unikalną dla każdego Wniosku o Certyfikat i nie używa Wartości Losowej po upływie 30 dni.

#### *3.2.2.3.2. Email, Fax, SMS, or Postal Mail to IP Address Contact (BR 3.2.2.5.2)*

Potwierdzenie kontroli wnioskodawcy nad adresem IP poprzez wysłanie wartości losowej e-mailem, SMS-em, a następnie otrzymanie odpowiedzi potwierdzającej otrzymanie tej wartości losowej. Wartość Losowa jest wysyłana na adres e-mail lub numer telefonu wskazany do kontaktu dla Adresu IP.

Każdy email, SMS może potwierdzić kontrolę nad wieloma adresami IP.

TSP może wysłać e-mail, SMS, o których mowa w niniejszej sekcji do więcej niż jednego odbiorcy, pod warunkiem, że każdy odbiorca jest zidentyfikowany przez Urząd Rejestracji Adresów IP jako podmiot do kontaktu z adresem IP, dla każdego Adresu IP podlegającego weryfikacji przy użyciu e-mail lub SMS.

Wartość Losowa jest unikalna w każdym e-mail lub SMS.

TSP może ponownie przesłać pierwotny email, SMS wraz z taką samą wartością losową pod warunkiem, że zawartość komunikacji i odbiorcy pozostają bez zmian.

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

#### *3.2.2.3.3. Reverse Address Lookup (BR 3.2.2.5.3)*

Potwierdzenie kontroli Aplikanta nad adresem IP poprzez uzyskanie Nazwy Domeny związanej z adresem IP poprzez odwrotne sprawdzenie adresu IP a następnie weryfikacja kontroli nad FQDN z użyciem dozwolonej metody na podstawie sekcji 3.2.2.2.

#### *3.2.2.3.4. Any Other Method (BR 3.2.2.5.4)*

Ta metoda nie jest wykorzystywana.

#### *3.2.2.3.5. Phone Contact with IP Address Contact (BR 3.2.2.5.5)*

Potwierdzenie kontroli Aplikanta nad adresem IP poprzez wykonanie telefonu na numer kontaktowy Adresu IP i uzyskanie odpowiedzi potwierdzającej żądanie walidacji Adresu IP Aplikanta. TSP wykonuje telefon pod numer zidentyfikowany przez Urząd Rejestracji Adresów IP jako numer do kontaktu z adresem IP. Każdy telefon powinien być wykonany na pojedynczy numer.

W przypadku gdy telefon odbiera ktoś inny niż Kontakt przypisany do Adresu IP, TSP może poprosić o przełączenie w odpowiednie miejsce.

W przypadku odebrania przez pocztę głosową, TSP może zostawić Wartość Losową i Adres(y) IP, podlegające weryfikacji. Wartość Losowa musi zostać zwrócona do TSP, w celu akceptacji żądania.

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

#### *3.2.2.3.6. ACME “http-01” method for IP Addresses (BR 3.2.2.5.6)*

Ta metoda nie jest wykorzystywana.

#### *3.2.2.3.7. ACME "tls-alpn-01" method for IP Addresses (BR 3.2.2.5.7)*

Ta metoda nie jest wykorzystywana.

### 3.2.3. Uwierzytelnienie tożsamości osoby fizycznej

Tożsamość osoby fizycznej musi być potwierdzona:

- Jeżeli podmiotem certyfikatu, który ma zostać wystawiony jest osoba fizyczna;
- Jeżeli osoba fizyczna działa w imieniu organizacji w celu uzyskania Certyfikatu Organizacyjnego lub Certyfikatu Uwierzytelniania Witryny Internetowej.

TSP sprawdza tożsamość osoby fizycznej stosując jedną z poniższych metod.

**1) Osobista weryfikacja tożsamości (przez fizyczną obecność).**

W przypadku certyfikatów z klasy certyfikacyjnej III:

- 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.
- 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;
  - Dokument podróży (paszport);
  - W przypadku identyfikacji osób fizycznych, które nie posiadają żadnego z wyżej wymienionych dokumentów, TSP stosuje osobistą weryfikację tożsamości w oparciu o dowód osobisty obywateli wyłącznie z krajów Unii Europejskiej. W takiej sytuacji, akceptowany jest dowód osobisty osoby fizycznej ze zdjęciem lub prawo jazdy opublikowane w publicznej bazie PRADO - Public Register of Authentic identity and travel Documents Online (29), wydane przez kraj Unii Europejski.
- Osoba fizyczna powinna oświadczyć na piśmie, w formie elektronicznej lub dokumentowej, że dane osobiste użyte do identyfikacji są prawdziwe i poprawne. Oświadczenie takie powinno być złożone w obecności osoby dokonującej weryfikacji tożsamości.
- 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 TSP 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.
- Adres osoby fizycznej powinien być sprawdzony na podstawie karty pobytu.
- Osoba dokonująca weryfikacji tożsamości sprawdza, czy dokument tożsamości nie został sfałszowany.

Podczas pierwszej weryfikacji tożsamości TSP może zaakceptować identyfikację przeprowadzoną przez notariusza jako sposób potwierdzania tożsamości równoważny z tym dokonanym przez Punkt Rejestracji, jeśli tożsamość może być potwierdzona na podstawie zaświadczenia notarialnego, dołączonego do wniosku o wydanie certyfikatu podpisanego w obecności notariusza, zawierającego

oświadczenie, że notariusz porównał dane osobowe wnioskodawcy, który się przed nim stawił z zawartością rejestru publicznego lub innej bazy centralnej.

W przypadku certyfikatów z klasy certyfikacyjnej II:

- Nie ma potrzeby spotkania osobistego, fizycznego w celu identyfikacji tożsamości, jeśli TSP może zidentyfikować wnioskodawcę zdalnie. Podczas zdalnej identyfikacji, TSP może poprosić osobę fizyczną, by zrobiła sobie zdjęcie i wysłała je do TSP;
- Wnioskodawca wysyła kopię dokumentu tożsamości w celu potwierdzenia tożsamości do TSP;
- Wnioskodawca wysyła kopię dokumentu tożsamości w celu potwierdzenia jego adresu do TSP;
- Osoba fizyczna powinna zweryfikować poprawność danych w celu rejestracji i weryfikacji tożsamości poprzez oświadczenia podpisane odręcznie;
- TSP dokonuje porównania danych z publicznym rejestrem w przypadku certyfikatów z klasy certyfikacyjnej II;
- Adres osoby fizycznej powinien być sprawdzony na podstawie karty pobytu;
- Wnioskodawca może udowodnić swoją tożsamość dowolna metodą przeznaczoną dla Certyfikatów klasy certyfikacyjnej III;
- Dane indentyfikacyjne powinny być sprawdzone przez Punkt Rejestracji przy udziale zaufanej strony trzeciej lub rejestru publicznego;
- Punkt Rejestracji weryfikuje autentyczność przedstawionych dokumentów tożsamości. Dodatkowo, TSP weryfikuje, czy wniosek o wydanie certyfikatu rzeczywiście został złożony przez danego wnioskodawcę przez zaufany kanał komunikacji. Następnie, TSP prosi wnioskodawcę o potwierdzenie poprzez kanał komunikacji inny niż podany podczas rejestracji. Nie ma potrzeby potwierdzania przez bardziej zaufane kanały komunikacji w przypadku gdy identyfikacja przeprowadzana jest w przy użyciu odpowiedniego urządzenia do identyfikacji elektronicznej lub wniosku o wydanie certyfikatu opatrzonego właściwym podpisem elektronicznym.

**Dodatkowe zasady weryfikacji tożsamości obywateli zagranicznych**

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

- przystąpiło do międzynarodowej dwustronnej umowy z Rzeczpospolitą Polską w sprawie wzajemnego uznawania dokumentów urzędowych; lub
- 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.

TSP uznaje wniosek o wydanie certyfikatu podpisany przed notariuszem, jeżeli na podstawie zaświadczenia notarialnego można stwierdzić, że

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

TSP każdorazowo akceptuje oryginalne dokumenty wydane w języku polskim lub angielskim. W przypadku dokumentów wydanych w innych językach TSP może zażądać tłumaczenia przysięgłego.

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

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

TSP 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 elektronicznego.**

W tym przypadku:

- Wnioskodawca składa wniosek o wydanie certyfikatu w formie elektronicznej opatrzony podpisem elektronicznym opartym o certyfikat nie-anonimowy będący w klasyfikacji bezpieczeństwa nie niższej niż wnioskowany certyfikat (zob. 1.2.3.);
- Podpisany elektronicznie Wniosek o wydanie certyfikatu powinien zawierać dane wymagane w celu jednoznacznej identyfikacji osoby fizycznej;
- TSP weryfikuje autentyczność i integralność wniosku o wydanie certyfikatu w całej ścieżce pełnomocnictw;
- 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, TSP 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), TSP może umieścić w nowym certyfikacie dane inne niż dane Podmiotu zawarte w certyfikacie użytym do poświadczenia żądania certyfikatu.

**3) Identyfikacja oparta na certyfikacie do uwierzytelniania.**

W tym przypadku:

Wnioskodawca loguje się na stronie internetowej TSP przy użyciu certyfikatu nie anonimowego, klasy certyfikacji (zob. sekcję 1.2.3) nie niższej niż wnioskowany certyfikat.

TSP weryfikuje ważność certyfikatu w całej ścieżce certyfikacji.

Wnioskodawca składa wniosek w formie elektronicznej przy użyciu formularza wniosku o certyfikat.

Wniosek o wydanie certyfikatu powinien zawierać wszystkie dane wymagane w celu jednoznacznej identyfikacji osoby fizycznej.

Dane podane we wniosku odpowiadają danym zawartym w certyfikacie do uwierzytelnienia.

TSP umieszcza te same dane Podmiotu w nowym certyfikacie, co w certyfikacie do uwierzytelniania.

**4) Inne metody identyfikacji**

Metody, które zapewniają poziom bezpieczeństwa równoważny fizycznej obecności.

TSP może zweryfikować tożsamość osoby fizycznej zgodnie z art. 24.1 eIDAS przy użyciu następujących metod:

a) Identyfikacja przy użyciu narzędzi komunikacji elektronicznej dostarczających biometrycznej technologii video (zwaną dalej: wideoweryfikacją) zgodnie z art. 24.1 lit. d eIDAS,
b) Identyfikacja przy użyciu środków identyfikacji elektronicznej zgodnie z art. 24.1 lit. b eIDAS.

W takim przypadku, TSP postępuje tak samo jak w przypadku opisanej wcześniej osobistej weryfikacji tożsamości, z tym, że zamiast fizycznego spotkania następuje zdalna weryfikacja tożsamości.

**Wideoweryfikacja**

a) TSP rejestruje wizerunek Klienta z transmisji audiowizualnej, a następnie porównuje go z fotografią w dokumencie tożsamości użytym do identyfikacji (zwanym dalej: dokumentem tożsamości). Identyfikacja kończy się wynikiem pozytywnym, kiedy TSP 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) TSP upewnia się, że Klient zapoznał się z warunkami identyfikacji zdalnej i spełnia te warunki oraz wyraził zgodę na poddanie się jej i postępowanie zgodnie z instrukcjami.
d) TSP 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 były widoczne, zapisane i zweryfikowane i
   - dane zawarte w dokumencie tożsamości mogły być powiązane z danymi klienta w bazie TSP, a Klient mógł zostać zidentyfikowany na podstawie zdjęcia przedstawionego w dokumencie tożsamości.
f) TSP powinien sprawdzić, czy przedłożony dokument jest odpowiedni do przeprowadzenia identyfikacji audiowizualnej, co oznacza, że

- Dokument spełnia wymogi urzędowe,
- Elementy zabezpieczające, takie jak hologram, kinegram oraz inne równoważne zabezpieczenia nie są zniszczone i nadają się do odczytu,
- Identyfikator dokumentu tożsamości jest tożsamy z dostarczonym przez Klienta, jest niezniszczony i nadaje się do odczytu.

g) Podczas transmisji audiowizualnej TSP sprawcza, czy:
   - Wizerunek Klienta odpowiada jego wizerunkowi przedstawionemu przez w jego dokumencie tożsamości,
   - Dane Klienta zawarte w dokumencie tożsamości odpowiadają danym, do których TSP ma dostęp.
h) Klient jest w trybie online podczas całej identyfikacji.

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

**Elektroniczny dowód osobisty**

a) TSP umożliwia klientom identyfikację przy użyciu usługi elektronicznej identyfikacji za pomocą dowodu osobistego zawierającego warstwę elektroniczną.
b) TSP uznaje elektroniczny dowód osobisty jako środek identyfikacji elektronicznej w rozumieniu art. 24.1.b eIDAS (1).
c) TSP może użyć tej usługi uwierzytelnienia za pośrednictwem brokera lub samodzielnie.

TSP 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 TSP.

### 3.2.4. Informacje o subskrybentach nieweryfikowane

W Certyfikacie mogą znaleźć się jedynie dane zweryfikowane przez TSP.

### 3.2.5. 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:

- Osoba uprawniona do reprezentowania danej organizacji,
- Osoba, posiadająca upoważnienie do reprezentowania organizacji od osoby uprawnionej,
- Administrator Organizacyjny wskazany przez osobę upoważnioną do reprezentowania organizacji.

Administrator Organizacyjny może być wyznaczony we wniosku o certyfikat lub w dowolnym momencie później na podstawie 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 TSP 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.

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

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

### 3.2.6. Kryteria interoperacyjności

TSP nie współpracuje z innymi Urzędami Certyfikacji podczas dostarczania usług.

### 3.2.7. Weryfikacja adresu e-mail

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

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

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

TSP utrzymuje rejestr metod walidacji użytych do walidacji każdej domeny lub adresu email zawartych w certyfikacie, zawierający odpowiednią wersję S/MIME Baseline Requirements (11) lub TLS Baseline Requirements (3).

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.**

TSP 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.

TSP 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 TSP, TSP 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 TSP 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, TSP 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 TSP wystawia podmiotowi certyfikat z podmienionym kluczem publicznym. O recertyfikację można wystąpić jedynie w okresie ważności umowy na usługę.

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

TSP 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.

W przypadku certyfikatów z klasy certyfikacyjnej II, TSP nie przeprowadza procesu recertyfikacji. Certyfikat z nowym kluczem jest wystawiany jedynie w ramach wniosku o nowy certyfikat.

### 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, TSP wykorzystuje wyniki i dowody pozyskane w trakcie pierwotnego procesu walidacji.

### 3.3.2. Identyfikacja i uwierzytelnianie dla nieważnych Certyfikatów

TSP przyjmuje wnioski 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 TSP 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 dla ważnych Certyfikatów

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

W przypadku, gdy TSP inicjuje odnowienie certyfikatu, może on 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 dla 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 wniosków o modyfikację

Modyfikacja certyfikatu to proces, w którym TSP 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 TSP 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

TSP 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).

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

Za każdym razem TSP weryfikuje autentyczność złożonego wniosku oraz tożsamość i upoważnienie 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, TSP weryfikuje jego numer telefonu, adres e-mail lub adres pocztowy jako zweryfikowane metody komunikacji z wnioskodawcą.

W celu sprawdzenia zweryfikowanej metody komunikacji z wnioskodawcą TSP:

- 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.
- Potwierdza użyteczność zweryfikowanej metody komunikacji. Inspektor ds. Rejestracji TSP 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

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

- Dla dokumentów w formie papierowej – podpisy odręczne zgodne ze wzorce podpisu i (opcjonalnie) pieczęć firmy, zgodnie z zasadami reprezentacji w firmie,
- Dla dokumentów w formie elektronicznej – kwalifikowane podpisy elektroniczne.

Podczas walidacji podpisu, TSP 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:

- W przypadku dokumentów w formie papierowej Wnioskodawca składa odręczny podpis w obecności Inspektora Rejestracji, po wcześniejszej walidacji tożsamości dokonanej przez Inspektora Rejestracji;
- Pozytywna walidacja kwalifikowanych podpisów elektronicznych;
- W przypadku podpisów odręcznych poświadczonych notarialnie, TSP 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;
- Inspektor Rejestracji kontaktuje się z Wnioskodawcą lub Subskrybentem przy użyciu zweryfikowanej metody komunikacji, po czym otrzymuje od tej 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 TSP 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:

- Odnowienie certyfikatu oznacza wystąpienie o wystawienie certyfikatu z takimi samymi danymi podmiotu, jak w poprzednim certyfikacie a obydwa certyfikaty są wydane dla tego

samego klucza publicznego. Szczegóły dotyczące odnawiania certyfikatu są omówione w sekcji 4.6.

- Modyfikacja certyfikatu oznacza wystąpienie o zmianę danych certyfikatu dotyczącą danych podmiotu zawartych w certyfikacie. TSP 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.
- 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.

TSP 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 TSP wniosek o rejestrację, na przykład, na stronie internetowej TSP. Wnioskodawca podaje dane, które mają pojawić się w certyfikacie i wskazuje na rodzaj certyfikatu. Wnioskodawca upoważnia TSP do zarządzania danymi osobowymi zawartymi we wniosku o rejestrację.

TSP 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 TSP przygotowuje umowę dla subskrybenta w oparciu o informacje podane we wniosku o rejestrację.

Umowa na świadczenie usług powinna zawierać informację o rodzajach 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.

TSP 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.

TSP 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:

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

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

- Dokumenty niezbędne do identyfikacji podmiotu – w przypadku organizacji, osoby ją reprezentującej – zgodnie z sekcją 3.2.3;
- W przypadku wniosku o Certyfikat Organizacyjny, dokumenty identyfikacyjne tej organizacji zgodnie z sekcją 3.2.2;
- Jeśli podmiot jest organizacją, zaświadczenie lub upoważnienie przekazane przez organizację, że wnioskodawca jest upoważniony do reprezentowania organizacji zgodnie z sekcją 3.2.5;
- W przypadku wniosku o Certyfikat Organizacyjny, dowody wydane przez organizację, że wnioskodawca jest uprawniony do reprezentowania organizacji zgodnie z sekcją 3.2.5;
- Jeśli podmiot jest osobą fizyczną wnioskującą o Certyfikat Organizacyjny - zgoda 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 dla 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 TSP) dotycząca wystawienia certyfikatu i jego utrzymania.

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

- w formie papierowej, podpisany odręcznie w punkcie obsługi klienta TSP lub w mobilnym punkcie rejestracji TSP w dniu uprzednio uzgodnionym (w przypadku certyfikatu klasy III w tym samym czasie odbywa się osobista identyfikacja);
- w formie papierowej, podpisany odręcznie i przesłany do punktu obsługi klienta TSP (w przypadku certyfikatu klasy III identyfikacja osobista odbędzie się w późniejszym czasie);
- W formie elektronicznej podpisany podpisem lub pieczęcią elektroniczną w oparciu o certyfikat nie-anonimowy z klasą certyfikacji nie niższą niż wnioskowany certyfikat (zob. sekcja 1.2.3), złożony poprzez portal klienta lub wysłany pod adres e-mail TSP.

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

### 4.1.2. Nabór i odpowiedzialność

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

TSP 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 organizacyjny, TSP 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).

Podmiot – w przypadku organizacji, jej przedstawiciel – powinien dostarczyć wszelkie niezbędne informacje w celu przeprowadzenia procesu identyfikacji.

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

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

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

TSP 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.

TSP rejestruje wniosek o wystawienie certyfikatu podpisany przez Podmiot - 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 TSP danych podanych we wniosku,
- Wyrażenie zgody (lub nie) na ujawnienie certyfikatu.

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

TSP 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, TSP 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

TSP identyfikuje wnioskodawcę zgodnie z sekcją 3.2 oraz weryfikuje autentyczność wniosku.

W przypadku wniosku o certyfikat organizacyjny, również sama organizacja musi być zidentyfikowana i weryfikacja uprawnień do reprezentacji odbywa się zgodnie z sekcją 3.2. TSP 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.

TSP 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.

TSP 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 TSP może użyć dokumentów i danych wskazanych w sekcji 3.2 w celu weryfikacji informacji w certyfikacie lub może użyć wyników swoich poprzednich walidacji, jednak nie starszych niż 398 dni.

TSP prowadzi listę wniosków wysokiego ryzyka, która zawiera wnioski odrzucone i wszystkie certyfikaty unieważnione ze względów bezpieczeństwa.

Przed zatwierdzeniem certyfikatu TSP sprawdza tę listę. Jeżeli na liście widnieje wnioskowana domena, subskrybent lub wnioskodawca, TSP zajmuje się wnioskiem priorytetowo w celu właściwej jego weryfikacji.

TSP rozwija, utrzymuje i wdraża udokumentowane procedury, które rozpoznają i wymagają dodatkowej, szczególnej weryfikacji dla Wniosków Wysokiego Ryzyka przed zatwierdzeniem certyfikatu, aby zapewnić prawidłową weryfikację takich wniosków.

