Polityka świadczenia usługi i deklaracja praktyk w zakresie wydawania niekwalifikowanych elektronicznych poświadczeń atrybutów EuroCert

Wersja 1.0

Data wejścia w życie: 23.10.2026

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

Metryczka regulacji

Informacje ogólne		
Sygnatura		1-PT-057-01
Status		Zatwierdzona
Zatwierdzony przez		Łukasz Konikiewicz
Data zatwierdzenia		23.10.2026
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
23.10.2026 r.	1	Wersja inicjalna.

Spis treści

1. Wstęp *7*

1.1. Wprowadzenie **7**

1.2. Identyfikator i nazwa dokumentu **7**

1.2.1. Identyfikatory polityk 7

1.3. Definicje i uczestnicy usługi **8**

1.4. Ogólne postanowienia dotyczące usługi **9**

1.5. Zarządzanie Polityką **9**

1.5.1. Organizacja zarządzająca dokumentem 9

1.5.2. Osoba do kontaktu 9

1.5.3. Osoba lub organizacja odpowiedzialna za zgodność 9

1.5.4. Procedury zatwierdzania polityki 10

2. Obowiązki związane z publikowaniem i repozytorium *10*

2.1. Repozytorium **10**

2.2. Kontrole dostępu do Repozytorium **10**

3. Identyfikacja i uwierzytelnianie *10*

3.1 Nadawanie nazw **10**

3.1.1 Typy nazw 10

3.1.2 Konieczność używania nazw znaczących 11

3.1.3 Prywatność danych 11

3.1.4 Zasady interpretacji różnych form nazw 11

3.2. Metody potwierdzenia tożsamości 11

3.3. Reprezentacja i działanie w imieniu innego podmiotu **12**

3.4. Powiązanie z portfelem i kontrola kryptograficzna **12**

3.5. Identyfikacja i uwierzytelnianie żądań unieważnienia **12**

4. Wymagania operacyjne dotyczące cyklu życia EAA *12*

4.1. Wniosek o wydanie EAA **12**

4.2. Przetwarzanie wniosku **12**

4.3. Pozyskiwanie i walidacja atrybutów **12**

4.4. Wydanie EAA **12**

4.5. Dostarczenie EAA **12**

4.6. Weryfikacja EAA **13**

4.7. Ponowne wydanie **13**

4.8. Unieważnienie EAA **13**

4.9. Usługa statusowa **13**

4.10. Zakończenie korzystania z EAA 13

5. Zabezpieczenia fizyczne, organizacyjne i operacyjne 13

5.1. Fizyczne środki kontroli 13
5.1.1. Lokalizacja i wymogi budowlane systemu 14
5.1.2. Dostęp fizyczny 14
5.1.3. Zasilanie i systemy chłodzące 14
5.1.4. Narażenie na wilgoć i zalanie 15
5.1.5. Ochrona przed pożarem 15
5.1.6. Przechowywanie nośników danych 15
5.1.7. Utylizacja odpadów 15
5.1.8. Kopia zapasowa poza siedzibą główną 16

5.2. Organizacyjne środki kontroli 16
5.2.1. Role Zaufane 16
5.2.2. Minimalny skład osobowy 17
5.2.3. Identyfikacja i uwierzytelnienie każdej z ról 17
5.2.4. Role wymagające oddzielnych obowiązków 18

5.3. Kontrole personelu 18
5.3.1. Kwalifikacje, doświadczenie i zezwolenia 18
5.3.2. Procedury sprawdzania kandydatów 18
5.3.3. Szkolenia 19
5.3.4. Częstotliwość szkoleń przypominających 19
5.3.5. Rotacja obowiązków służbowych 19
5.3.6. Kary za nieuprawnione działania 19
5.3.7. Wymagania dotyczące niezależnego wykonawcy 20
5.3.8. Dokumentacja dostarczona personelowi 20