TSP weryfikuje czy:

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

TSP nie wydaje Certyfikatu w takim wypadku.

### 4.2.2. Zatwierdzenie lub odrzucenie wniosku o certyfikat

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

Przed wystawieniem certyfikatu, TSP 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, TSP weryfikuje dany adres e-mail. TSP sprawdza czy ten adres jest prawdziwy i rzeczywiście należy do podmiotu.

TSP sprawdza rekordy CAA (Certification Authority Authorization) dla każdej nazwy dNSName w rozszerzeniu certyfikatu subjectAltName zgodnie z procedurą opisaną w IETF RFC 8659 (26), postępując zgodnie z instrukcjami IETF RFC 8659 (26) dla każdego znalezionego rekordu.

TSP 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 TSP ponownie sprawdza automatycznie rekordy CAA.

TSP akceptuje lub odrzuca wnioski o wystawienie certyfikatu po ich 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 TSP, TSP odrzuca wniosek.

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

TSP rozwija procedury, które rozpoznają wnioski o certyfikaty uwierzytelnienia witryn internetowych wysokiego ryzyka. Proces identyfikacji i ściślejszego monitorowania podejrzanych wniosków zostały opisane poniżej.

**Zarządzanie certyfikatami wysokiego ryzyka**

TSP prowadzi rejestr certyfikatów do podpisywania kodu wysokiego ryzyka oraz osób fizycznych i prawnych, które mogą być z nimi powiązane, zgodnie z wymaganiami CA/Browser Forum.

TSP rejestruje dane, jeśli:

- Odrzuca złożony wniosek o wystawienie certyfikatu z powodów bezpieczeństwa,
- Ważny certyfikat do podpisywania kodu musi zostać unieważniony po wystąpieniu incydentu związanego z bezpieczeństwem,
- Unieważnia zawieszony certyfikat do podpisywania kodu po upływie określonego terminu.

TSP dokłada najwyższej staranności przy ocenie nowego wniosku o wystawienie certyfikatu złożonego przez osobę fizyczną lub prawną znajdującą się w ww. rejestrze.

TSP wydaje certyfikat do podpisywania kodu wyłącznie na sprzętowym urządzeniu kryptograficznym posiadającym odpowiednią certyfikację.

Jeżeli Klient po raz drugi wnioskuje o unieważnienie certyfikatu do podpisywania kodu z powodu kompromitacji klucza lub jeśli jego zawieszony Certyfikat został unieważniony przez Dostawcę Usług Zaufania po upłynięciu terminu na jego przywrócenie, kolejny certyfikat do podpisywania kodu nie może być wystawiony dla tego podmiotu.

#### 4.2.3. Czas przetwarzania wniosków o wystawienie certyfikatu

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

### 4.3. Wystawianie certyfikatu

TSP wystawia certyfikat podmiotowi w przypadku certyfikatów III klasy certyfikacyjnej jedynie po zatwierdzeniu wniosku o wystawienie certyfikatu.

Wystawiony certyfikat zawiera jedynie te dane podmiotu, które zostały podane we wniosku o certyfikat, i które zostały zweryfikowane przez TSP.

Jeśli TSP dostarcza Podmiotowi osobiste kwalifikowane urządzenie do składania podpisu (pieczęci) elektronicznego. TSP w procesie personalizacji generuje dla wnioskodawcy parę kluczy, ale certyfikat nie jest wystawiany. Przekazanie kwalifikowanego urządzenia QSCD zawierającego klucz prywatny odbywa się w sposób kontrolowany zgodnie z przepisami bezpieczeństwa opisanymi w sekcji 6.1.2.

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

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

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

TSP wystawia certyfikaty wyłącznie po weryfikacji, czy QSCD znajduje się już w posiadaniu wnioskodawcy.

Po wydaniu certyfikatu TSP 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.

W przypadku certyfikatów klasy II, TSP wystawia certyfikat wyłącznie po weryfikacji danych podanych we wniosku o rejestrację i po otrzymaniu podpisanego wniosku o wystawienie certyfikatu i umowy na świadczenie usług. Wystawiony certyfikat zawiera wyłącznie te dane podmiotu, które zostały umieszczone we wniosku o certyfikat, i które zostały zweryfikowane przez TSP.

#### 4.3.1. Czynności Urzędu Certyfikacji podczas wystawiania certyfikatu

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

TSP opracował swoje wewnętrzne procesy administracyjne na podstawie analizy ryzyka i stosuje zasadę „Dual Control" podczas zapisywania danych umieszczanych w certyfikacie i weryfikowania autentyczności danych. TSP 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. TSP nigdy nie antydatuje certyfikatów.

#### 4.3.2. Powiadamianie subskrybenta o wystawieniu certyfikatu

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

### 4.4. Akceptacja certyfikatu

#### 4.4.1. Proces akceptacji certyfikatu

W przypadku certyfikatów klasy III Podmiot lub - jeśli certyfikat ma być wystawiony dla organizacji - przedstawiciel podmiotu, powinien zweryfikować poprawność danych zawartych w certyfikacie podczas odbierania certyfikatu.

W przypadku certyfikatów klasy II Wnioskodawca (lub jego przedstawiciel) nie musi osobno potwierdzać odebrania certyfikatu. Poprzez podpisanie umowy na świadczenie usług, subskrybent ponadto potwierdza akceptację PCKPC i innych dokumentów zawierających warunki umowne.

Jeżeli TSP dostarcza podmiotowi QSCD, po otrzymaniu tego urządzenia zawierającego klucz prywatny i kodu potrzebnego do aktywacji, wnioskodawca odręcznie podpisuje oświadczenie o odebraniu urządzenia, w którym potwierdza, że otrzymał kody aktywacyjne i że zapoznał się z technicznymi i prawnymi wymogami dotyczącymi użycia kwalifikowanego urządzenia do składania podpisów elektronicznych.

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

#### 4.4.2. Publikacja certyfikatu przez Urząd Certyfikacji

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

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

#### 4.4.3. Powiadomienie przez CA innych osób o wystawieniu certyfikatu

W przypadku certyfikatu organizacyjnego wydanego dla osoby fizycznej do składania podpisu elektronicznego w imieniu organizacji, TSP niezwłocznie powiadamia osobę kontaktową reprezentowanej organizacji o wystawieniu certyfikatu.

TSP 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 może być użyty jedynie w zgodzie z dopuszczalnym 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 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.

W przypadku klucza prywatnego zarządzanego przez TSP w imieniu Podmiotu, TSP zawsze sprawdza ważność certyfikatu i odmawia użycia klucza dla certyfikatu wygasającego później niż długość życia zastosowanych dla niego algorytmów kryptograficznych.

Użycie klucza wymaga za każdym razem identyfikacji i zgody Podmiotu.

### 4.5.2. Użycie klucza publicznego i certyfikatu przez strony ufające

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

- Strona ufająca musi zweryfikować status certyfikatu: ważny czy unieważniony;
- Certyfikaty do podpisów elektronicznych i odpowiadające im klucze publiczne powinny być użyte jedynie w celu walidacji podpisu elektronicznego;
- Certyfikaty do pieczęci elektronicznej i odpowiadające im klucze publiczne powinny być użyte jedynie w celu walidacji pieczęci elektronicznej;
- Klucze publiczne należące do certyfikatów uwierzytelnienia witryn internetowych mogą być użyte jedynie w celu uwierzytelnienia witryny internetowej lub klienta;
- Klucze publiczne mogą być zaakceptowane wyłącznie jeśli użyto ich zgodnie z przeznaczeniem, określonym w polach „Użycie klucza" (Key Usage) i „Rozszerzone użycie klucza" (Extended Key Usage) w certyfikacie;
- Weryfikacja certyfikatu powinna zostać przeprowadzona dla całej ścieżki certyfikacyjnej aż do zaufanego root lub certyfikatu pośredniego wystawcy;
- Weryfikacja podpisu elektronicznego lub pieczęci elektronicznej powinna zostać przeprowadzona w wiarygodnej aplikacji, która spełnia określone wymagania techniczne, może być trwale skonfigurowana, została prawidłowo przygotowana i jest wolna od wirusów;

- W przypadku certyfikatów osobistych powiązanych z organizacją zaleca się sprawdzenie, czy tytuł osoby podpisującej (upoważniający do podpisania dokumentu w imieniu organizacji) można ustalić na podstawie certyfikatu (na przykład, w polu „Tytuł”);
- Zaleca się sprawdzenie, czy certyfikat został wystawiony zgodnie z właściwą polityką certyfikacji;
- zaleca się sprawdzenie, czy występuje w certyfikacie limit wartości zobowiązań jakie można zaciągnąć jednorazowo przy użyciu certyfikatu (limit ten oznacza, że TSP nie ponosi odpowiedzialności za roszczenia i szkody wynikające z użycia podpisu lub pieczęci elektronicznej do zawarcia transakcji powyżej tej kwoty);
- Strony Ufające powinny zwrócić uwagę na wszelkie ograniczenia zawarte w certyfikacie lub w regulacjach przywołanych w Certyfikacie.

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

## 4.6. Odnowienie certyfikatu

Usługa wystawienia nowego certyfikatu przez TSP 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 jego wygaśnięciu, powinien zainicjować procedurę jego odnowienia. Odnowienie certyfikatu oznacza wystawienie nowego certyfikatu z tymi samymi danymi identyfikacyjnymi danego podmiotu ale na nowy okres. Inne dane w certyfikacie mogą ulec zmianie np. CRL, OCSP czy klucz wystawcy użyty do podpisania certyfikatu.

### 4.6.1. Uwarunkowania dla odnowienia certyfikatu

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

- Wniosek o odnowienie certyfikatu został złożony w okresie ważności certyfikatu lub po jego upływie;
- Certyfikat, który ma być odnowiony nie jest zawieszony ani unieważniony;
- Klucz prywatny odpowiadający certyfikatowi nie jest skompromitowany;
- Dane identyfikacyjne podmiotu wpisane w certyfikacie są nadal aktualne.

TSP akceptuje wnioski o odnowienie certyfikatu jedynie w ramach obowiązującej umowy o świadczenie usług.

Jeżeli poprzedni certyfikat podmiotu jest unieważniony, to o nowy certyfikat można wnioskować tylko w ramach usługi recertyfikacji „Re-key” (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 ważnej 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 o odnowienie certyfikatu, że dane identyfikacyjne podmiotu podane w certyfikacie są nadal ważne.

TSP 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) TSP pozyskał wiedzę, że dany certyfikat nie jest zgodny z PCKPC;
c) klucz podpisujący (klucz prywatny) dostawcy usług użyty do wystawienia certyfikatu musi być wymieniony.

W celu zapewnienia kontynuacji świadczenia usług, TSP jest uprawniony do rozpoczęcia odnowienia certyfikatu podczas ostatniego miesiąca ważności certyfikatu jeśli:

a) Umowa o świadczenie usług będzie nadal obowiązywać w następnym dniu kalendarzowym następującym po okresie ważności certyfikatu,
b) Subskrybent z góry zgodził się na automatyczne odnowienie certyfikatu w ciągu całego okresu ważności umowy o świadczenie usług.

Wniosek o odnowienie można złożyć w następujący sposób:

- W formie papierowej, podpisany odręcznie w biurze obsługi klienta TSP lub u mobilnego partnera ds. rejestracji TSP w ustalonym wcześniej terminie;
- W formie elektronicznej za pomocą podpisu elektronicznego lub pieczęci elektronicznej w oparciu o certyfikat nie-pseudonimowy o klasie bezpieczeństwa nie niższej niż klasa odnawianego certyfikatu (zob. sekcja 1.2.3), na adres email TSP wskazany we wniosku;
- używając osobistego konta klienta na portalu internetowym, używając unikalnych danych uwierzytelniających do konta;
- W formie papierowej, podpisany odręcznie i przesłany do biura obsługi klienta TSP (w przypadku certyfikatów klasy III osobista identyfikacja tożsamości następuje w innym terminie).

### 4.6.3. Przetwarzanie wniosków o odnowienie certyfikatu

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

- Złożony wniosek jest autentyczny;
- Wnioskodawca posiada stosowne umocowanie i upoważnienie;
- Wnioskodawca oświadczył, że dane podmiotu, które mają zostać umieszczone w certyfikacie się nie zmieniły i są poprawne;
- Certyfikat podlegający odnowieniu nie jest zawieszony ani unieważniony;
- 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

TSP 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 procesu 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 TSP wraz z instrukcją obsługi, a jeśli jest to konieczne – z asystą telefoniczną.

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

#### 4.6.6. Publikacja odnowionego certyfikatu przez Urząd Certyfikacji

TSP publikuje odnowiony certyfikat w taki sam sposób jak pierwotny certyfikat.

#### 4.6.7. Powiadomienie innych podmiotów o wystawieniu certyfikatu

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

### 4.7. Wymiana kluczy Certyfikatu (Re-Key)

Re-key oznacza proces, w którym TSP wystawia nowy certyfikat dla podmiotu w sposób 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.

W przypadku kluczy z II klasy certyfikacji TSP nie przeprowadza tego procesu. Wystawienie certyfikatu z nowym kluczem ma miejsce jedynie w ramach wniosku o wystawienie nowego certyfikatu.

#### 4.7.1. Okoliczności dla Re-Key

Ważność poprzedniego certyfikatu nie jest warunkiem koniecznym dla procesu Re-key, jednak TSP zatwierdza wnioski o Re-key jedynie w ramach ważnej umowy na świadczenie usług.

Podczas procesu Re-key wnioskodawca zostaje poinformowany przez TSP, jeśli warunki świadczenia usług zmieniły się 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 ważnej umowy na świadczenie usług, nie ma potrzeby jej zmiany.

#### 4.7.2. Kto może wnioskować o certyfikację nowego klucza publicznego

Proces Re-key musi być zainicjowany przez osobę, która jest uprawniona do złożenia wniosku o nowy certyfikat.

Wnioskodawca potwierdza we wniosku o wystawienie certyfikatu Re-key, że dane identyfikacyjne podmiotu wpisane do certyfikatu są nadal ważne lub podaje nowe aktualne dane i potwierdza ich ważność.

TSP zapewnia następujące możliwości złożenia wniosku o recertyfikację:

- W formie papierowej, podpisany odręcznie w biurze obsługi klienta TSP lub u mobilnego partnera ds. rejestracji TSP w ustalonym wcześniej terminie (w takiej sytuacji, w przypadku certyfikatów z klasy certyfikacji III w tym samym czasie następuje równocześnie osobista weryfikacja tożsamości);
- W formie elektronicznej za pomocą podpisu elektronicznego lub pieczęci elektronicznej w oparciu o certyfikat nie-pseudonimowy o klasie bezpieczeństwa nie niższej niż klasa nowego certyfikatu (zob. sekcja 1.2.3). Taki wniosek wysyłany jest na adres email TSP;
- W formie papierowej, podpisany odręcznie i przesłany do biura obsługi klienta TSP (w przypadku certyfikatów klasy III osobista identyfikacja tożsamości odbywa się w innym terminie).

### 4.7.3. Przetwarzanie wniosków o Re-key

W trakcie weryfikacji wniosku o Re-key TSP sprawdza, czy:

- Złożony wniosek jest autentyczny;
- Osoba składająca wniosek posiada stosowne umocowanie i upoważnienie;
- Dane wpisane we wniosku są poprawne;
- na podstawie aktualnej wiedzy, algorytmy kryptograficzne będą wystarczająco odporne przez cały nowy okres ważności nowego certyfikatu.

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

### 4.7.4. Powiadamianie klienta o wystawieniu nowego certyfikatu

TSP informuje wnioskodawcę i subskrybenta o wystawieniu certyfikatu.

### 4.7.5. Akceptacja recertyfikowanego certyfikatu

TSP 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. TSP wystawia tylko certyfikat dla nowego klucza publicznego.

Jeżeli konieczne jest wystawienie nowego kwalifikowanego urządzenia do składania podpisu elektronicznego podczas procesu re-key, TSP personalizuje nowe urządzenie i dostarcza je wnioskodawcy, tak jak opisano w rozdziale 4.3. TSP wystawia certyfikat wyłącznie po sprawdzeniu w sposób wiarygodny, że kwalifikowane urządzenie do składania podpisu elektronicznego znajduje się już w posiadaniu wnioskodawcy.

Jeżeli nowy klucz publiczny użyty podczas procesu re-key został dostarczony przez podmiot, nie jest konieczne przekazanie klucza i kwalifikowanego urządzenia do składania podpisu elektronicznego.

Nowy certyfikat wydany w ramach re-key może zostać pobrany online bez konieczności osobistej wizyty.

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

#### 4.7.6. Publikacja certyfikatu re-key

TSP publikuje nowy certyfikat re-key w ten sam sposób jak pierwotny certyfikat.

#### 4.7.7. Powiadomienie innych podmiotów o wystawieniu certyfikatu

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

### 4.8. Modyfikacja certyfikatu

Modyfikacja certyfikatu oznacza proces, w którym TSP wystawia nowy certyfikat ze zmienionymi danymi identyfikacyjnymi podmiotu, bez wymiany klucza publicznego.

Pod względem technicznym, zmiana certyfikatu oznacza wystawienie nowego certyfikatu.

TSP 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 TSP użyty do podpisania certyfikatu.

#### 4.8.1. Okoliczności zmiany certyfikatu

Modyfikacja certyfikatu jest konieczna w następujących przypadkach:

- Zmiana danych w Certyfikacie;
- zmiana danych Certyfikatu wystawiającego Urzędu Certyfikacji, wpisanych w polu „Podmiot DN”, lub zmiana klucza publicznego;
- Zmiana profilu certyfikatu określonego przez TSP.

Warunki modyfikacji certyfikatu:

- wniosek o modyfikację certyfikatu został złożony w okresie ważności danego certyfikatu;
- certyfikat nie jest zawieszony ani unieważniony;
- klucz prywatny odpowiadający certyfikatowi nie jest skompromitowany.

TSP zatwierdza wnioski o modyfikację jedynie w ramach obowiązującej umowy na świadczenie usług.

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

W trakcie modyfikacji certyfikatu wnioskodawca zostaje poinformowany, jeśli od czasu wystawienia poprzedniego certyfikatu wystąpiły zmiany warunków świadczenia usługi.

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

#### 4.8.2. Kto może wnioskować o zmianę certyfikatu

Modyfikacja certyfikatu może być zainicjowana tylko przez osobę uprawnioną do złożenia wniosku o wystawienie nowego certyfikatu.

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

TSP samodzielnie inicjuje proces modyfikacji certyfikatu jeśli posiada wiedzę, że dane podmiotu wpisane do certyfikatu się zmieniły.

TSP zapewnia następujące możliwości złożenia wniosku o modyfikację certyfikatu:

- W formie papierowej, podpisany odręcznie w biurze obsługi klienta TSP lub u mobilnego partnera ds. rejestracji TSP w ustalonym wcześniej terminie (w , w przypadku certyfikatów z klasy III tym samym czasie następuje osobista weryfikacja tożsamości);
- W formie elektronicznej za pomocą podpisu elektronicznego lub pieczęci elektronicznej złożonych przy użyciu certyfikatu nie-anonimowego o klasie bezpieczeństwa nie niższej niż klasa nowego certyfikatu (zob. sekcja 1.2.3). Taki wniosek może być złożony poprzez portal klienta lub wysłany na adres email TSP;
- W formie papierowej, podpisany odręcznie i przesłany do biura obsługi klienta TSP (w przypadku certyfikatów klasy III osobista identyfikacja tożsamości następuje w późniejszym terminie).

### 4.8.3. Przetwarzanie wniosku o zmianę certyfikatu

W trakcie weryfikacji wniosku TSP sprawdza, czy:

- Złożony wniosek jest autentyczny;
- Osoba składająca wniosek posiada stosowne umocowanie i upoważnienie;
- Dane podane we wniosku są poprawne;
- Wniosek został złożony w okresie ważności certyfikatu;
- na podstawie aktualnej wiedzy, algorytmy kryptograficzne będą wystarczająco odporne przez cały nowy okres ważności wydanego certyfikatu.

TSP weryfikuje ważność i autentyczność danych Podmiotu w taki sam sposób jak przy pierwotnej weryfikacji przeprowadzonej przed wydaniem certyfikatu po raz pierwszy.

Przed rozpatrzeniem wniosku, tożsamość osoby składającej wniosek jest sprawdzana zgodnie z sekcją 3.5.

### 4.8.4. Powiadomienie klienta o wystawieniu nowego certyfikatu

TSP informuje wnioskodawcę i subskrybenta o wystawieniu certyfikatu.

### 4.8.5. Akceptacja certyfikatu

W trakcie modyfikacji certyfikatu nie generuje się klucza i dlatego nie ma potrzeby przekazania go podmiotowi. Nowy 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 TSP zapewnia aplikację do zarządzania kartą wraz z instrukcją obsługi, i jeśli jest to konieczne – asystę telefoniczną.

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

### 4.8.6. Publikacja zmienionego certyfikatu przez Urząd Certyfikacji

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

### 4.8.7. Powiadomienie innych podmiotów o wystawieniu certyfikatu przez CA

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

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

## 4.9. Unieważnienie i zawieszenie certyfikatu

Unieważnienie certyfikatu oznacza zakończenie jego ważności przed upływem pierwotnie planowanego okresu ważności. Unieważnienie certyfikatu skutkuje trwałą i nieodwracalną zmianą statusu certyfikatu, innymi słowy, unieważniony certyfikat już nigdy nie będzie ponownie ważny.

Zawieszenie certyfikatu następuje wtedy, gdy TSP 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**

TSP 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 TSP 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 TSP 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. Klucz prywatny należący do unieważnionego certyfikatu powinien być zniszczony natychmiast po unieważnieniu.

Certyfikat do uwierzytelniania witryn internetowych nie może być zawieszony.

Regulacje dotyczące odpowiedzialności w związku z unieważnieniem lub zawieszeniem:

- Jeżeli TSP opublikował już status unieważnienia certyfikatu, TSP nie ponosi żadnej odpowiedzialności, w przypadku, gdy Strony Ufające uznają certyfikat za ważny.

### 4.9.1. Okoliczności unieważnienia certyfikatu

**Unieważnienie Certyfikatu Subskrybenta**

TSP unieważnia certyfikat w następujących przypadkach:

- na podstawie prawidłowego wniosku o unieważnienie złożonego przy użyciu formularza online (patrz 4.9.3);
- Wnioskodawca lub subskrybent występuje z pisemnym wnioskiem o unieważnienie certyfikatu (patrz 4.9.3);
- Wnioskodawca lub subskrybent powiadamia Urząd Certyfikacji, o tym że wniosek o wydanie certyfikatu nie został zatwierdzony i w konsekwencji nie została wyrażona zgoda;
- Urząd Certyfikacji dowiaduje się, że klucz prywatny odpowiadający kluczowi publicznemu został skompromitowany;
- Urząd Certyfikacji uzyskuje dowód na to, że uprawnienia do domeny lub kontrola nad FQDN lub adresem IP są niewiarygodne;
- Urząd Certyfikacji dowiaduje się, że klucz publiczny w certyfikacie nie odpowiada wymaganiom opisanym w sekcji 6.1.5. i 6.1.6.;
- Urząd Certyfikacji dowiaduje się, że certyfikat został niewłaściwie (niezgodnie z prawem) użyty;
- Urząd Certyfikacji dowiaduje się, że subskrybent naruszył kluczowe obowiązki w umowie na świadczenie usług lub Regulaminie usług zaufania;
- Urząd Certyfikacji dowiaduje się o wszelkich okolicznościach wskazujących na to, że użycie FQDN lub adresu IP wskazanych w certyfikacie przestało być prawnie dozwolone (np. decyzją sądu odebrano prawo do posługiwania się daną domeną, zakończyła się odpowiednia umowa (licencji, usługi) pomiędzy właścicielem a Subskrybentem lub właściciel nie przedłużył rejestracji domeny);
- Urząd Certyfikacji dowiaduje się, że certyfikat typu wildcard został użyty do uwierzytelnienia nieuczciwie wprowadzającej w błąd podległej nazwy domeny;
- Urząd Certyfikacji dowiaduje się, że zawarte w certyfikacie informacje istotnie się zmieniły;
- Z powodu modyfikacji certyfikatu w przypadku zmiany danych podmiotu;
- Urząd Certyfikacji dowiaduje się, że certyfikat został wydany niezgodnie z wymaganiami CABF Baseline Requirements lub z Polityką Certyfikacji lub z Kodeksem Postępowania Certyfikacyjnego;
- dane w certyfikacie są niepoprawne;
- Urząd Certyfikacji przestał być podmiotem upoważnionym do wydawania certyfikatów i nie zapewnia utrzymania istniejących CRL i usług OCSP;
- unieważnienie jest wymagane przez Politykę Certyfikacji i/lub Kodeks Postępowania Certyfikacyjnego z powodów innych niż określone w tym rozdziale;
- Urząd Certyfikacji dowiaduje się o istnieniu metody, która może prowadzić do kompromitacji 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;

- Urząd Certyfikacji wystawił certyfikat na podstawie dokumentu pochodzącego od strony trzeciej, a następnie strona ta pisemnie wycofała ten dokument;
- Format i techniczna zawartość certyfikatu stanowią nieakceptowalne ryzyko dla Stron Ufających (np. w przypadku kiedy algorytm kryptograficzny lub rozmiar klucza nie są już bezpieczne);
- Urząd Certyfikacji dowiaduje się, że prywatny klucz jednostki certyfikacyjnej (wystawcy) mógł zostać skompromitowany;
- Urząd Certyfikacji dowiaduje się, że subskrybent nie dopełnił finansowych zobowiązań wynikających z umowy na świadczenie usług;
- 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;
- Certyfikat został zawieszony i nie został przywrócony w przysługującym terminie (zob. sekcja 4.9.16.);
- Zakończyła się umowa na świadczenie usług;
- Urząd Certyfikacji zakończył działalność;
- Organ Nadzoru wydał wiążącą prawnie i skuteczną decyzję;
- Wymów unieważnienia wynika z przepisów prawa.

**Powody unieważnienia Certyfikatu Dostawcy Usług Zaufania**

Urząd Certyfikacji jest zobowiązany do unieważnienie Certyfikatu pośredniej jednostki certyfikacyjnej w następujących przypadkach:

- urząd certyfikacji obsługujący pośrednią jednostką certyfikacyjną zwraca się z pisemną prośbą o unieważnienie certyfikatu;
- urząd certyfikacji obsługujący pośrednią jednostką certyfikacyjną powiadamia wystawiający Urząd Certyfikacji, że pierwotny wniosek o wystawienie certyfikatu nie został zatwierdzony i nie przyznaje autoryzacji wstecznie;
- Urząd Certyfikacji dowiaduje się, że klucz prywatny nie jest już w jego wyłącznym posiadaniu;
- Urząd Certyfikacji dowiaduje się, że klucz publiczny zawarty w certyfikacie nie jest zgodny z wymaganiami określonymi w sekcjach 6.1.5 i 6.1.6;
- Urząd Certyfikacji dowiaduje się, że certyfikat został użyty niezgodnie z prawem;
- Certyfikat został wystawiony niezgodnie z odpowiednią Polityką Certyfikacji i Kodeksem Postępowania Certyfikacyjnego lub działania pośredniej jednostki certyfikacyjnej nie są zgodne z tymi dokumentami;
- Urząd Certyfikacji stwierdza, że niektóre informacje znajdujące się w certyfikacie są fałszywe lub wprowadzające w błąd;
- Wydający Urząd Certyfikacji lub pośredni CA kończy działalność z jakiegokolwiek powodu i nie upoważnił innego Urzędu do utrzymywania listy CRL i unieważniania certyfikatów;
- Urząd Certyfikacji utracił uprawnienia do wydawania certyfikatów i nie zapewnia utrzymania CRL i OCSP dla certyfikatów;
- wymóg unieważnienia wynika z Polityki Certyfikacji i/lub Kodeksu Postępowania Certyfikacyjnego wydającego Urzędu Certyfikacji;
- Nastąpiła modyfikacja certyfikatu z powodu zmiany danych jednostki certyfikującej lub Urzędu Certyfikacji;

- Format i techniczna zawartość certyfikatu stanowią niedopuszczalne ryzyko dla Stron Ufających (np. w przypadku kiedy algorytm kryptograficzny lub rozmiar klucza nie są bezpieczne);
- Urząd Certyfikacji zakończył działalność;
- Unieważnienie certyfikatu wynika z obowiązujących przepisów prawa.

**Powody unieważnienia certyfikatu pośredniego Urzędu Certyfikacji (CA) nadzorowanego przez inny Urząd Certyfikacji**

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

- urząd certyfikacji obsługujący pośrednią jednostkę certyfikacji zwraca się z pisemną prośbą o unieważnienie certyfikatu;
- urząd certyfikacji obsługujący pośrednią jednostkę certyfikacji powiadamia wystawiający Urząd Certyfikacji, że pierwotny wniosek o wystawienie certyfikatu nie został zatwierdzony i nie przyznaje autoryzacji wstecznie;
- Wystawiający Urząd Certyfikacji dowiaduje się, że CA obsługujący pośrednią jednostkę certyfikacji nie jest już w wyłącznym posiadaniu klucza prywatnego;
- Wystawiający Urząd Certyfikacji dowiaduje się, że klucz publiczny w certyfikacie nie jest już zgodny z wymaganiami określonymi w sekcjach 6.1.5 i 6.1.6.;
- Wystawiający Urząd Certyfikacji dowiaduje się, że certyfikat został użyty niezgodnie z prawem;
- Certyfikat został wystawiony niezgodnie z odpowiednią Polityką Certyfikacji i Kodeksem Postępowania Certyfikacyjnego lub działania CA obsługującego pośrednią jednostkę certyfikacji nie są zgodne z tymi dokumentami;
- Urząd Certyfikacji stwierdza, że niektóre informacje znajdujące się w certyfikacie są fałszywe lub wprowadzają w błąd;
- Wydający Urząd Certyfikacji lub pośredni CA kończy działalność z jakiegokolwiek powodu i nie upoważnił innego Urzędu do utrzymywania listy CRL i unieważniania certyfikatów;
- Urząd Certyfikacji utracił uprawnienia do wydawania certyfikatów i nie zapewnia utrzymania usług CRL i OCSP dla certyfikatów;
- wymóg unieważnienia wynika z Polityki Certyfikacji i/lub Kodeksu Postępowania Certyfikacyjnego wystawiającego Urzędu Certyfikacji;
- Nastąpiła modyfikacja certyfikatu z powodu zmiany danych jednostki certyfikującej lub obsługującego ją Urzędu Certyfikacji;
- Urząd Certyfikacji wystawił certyfikat na podstawie dokumentu pochodzącego od strony trzeciej, a następnie strona ta pisemnie wycofała ten dokument;
- Format i techniczna zawartość Certyfikatu stanowią niedopuszczalne ryzyko dla Stron Ufających (np. w przypadku kiedy algorytm kryptograficzny lub rozmiar klucza nie są bezpieczne);
- urząd certyfikacji obsługujący jednostkę certyfikacyjną lub Urząd Certyfikacji (wystawca certyfikatu tej jednostki) zakończył działalność;
- Unieważnienie certyfikatu wynika z obowiązujących 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:

- Subskrybent;
- Wnioskodawca;
- W przypadku Certyfikatu Organizacyjnego – osoba upoważniona do reprezentowania danej organizacji;
- Osoba do kontaktu wymieniona w umowie na świadczenie usług;
- administrator organizacyjny powołany przez subskrybenta;
- Organ nadzoru, który wydał podmiotowi licencję na świadczenie usług finansowych, w przypadku certyfikatu zawierającego dane podmiotu dotyczące Dyrektywy PSD2 (21) lub Open Banking;
- TSP.

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

TSP udostępnia przejrzyste instrukcje jak raportować podejrzenia kompromitacji klucza prywatnego, nadużycia certyfikatu lub inne rodzaje oszustw, kompromitacje, 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

TSP umożliwia klientom następujące sposoby złożenia wniosku o unieważnienie certyfikatu:

- **Na stronie internetowej Dostawcy Usług**

Klient wypełnia formularz na stronie 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 (24h/7) 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))

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

- **Przez portal Klienta**

Żądanie unieważnienia może być wysłane na portalu klienta pod adresem https://eurocert.portal.pl w trybie 24h/7. 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 na portalu przy użyciu nieanonimowego certyfikatu Aplikanta o klasie bezpieczeństwa nie niższej niż klasa unieważnianego certyfikatu (zob. sekcja 1.2.3). 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 o klasie bezpieczeństwa nie niższej niż klasa unieważnianego certyfikatu (zob. sekcja 1.2.3), pod adres email TSP 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 TSP 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 wniosków na piśmie (w formie papierowej), przy rozpatrywaniu wniosku, TSP weryfikuje autentyczność wniosku 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, podpisanego odręcznie, złożonego poprzez e-mail, TSP weryfikuje podpis odręczny na tym wniosku.

Wnioskodawca musi podać powód unieważnienia. Jeżeli o unieważnienie wystąpił klient, ale nie podał powodu unieważnienia, TSP 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 kompromitacji klucza, TSP od razu zapewnia możliwość wystąpienia z wnioskiem o nowy certyfikat w ramach procedury Recertyfikacji. Zasady tej procedury są opisane w sekcji 4.7.

Jeżeli o unieważnienie wystąpiono pisemnie, TSP udostępnia możliwość unieważnienia 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:

- Dokładną nazwę podmiotu;
- Unikalny identyfikator certyfikatu;
- Wnioskowaną datę unieważnienia, w przypadku, gdy unieważnienie nie następuje natychmiastowo;
- Dane identyfikacyjne klienta.

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

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

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

Dalsze informacje o zawieszeniu i unieważnieniu można znaleźć na stronie TSP pod następującym linkiem:

https://eurocert.pl/index.php/en-us/documents/suspend-or-revoke-of-the-certificate

**Zgłaszanie priorytetowych problemów dotyczących certyfikatów**

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

TSP 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.

TSP rozpoczyna dochodzenie w ciągu 24 godzin od otrzymania zgłoszenia i podejmuje decyzję w sprawie unieważnienia, na podstawie następujących kryteriów:

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

TSP udostępnia wstępny raport o wynikach dochodzenia zarówno subskrybentowi jak i podmiotowi, który zgłosił problem.

Po dokładnym rozpatrzeniu wszystkich faktów i okoliczności, TSP 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 TSP przesyła również organowi nadzoru sprawozdanie zawierające wyniki postepowania wyjaśniającego (dochodzenia).

### 4.9.4. Dopuszczalny okres zwłoki w unieważnieniu

TSP nie przewiduje zwłoki w trakcie realizacji wniosku o unieważnienie.

### 4.9.5. Czas przetwarzania wniosku o unieważnienie

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

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

TSP 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 TSP. 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, za datę przyjęcia uznaje się moment, w którym pracownik biura obsługi klienta TSP otrzymuje wniosek.
d) W przypadku wniosków przesłanych pocztą, za datę otrzymania uznaje się moment w godzinach pracy, kiedy list dociera do TSP.

TSP 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 TSP lub pracownika) lub innymi kanałami, wnioski pozostaną bez rozpatrzenia.

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

TSP rozpoczyna dochodzenie ws. problemu z certyfikatem uwierzytelniania witryny internetowej i podejmuje odpowiednie kroki w ciągu 24 godzin od otrzymania zgłoszenia.

TSP dostarcza wstępny raport z przeprowadzonego dochodzenia subskrybentowi i podmiotowi, który zgłosił problem dotyczący certyfikatu.

TSP unieważnia certyfikat uwierzytelnienia witryny internetowej w ciągu 24 godzin po spełnieniu warunków opisanych w sekcji 4.9.1.

TSP 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 TSP, przed akceptacją i użyciem informacji zawartych w certyfikacie, Strony Ufające muszą działać z należytą starannością i ostrożnością. Zaleca się, by weryfikowały one wszystkie certyfikaty tworzące ścieżkę certyfikacyjną zgodnie z odpowiednimi standardami technicznymi. Weryfikacja powinna obejmować sprawdzenie ważności certyfikatów, wymagań polityk i dozwolonego użycia klucza oraz sprawdzenie informacji o unieważnieniu przy wykorzystaniu listy CRL i OCSP.

### 4.9.7. Częstotliwość publikacji list CRL

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

Ważność tych list wynosi 25 godziny.

TSP wystawia nową listę CRL dla swoich pośrednich jednostek certyfikacyjnych codziennie o tej samej porze oraz w ciągu 1 godziny od unieważnienia. Ważność list CRL wynosi 25 godziny.

### 4.9.8. Maksymalny czas opóźnienia dla list CRL

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

### 4.9.9. Dostępność weryfikacji statusu Certyfikatu online

TSP 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.

TSP udostępnia usługę OCSP za pomocą metody GET.

### 4.9.11. Inne formy publikacji informacji o unieważnieniu

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

### 4.9.12. Specjalne wymagania w przypadku kompromitacji klucza

Każda zainteresowana osoba może zgłosić do TSP zdarzenie kompromitacji klucza, jeśli uzyska informacje, że klucz prywatny jakiegokolwiek Certyfikatu wystawionego przez TSP został skompromitowany.

Najszybciej takiego zgłoszenia można dokonać poprzez stronę: https://eurocert.pl/repozytorium/

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

a. ujawniony klucz prywatny, lub
b. Żądanie certyfikacji w formacie PKCS#10 podpisane skompromitowanym kluczem, zawierające w polu CN: „Proof of Key Compromise”.

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

### 4.9.13. Okoliczności zawieszenia certyfikatu

Certyfikaty uwierzytelniania witryn internetowych nie mogą być zawieszone.

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

- Subskrybent nie zapłacił w terminie za certyfikat;
- TSP podejrzewa, że dane wskazane w certyfikacie są nieprawidłowe, fałszywe. W takim przypadku TSP rozpoczyna procedurę zawieszenia lub unieważnienia certyfikatu;
- TSP podejrzewa, że klucz prywatny należący do certyfikatu nie jest w posiadaniu Podmiotu i ma na to twarde dowody. Jeżeli TSP ma wiedzę, na temat tego, że SCDev znalazło się w posiadaniu osoby nieuprawnionej, TSP zawiesza każdy certyfikat, który znajduje się na tym urządzeniu;
- Organ Nadzoru wydaje prawomocną i skuteczną decyzję.

TSP nie przyjmuje wniosków o zawieszenie certyfikatów nieważnych.

### 4.9.14. Kto może wnioskować o zawieszenie certyfikatu

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

### 4.9.15. Procedura rozpatrywania wniosków o zawieszenie

TSP zapewnia możliwość zainicjowania zawieszenia każdego dnia o dowolnej godzinie.

TSP 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.

TSP udostępnia następujące kanały rozpoczęcia procedury zawieszenia:

- Przez stronę internetową;
- Poprzez portal klienta;
- W ten sam sposób, w jaki składa się wnioski o unieważnienie.

**Zawieszenie przez stronę internetową**

Zawieszenie jest możliwe 24h/7 poprzez stronę internetową TSP pod adresem:
https://eurocert.pl/index.php/en-us/documents/suspend-or-revoke-of-the-certificate

Przy zawieszeniu poprzez stronę internetową TSP klient musi dostarczyć następujące informacje:

- Hasło do zawieszenia uwierzytelniające wniosek o zawieszenie,
- Trzy ostatnie znaki Numeru Seryjnego Podmiotu Certyfikatu (np. 123) lub w przypadku osób fizycznych datę urodzenia podmiotu.

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

W przypadku pomyślnego unieważnienia, jest ono natychmiast odnotowywane w wewnętrznym Rejestrze Statusu Unieważnienia. Cały proces trwa maksymalnie 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)).

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

**Zawieszenie 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**

TSP 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, TSP uznaje, że doszło do kompromitacji klucza prywatnego.

Jeżeli klient wnioskuje o zawieszenie z powodu kompromitacji klucza, TSP umożliwia klientowi wystawienie nowego certyfikatu w ramach procedury Recertyfikacji, 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 od zawieszenia. Jeśli wznowienie certyfikatu nie nastąpi w ciągu tego okresu TSP unieważnia certyfikat bez powiadomienia o tym fakcie.

Wniosek o wznowienie może być złożony jedynie w następujących formach:

- Osobiście w punkcie obsługi klienta TSP;
- Elektronicznie, podpisany elektronicznie przy użyciu certyfikatu nie-pseudonimowego o klasie bezpieczeństwa nie niższej niż zawieszony certyfikat (zob. sekcja 1.2.3.).

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

## 4.10. Usługi statusu certyfikatu

TSP umożliwia następujące możliwości zapytania o status unieważnienia certyfikatu:

- OCSP – usługa online sprawdzenia statusu unieważnienia certyfikatu,
- 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).

W przypadku certyfikatów do podpisywania kodu (codesigning) TSP gwarantuje dostępność informacji o unieważnieniu w oparciu o OCSP po wygaśnięciu daty ważności takich certyfikatów przez co najmniej 10 lat.

TSP prowadzi wewnętrzny Rejestr Statusu Unieważnienia, który zawiera informację na temat bieżącego statusu unieważnienia wszystkich certyfikatów wydanych przez TSP, 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).

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

Odpowiedzi OCSP wygenerowane przez TSP (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 daną jednostkę certyfikacji TSP (za pośrednictwem OCSP Responder) może zawierać status „dobry” tylko dla certyfikatów wydanych przez tą jednostkę i przechowywanych w Repozytorium Certyfikatów TSP (pozytywne OCSP).