5.4. Rejestrowanie zdarzeń 20
5.4.1. Rodzaje zapisywanych zdarzeń 20
5.4.2. Częstotliwość przetwarzania logów audytowych 22
5.4.3. Okres przechowywania logów 23
5.4.4. Ochrona logów 23
5.4.5. Procedury tworzenia kopii zapasowej dziennika zdarzeń 23
5.4.6. System zbierania logów (wewnętrzny/zewnętrzny) 23
5.4.7. Powiadomienie podmiotu powodującego zdarzenie 23
5.4.8. Ocena podatności 24

5.5. Archiwizacja zapisów 24
5.5.1. Typy archiwizowanych zapisów 24
5.5.2. Okres utrzymywania archiwum 24
5.5.3. Ochrona archiwum 24
5.5.5. Wymagania dotyczące znakowania czasem zapisów 25
5.5.6. System archiwizacji (wewnętrzny lub zewnętrzny) 25
5.5.7. Procedury uzyskania i weryfikacji dokumentacji w archiwum 25

5.6. Zmiana klucza wystawcy EAA 25
5.7. Środki naprawcze w przypadku kompromitacji i wypadków losowych 25
5.7.1. Procedury postępowania z incydentami i kompromitacją 25
5.7.2. Uszkodzenie zasobów obliczeniowych, oprogramowania i/lub danych 26
5.7.3. Kompromitacja klucza wystawcy EAA lub list statusowych 26

5.7.4. Zachowanie ciągłości działań po wydarzeniu losowym 26
5.8. Zakończenie Usługi EAA 27
6. Techniczne środki bezpieczeństwa 27
6.1. Generowanie i przeznaczenie kluczy 27
6.2. Ochrona i cykl życia kluczy prywatnych 28
6.3. Certyfikaty i okresy użycia 28
6.4. Dane aktywacyjne 28
6.5. Środki kontroli bezpieczeństwa komputerowego 28
6.5.1. Szczególne wymagania techniczne dotyczące bezpieczeństwa komputerowego 28
6.5.2. Ocena bezpieczeństwa komputerowego 28
6.6. Techniczne kontrole cyklu życia 29
6.6.1. Kontrola rozwoju systemu 29
6.6.2. Kontrola zarządzania bezpieczeństwem 29
6.6.3. Kontrola cyklu życia zabezpieczeń 30
6.7. Kontrola bezpieczeństwa sieci 30
6.8. Znakowanie czasem 31
7. Profile techniczne EAA i informacje o statusie 31
7.1. Profil certyfikatu wydawcy EAA 31
7.2 Format EAA 31
7.3. Profil listy statusowej 31
7.4. Publikacja i dostępność Token Status List 31
8. Audyt zgodności i inne rodzaje oceny 32
8.1. Częstotliwość i okoliczności oceny 32
8.2. Kwalifikacje osoby dokonującej oceny 32
8.3. Powiązania pomiędzy osobą dokonującą oceny a ocenianym podmiotem 32
8.4. Obszary podlegające ocenie 32
8.5. Czynności podjęte w wyniku stwierdzenia nieprawidłowości 32
8.6. Przekazywanie informacji o wynikach 33
9. Inne postanowienia biznesowe i prawne 33
9.1. Zobowiązania uczestników 33
9.1.1. Obowiązki TSP 33
9.1.2. Obowiązki źródła danych 33
9.1.3. Obowiązki Subskrybenta oraz Posiadacza EAA 33
9.1.4. Obowiązki strony ufającej 33
9.2. Odpowiedzialność TSP 33
9.3. Prywatność i ochrona danych 34

9.4. Reklamacje i spory 34

9.5. Zmiany 35

9.5.1. Procedura wprowadzania zmian 35

9.6. Prawo właściwe 35

9.7. Zgodność z obowiązującym prawem 35

Bibliografia*..... *36

1. Wstęp

Niniejszy dokument określa zasady świadczenia przez EuroCert Sp. z o.o. niekwalifikowanej usługi zaufania polegającej na wydawaniu elektronicznych poświadczeń atrybutów (usługa EAA).

Dokument obejmuje deklarację dostawcy usługi zaufania w zakresie stosowania zabezpieczeń organizacyjnych, operacyjnych i technicznych dotyczących wydawania poświadczeń atrybutów.