### 4.10.1. Szczegóły operacyjne

Każda jednostka certyfikacji TSP wystawia listę CRL z następującą częstotliwością:

- Jednostka certyfikacji Root "EuroCert Commercial": w ciągu 60 minut po unieważnieniu każdego wystawionego certyfikatu, ale nie rzadziej niż raz na 24 godziny.
- Pośrednie Jednostki Certyfikacyjne – w ciągu 60 minut po unieważnieniu każdego wystawionego certyfikatu przez tą 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. TSP zaleca jego użycie.

**Protokół Statusu Certyfikatu Online (OCSP)**

TSP publikuje status unieważnienia certyfikatów również przy użyciu usługi OCSP.

TSP udostępnia usługę OCSP zgodnie z zasadą “authorized responder" IETF RFC 6960 (30), 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).

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

**Usługa OCSP dla Klientów**

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

**Ogólnodostępna i darmowa usługa OCSP**

- 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.
- Ta wersja usługi OCSP jest dostępna przez adres URL wpisany w certyfikacie.

- Usługa OCSP dostarczana dla certyfikatów poczty e-mail (S/MIME) jest zgodna z wymaganiami IETF RFC 5019 (31), wspierając w ten sposób systemy PKI o dużym obciążeniu, które wymagają lekkiego rozwiązania w celu zmniejszenia wymagań dotyczących komunikacji i przetwarzania po stronie klienta.
- Odpowiedź OCSP wygenerowana na podstawie procesu “Response Pre-production” IETF RFC 6960 (30) może być stworzona przed zapytaniem i nie musi koniecznie zawierać elementu „nonce”. TSP może wydać tę samą odpowiedź dla wielu zapytań. Wartości czasu dla "thisUpdate" i "producedAt" są identyczne ale mogą być wcześniejsze niż czas zapytania.
- W przypadku innych certyfikatów, pole "nextUpdate" wpisane w odpowiedzi nie jest wypełniane lub zawiera wartość czasu nie późniejszą niż termin wygaśnięcia certyfikatu OCSP respondera.
- W przypadku S/MIME oraz QWACs: czas „nextUpdate” wskazany w odpowiedzi jest zawsze wypełniany i zawiera czas nie późniejszy niż data wygaśnięcia certyfikatu respondera.

a) Wartość "thisUpdate" w odpowiedzi OCSP nigdy nie może być starsza niż 24 godziny, gdyż TSP tworzy nową odpowiedź OCSP przynajmniej co 24 godziny.
b) W przypadku S/MIME oraz QWACs: różnica czasu pomiędzy „nextUpdate” i „thisUpdate” w odpowiedzi OCSP nigdy nie jest mniejsza niż 8 godzin.
c) Dla pozostałych certyfikatów, różnica czasu pomiędzy wartościami "nextUpdate" i "thisUpdate" w wystawionej odpowiedzi OCSP nie może być dłuższa niż 10 dni.
d) 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”.
e) Odpowiedzi OCSP zawsze zawierają bieżącą informację zawartą w rejestrze unieważnionych certyfikatów TSP 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:

- 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.
- Jeśli okres czasu pomiędzy czasem zapytania a czasem na który jest dokonywana weryfikacja jest dłuższy niż różnica pomiędzy „nextUpdate” i „thisUpdate” w odpowiedzi OCSP (która może wynosić najwyżej okres ważności certyfikatu OCSP Respondera który podpisał odpowiedź). 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.
- 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.

TSP zapewnia obie wersje usługi OCSP z tą samą dostępnością.

#### 4.10.2. Dostępność usługi

TSP zapewnia ciągłą dostępność do Repozytorium Certyfikatów i warunków użytkowania certyfikatów wystawionych przez TSP, na poziomie co najmniej 99,9% w skali roku a jednorazowe przerwy nie mogą przekroczyć 3 godzin.

TSP zapewnia dostępność informacji o statusie unieważnienia, usługi unieważnienia i wewnętrznego rejestru unieważnień na poziomie co najmniej 99,9% w skali roku a jednorazowe przerwy nie mogą przekroczyć 3 godzin.

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

#### 4.10.3. Usługi opcjonalne

TSP udostępnia różne usługi (CRL i dwa typy OCSP) zgodnie z opisem w niniejszej sekcji w ramach których Klienci i Strony Ufające mogą zweryfikować status unieważnienia certyfikatów wystawionych przez TSP. Oprócz tego, TSP udostępnia w swoim publicznym Repozytorium Certyfikatów unieważnione i zawieszone certyfikaty, wraz z wskazanym statusem, po to, aby podczas przeszukiwania Repozytorium Certyfikatów Klienci i Strony Ufające mogli samodzielnie (bez specjalnej aplikacji) zweryfikować status unieważnienia certyfikatu.

### 4.11. Koniec subskrypcji

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

### 4.12. Deponowanie i odzyskiwanie klucza

TSP udostępnia usługę deponowania klucza wyłącznie w przypadku klucza prywatnego należącego do certyfikatów służących do szyfrowanych.

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

W trakcie usługi deponowania, klucz prywatny do odszyfrowywania należący do Certyfikatu służącego do szyfrowania jest przechowywany przez TSP w zaszyfrowanym, unikalnym elektronicznym folderze z użyciem algorytmu AES 256 i z unikalnym kluczem dla każdego pliku. Tak przechowywany klucz jest przekazywany upoważnionej osobie na żądanie. Zgodnie z wewnętrznymi przepisami TSP, TSP powierza swoim pracownikom uczestniczącym w świadczeniu usług zaufania - role zaufane. Pracownik TSP pełniący odpowiednią rolę zaufaną przywraca zdeponowane klucze odszyfrowujące wyłącznie na żądanie klienta i tylko ci pracownicy mają środki i uprawnienia niezbędne do odzyskania kluczy odszyfrowujących.

#### 4.12.1. Deponowanie klucza i polityka odzyskiwania klucza

**Deponowanie klucza odszyfrowującego**

Klucze odszyfrowujące wydane na urządzeniu do składania podpisu elektronicznego są automatycznie deponowane przez TSP. TSP przechowuje klucze odszyfrowujące certyfikatów wystawionych bez urządzenia w następujących sytuacjach:

- Klient wnioskował o certyfikat, który może być użyty do celów administracji elektronicznej i polityka certyfikacji wymaga zdeponowania klucza odszyfrowującego;

- Subskrybent lub podmiot wnioskuje o zdeponowanie klucza.

W przypadku certyfikatu wystawionego bez urządzenia, Klient szyfruje klucz odszyfrowujący w formacie pfx za pomocą certyfikatu do szyfrowania dostarczonego przez TSP a następnie Klient wysyła go jako zaszyfrowany elektroniczny folder na adres e-mail obsługi klienta TSP (handlowy@eurocert.pl). Klient jest odpowiedzialny za zawartość zaszyfrowanego folderu elektronicznego i musi upewnić się, że zaszyfrowany plik rzeczywiście zawiera odpowiedni klucz odszyfrowujący.

**Odzyskiwanie zdeponowanego klucza odszyfrowującego**

Klient musi poprosić o odzyskanie klucza odszyfrowującego, TSP nie narzuca żadnych specjalnych wymogów co do formy takiego wniosku. Wniosek Klienta może być przyjęty np. przez telefon lub e-mail. Klucz może być odebrany przez Klienta, osobę upoważnioną do reprezentowania klienta lub podmiotu osobiście w siedzibie TSP lub na podstawie osobnego wniosku złożonego na miejscu. Przed przekazaniem klucza, przedstawiciel działu obsługi klienta z przypisaną odpowiednią rolą zaufaną identyfikuje odbiorcę i, jeśli zajdzie taka potrzeba, prosi o przedstawienie dokumentów poświadczających upoważnienie do reprezentacji. Identyfikacja tożsamości następuje po okazaniu dowodu tożsamości. TSP uznaje jedynie dokumenty ze zdjęciem. TSP przekazuje zdeponowany klucz na optycznym nośniku danych (np. CD lub DVD) lub na urządzeniu do składania podpisów elektronicznych na wniosek Klienta za dodatkową opłatą.

### 4.12.2. Enkapsulacja symetrycznego klucza szyfrującego i przywracanie

TSP nie używa kluczy symetrycznych w usłudze deponowania klucza.

Klucz prywatny należący do certyfikatu uwierzytelniania witryn internetowych nie może być zdeponowany a zatem nie ma potrzeby zarządzania symetrycznymi kluczami szyfrującymi.

Klucz prywatny należący do certyfikatów podpisów i pieczęci elektronicznych 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

TSP 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 (17) i RFC 5755 (32).

Dane, które mogą zostać zweryfikowane przez TSP:

- Numer seryjny podmiotu (OID),
- imię podmiotu,
- Nazwisko podmiotu,
- Miejsce urodzenia,
- Data urodzenia,
- Nazwisko matki,
- Nazwa i identyfikator dokumentu tożsamości użytego podczas pierwszej weryfikacji tożsamości.

# 5. Zabezpieczenia fizyczne, organizacyjne i operacyjne

TSP stosuje fizyczne, organizacyjne i personalne środki bezpieczeństwa zgodne z powszechnie uznanymi standardami i stosuje procedury administracyjne i zarządzania egzekwujące te środki.

TSP 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.

TSP monitoruje wymagania dotyczące przepustowości i zapewnia odpowiednią moc obliczeniową i pamięć do prawidłowego świadczenia usług.

## 5.1. Fizyczne środki kontroli

TSP 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 TSP.

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) TSP 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 TSP 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 TSP.

### 5.1.2. Dostęp fizyczny

TSP chroni swoje urządzenia i sprzęt, który bierze udział w procesie świadczenia usług przed nieautoryzowanym dostępem fizycznym.

TSP 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

TSP 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.

TSP 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 przed pożarem

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

TSP 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

TSP przestrzega przepisów ochrony środowiska dotyczących niszczenia zbędnych urządzeń i nośników danych.

TSP 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. TSP 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. TSP zapewnia zachowanie poufności informacji które nie zostały zaklasyfikowano jako jawne.

#### 5.1.8. Kopia zapasowa poza siedzibą główną

TSP 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. TSP 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

TSP 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 TSP 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

TSP 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.

TSP powołał następujące role zaufane i obowiązki w następujący sposób:

a) Kierownik z pełną odpowiedzialnością za system IT TSP: 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 TSP. 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 TSP, jest odpowiedzialna za kontrolę przestrzegania środków kontroli wdrożonych przez TSP niezbędnych do prawidłowego funkcjonowania TSP i za bieżący przegląd i monitorowanie istniejących wdrożonych procesów i realizację procedur.

Role zaufane mogą piastować zarówno osoby zatrudnione przez TSP 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.

TSP 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 TSP 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 TSP 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 TSP 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 TSP nadawane są prawa dostępu w zakresie absolutnie koniecznym do wykonywania jego obowiązków.

### 5.2.4. Role wymagające oddzielnych obowiązków

Członkowie Personelu TSP 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.

TSP dąży do niełączenia żadnych ról zaufanych.

## 5.3. Kontrole personelu

TSP wymaga, aby jego polityka dot. personelu i praktyki dotyczące zatrudniania wzmacniały i wspierały wiarygodność działalności TSP. Celem środków bezpieczeństwa zastosowanych wobec personelu i przez personel jest zminimalizowanie ryzyka wystąpienia błędów ludzkich, kradzieży, oszustwa czy nadużyć.

TSP 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, TSP 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 TSP wymaga przynajmniej wykształcenia średniego, ale TSP zapewnia przeprowadzenie odpowiedniego szkolenia stanowiskowego. Zaraz po zatrudnieniu TSP 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 TSP (dowód tożsamości, paszport i prawo jazdy). TSP 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 TSP. Personel pełniący role zaufane musi być wolny od konfliktu interesów, który mógłby negatywnie wpłynąć na bezstronność działalności TSP.

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

TSP 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 TSP weryfikuje informacje podane przez kandydata w CV takie jak: poprzednie miejsce zatrudnienia, referencje, kwalifikacje zawodowe.

### 5.3.3. Szkolenia

TSP 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 TSP i sposób zarządzania nim;
c) niezbędna specjalistyczna wiedza do wykonywania powierzonych zadań;
d) procesy i procedury określone w publicznych i wewnętrznych regulacjach TSP;
e) konsekwencje prawne działań;
f) zasad bezpieczeństwa IT w zakresie niezbędnym do wykonywania konkretnych zadań;
g) zasad ochrony danych osobowych.

TSP 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 TSP otrzymują wyłącznie osoby, które pomyślnie przeszły wymagane szkolenia.

### 5.3.4. Częstotliwość szkoleń przypominających

TSP 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 TSP.

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

TSP nie stosuje obowiązkowej rotacji pomiędzy indywidualnymi planami (harmonogramami) pracy.

### 5.3.6. Kary za nieuprawnione działania

TSP 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, TSP 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 niezależnego wykonawcy

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, TSP w miarę możliwości wybiera podwykonawców i wykonawców z listy wcześniej zakwalifikowanych dostawców. TSP 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 TSP nie przeprowadza dla nich żadnych szkoleń.

#### 5.3.8. Dokumentacja dostarczona personelowi

TSP 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 TSP,
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 TSP.

### 5.4. Rejestrowanie zdarzeń

W celu zachowania bezpiecznego środowiska IT, TSP wdraża i prowadzi kompleksowy system rejestrowania i monitorowania zdarzeń w całym swoim systemie IT.

#### 5.4.1. Rodzaje zapisywanych zdarzeń

TSP 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 TSP.

TSP 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 TSP.
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 TSP.

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 zaufania;
- 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 TSP 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, TSP 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 logów

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 TSP zapewnia, że dane można odczytać i w tym celu utrzymuje niezbędne oprogramowanie i sprzęt.

### 5.4.4. Ochrona logów

TSP 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.

TSP 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) TSP zapewnia bezpieczne (poufne) przechowywanie takich danych. Dostęp do wpisów dziennika mają wyłącznie upoważnione osoby, które absolutnie potrzebują ich do poprawnego wykonania swoich obowiązków służbowych. TSP kontroluje dostęp do zapisów dziennika w sposób bezpieczny. TSP przechowuje pliki dziennika w bezpiecznym środowisku, a kopie plików – w innym miejscu niepodlegającym tym samym zagrożeniom środowiskowym.

### 5.4.5. Procedury tworzenia kopii zapasowej dziennika zdarzeń

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 TSP.

### 5.4.6. System zbierania logów (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 TSP 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, TSP angażuje ich w dochodzenie dotyczące zdarzenia. W takim przypadku Klienci, którzy zostali dotknięci lub wywołali zdarzenie współpracują z TSP w celu jego wyjaśnienia. TSP 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 TSP 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 TSP 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 TSP:

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 TSP 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. Typy archiwizowanych zapisów

Dokumenty w formie papierowej i elektronicznej są odpowiednio przygotowane przez TSP w celu bezpiecznego długoterminowego archiwizowania.

TSP archiwizuje przynajmniej następujące rodzaje informacji:

a) dokumenty związane z akredytacją TSP;
b) wszystkie wydane wersje Polityki Certyfikacji i Kodeksu Postępowania Certyfikacyjnego;
c) wszystkie wersje Warunków Świadczenia Usług Zaufania EuroCert;
d) umowy związane z działalnością TSP;
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 utrzymywania archiwum

TSP przechowuje zarchiwizowane dane przez następujące okresy (chyba że przepisy prawa stanowią inaczej):

a) Politykę Certyfikacji przez co najmniej 10 lat od daty uchylenia;
b) Kodeks Postępowania Certyfikacyjnego przez co najmniej 10 lat od daty uchylenia;
c) Warunki świadczenia usług zaufania przez co najmniej 10 lat od daty uchylenia;
d) w przypadku identyfikacji tożsamości z wykorzystaniem systemu video, cały jej przebieg (nagrany) przez co najmniej 10 lat od daty nagrania;
e) główne dane związane z wydawaniem znacznika czasu przez co najmniej 10 lat od wydania;
f) wszystkie elektroniczne i papierowe dokumenty związane z certyfikatami przez co najmniej:
   - 10 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 10 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 TSP 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 kopii zapasowej archiwum

TSP 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, TSP 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 TSP, 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).

TSP synchronizuje swój wewnętrzny zegar z powyższymi niezależnymi źródłami Stratum-1 z dokładnością do 0.1 sekundy co najmniej cztery razy dziennie.

W ten sposób TSP zapewnia, że odchylenie czasu wskazanego w znaczniku czasu w stosunku do czasu UTC wynosi co najwyżej jedną sekundę.

TSP 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 archiwizacji (wewnętrzny lub zewnętrzny)

Wpisy dziennika są generowane w chronionym systemie komputerowym TSP, 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 TSP w wewnętrznym repozytorium.

#### 5.5.7. Procedury uzyskania i weryfikacji dokumentacji w archiwum

TSP codziennie generuje podpisane pliki dziennika automatycznie.

Pliki zarchiwizowane są chronione przed nieautoryzowanym dostępem i utraceniem.

TSP 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

TSP zapewnia, że Jednostki Certyfikacyjne posiadają zawsze ważny klucz i certyfikat do swojej działalności. W tym celu, odpowiednio przed wygaśnięciem ich certyfikatu lub kluczy, TSP 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 TSP 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) TSP 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, TSP podejmuje wszelkie niezbędne środki w celu zminimalizowania szkód powstałych wskutek wstrzymania usług i przywraca je najszybciej jak to możliwe.

Na podstawie oceny powstałego incydentu, TSP podejmuje niezbędne zmiany i działania naprawcze, aby zapobiec wystąpieniu podobnych incydentów w przyszłości.

TSP 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

TSP postępuje według planu ciągłości działania.

Plan ciągłości działania zawiera procedury na wypadek ujawnienia klucza, podejrzenia ujawnienia oraz awarii zegara Jednostki Znakowania Czasem. TSP ujawnia informacje o wyżej wymienionych zdarzeniach. TSP nie wystawia znacznika czasu w przypadku wystąpienia powyższych zdarzeń do czasu wyjaśnienia sytuacji.

TSP ujawnia informacje niezbędne do zidentyfikowania dotkniętych znaczników czasu w przypadku wystąpienia powyższych zdarzeń.

TSP 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.

TSP na okresowo testuje przełączenie na działanie systemu zapasowego według posiadanego planu odtwarzania usług i przeprowadza coroczny przegląd aktualności swojego planu ciągłości działania.

TSP 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.

TSP 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 TSP, 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 TSP szczegółowo określają obowiązki związane z obsługą incydentów bezpieczeństwa. Wszelkie odstępstwa od normalnych operacji są rejestrowane w wewnętrznym systemie zarządzania zadaniami po ich wykryciu. TSP, 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 TSP.

We wszystkich przypadkach TSP 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.

TSP 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. Uszkodzenie zasobów obliczeniowych, oprogramowania i/lub danych

Systemy IT TSP 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.

TSP każdego dnia wykonuje pełny backup swoich baz danych i zarejestrowanych logów (zdarzeń).

TSP wykonuje pełny backup systemu z taką częstotliwością, aby być w stanie przywrócić pełny zakres usług w przypadku krytycznego zdarzenia losowego.

Plan ciągłości TSP 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 TSP.

Po usunięciu problemu i przywróceniu integralności systemu, TSP wznawia swoje usługi najszybciej jak to możliwe.

Usługi publikacji informacji o statusie certyfikatu mają pierwszeństwo podczas przywracania usług.

### 5.7.3. Procedury związane z kompromitacją klucza prywatnego

W przypadku ujawnienia klucza lub podejrzenia ujawnienia klucza prywatnego TSP, 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. TSP 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 TSP - TSP natychmiast informuje ten wydający urząd certyfikacji o wystąpieniu ujawnienia i rozpoczyna procedurę unieważnienia certyfikatu należącego do danego klucza.

TSP 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, TSP 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.

TSP 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).

TSP zobowiązany jest jak najszybciej powiadomić poszkodowanych użytkowników o wdrożeniu Planu Odtwarzania Systemów i (ewentualnie) o przyczynach jego wdrożenia.

Po przywróceniu usług, TSP niezwłocznie powraca do trybu działania biznesowego z zachowaniem poziomu bezpieczeństwa akceptowanego dla usług przed zdarzeniem.

## 5.8. Zakończenie działań CA lub RA

W przypadku planowanego zakończenia świadczenia usług, TSP 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, TSP 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, TSP:

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, TSP 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.

TSP unieważnia certyfikaty odpowiadające zdalnym kluczom prywatnym zarządzanym przez TSP niezwłocznie po zamknięciu Usługi Zdalnego Podpisu/Pieczęci. TSP 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, TSP przeprowadzi negocjacje z innym Dostawcą Usług Zaufania w sprawie przejęcia usług. TSP 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.

TSP podejmuje działania w zakresie unieważnienia certyfikatów dostawcy (i niszczy klucze prywatne) w ciągu 60 dni, w zależności od wyniku negocjacji.

TSP informuje Organ Nadzoru i Klientów o ostatecznym wyniku negocjacji. TSP informuje swoich klientów za pomocą e-maila a Strony Ufające poprzez publikację na stronie internetowej.

TSP publikuje ogłoszenie o zamknięciu aktywnych jednostek certyfikacji przynajmniej 5 dni przed zamknięciem, zgodnie z sekcją 2.1.

TSP niszczy klucze prywatne zlikwidowanych urzędów certyfikacji w ciągu 5 dni roboczych po likwidacji w sposób rejestrowany.

Po zakończeniu usług, TSP generuje pełną kopię zapasową danych przechowywanych w swoim systemie IT i pieczętuje ją kwalifikowanym znacznikiem czasu.

TSP umożliwia upoważnionym stronom pomoc w zrozumieniu danych znajdujących się w rejestrach unieważnionych i zawieszonych certyfikatów, jeśli zajdzie taka potrzeba.

W celu przekazania danych innemu Dostawcy Usług Zaufania, TSP umieszcza dane na nośnikach w formacie, który nowy Dostawca Usług Zaufania może odczytać lub przekazuje dane w oryginalnym formacie i zapewnia narzędzie, dokumentację lub wiedzę w celu odczytania danych.

# 6. Technicznego środki bezpieczeństwa

TSP do świadczenia swoich usług wykorzystuje systemy złożone z niezawodnego i bezpiecznego pod względem technicznym sprzętu. TSP zarządza swoimi kryptograficznymi kluczami prywatnymi podczas całego cyklu ich życia w module HSM, który posiada odpowiednią certyfikację.

Zarówno TSP 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.

TSP nieustannie monitoruje zapotrzebowanie na wydajność systemu (przepustowość) i na podstawie wyznaczenia trendu szacuje oczekiwane przyszłe zapotrzebowanie na wydajność. TSP może zwiększyć wydajność w razie potrzeby, aby zapewnić niezbędną moc obliczeniową i ciągłą dostępność magazynu pamięci.

## 6.1. Generowanie i instalacja pary kluczy

TSP gwarantuje, że generowanie i zarządzanie wszystkimi kluczami prywatnymi wydanymi dla podmiotów, dla siebie lub swoich jednostek (np. repozytorium certyfikatów, urzędów rejestracji), jest bezpieczne i zgodne z aktualnymi wymaganiami i standardami technicznymi.

### 6.1.1. Generowanie pary kluczy

TSP wykorzystuje algorytmy generowania pary kluczy, które są zgodne z wymogami przedstawionymi w poniższych normach:

- ETSI TS 119 312 (33);
- Rekomendacje CABF.

**Generowanie pary kluczy Dostawcy**

Przy generowaniu własnej pary kluczy TSP 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 TSP 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 TSP 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, TSP 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 TSP (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 pary kluczy dostawcy przeprowadzane jest na urządzeniu, które:
   - Spełnia wymagania ISO/IEC 19790 (34), lub
   - Spełnia wymagania FIPS 140-2 (8) poziom 3 lub wyższy, lub
   - Spełnia wymagania FIPS 140-3 (9) poziom 3 lub wyższy, lub
   - Spełnia wymagania CEN 419 221-5 (7), lub
   - Jest bezpiecznym systemem spełniającym ISO/IEC 15408 (35) lub inne równoważne kryteria bezpieczeństwa na poziomie EAL4 lub wyższym. Ocena opiera się na konstrukcji systemu bezpieczeństwa lub regulacjach dotyczących bezpieczeństwa spełniających wymogi niniejszego dokumentu.
8) Szczegółowe logi z ceremonii są rejestrowane.
9) TSP podejmuje odpowiednie środki aby zapewnić, że klucz prywatny został wygenerowany i zabezpieczony zgodnie z określonymi procesami podczas ceremonii.

**Generowanie pary kluczy infrastruktury**

W przypadku generowania kluczy infrastruktury używanych w celach własnych, w swoich własnych systemach IT, TSP upewnia się, że:

- Generowanie kluczy infrastruktury Dostawcy Usług odbywa się w fizycznie bezpiecznym środowisku (zob. sekcja 5.1) przez osobę pełniącą rolę zaufaną (zob. sekcja 5.2.1), z wyłączeniem obecności innych nieautoryzowanych osób;
- Generowanie klucza jest w pełni zgodne z instrukcją zawartą w dokumentacji urządzenia.

**Generowanie pary kluczy Subskrybenta**

W przypadku generowania pary kluczy dla podmiotu, TSP zapewnia, że:

- klucze są generowane w fizycznie bezpiecznym środowisku wyłącznie w obecności osób pełniących role zaufane.
- Jeśli Polityka Certyfikacji wymaga użycia urządzenia kryptograficznego, TSP generuje klucz prywatny na urządzeniu kryptograficznym użytkownika, które uniemożliwia ujawnienie klucza prywatnego.
- TSP nigdy nie generuje pary kluczy do pliku, nie chronionych żadnym urządzeniem.
- TSP 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.
- Wygenerowane klucze prywatne na urządzeniach są przechowywane przez TSP aż do momentu udokumentowanego ich wydania Podmiotowi, w odpowiednim bezpiecznym środowisku w celu zapobieżenia ujawnieniu. Po udokumentowanym przekazaniu klucza prywatnego wnioskodawcy, TSP niszczy każdą przechowywaną kopię przekazanego klucza – z wyjątkiem kluczy szyfrujących, które są przekazane do depozytu – w taki sposób że ich odzyskanie i użycie jest niemożliwe.
- w przypadku Usługi Zdalnego Podpisu: klucze są generowane w fizycznie chronionym środowisku, automatycznie lub przy udziale wyłącznie ról zaufanych.

TSP nigdy nie generuje par kluczy dla certyfikatów uwierzytelniania witryn internetowych.

W przypadku pary kluczy wygenerowanej przez Aplikującego:

- klucze są generowane w bezpiecznym środowisku, znajdującym się pod kontrolą wnioskodawcy;
- Wnioskodawca zapewnia odpowiednią ochronę wygenerowanego klucza prywatnego;
- TSP 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 TSP 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) TSP wie o zademonstrowanej lub udowodnionej metodzie, która może prowadzić do ujawnienia klucza prywatnego podmiotu;
d) TSP dowiedział się, że klucz prywatny Podmiotu został ujawniony, zgodnie z postanowieniami w sekcji 4.9.1;
e) TSP 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 niezabezpieczonych urządzeniem kryptograficznym, klient sam generuje klucz prywatny, zatem nie ma potrzeby jego dostarczania.

TSP nigdy nie generuje par kluczy dla certyfikatów uwierzytelniania witryny internetowej.

Jeżeli TSP wygenerował prywatny klucz podmiotu, spełnione muszą zostać następujące wymagania:

**Jeżeli klucz prywatny jest przekazywany podmiotowi:**

- Do momentu przekazania klucza, TSP przechowuje wygenerowane dla podmiotu klucze prywatne i dane aktywacyjne w bezpiecznym miejscu uniemożliwiającym ich ujawnienie, skopiowanie, zmianę, zniszczenie czy użycie przez osoby nieupoważnione.
- TSP gwarantuje, że klucze prywatne i ich dane aktywacyjne mogą być odebrane wyłącznie przez uprawnionego wnioskodawcę.
- TSP rejestruje dowody przekazania klucza prywatnego wnioskodawcy i dokładny czas.
- Po przekazaniu wnioskodawcy klucza prywatnego, TSP nie zatrzymuje żadnej kopii klucza prywatnego.

W przypadku Polityk Certyfikacji wymagających użycia urządzenia kryptograficznego, prywatny klucz podmiotu wraz z urządzeniem kryptograficznym, które zapewnia bezpieczne przechowywanie i użycie klucza prywatnego jest przekazywany wnioskodawcy osobiście z zaklejoną kopertą, która zawiera kod aktywacyjny.

TSP może również dostarczyć wnioskodawcy urządzenie kryptograficzne za pośrednictwem strony trzeciej, gwarantując, że:

- Urządzenie kryptograficzne jest w trybie transportu aż do momentu dostarczenia wnioskodawcy;
- Kod aktywacyjny do urządzenia jest przekazywany wnioskodawcy innym osobnym kanałem;
- Certyfikat zostanie wystawiony wyłącznie po uprzednim potwierdzeniu dostarczenia urządzenia wnioskodawcy.

Po wygenerowaniu klucza, QSCD 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, klient sam generuje klucz prywatny, a zatem nie ma potrzeby dostarczania go do klienta.

W przypadku usługi zdalnego podpisu:

a) W trakcie całej usługi TSP przechowuje klucz prywatny i dane aktywacyjne wygenerowane przez TSP dla Podmiotu w bezpieczny sposób w celu uniknięcia ujawnienia klucza, skopiowania, modyfikacji, zniszczenia i użycia przez nieupoważnione osoby.
b) TSP stosuje procedurę identyfikacji, która zapewnia, że klucz prywatny może zostać użyty wyłącznie przez uprawniony Podmiot.
c) TSP przechowuje wystarczające dowody na to, że przekazanie kontroli nad kluczem prywatnym Podmiotowi nastąpiło w konkretnym autentycznym czasie.
d) TSP 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:

- Klucz publiczny musi zostać wysłany do TSP w taki sposób, aby można go było jednoznacznie przypisać do wnioskodawcy;

- 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 TSP żądanie w formacie PKCS#10, który podpisany jest kluczem prywatnym odpowiadającym kluczowi publicznemu. Żądanie PKCS#10 zawiera klucz publiczny wygenerowany przez wnioskodawcę i dane podmiotu, które mają się znaleźć w certyfikacie, a zatem obydwa powyższe warunki zostają spełnione.

TSP sam wystawia własne certyfikaty i pary kluczy niezbędne do świadczenia usług zaufania, więc nie musi dostarczać nikomu kluczy publicznych do certyfikacji. W przypadku certyfikatu dostawcy wystawionego przez inne CA, TSP wysyła wystawcy żądanie PKCS#10, który jest podpisany kluczem prywatnym należącym do klucza publicznego, który ma się znaleźć w certyfikacie.

### 6.1.4. Dostarczenie publicznego klucza CA stronom ufającym

TSP publikuje certyfikaty obsługiwanych jednostek certyfikacji oraz informacje o statusie tych certyfikatów stronom zainteresowanym w następujący sposób:

- TSP 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).
- Nazwy głównych i pośrednich jednostek certyfikacyjnych i hash certyfikatów root znajdują się w sekcji 1.3.1.
- Certyfikaty pośrednich jednostek certyfikacyjnych są publikowane na polskiej zaufanej liście (36) zarządzanej i publikowanej przez Organ Nadzoru w ramach wspólnego rozporządzenia europejskiego (37). Lista zawiera wszystkie certyfikaty dostawcy (łącznie z certyfikatami wygasłymi i unieważnionymi).

TSP ujawnia stronom ufającym status certyfikatu swoich jednostek certyfikacyjnych za pomocą następujących metod:

- Status certyfikatu jednostek certyfikacyjnych root jest dostępny na stronie internetowej TSP.
- Status certyfikatu pośrednich jednostek certyfikacyjnych jest ujawniony na liście CRL, na stronie internetowej i w ramach usługi odpowiedzi statusu certyfikatu online.

Odnośnie metod ujawniania informacji na temat statusu, zobacz również Sekcję 4.10.

### 6.1.5. Rozmiary kluczy

TSP używa tylko algorytmów kryptograficznych i minimalnych rozmiarów kluczy, które są zgodne z wymogami przedstawionymi w poniższych normach:

- ETSI TS 119 312 (33);
- Rekomendacje CABF.

TSP używa przynajmniej 4096 bitowych kluczy RSA lub co najmniej 256 bitowych kluczy ECC we wszystkich aktualnych certyfikatach pośrednich i root oraz certyfikatach urzędu znacznika czasu i jednostek podpisujących odpowiedzi OCSP.

TSP wydaje certyfikaty użytkownika końcowego wyłącznie dla kluczy RSA przynajmniej 2048 bitowych lub kluczy ECC co najmniej 256 bitowych.

Podczas świadczenia usługi zdalnego podpisu, TSP 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
   a) długość klucza: 256 bits
   b) algorytm hash: SHA-256
   c) krzywa:
      - ECC NIST P-256
      - ECC NIST P-384 (384 bit)
      - ECC NIST P-521 (521 bit)

### 6.1.6. Parametry generowanie klucza publicznego i kontrola jakości

TSP generuje klucze zgodnie z opisem zamieszczonym w Sekcji 6.1.1.

**Weryfikacja zgodności parametrów**

TSP weryfikuje zgodność każdego klucza dostawcy i użytkownika końcowego przed wygenerowaniem certyfikatu, zgodnie z poniższymi 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 (38))

### 6.1.7. Cel użycia klucza (pole X.509 v3)

Klucz prywatny jednostki certyfikacyjnej typu root TSP może być wykorzystany wyłącznie do następujących celów:

- Wystawienie auto-certyfikatów dla siebie samej,
- Podpisanie certyfikatów pośrednich jednostek certyfikacyjnych,
- Podpisanie certyfikatu dla wystawców odpowiedzi OCSP,
- Podpisanie list CRL.

Klucz prywatny pośredniej jednostki certyfikacyjnej TSP – oraz klucz prywatny wystawiony dla pośredniej jednostki certyfikacyjnej obcej organizacji – może być wykorzystany wyłącznie do następujących celów:

- Podpisanie certyfikatów pośrednich jednostek certyfikacyjnych,
- Podpisanie certyfikatu użytkownika końcowego,
- Podpisanie certyfikatu urzędu znacznika czasu,
- Podpisanie certyfikatu dla usługi OCSP,

- Podpisanie list CRL.

TSP 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 (39). Wymagania dotyczące wartości w tym polu omówiono w Sekcji 7.1.2.

Klucz prywatny podmiotu może być użyty wyłącznie zgodnie z dozwolonym 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 niedozwolone.

Klucz prywatny pieczęci może być użyty wyłącznie w celu złożenia pieczęci elektronicznej, każde inne użycie jest niedozwolone.

Klucze prywatne wystawców odpowiedzi OSCP mogą być użyte wyłącznie do podpisywania odpowiedzi OCSP.

## 6.2. Ochrona klucza prywatnego i kontrole modułu kryptograficznego

TSP gwarantuje bezpieczne zarządzanie posiadanymi kluczami prywatnymi, zapobiega ich ujawnieniu, skopiowaniu, usunięciu, modyfikacji i nieautoryzowanemu użyciu. TSP może przechowywać klucz prywatny tylko tak długo jak wymaga tego dana usługa.

TSP 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 TSP wykorzystywane do wystawiania Certyfikatów są przechowywane w bezpiecznym miejscu w module HSM.

TSP usuwa klucze prywatne przechowywane w modułach HSM, które są uszkodzone, wycofane z użytku, zgodnie z instrukcją obsługi urządzenia w sposób uniemożliwiający przywrócenie kluczy.

Urządzenie 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, TSP nie wystawia podmiotowi wcześniej kluczy prywatnych, co eliminuje konieczność zabezpieczania kluczy prywatnych użytkownika końcowego.

W przypadku certyfikatów służących do uwierzytelniania witryn internetowych, TSP nigdy nie generuje wnioskodawcy par kluczy, co eliminuje konieczność zabezpieczania kluczy prywatnych użytkownika końcowego.

### 6.2.1. Standardy dotyczące modułu kryptograficznego i kontroli

Systemy TSP wystawiające certyfikaty, podpisujące odpowiedzi OCSP i listy CRL przechowują klucze prywatne w bezpiecznych urządzeniach sprzętowych, które spełniają następujące wymagania:

- ISO/IEC 19790 (34), lub
- FIPS 140-2 (8) poziom 3 lub wyższy, lub
- FIPS 140-3 (9) poziom 3 lub wyższy, lub
- CEN 419 221-5 (7), lub
- EAL 4+ ISO/IEC 15408 (35) lub równoważne kryteria oceny poziomu bezpieczeństwa produktów IT.

W usłudze Zdalnego Podpisu (Pieczęci) TSP zarządza kluczami prywatnymi użytkowników końcowych w module kryptograficznym który:

- Posiada certyfikat zgodności z Common Criteria, przynajmniej poziom EAL 4+, który potwierdza zgodność z wymogami CEN 419 241-1 (40) i jest opublikowany na liście QSCD Komisji UE (41).

TSP 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 TSP 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 TSP dokonuje zniszczenia zaszyfrowanych kluczy lub koduje je ponownie przy użyciu algorytmu i parametrów klucza, które zapewniają wyższą ochronę.

### 6.2.2. Ochrona klucza prywatnego (N z M)

TSP stosuję podział sekret „n z m” przy aktywacji klucza prywatnego. Parametry są określone w ten sposób że wymagana jest jednoczesna obecność przynajmniej dwóch pracowników (spośród „m”) z przypisanymi rolami zaufanymi do wykonania kluczowych operacji przy użyciu prywatnych kluczy dostawcy.

### 6.2.3. Deponowanie klucza prywatnego

TSP nie deponuje swoich własnych kluczy prywatnych dostawcy ani użytkowników końcowych.

### 6.2.4. Kopia zapasowa klucza prywatnego

TSP 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 przywracanie klucza mogą się odbywać wyłącznie przy użyciu mechanizmów zabezpieczających opisanych w sekcji 6.2.2.

TSP przechowuje kopię zapasową w dwóch egzemplarzach, z których przynajmniej jedna kopia jest przechowywana w innym miejscu niż miejsce świadczenia usług.

Takie same surowe standardy bezpieczeństwa stosuje się przy zarządzaniu i przechowywaniu kopii zapasowych jak przy działaniu systemu produkcyjnego.

TSP nie wykonuje kopii kluczy prywatnych użytkownika końcowego, z wyjątkiem usługi zdalnego podpisu.

### 6.2.5. Archiwizacja klucza prywatnego

TSP nie archiwizuje swoich kluczy prywatnych i kluczy prywatnych użytkowników końcowych.

### 6.2.6. Przeniesienie klucza prywatnego z lub do modułu kryptograficznego

Wszystkie własne klucze prywatne TSP i klucze prywatne użytkowników końcowych zarządzane przez TSP są generowane w module HSM, który spełnia określone wymagania.

Klucze prywatne nie występują w formie jawnej poza modułem HSM.

TSP eksportuje klucz prywatny z modułu HSM 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

TSP przechowuje swoje klucze prywatne używane do świadczenia usług oraz zdalne klucze klientów 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

TSP przechowuje swoje klucze prywatne dostawcy w HSM i przestrzega instrukcji obsługi oraz wymagań 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. TSP przechowuje karty operatorskie należące do HSM, w bezpiecznym środowisku. Dostęp do tych kart mają wyłącznie upoważnieni pracownicy TSP.

TSP 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 TSP, 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 celu aktywacji klucza do zdalnego podpisu, Podmiot przedstawia hasło i unikalne krótkoterminowe hasło (TOTP).

W przypadku kluczy prywatnych przekazywanych wnioskodawcy przez TSP na urządzeniu kryptograficznym (takim jak karta inteligentna lub token), urządzenie jest przygotowane dla Podmiotu, skonfigurowane i przekazane Podmiotowi w taki sposób, że:

- Można jednoznacznie stwierdzić, że urządzenie nie było używane przed przekazaniem,
- Przed użyciem klucza prywatnego do wnioskodawca uwierzytelnia się w urządzeniu kryptograficznym.

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 TSP i zarządzany przez urządzenia kryptograficzne zostaje dezaktywowany jeśli urządzenie traci status aktywny. Ma to miejsce kiedy:

- Użytkownik dezaktywuje klucz;
- Zasilanie urządzeń zostaje przerwane (wyłączenie prądu lub problemy z dostawą prądu);
- 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:

- Zasilanie urządzenia zostaje przerwane;
- Wnioskodawca wychodzi z aplikacji, używającej urządzenia zawierającego klucz prywatny;
- Wnioskodawca wydaje w aplikacji polecenie dezaktywacji urządzenia.

Dezaktywowany klucz i urządzenie kryptograficzne mogą być użyte do złożenia podpisu/pieczęci wyłącznie po ponownym uwierzytelnieniu wnioskodawcy.

W przypadku, gdy Polityki Certyfikacyjne nie wymagają użycia 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 skompromitowane klucze prywatne TSP są niszczone w sposób, który uniemożliwia ich dalsze użycie.

TSP 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 TSP (administratora infrastruktury i inspektors.ds. bezpieczeństwa) z wyłączeniem obecności osób trzecich.

TSP 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**

Jeżeli Polityka certyfikacji wymaga użycia urządzenia kryptograficznego, niepotrzebne klucze prywatne powinny 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.

Rekomenduje się, aby zużyte klucze prywatne użytkownika końcowego do uwierzytelniania były niszczone, natomiast w przypadku kluczy prywatnych do szyfrowania zaleca się ich zachowanie po to, aby uprzednio zaszyfrowane dokumenty mogły być później rozszyfrowane.

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 TSP są przechowywany w module kryptograficznym, który:

- Posiada certyfikat zgodności z ISO/IEC 19790 (34), lub
- Posiada certyfikat zgodności z FIPS 140-2 Level 3 (8), lub
- Posiada certyfikat zgodności z FIPS 140-3 Level 3 , lub
- Posiada certyfikat zgodności z Common Criteria (5), EAL 4+, który potwierdza zgodność z wymaganiami CEN 419 221-5 (7), lub
- Posiada certyfikat wystawiony przez niezależną organizację certyfikującą uprawnioną do przeprowadzenia oceny produktów umożliwiających składanie podpisów elektronicznych, zarejestrowaną przez Organ Nadzoru lub w kraju członkowskim Unii Europejskiej.

Zgodnie z wymogami sekcji 6.2.1 TSP w ramach Usługi Zdalnego Podpisu zarządza kluczami użytkowników końcowych w module HSM zgodnym z wymaganiami CEN 419 241-1 (40), opublikowanym na liście QSCD Komisji UE (41).

### 6.3. Inne aspekty zarządzania parą kluczy

#### 6.3.1. Archiwizacja klucza publicznego

TSP archiwizuje wszystkie certyfikaty przez okres 10 lat od ich wygaśnięcia lub do czasu prawomocnego zakończenia zaistniałego sporu prawnego związanego z certyfikatem (lub podpisem elektronicznym opartym na Certyfikacie).

Przez ten sam okres TSP 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 TSP 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 root TSP oraz kluczy prywatnych:

- Klucz jednostki certyfikującej root „EuroCert Commercial” jest ważny do 2046-05-31.

**Klucze i certyfikaty pośrednich jednostek certyfikacyjnych**

Okres ważności certyfikatów pośrednich jednostek certyfikacyjnych TSP oraz kluczy prywatnych do nich należących:

- Nie powinien przekroczyć okresu czasu, w ciągu którego wykorzystywane algorytmy kryptograficzne - zgodnie z normami - mogą być bezpiecznie używane;
- Nie powinien przekroczyć okresu ważności certyfikatu jednostki głównej root lub pośredniej, która wydała certyfikat pośredniej jednostce certyfikacyjnej.

Klucze jednostki pośredniej (nie root) TSP są ważne do momentu wygaśnięcia odpowiadających im certyfikatów.

**Certyfikaty użytkowników końcowych**

Okres ważności certyfikatów użytkowników końcowych wystawionych przez TSP:

- Wynosi maksimum
  - 398 dni ( =˜13 miesięcy) od wystawienia – w przypadku certyfikatów uwierzytelniania witryn internetowych;
  - 39 miesięcy od wystawienia - przypadku certyfikatów Code Signing;
  - 824 dni (=˜ 27 miesięcy) od wystawienia w przypadku certyfikatów Email S/MIME;
  - 3 lat od wystawienia w przypadku innych certyfikatów;
- Nie powinien przekroczyć okresu czasu, w ciągu którego wykorzystywane algorytmy kryptograficzne mogą być bezpiecznie używane zgodnie z normami;
- Nie powinien przekroczyć daty wygaśnięcia certyfikatu dostawcy, który wystawił dany certyfikat.

Podczas odnawiania i modyfikacji certyfikatu TSP może wystawić nowy certyfikat dla tego samego klucza prywatnego użytkownika końcowego.

Okres ważności klucza dostawcy lub klienta 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, TSP unieważni te certyfikaty.

TSP niszczy zdalny klucz prywatny użytkownika zarządzany przez TSP odpowiadający unieważnionemu certyfikatowi.

## 6.4. Dane aktywacyjne

### 6.4.1. Generowanie i instalacja danych aktywacyjnych

Klucze prywatne TSP 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 urządzenia kryptograficznego dostarczonego przez TSP na rzecz wnioskodawcy, TSP zapewnia, że:

- Dane aktywacyjne są tworzone i instalowane dla urządzenia kryptograficznego w fizycznie bezpiecznym środowisku przy użyciu odpowiedniej jakości generatora liczb losowych;
- Dane aktywacyjne są przekazywane wnioskodawcy przy użyciu bezpiecznej metody.

TSP nigdy nie generuje kluczy prywatnych do pliku (niezabezpieczonych urządzeniem kryptograficznym) 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 TSP 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 urządzenia kryptograficznego wydawanego wnioskodawcom przez TSP:

- TSP zapisuje dane aktywacyjne wyłącznie w celu przekazania ich wnioskodawcy;
- TSP 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 TSP zapewnia zgodność z następującymi wymaganiami:

- przed udzieleniem dostępu do systemu lub aplikacji, tożsamość użytkownika jest weryfikowana za pomocą uwierzytelniania dwuskładnikowego z użyciem certyfikatów VPN przechowywanych na karcie;
- przydziela role użytkownikom, co zapewnia, że użytkownicy mają uprawnienia odpowiadające wyłącznie ich rolom;
- dla każdej transakcji tworzony jest wpis dziennika, a wpisy dziennika są archiwizowane;
- dla procesów krytycznych dla bezpieczeństwa zapewnia się, że domeny sieci wewnętrznej TSP są wystarczająco chronione przed nieautoryzowanym dostępem;
- wdrożone są odpowiednie procedury zapewniające przywrócenie 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 TSP:

- podejmuje działania w celu wyeliminowania wykrytych podatności, lub/i
- akceptuje zidentyfikowane ryzyka rezydualne, podając powód decyzji.

## 6.6. Techniczne kontrole cyklu życia

### 6.6.1. Kontrola rozwoju systemu

W swoim produkcyjnym systemie IT, TSP 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 TSP, zaprojektowanymi przy zastosowaniu ustrukturyzowanych metod rozwoju i kontrolowanego środowiska programistycznego, lub;
c) dopasowanymi rozwiązaniami sprzętowymi i programowymi opracowanymi przez wiarygodną stronę trzecią dla TSP, 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 TSP do innych celów.

TSP 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.

TSP zachowuje taką samą ostrożność przy zakupie lub tworzeniu aktualizacji oprogramowania, jak przy zakupie pierwszej wersji.

TSP zatrudnia rzetelny, odpowiednio przeszkolony personel do obsługi i instalacji oprogramowania i sprzętu.

TSP instaluje dla sprzętu informatycznego wyłącznie oprogramowanie niezbędne do świadczenia usług.

TSP posiada system śledzenia zmian, w którym każda zmiana systemu informatycznego jest rejestrowana.

TSP 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

TSP 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 TSP za każdym razem upewnia się, że instalowany program ma właściwą wersję i jest wolny od jakichkolwiek nieautoryzowanych modyfikacji. TSP regularnie sprawdza integralność oprogramowania w swoim systemie wykorzystywanym do świadczenia usług.

Każdy moduł HSM używany przez TSP został zweryfikowany, przetestowany i oceniony. TSP weryfikuje integralność modułów:

a) po nabyciu urządzeń w trakcie odbioru,
b) bezpośrednio przed pierwszym użyciem,
c) regularnie podczas pracy.

TSP usuwa klucze dostawcy z modułu HSM trwale lub czasowo wycofanego z użycia.

TSP przechowuje nieużywane moduły HSM w fizycznie chronionym miejscu.

### 6.6.3. Kontrola cyklu życia zabezpieczeń

TSP zapewnia ochronę używanych modułów HSM w trakcie całego cyklu ich życia.

Podczas eksploatacji sprzętu i systemów informatycznych wykorzystywanych do świadczenia usług TSP 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

TSP przestrzega najlepszych praktyk branżowych w celu zapewnienia bezpieczeństwa sieci. Stosuje się do wymagań CA/B Forum's Network and Certificate System Security Requirements (42).

TSP utrzymuje konfigurację swojego systemu informatycznego pod ścisłą kontrolą i dokumentuje każdą zmianę, w tym nawet najmniejszą modyfikację, ulepszenie i aktualizację oprogramowania. TSP stosuje odpowiednie procedury do wykrywania wszelkich zmian sprzętu lub oprogramowania, do instalacji systemu oraz konserwacji systemu informatycznego. TSP sprawdza autentyczność i integralność każdego komponentu oprogramowania przy pierwszej instalacji.

TSP 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.

TSP 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.

TSP sprawdza konfigurację urządzeń sieci lokalnej (np. routerów) na zgodność z wymaganiami określonymi przez TSP co najmniej raz na trzy miesiące.

Po dokonaniu wszelkich istotnych zmian w systemie IT i przynajmniej co rok, TSP 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 logów i innych plików elektronicznych, podlegających archiwizacji, TSP stosuje kwalifikowane elektroniczne znaczniki czasu wydane przez EuroCert QTSA.

## 7. Profile certyfikatu, CRL i OCSP

### 7.1. Profil certyfikatu

Certyfikaty użytkowników końcowych wystawione przez TSP oraz wszystkie certyfikaty główne i pośrednie dostawcy, które znajdują się w ścieżce certyfikacyjnej używanej do wystawiania certyfikatów, są zgodne z następującymi zaleceniami i wymaganiami:

- ITU X.509 Information technology - Open Systems Interconnection - The Directory: Public- key and attribute certificate frameworks (39);
- IETF RFC 3739 (43)
- IETF RFC 5280 (17);
- IETF RFC 6818 (18);
- IETF RFC 6962 (44);
- ETSI EN 319 412-1 (23);
- ETSI EN 319 412-2 (45) w przypadku certyfikatów wydanych osobom fizycznym;
- ETSI EN 319 412-3 (46) w przypadku certyfikatów wydanych osobom prawnym;

- ETSI EN 319 412-4 (47) w przypadku certyfikatów uwierzytelniania witryn;
- ETSI EN 319 412-5 (48);
- ETSI TS 119 411-6 (49);
- CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates (3);
- Guidelines for the Issuance and Management of Extended Validation Certificates (4);
- CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates (11).

### 7.1.1. Numery wersji

Certyfikaty głównej i pośredniej jednostki certyfikacyjnej używane przez TSP oraz Certyfikaty użytkowników końcowych wydane przez TSP są certyfikatami w wersji "v3" zgodnie ze specyfikacją X.509 (39).

Certyfikaty mają następujące podstawowe pola:

- Wersja (Version)

Certyfikat jest zgodny z wersją "v3" zgodnie ze specyfikacją X.509, więc w tym polu znajduje się wartość "2" (17).

- Numer seryjny (Serial Number)

Unikalny identyfikator wygenerowany przez jednostkę certyfikacyjną wystawiającą certyfikat.

W przypadku certyfikatów użytkownika końcowego pole "Numer seryjny" zawiera losową liczbę, z entropią na poziomie co najmniej 8 bajtów (64 bit), wygenerowaną przez HSM zgodny z CSPRNG.

- Algorytm podpisu (Algorithm Identifier)

Identyfikator (OID) zestawu algorytmów kryptograficznych używanych do składania pieczęci elektronicznej poświadczającej certyfikat.

TSP 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)

- Podpis (Signature)

Pieczęć elektroniczna stworzona przez TSP poświadczająca certyfikat, która została utworzona za pomocą zestawu algorytmów zdefiniowanych w polu "Algorytm podpisu".

- Wystawca (Issuer)

Unikalna nazwa jednostki certyfikacyjnej wystawiającej certyfikat zgodnie z formatem nazwy ITU X.501 (patrz 3.1).

- 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 (możliwe tylko dla certyfikatów TLS).

TSP nigdy nie antydatuje certyfikatów.

Czas jest rejestrowany zgodnie z UTC i jest zgodny z kodowaniem IETF RFC 5280 (17).

- Podmiot (Subject)

Unikalna nazwa podmiotu zgodnie z formatem nazwy ITU X.501 (patrz 3.1). Zawsze wypełniane.

- Identyfikator algorytmu klucza publicznego podmiotu (Subject Public Key Algorithm Identifier)

TSP obsługuje algorytmy RSA i ECC w certyfikatach użytkowników końcowych.

Wartość, która ma być podana w tym polu:

   - "rsaEncryption" (1.2.840.113549.1.1.1)
   - "ecPublicKey" (1.2.840.10045.2.1)

- Wartość klucza publicznego podmiotu (Subject Public Key Value)

Klucz publiczny podmiotu.

- Unikalny identyfikator wystawcy (Issuer Unique Identifier)

Nie wypełniane.

- Unikalny identyfikator podmiotu (Subject Unique Identifier)

Nie wypełniane.

### 7.1.2. Zawartość certyfikatu i rozszerzenia

TSP korzysta wyłącznie z następujących rozszerzeń certyfikatów zgodnie ze specyfikacją X.509 (39):

**Certyfikat jednostki certyfikującej root**

- Polityki certyfikacji (Certificate Policies) – niekrytyczne
  OID: 2.5.29.32

To pole nie występuje.

- 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.

- 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.

Zawsze wypełnione.

- Alternatywne nazwy podmiotu – niekrytyczne
  OID: 2.5.29.17

Wypełnienie jest opcjonalne.

Wypełnia się zgodnie z sekcją 3.1.1.

- 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.

- Użycie klucza – krytyczne
  OID: 2.5.29.15

Określenie dozwolonego zakresu użycia klucza. Pole jest obowiązkowe, a używane wartości to:

  - "keyCertSign",
  - "cRLSign".

- 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**

- 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 TSP, 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".

- 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.

- 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.

Zawsze wypełnione.

- Alternatywne nazwy podmiotu – niekrytyczne
  OID: 2.5.29.17

Wypełnienie jest opcjonalne. Wypełnia się go zgodnie z sekcją 3.1.1.

- 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.

- Użycie klucza – krytyczne
  OID: 2.5.29.15

Określenie dozwolonego zakresu użycia klucza.

Pole zawiera następujące wartości:

- "keyCertSign",
- "cRLSign".

- Rozszerzone użycie klucza – niekrytyczne
  OID: 2.5.29.37

Dodatkowy zakres użycia klucza.

Certyfikaty pośrednich jednostek certyfikacyjnych zawierają co najmniej jedną wartość w polu "Rozszerzone użycie klucza", jak opisano poniżej:

Certyfikat każdej pośredniej jednostki certyfikującej zawiera wszystkie wartości rozszerzonego użycia klucza, które są zawarte w wydanych certyfikatach użytkownika końcowego wydanych przez tę jednostkę certyfikującą zgodnie z tabelą 7.1.2.

Certyfikaty pośrednich jednostek certyfikacyjnych do wystawiania certyfikatów do podpisów elektronicznych (pieczęci) zawierają:

– Document Signing (1.3.6.1.4.1.311.10.3.12).

Certyfikaty pośrednich jednostek certyfikacyjnych do wystawiania certyfikatów Email (S/MIME) zawierają:

– Secure E-mail (1.3.6.1.5.5.7.3.4).

Certyfikaty pośrednich jednostek certyfikacyjnych do wystawiania certyfikatów do podpisywania kodu:

– Code Signing (1.3.6.1.5.5.7.3.3).

Certyfikaty pośrednich jednostek certyfikacyjnych do wystawiania certyfikatów uwierzytelniania witryn zawierają następujące wartości rozszerzonego użycia klucza:

– Uwierzytelnienie serwera (1.3.6.1.5.5.7.3.1);

– Uwierzytelnienie klienta (1.3.6.1.5.5.7.3.2).

- Punkty dystrybucji list CRL – niekrytyczne
  OID: 2.5.29.31

Pole zawiera dostępność list CRL za pośrednictwem protokołu http.

Zawsze wypełniane.

- Dostęp do informacji o urzędzie – niekrytyczne
  OID: 1.3.6.1.5.5.7.1.1

Określenie pozostałych usług związanych z korzystaniem z certyfikatu, świadczonych przez TSP.

Pole jest obowiązkowe i zawiera następujące dane:

- W celu szybkiej i rzetelnej weryfikacji aktualnego statusu unieważnienia certyfikatu, TSP świadczy usługę statusu certyfikatu online. Dostępność tej usługi jest wskazana tutaj.
- Aby ułatwić budowanie ścieżki certyfikacyjnej, TSP udostępnia ścieżkę dostępu poprzez protokół http do certyfikatu jednostki certyfikacyjnej wystawiającej certyfikat.

Powyższe pola są zawsze wypełniane. Nie ma innych rozszerzeń certyfikatów.

**Certyfikat użytkownika końcowego**

- 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, to pole zawiera następujące dane:

- identyfikator polityki certyfikacji (OID zgodnie z sekcją 1.2.1);
- dostępność KPC;
- ostrzeżenie tekstowe w języku angielskim i polskim[5], na podstawie którego można ustalić:
  - czy certyfikat należy do II lub III klasy certyfikacyjnej, czyli, czy przy rejestracji miało miejsce osobiste stawiennictwo,
  - czy podmiotem certyfikatu jest osoba fizyczna,
  - czy klucz prywatny związany z certyfikatem jest chroniony sprzętowym urządzeniem kryptograficznym,
  - okres archiwizacji danych związanych z certyfikatem.
- Identyfikator polityki certyfikacji określony w ETSI EN 319 411-1 (12), z którą certyfikat jest zgodny:
  - W przypadku certyfikatu LCP OID 0.4.0.2042.1.3,
  - W przypadku certyfikatu NCP OID 0.4.0.2042.1.1,
  - W przypadku certyfikatu NCP+ OID 0.4.0.2042.1.2,
  - W przypadku certyfikatu DVCP OID 0.4.0.2042.1.6,
  - W przypadku certyfikatu OVCP OID 0.4.0.2042.1.7,
  - W przypadku certyfikatu IVCP OID 0.4.0.2042.1.8,
  - W przypadku certyfikatu EVCP OID 0.4.0.2042.1.4.
- W przypadku certyfikatu do podpisywania kodu, polityka certyfikacyjna zdefiniowana przez CA/Browser Forum:
  - OID 2.23.140.1.4.1.
- W przypadku certyfikatu urzędu znacznika czasu używanego do podpisywania kodu, polityka certyfikacji zdefiniowana przez CA/Browser Forum:
  - OID 2.23.140.1.4.2.
- Polityka certyfikacyjna zdefiniowana przez CA/Browser Forum w następujący sposób:
  - W przypadku certyfikatu DVCP OID 2.23.140.1.2.1,
  - W przypadku certyfikatu OVCP OID 2.23.140.1.2.2,
  - W przypadku certyfikatu IVCP OID 2.23.140.1.2.3,
  - W przypadku certyfikatu EVCP 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 certyfikatów użytkowników końcowych należy wskazać co najmniej jedną politykę certyfikacyjną zgodnie z którą został wystawiony certyfikat. Co najmniej jeden identyfikator takiej

[5] Ta sama informacja jest również zawarta w formacie odczytywanym maszynowo w rozszerzeniu Qualified Certificate Statements również umieszczonym w certyfikacie.

polityki certyfikacji (OID) i związany z nią KPC (URL) są wskazywane w certyfikatach wydanych przez TSP.

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.

- 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.

- 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.

Zawsze wypełnione.

- Alternatywne nazwy podmiotu – niekrytyczne
  OID: 2.5.29.17

Zob. sekcja: 3.1.1.

- 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.

- Użycie klucza – krytyczne
  OID: 2.5.29.15

Wskazanie zakresu dozwolonego użycia klucza.

W przypadku różnego celu użycia certyfikatów, są ustawiane następujące bity użycia klucza (inna wartość nie jest obecna):

Tabela 7.1.2. Użycie klucza i rozszerzone użycie klucza

| Typ certyfikatu | Użycie klucza (krytyczne) | Rozszerzone użycie klucza |
|---|---|---|
| Authentication | digitalSignature, keyAgreement (ECC) | clientAuth (1.3.6.1.5.5.7.3.2) |

| | | |
|---|---|---|
| Cisco VPN client | digitalSignature, keyAgreement (ECC), keyEncipherment (RSA) | clientAuth (1.3.6.1.5.5.7.3.2), ipsecEndSystem (1.3.6.1.5.5.7.3.5), ipsecIntermediateSystem (1.3.6.1.5.5.8.2.2) |
| Email encryption (S/MIME) | keyAgreement (ECC), keyEncipherment (RSA) | emailProtection (1.3.6.1.5.5.7.3.4) |
| Email protection (S/MIME) | digitalSignature | emailProtection (1.3.6.1.5.5.7.3.4) |
| Code Signing | digitalSignature | codeSigning (1.3.6.1.5.5.7.3.3) |
| Encryption | keyAgreement (ECC), keyEncipherment (RSA) | Document Encryption (1.3.6.1.4.1.311.80.1) |
| SCEP server | digitalSignature, keyAgreement (ECC), keyEncipherment (RSA) | clientAuth (1.3.6.1.5.5.7.3.4) |
| Smartcardlogon | digitalSignature, keyAgreement (ECC), keyEncipherment (RSA) | clientAuth (1.3.6.1.5.5.7.3.2), smartcardLogon (1.3.6.1.4.1.311.20.2.2) |

W przypadku certyfikatów użytkownika końcowego do podpisu elektronicznego (pieczęci) pole jest obowiązkowe, a wartość jest ustawiona wyłącznie na następujące wartości:

- "digitalSignature";
- "nonRepudiation".

Dla certyfikatu do uwierzytelniania witryny internetowej dozwolone są wyłącznie następujące wartości:

- "digitalSignature" (obowiązkowe)
  oraz opcjonalne:
  "keyEncipherment" – w przypadku RSA
  "keyAgreement" – w przypadku ECC

Te same wartości użycia klucza są używane w certyfikatach uwierzytelniania serwera, takich jak serwer VPN CISCO, kontroler domeny lub certyfikatach uwierzytelniania serwera sieci VPN.

- Rozszerzone użycie klucza – niekrytyczne
  OID: 2.5.29.37

Dodatkowy zakres dozwolonego użycia klucza.

Dla certyfikatów użytkownika końcowego stosowane są wartości rozszerzonego użycia klucza z powyższej tabeli 7.1.2.

Obowiązkowe do wypełnienia.

Dla certyfikatów do podpisu lub pieczęci dopuszczalna jest wartość:

- "Document Signing (1.3.6.1.4.1.311.10.3.12)";

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)".

W certyfikatach uwierzytelniania serwera wskazane są następujące bity rozszerzonego użycia klucza:

| Typ certyfikatu | ExtKeyUsage |
|---|---|
| Cisco VPN Server | serverAuth (1.3.6.1.5.5.7.3.1),<br>ipsecEndSystem (1.3.6.1.5.5.7.3.5),<br>ipsecIntermediateSystem (1.3.6.1.5.5.8.2.2) |
| DomainController | clientAuth (1.3.6.1.5.5.7.3.2),<br>serverAuth (1.3.6.1.5.5.7.3.1) |
| RDP Gateway | serverAuth (1.3.6.1.5.5.7.3.1) |

- 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.

- Dostęp do informacji o urzędzie – niekrytyczne
  OID: 1.3.6.1.5.5.7.1.1

Określenie pozostałych usług związanych z korzystaniem z certyfikatu, świadczonych przez TSP.

W przypadku certyfikatu użytkownika końcowego pole zawiera następujące dane:

- W celu szybkiej i rzetelnej weryfikacji aktualnego statusu unieważnienia certyfikatu, TSP świadczy usługę statusu certyfikatu online, której dostępność jest wskazana w tym polu.
- Aby ułatwić budowanie ścieżki certyfikacyjnej, TSP udostępnia ścieżkę dostępu poprzez protokół http do certyfikatu jednostki certyfikacyjnej wystawiającej certyfikat.

TSP może podać w tym polu dane więcej niż jednej usługi i certyfikatu jednostki certyfikującej wystawiającej certyfikat.

- 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) (21) (OID: 0.4.0.19495.2). W takim wypadku w polu umieszcza się: rodzaj usług finansowych PSD2 podmiotu oraz nazwę i skrót organu nadzorczego nadzorującego usługi finansowe podmiotu.

W każdym innym przypadku pole nie występuje.

Dozwolone jest tylko użycie pola QCType.

Pole QCType może być wypełnione zgodnie z celem użycia (do podpisywania: "id-etsi-qct- esign", do pieczętowania: "id-etsi-qct- eseal", do uwierzytelniania witryn: “id-etsi-qct-web”).

Powyższe pola są zawsze wypełniane zgodnie z podanymi regułami.

Inne rozszerzenia certyfikatów nie są wypełniane.

**Certyfikat urzędu znacznika czasu**

- Polityki certyfikacji – niekrytyczne
  OID: 2.5.29.32

To pole zawiera identyfikator aktualnej polityki certyfikacyjnej (patrz sekcja 1.2.1) w momencie wystawiania i używania certyfikatu urzędu znacznika czasu oraz inne informacje na temat innych zastosowań certyfikatu.

Wypełnienie pola jest obowiązkowe i pole nie jest krytyczne.

Odniesienie do powiązanego KPC związanego z Polityką Certyfikacji można podać w tym polu.

- 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.

- 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.

- Alternatywne nazwy podmiotu– niekrytyczne
  OID: 2.5.29.17

Główny adres e-mail TSP może znajdować się w tym polu.

- 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.

- 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".

- 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".

- 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)".

- 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.

- 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 TSP. Obowiązkowe pole, zawiera następujące dane:

- W celu szybkiej i wiarygodnej weryfikacji aktualnego statusu unieważnienia certyfikatu, TSP świadczy usługę statusu certyfikatu online. Dostępność tej usługi jest wskazana tutaj.
- Aby ułatwić budowanie ścieżki certyfikacyjnej, TSP 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.

**Certyfikat wydane dla OCSP Responder**

- Polityki certyfikacji – niekrytyczne
  OID: 2.5.29.32

To pole zawiera identyfikator aktualnej polityki certyfikacyjnej (patrz sekcja 1.2.1) 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.

- 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.

- 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.

- Alternatywne nazwy podmiotu – niekrytyczne
  OID: 2.5.29.17

Nigdy niewypełniane

- 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.

- Użycie klucza – krytyczne
  OID: 2.5.29.15

Określenie dozwolonego zakresu użycia klucza.

W certyfikatach wystawionych dla OCSP Responder występują wyłącznie następujące wartości:

  - "digitalSignature".

- Okres użycia klucza prywatnego – niekrytyczne
  OID: 2.5.29.16

Określenia dopuszczalnego okresu użycia klucza prywatnego.

Nie wypełnia się.

- 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)".

- 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.

- 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, TSP udostępnia ścieżkę dostępu poprzez protokół http do certyfikatu jednostki certyfikacyjnej wystawiającej certyfikat;
- W celu szybkiej i wiarygodnej weryfikacji aktualnego statusu unieważnienia certyfikatu, TSP 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. TSP 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

TSP posługuje się nazwą wyróżniającą „DN” – złożoną z atrybutów zdefiniowanych w standardach: IETF RFC 5280 (17), ETSI EN 319 412-2 (45), ETSI EN 319 412-3 (46) i ETSI EN 319 412-4 (47) – 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

TSP nie stosuje ograniczeń nazwy z wykorzystaniem pola "nameConstraints".

### 7.1.6. Identyfikator polityki certyfikacyjnej

TSP 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

TSP 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

TSP wystawia listy unieważnionych certyfikatów w wersji "v2" zgodnie ze specyfikacją IETF RFC 5280 (17).

#### 7.2.2. Listy CRL i rozszerzenia wpisów list CRL

Listy unieważnionych certyfikatów wydane przez TSP 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 (17), 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 (17). W przypadku list CRL wystawionych przez TSP 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 (17).

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 (17).

Opcjonalne rozszerzenia list CRL (crlEntryExtensions), które mogą być używane przez TSP:

- 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 TSP:

- Wygasłe certyfikaty na liście CRL (expiredCertsOnCRL) – niekrytyczne OID: 2.5.29.60
  Wskazanie, zgodnie ze specyfikacją X.509, że TSP 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 TSP:

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 TSP poświadczająca listę unieważnionych certyfikatów. Dana jednostka certyfikująca poświadcza CRL za pomocą klucza używanego do podpisywania certyfikatów.

TSP nie jest zobowiązany do wypełniania rozszerzeń.

## 7.3. Profil OCSP

TSP świadczy usługę statusu certyfikatu online zgodnie ze standardem IETF RFC 6960 (30) oraz IETF RFC 8954 (50).

Odpowiedzi OCSP wystawione przez TSP zawierają następujące pola:

- Identyfikator algorytmu (signatureAlgorithm)

Identyfikator algorytmu kryptograficznego używanego do podpisywania odpowiedzi OCSP (OID). TSP 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)

- Podpis (Signature)

Podpis elektroniczny lub pieczęć elektroniczna TSP.

- Identyfikator OCSP Respondera (responderID)

Niepowtarzalny identyfikator OCSP Respondera, który wystawił odpowiedź OCSP.

- Data wprowadzenia (thisUpdate)

Data wejścia w życie odpowiedzi OCSP. Wartość UTC kodowana zgodnie z IETF RFC 5280 (17).

- Następna aktualizacja (nextUpdate)

Najpóźniejszy czas wydania następnej odpowiedzi OCSP. Wartość UTC kodowana zgodnie z IETF RFC 5280 (17). Opcjonalna wartość. W przypadku certyfikatów uwierzytelniania witryny - obowiązkowa, równa czasowi wystawienia + 12 godzin.

- Odpowiedź dotycząca statusu certyfikatu (SingleResponse)

Pole zawiera identyfikator certyfikatu (CertID) i status unieważnienia certyfikatu (CertStatus).

TSP wydaje pozytywną odpowiedź OCSP zgodnie z wymaganiami CABF BR. Odpowiedź zawiera wartość "good" tylko wtedy, gdy certyfikat znajduje się w Repozytorium Certyfikatów TSP, a jego status nie jest zawieszony ani unieważniony.

### 7.3.1. Numer wersji

TSP obsługuje żądania i odpowiedzi dotyczące statusu certyfikatu online zgodne z wersją "v1", zgodnie ze standardem IETF RFC 6960 (30). Domyślna wartość pola (Wersja) to "v1", zatem to pole nie jest uwzględniane w odpowiedzi OCSP.

### 7.3.2. Rozszerzenia OCSP

TSP może warunkowo umieścić następujące rozszerzenie OCSP:

- ArchiveCutoff – niekrytyczne

TSP może wskazać za pomocą standardowej notacji zgodnie ze specyfikacją IETF RFC 6960 (30), że zachowuje informacje o unieważnieniu po wygaśnięciu certyfikatu. (Patrz punkt 4.10).

TSP może opcjonalnie umieścić następujące rozszerzenie OCSP:

- 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 (51) i IETF RFC 5816 (52). Profil znacznika opisano w sekcji 6.8 Polityki Certyfikacji i Kodeksu Postępowania Certyfikacyjnego Kwalifikowanych Usług Zaufania.

# 8. Audyt zgodności i inne rodzaje oceny

Działalność TSP jest okresowo sprawdzana przez niezależnego audytora zewnętrznego. Podczas audytu sprawdza się, czy działalność TSP jest zgodna z następującymi dokumentami normatywnymi:

- 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);
- ETSI EN 319 401; Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers (53);
- ETSI EN 319 411-1; Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements (12);
- ETSI TR 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; (49);
- ETSI TS 119 461 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects (54).

Wynikiem kontroli jest poufny dokument dostępny tylko dla upoważnionych osób.

Certyfikat zgodności wydany zgodnie ze sprawozdaniem z oceny zgodności publikowany jest na stronie internetowej TSP.

Do świadczenia usług, TSP stosuje zweryfikowane i certyfikowane elementy (produkty podpisu elektronicznego, elementy systemu IT itd.).

TSP ocenił każdy z elementów systemu wykorzystywanych do świadczenia usług według klas bezpieczeństwa na podstawie swojego systemu oceny ryzyka. TSP prowadzi ewidencję elementów systemu oraz związanych z nimi klas bezpieczeństwa w ramach swojego systemu zarządzania ryzykiem.

Oprócz audytu zewnętrznego TSP 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

TSP przeprowadza raz do roku ocenę zgodności swojego systemu informatycznego świadczącego usługi.

TSP regularnie monitoruje swoje procesy wewnętrzne, których szczegóły określone są w PCKPC i regulacjach wewnętrznych. Co najmniej raz w roku przeprowadza kompleksowy audyt wewnętrzny w celu zweryfikowania adekwatności swoich działań.

TSP przeprowadza co kwartał wyrywkową kontrolę co najmniej 3% certyfikatów do podpisywania kodu i 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, działalność zewnętrznej jednostki certyfikującej jest kontrolowana raz do roku.

## 8.2. Kwalifikacje osoby dokonującej oceny

TSP regularnie przeprowadza audyty wewnętrzne za pomocą swoich pracowników, którzy pełnią rolę niezależnego audytora systemu.

Ocena zgodności z wymogami eIDAS i ETSI jest przeprowadzana przez organizację, która posiada kwalifikacje wydane przez krajową organizację akredytacyjną państwa członkowskiego UE.

## 8.3. Powiązania pomiędzy osobą dokonującą oceny a ocenianym podmiotem

Audyt zewnętrzny przeprowadza osoba, która:

- jest niezależna od właścicieli, kierownictwa i działalności ocenianego TSP;
- jest niezależna od ocenianej organizacji, tzn. ani ta osoba, ani jej najbliżsi krewni nie mają żadnych stosunków pracy lub stosunków handlowych, służbowych z TSP.
- wynagrodzenie nie jest uzależnione od wyników przeprowadzonego audytu.

## 8.4. Obszary podlegające ocenie

Przegląd obejmuje następujące obszary:

- zgodność z obowiązującymi przepisami prawa;
- zgodność z normami technicznymi;
- zgodność z Polityką Certyfikacji i KPC;
- adekwatność zastosowanych procesów;
- dokumentacja;
- bezpieczeństwo fizyczne;
- adekwatność personelu;
- Bezpieczeństwo IT;
- zgodność z zasadami ochrony danych osobowych.

Audyt obejmuje wszystkie aktywne pośrednie jednostki certyfikacji, które wydała wciąż jeszcze ważny certyfikat lub są zdolne do wystawienia certyfikatu.

Jeśli TSP wydał certyfikat podrzędny dla jednostki certyfikującej innej organizacji, wówczas wymienione obszary są również badane w tych organizacjach 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 oraz wyniki oceny. Rozbieżności ujawnione podczas oceny oraz terminy na ich poprawienie są odnotowywane w osobnym rozdziale raportu.

Na podstawie powagi wykrytych różnic i rozbieżności, niezależny audytor może:

- Zaproponować propozycje modyfikacji, które należy opcjonalnie uwzględnić;
- Wymienić odstępstwa, które należy obowiązkowo naprawić.

## 8.6. Przekazywanie informacji o wynikach

TSP publikuje podsumowanie raportu z oceny na swojej stronie internetowej: https://eurocert.pl

TSP nie publikuje szczegółowych wyników oceny, gdyż są one traktowane jako informacje poufne.

# 9. Pozostałe biznesowe i prawne kwestie

## 9.1. Opłaty

TSP publikuje informacje o opłatach i cenach na swojej stronie internetowej oraz udostępnia je w formie papierowej w swoim biurze obsługi klienta.

TSP może jednostronnie zmienić cennik. TSP 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

TSP udziela stronom ufającym bezpłatnego dostępu on-line do swojego repozytorium certyfikatów.

### 9.1.3. Opłaty za unieważnienie lub za dostęp do informacji o statusie

TSP 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

TSP 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

TSP 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

TSP posiada ubezpieczenie od odpowiedzialności cywilnej.

Polisa ubezpieczeniowa od odpowiedzialności cywilnej obejmuje następujące szkody wyrządzone przez TSP w związku ze świadczeniem usług:

- szkody spowodowane naruszeniem umowy o świadczenie usług na rzecz odbiorców usług zaufania;
- szkody wyrządzone poza umową odbiorcom usług zaufania lub osobom trzecim;
- szkody wyrządzone Organowi Nadzoru przez TSP, wynikające z zakończenia świadczenia usług zaufania;

- zgodnie z Rozporządzeniem eIDAS (1) paragraf 17, ustęp 4, lit. e, koszty jednostki przeprowadzającej ocenę zgodności na wniosek organu nadzoru.

Polisa ubezpieczeniowa od odpowiedzialności cywilnej wynosi 250 000 euro za każde zdarzenie (przy czym maks. 1 000 000 euro za wszystkie zdarzenia). Szkody powstałe z tego samego powodu stanowią pojedyncze zdarzenie ubezpieczeniowe.

Ubezpieczenie OC zapewnia pokrycie całej szkody poszkodowanego – do limitu ubezpieczenia – powstałej w wyniku szkodliwego działania TSP 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

TSP przetwarza dane klientów zgodnie z przepisami prawa. TSP 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 TSP ich danych osobowych (w sposób zgodny z przepisami o przetwarzaniu danych). Zgoda taka dotyczy przekazywania osobom trzecim informacji określonych prawem w przypadku zakończenia działalności TSP. Ponadto zgoda dotyczy przekazywania informacji podwykonawcom TSP – wyłącznie w celu realizacji zadań związanych ze świadczeniem usługi.

Wnioskodawcy w formularzu wniosku o certyfikat mogą wyrazić zgodę na ujawnienie certyfikatu.

TSP wykorzystuje dane klientów wyłącznie w celu świadczenia usług. TSP ujawnia dane podmiotów i reprezentowanych organizacji pojawiające się w certyfikacie wraz z certyfikatem.

TSP 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. TSP przechowuje dane, zgodnie z wymogami ustawowymi, przez określony czas. W trakcie przechowywania danych TSP 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.

TSP zapewnia poufność i integralność informacji niejawnych, podczas przekazywania danych klientów.

### 9.3.1. Zakres informacji poufnych

TSP 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 TSP uznaje w tym dokumencie ogólnie dane które nie należą do jawnych, takie jak:

- wszystkie dane klienta, z wyjątkiem tych, które kwalifikują się jako informacje niepoufne (patrz 9.3.2);
- oprócz danych klienta:
  - klucze prywatne i kody aktywacyjne,
  - wnioski o certyfikaty i umowy o świadczenie usług,
  - dane związane z transakcjami i dane dziennika logów,
  - regulacje wewnętrzne, niedostępne publicznie,
  - wszystkie dane, których publiczne ujawnienie miałoby niekorzystny wpływ na bezpieczeństwo usługi.

### 9.3.2. Informacje niepoufne

TSP uznaje za publiczne (jawne) wszystkie dane, które można uzyskać ze źródła publicznego lub na których ujawnienie subskrybent wyraził uprzednio pisemną zgodę.

TSP 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.

TSP 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

TSP jest odpowiedzialny za ochronę przetwarzanych danych poufnych.

TSP zobowiązuje swoich pracowników, podwykonawców i kontrahentów do ochrony wszystkich poufnych danych poprzez podpisanie oświadczenia o zachowaniu poufności lub w drodze umowy.

TSP przetwarza dane osobowe zgodnie z przepisami rozporządzenia RODO oraz ustawy o ochronie danych osobowych (55), i ujawnia je na podstawie przepisów prawa osobom/organizacjom tylko w następujących przypadkach:

- obowiązkowe przekazywanie informacji organowi nadzorczemu, organom władzy,
- udzielanie informacji w sporach cywilnych,
- ujawnienie na wniosek właściciela.

TSP 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, TSP – jeżeli spełnione są ustawowe kryteria udostępnienia danych – nieodpłatnie ujawnia informacje dotyczące tożsamości oraz informacje zweryfikowane przez TSP zgodnie z art. 15 ustawy o usługach zaufania (14) organom śledczym i krajowym służbom bezpieczeństwa.

TSP 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 TSP może przekazać informacje o tożsamości podmiotu oraz informacje zweryfikowane przez TSP, na podstawie przepisów prawa stronom postepowania, organom i instytucjom do tego upoważnionym.

TSP 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, TSP ujawnia osobom trzecim poufne informacje dotyczące klienta.

**Inne okoliczności powodujące ujawnienie informacji**

W przypadku zakończenia działalności TSP 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 (14).

## 9.4. Prywatność danych osobowych

TSP zapewnia ochronę danych osobowych, działalność i regulacje TSP są zgodne z wymogami ustawy o ochronie danych osobowych (55) i Rozporządzenia UE 2016/679 (GDPR) (56).

TSP zgodnie z wymaganiami prawnymi:

- przechowuje,
- 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.

TSP 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.

TSP 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

TSP posiada Politykę Prywatności i klauzule informacyjne, które zawierają szczegółowe przepisy dotyczące postępowania z danymi osobowymi.

Polityka prywatności jest publikowana na stronie internetowej TSP pod następującym adresem: https://eurocert.pl/

Klauzula informacyjna jest publikowana na stronie TSP: https://eurocert.pl/repozytorium/

### 9.4.2. Informacje traktowane jako prywatne

TSP 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

TSP może ujawnić publicznie dane Podmiotów zawarte w certyfikacie na podstawie pisemnej zgody Podmiotu lub osoby reprezentującej Podmiot.

TSP może wskazać w certyfikacie unikalny identyfikator dostawcy przypisany do Podmiotu.

#### 9.4.4. Odpowiedzialność za ochronę informacji prywatnych

TSP 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.

TSP 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

TSP ujawnia dane osobowe wskazane w certyfikacie wyłącznie na podstawie pisemnej zgody klienta.

TSP 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 TSP 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 TSP nie może naruszać żadnych praw własności intelektualnej osoby trzeciej.

Właścicielem klucza prywatnego i publicznego wydawanego przez TSP klientom jest subskrybent, a wyłącznym użytkownikiem jest wnioskodawca bez względu na nośnik fizyczny, który zawiera i chroni klucze.

Właścicielem certyfikatu wydanego przez TSP swoim klientom jest TSP, a jego wyłącznym użytkownikiem jest wnioskodawca.

TSP 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 TSP, która jest ujawniana zgodnie z zasadami w punktach 7.2. oraz 7.3.

Unikalny identyfikator przydzielony klientom przez TSP jest własnością TSP, który jest ujawniany w ramach certyfikatu przez TSP w Repozytorium Certyfikatów.

Klient jest uprawniony do użycia identyfikatora podanego w certyfikacie (który identyfikuje podmiot certyfikatu).

Niniejszy dokument jest wyłączną własnością TSP. 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 TSP 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 TSP opisana jest w niniejszym dokumencie oraz umowie o świadczenie usług z klientem i w załącznikach do tej umowy:

- TSP przyjmuje na siebie odpowiedzialność za potwierdzenie, że wnioskodawca miał prawo do używania lub sprawował kontrolę nad Nazwami Domen i adresami IP wymienionymi w certyfikacie;
- TSP ponosi odpowiedzialność za przestrzeganie procedur opisanych w obsługiwanych przez siebie Politykach Certyfikacyjnych;
- TSP ponosi odpowiedzialność za szkody wyrządzone podczas świadczenia usługi przez jego podwykonawców;
- TSP ponosi odpowiedzialność na zasadach odpowiedzialności za naruszenie umowy w Kodeksie cywilnym w stosunku do klientów będących z nim w stosunku umownym.
- TSP 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.
- TSP wypłaci Klientom odszkodowanie za udowodnione szkody, które wystąpią w zakresie jego odpowiedzialności, ograniczone do kwoty określonej w polisie i umowie (patrz punkt Ograniczenie Odpowiedzialności 9.8.).
- 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.

TSP nie jest odpowiedzialny za:

- Działania podmiotu związane z kluczem prywatnym;
- Działania podmiotu związane z urządzeniem do składania podpisu elektronicznego;
- Weryfikację i użycie certyfikatów przez strony ufające;
- Regulacje wydane przez strony ufające lub inne podmioty.

**Obowiązki Dostawcy Usług Zaufania**

Podstawowym obowiązkiem TSP 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 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 TSP określają sposób funkcjonowania organizacji certyfikującej. Certyfikaty urzędów certyfikacji wydane przez jednostki certyfikacji (dla członków personelu ds. rejestracji, dyżurujących itp.) są zarządzane zgodnie z przepisami regulacji operacyjnych. Niniejszy akapit zawiera jedynie postanowienia dotyczące kluczy publicznych 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 TSP przed użytkownikami końcowymi. Wykonuje następujące zadania:

- uczestniczy w sprzedaży usług;
- dokonuje rejestracji podmiotów;

- otrzymuje wnioski dotyczące certyfikatów (zawieszenie, unieważnienie, uchylenie zawieszenia, wymiana certyfikatu);
- otrzymuje i obsługuje zgłoszenia związane z modyfikacją danych;
- uczestniczy w publikacji statusu unieważnienia;
- udziela klientom i stronom ufającym niezbędnych informacji w związku z prowadzoną przez nich działalnością związaną z usługami świadczonymi przez TSP.

Urząd Rejestracji jest odpowiedzialny za:

- ustalenie tożsamości osobistej Aplikujących;
- ustalenie tożsamości osoby upoważnionej do reprezentowania Aplikujących;
- ustalenie tożsamości organizacyjnej reprezentowanych organizacji i za ustalenie prawa do reprezentacji osoby fizycznej działającej w imieniu organizacji, w tym potwierdzenie tożsamości tej osoby;
- autentyczność zarejestrowanych danych rejestracyjnych;
- udzielanie informacji osobom korzystających z usług o treści i dostępności PCKPC, a także warunkach korzystania z usługi przed zawarciem umowy o świadczenie usług;
- 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 umową i regulacjami TSP 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 kompromitacji klucza prywatnego związanego z kluczem publicznym zawartym w certyfikacie należącym do subskrybenta, jest on zobowiązany do:

- niezwłocznego zgłoszenia tego faktu TSP,
- niezwłocznego żądania unieważnienia lub zawieszenia certyfikatu,
- 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 adresem 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**

- Subskrybenci mają prawo do korzystania z usług zgodnie z niniejszym PCKPC.
- Subskrybenci są uprawnieni do określenia na piśmie, które podmioty powinny mieć możliwość otrzymania certyfikatów.
- Subskrybenci mają prawo zażądać zawieszenia i unieważnienia certyfikatów.
- Subskrybenci są uprawnieni do wyznaczania administratorów organizacyjnych.

**Odpowiedzialność wnioskodawcy**

Wnioskodawca jest odpowiedzialny za:

- uwierzytelnienie, poprawność i prawdziwość danych podanych podczas rejestracji;
- weryfikację danych wskazanych w certyfikacie;
- udzielanie natychmiastowej informacji o zmianach swoich danych oraz danych wskazanych w certyfikacie;
- korzystanie z urządzenia do składania podpisu elektronicznego (pieczęci), klucza prywatnego i certyfikatu zgodnie z regulacjami;
- bezpieczne zarządzanie kluczem prywatnym i kodem aktywacyjnym;
- bezpieczne zarządzanie urządzeniem do składania podpisu elektronicznego (pieczęci);
- natychmiastowe powiadomienie i pełne informowanie TSP w przypadkach spornych;
- ogólne wywiązywanie się ze swoich zobowiązań.

**Obowiązki wnioskodawcy**

Wnioskodawca powinien:

- przeczytać uważnie niniejszy dokument przed skorzystaniem z usług;
- podać wszystkie i wyłącznie prawdziwe dane wymagane przez TSP niezbędne do korzystania z usługi;
- 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 TSP na piśmie,
  - zażądać zawieszenia lub unieważnienia certyfikatu oraz
  - zakończyć korzystanie z certyfikatu;
- niezwłocznie zakończyć korzystanie z klucza prywatnego należącego do certyfikatu, jeżeli podmiot dowie się o tym, że jego certyfikat został unieważniony lub że wystawiający urząd certyfikacji został skompromitowany;
- korzystać z usługi wyłącznie w celach dozwolonych (lub nie zabronionych) przez przepisy prawa, zgodnie z określonymi regulacjami i dokumentami;
- zainstalować certyfikat uwierzytelniania witryny tylko na tym serwerze, który jest dostępny pod nazwą domeny lub adresem IP wskazanymi w certyfikacie;
- zapewnić, że żadne nieupoważnione osoby nie mają dostępu do danych i narzędzi (haseł, tajnych kodów, urządzeń do składania podpisów) niezbędnych do korzystania z usługi;
- niezwłocznie powiadomić TSP na piśmie w przypadku rozpoczęcia sporu prawnego w związku z jakimkolwiek podpisem elektronicznym (pieczęcią) lub certyfikatami związanymi z usługą;
- współpracować z TSP w celu walidacji danych niezbędnych do wydania certyfikatów oraz zrobić wszystko, co w ich mocy, aby umożliwić jak najszybsze zakończenie takiej weryfikacji;
- 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 TSP, a także do zainicjowania unieważnienia i/lub zawieszenia certyfikatów oraz zakończenia korzystania z certyfikatu;
- odpowiedzieć na żądania TSP w terminie określonym przez TSP w przypadku naruszenia bezpieczeństwa klucza (ujawnienia) lub podejrzenia nielegalnego użycia;

- przyjąć do wiadomości, że subskrybenci są uprawnieni do żądania unieważnienia i/lub zawieszenia certyfikatu;
- przyjąć do wiadomości, że TSP wydaje certyfikaty w sposób określony w PCKPC, po zakończeniu opisanych w nim etapów walidacji;
- przyjąć do wiadomości, że TSP umieszcza w certyfikatach tylko te dane, które odpowiadają rzeczywistości. W związku z tym TSP potwierdza dane, które mają być wprowadzone w Certyfikatach zgodnie z PCKPC;
- w przypadku wnioskowania o certyfikat organizacyjny, przyjąć do wiadomości, że TSP wyda certyfikat wyłącznie w przypadku zgody reprezentowanej organizacji;
- w przypadku wnioskowania o certyfikat organizacyjny, przyjąć do wiadomości, że reprezentowana organizacja ma prawo żądać unieważnienia certyfikatu;
- przyjąć do wiadomości i zaakceptować, że TSP 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;
  - TSP 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**

- Wnioskodawcy mają prawo ubiegać się o certyfikaty zgodnie z PCKPC.
- 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. Oświadczenia i gwarancje 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 TSP, 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 użycia 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 TSP.

**Prawa reprezentowanej organizacji**

- TSP wystawia certyfikaty, w których wskazana jest nazwa reprezentowanej organizacji, wyłącznie za jej zgodą.
- Reprezentowana organizacja jest uprawniona do zawieszenia i unieważnienia certyfikatów, w których wskazana została jej nazwa.

## 9.7. Wyłączenie odpowiedzialności z tytułu gwarancji

TSP wyłącza swoją odpowiedzialność, jeżeli:

- Wnioskodawcy nie przestrzegają wymogów związanych z zarządzaniem urządzeniem do składania podpisu elektronicznego (pieczęci) i kluczem prywatnym i danymi aktywacyjnymi;
- klient nie może uzyskać dostępu do Usługi Zdalnego Podpisu z powodu czynników za które nie odpowiada TSP;
- nie jest w stanie dostarczyć informacji lub wypełnić swoich innych obowiązków komunikacyjnych z powodu problemów z Internetem lub jego częścią;
- 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**

TSP nie ponosi odpowiedzialności za jakiekolwiek szkody, które wynikają z tego, że strona ufająca nie postępuje zgodnie z obowiązującymi przepisami prawa i regulacjami TSP w trakcie walidacji i korzystania z certyfikatów, oraz gdy strona ufająca nie postępuje zgodnie z wymaganiami w danej sytuacji.

TSP 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.

TSP 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 TSP przeprowadza porównanie danych z autentyczną bazą danych przed wydaniem certyfikatu, polega na danych otrzymanych z autentycznej bazy danych. TSP nie ponosi żadnej odpowiedzialności za szkody wynikające z niepoprawności informacji dostarczanych przez takie publiczne autoryzowane bazy danych.

TSP 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**

TSP 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**

TSP posiada depozyt zgodny z wymogami prawnymi na pokrycie swojej odpowiedzialności finansowej i kosztów jej rozwiązania.

TSP posiada ubezpieczenie od odpowiedzialności cywilnej zgodnie z wymaganymi przepisami prawa w celu zapewnienia swojej wiarygodności.

**Ograniczenie odpowiedzialności finansowej**

TSP 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. Odszkodowanie ze strony Dostawcy Usług

Szczegółowe zasady odpowiedzialności odszkodowawczej TSP 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 i straty poniesione przez TSP spowodowane nieprzestrzeganiem przez Subskrybenta jego obowiązków i odpowiednich zaleceń.

### 9.9.3. Odszkodowanie ze strony stron ufających

Zob. sekcja: 9.8.

## 9.10. Obowiązywanie 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 TSP wydał w trakcie obowiązywania PCKPC.

### 9.10.3. Skutki wygaśnięcia

W przypadku odstąpienia od PCKPC, TSP publikuje na swojej stronie internetowej szczegółowe zasady odstąpienia oraz prawa i obowiązki utrzymujące się po odstąpieniu.

TSP gwarantuje, że nawet w przypadku uchylenia PCKPC, przepisy dotyczące ochrony poufnych danych pozostają w mocy.

## 9.11. Indywidualne powiadomienia i komunikacja z klientami

TSP posiada biuro obsługi klienta w celu utrzymywania kontaktu ze swoimi klientami.

Klienci mogą składać TSP 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.

TSP utrzymuje komunikację ze swoimi klientami poprzez swoją stronę internetową lub pocztę elektroniczną.

## 9.12. Zmiany

TSP zastrzega sobie prawo do zmiany niniejszego dokumentu w przypadku zmiany zasad normatywnych, wymogów bezpieczeństwa, warunków rynkowych lub innych okoliczności.

### 9.12.1. Procedura wprowadzania zmian

TSP ujawnia w swoich regulacjach publicznych wyłącznie te procedury, których znajomość nie zagraża bezpieczeństwu usług. TSP 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 TSP. TSP 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 TSP Metodyką Zatwierdzania Regulacji.

TSP publikuje zatwierdzony PCKPC na swojej stronie internetowej co najmniej 14 dni przed planowanym wejściem w życie.

### 9.12.2. Mechanizm i termin powiadamiania

TSP powiadamia strony ufające o wydaniu nowych wersji dokumentu zgodnie z opisem w sekcji 9.12.1.

### 9.12.3. Okoliczności zmiany OID

TSP wydaje nową wersję z nowym numer wersji w przypadku każdej zmiany PCKPC. Nie wpływa to na zmianę OID dokumentu.

## 9.13. Rozwiązywanie sporów

TSP dąży do polubownego rozstrzygnięcia w drodze negocjacji powstałych sporów w związku z usługami.

TSP 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 TSP lub z korzystaniem z wydanych certyfikatów należy kierować do Centralnego Biura Obsługi Klienta w formie pisemnej.

W ciągu 3 dni roboczych od otrzymania zgłoszenia, TSP poinformuje stronę zgłaszającą na podany przez nią adres o otrzymaniu zgłoszenia i czasie potrzebnym na jego rozpatrzenie. TSP jest zobowiązany do udzielenia pisemnej odpowiedzi zgłaszającemu w wyznaczonym terminie.

TSP może zażądać od podmiotu podania informacji niezbędnych do udzielenia odpowiedzi podmiotowi. TSP 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 TSP oraz ze stronami zainteresowanymi.

Wszyscy uczestnicy takich konsultacji otrzymują pisemne powiadomienie o terminie konsultacji z 10-dniowym wyprzedzeniem. Zgłoszenie, odpowiedź TSP, 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 TSP.

## 9.14. Obowiązujące prawo

TSP przez cały czas działa zgodnie z obowiązującymi przepisami prawa polskiego. Prawo polskie jest prawem właściwym dla umów, regulacji i ich egzekwowania.

## 9.15. Zgodność z obowiązującym prawem

Obowiązujące przepisy:

- Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 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);
- 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;
- Ustawa o ochronie danych osobowych z dn. 10 maja 2018 r. (55);
- Kodeks cywilny z 23 kwietnia 1964 (57);
- Ustawa o usługach zaufania (14).

## 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 TSP.

### 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 (11), TSP powiadamia CAB Forum o faktach, okolicznościach i przepisach prawa przed wydaniem certyfikatów S/MIME.

W przypadku konfliktu między przepisami krajowymi lub Unii Europejskiej a obowiązkowymi wymogami CABF BR (3) lub CABF EV Guidelines (4), TSP powiadamia CAB Forum o faktach, okolicznościach i przepisach prawa przed wydaniem certyfikatów S/MIME.

#### 9.16.4. Egzekucja (opłaty adwokackie i zrzeczenie się praw)

TSP może dochodzić odszkodowania i zwrot kosztów obsługi prawnej w celu zrekompensowania szkód, strat, kosztów spowodowanych przez jego partnerów. Jeżeli w konkretnej sprawie TSP 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

TSP 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 TSP.

### 9.17. Inne postanowienia

Nie ustalono.

# A Interpretacja skrótów nazw polityk certyfikacji

W celu łatwiejszego zapanowania nad Politykami Certyfikacyjnymi, TSP 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.** ***IETF RFC 3647: Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework, November 2003.***

**3.** ***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/.***

**4.** ***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/.***

**5.** ***Common Criteria for Information Technology Security Evaluation, Part 1 - 3.***

**6.** ***CEN CWA 14169: Secure signature-creation devices "EAL 4+", March 2004.***

**7.** ***CEN 419 221-5; Protection Profiles for TSP Cryptographic Modules - Part 5: Cryptographic Module for Trust Services.***

**8.** ***FIPS PUB 140-2 (2001 May 25): Security Requirements for Cryptographic Modules.***

**9.** ***FIPS PUB 140-3 (2019 March 22): Security Requirements for Cryptographic Modules.***

**10.** ***CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates, v.3.7.0., https://cabforum.org/working-groups/code-signing/documents/.***

**11.** ***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/.***

**12.** ***ETSI EN 319 411-1; Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.***

**13.** ***USTAWA z dnia 18 września 2001 r. o podpisie elektronicznym (uchylony z dniem 1 lipca 2016 r. wraz z wejściem eIDAS).***

**14.** ***Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej.***

**15.** ***Regulamin Usług Zaufania EuroCert; https://eurocert.pl/repozytorium/Zasady_i_warunki_swiadczenia_uslug/aktualne/.***

**16.** ***ITU X.520 Information technology - Open Systems Interconnection - The Directory: Selected attribute types.***

**17.** ***IETF RFC 5280: Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile, May 2008.***

**18.** ***IETF RFC 6818: Updates to the Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile, January 2013.***

**19.** ***IETF RFC 3986: Uniform Resource Identifier (URI): Generic Syntax, January 2005.***

**20.** ***IETF RFC 5952: A Recommendation for IPv6 Address Text Representation, August 2010.***

**21.** ***DIRECTIVE (EU) 2015/2366 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2015 on payment services in the internal market.***

**22.** ***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.***

**23.** ***ETSI EN 319 412-1; Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures.***

**24.** ***ISO 3166-1:2013, Codes for the representation of names of countries and their subdivisions - Part 1: Country codes.***

**25.** ***IETF RFC 3490: Internationalizing Domain Names in Applications (IDNA), March 2003.***

**26.** ***IETF RFC 8659: DNS Certification Authority Authorization (CAA) Resource Record, November 2019.***

**27.** ***IETF RFC 6532: Internationalized Email Headers, February 2012.***

**28.** ***IETF RFC 3966: The tel URI for Telephone Numbers, December 2004.***

**29.** ***PRADO - Public Register of Authentic identity and travel Documents Online, https://www.consilium.europa.eu/prado/en/prado-start-page.html.***

**30.** ***IETF RFC 6960: X.509 Internet Public Key Infrastructure - Online Certificate Status Protocol (OCSP), June 2013.***

**31.** ***IETF RFC 5019: The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environment, September 2007.***

**32.** ***IETF RFC 5755: An Internet Attribute Certificate Profile for Authorization, January 2010.***

**33.** ***ETSI TS 119 312; Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.***

**34.** ***ISO/IEC 19790:2012: Information technology – Security techniques – Security requirements for cryptographic modules.***

**35.** ***ISO/IEC 15408-2002, Information Technology - Methods and Means of a Security - Evaluation Criteria for IT Security.***

**36.** ***https://www.nccert.pl.***

**37.** ***EU Trusted Lists of Certification Service Providers, https://eidas.ec.europa.eu/efda/tl-browser/#/screen/home.***

**38.** ***NIST Special Publication 800-56A Revision 3 (April 2018): Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography.***

**39.** ***ITU X.509 Information technology - Open Systems Interconnection - The Directory: Public- key and attribute certificate frameworks.***

**40.** ***CEN EN 419 241-1:2018 (July 2018); Trustworthy Systems Supporting Server Signing – Part 1: General System Security Requirements.***

**41.** ***European Commission eIDAS Dashboard, Qualified Signature/Seal Creation Devices and Secure Signature Creation Devices, https://eidas.ec.europa.eu/efda/browse/notification/qscd-sscd.***

**42.** ***CA/Browser Forum Network and Certificate System Security Requirements, v.1.7., https://cabforum.org/working-groups/netsec/documents/.***

**43.** ***IETF RFC 3739: Internet X.509 Public Key Infrastructure - Qualified Certificates Profile, MARCH 2004.***

**44.** ***IETF RFC 6962: Certificate Transparency, June 2013.***

**45.** ***ETSI EN 319 412-2; Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons.***

**46.** ***ETSI EN 319 412-3; Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons.***

**47.** ***ETSI EN 319 412-4; Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates.***

**48.** ***ETSI EN 319 412-5; Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements.***

**49.** ***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.***

**50.** ***IETF RFC 8954: Online Certificate Status Protocol (OCSP) Nonce Extension, November 2020.***

**51.** ***IETF RFC 3161: Internet X.509 Public Key Infrastructure - Time-Stamp Protocol (TSP), August 2001.***

**52.** ***IETF RFC 5816: ESSCertIDv2 Update for RFC 3161, April 2010.***

**53.** ***ETSI EN 319 401; Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.***

**54.** ***ETSI TS 119 461; Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects.***

**55.** ***Ustawa o ochronie danych osobowych z dn. 10 maja 2018 r.***

**56.** ***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.***

**57.** ***Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny.***