1.1. Wprowadzenie

Niniejsza Polityka określa wymagania i zasady dla Usługi EAA. Każde EAA jest wydawane zgodnie z właściwą polityką poświadczenia atrybutów (polityka EAAP) utrzymywaną przez TSP.

Polityka poświadczenia atrybutów określa szczegółowe zasady mające zastosowanie do danego rodzaju wydawanego elektronicznego poświadczenia atrybutów, w szczególności w zakresie: zestawu i semantyki poświadczanych atrybutów, źródeł danych, wymaganego poziomu ich weryfikacji, wymagań dotyczących identyfikacji i uwierzytelniania, okresu ważności poświadczenia, sposobu jego dostarczenia, powiązania z portfelem, przesłanek unieważnienia, mechanizmu weryfikacji statusu oraz stosowanego profilu technicznego.

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

1.2. Identyfikator i nazwa dokumentu

Główne dane identyfikacyjne Polityki stanowią:

Wydawca	EuroCert Sp. z o.o.
Nazwa dokumentu	Polityka świadczenia usługi i deklaracja praktyk w zakresie wydawania niekwalifikowanych elektronicznych poświadczeń atrybutów EuroCert
OID	1.2.616.1.113791.2.1.1.22
Wersja dokumentu	1.0
Data obowiązywania	23.10.2026

Identyfikatory Polityk EAAP są przypisywane według zasad w sekcji 1.2.1.

1.2.1. Identyfikatory polityk

Wszystkie EAA wydane przez TSP odnoszą się do tej Polityki EAAP, na podstawie której zostały wydane. Pierwsze pięć liczb OID, które identyfikują niniejszy dokument stanowi unikalny identyfikator EuroCert:

(1)	International Organization for Standardization (ISO)
(2)	ISO Member Bodies
(616)	Poland
(1)	Organizations

(113791)	EuroCert Sp. z o.o.
(2)	Usługi niekwalifikowane
(1)	Dokumenty
(1)	Publiczne dokumenty
(x)	Unikalny identyfikator Polityki EAAP

1.3. Definicje i uczestnicy usługi

Atrybut - cecha charakterystyczna, właściwość, prawo lub zezwolenie lub inna informacja odnosząca się do osoby fizycznej, osoby prawnej lub innego podmiotu/obiektu.

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).

Elektroniczne poświadczenie atrybutów (EAA) - poświadczenie w postaci elektronicznej, które umożliwia uwierzytelnienie i weryfikację atrybutów zgodnie z rozporządzeniem eIDAS.

TSP / EuroCert - EuroCert Sp. z o.o. jako dostawca niekwalifikowanej Usługi EAA.

Polityka - niniejsza Polityka usługi zaufania dla niekwalifikowanej usługi wydawania elektronicznych poświadczeń atrybutów świadczonej przez Eurocert Sp. z o.o., definiująca zasady i środki mające zastosowanie do Usługi Zaufania.

Polityka poświadczenia atrybutów (polityka EAAP lub EAAP) - zbiór reguł mających zastosowanie do co najmniej jednego typu elektronicznego poświadczenia atrybutów.

Podmiot Atrybutu - osoba lub inny podmiot, którego dotyczą atrybuty zawarte w EAA.

Subskrybent - osoba fizyczna, osoba prawna lub fizyczna związana z TSP regulaminem lub umową w zakresie wnioskowania o Usługę EAA lub korzystania z niej.

Posiadacz EAA - podmiot, któremu EAA jest dostarczane do portfela albo poza portfel; może być tożsamy z Podmiotem Atrybutu.

Źródło danych - źródło, z którego TSP pozyskuje dane wykorzystywane do wydania EAA, w tym źródło autentyczne, źródło prywatne, inne zaakceptowane źródło lub – jeżeli EAAP na to pozwala – dane samodeklarowane przez Podmiot Atrybutu.

Portfel - rozwiązanie technologiczne umożliwiające przechowywanie i prezentację EAA.

Jednostka portfela - oznacza unikalną konfigurację rozwiązania portfelowego, która w szczególności obejmuje aplikację zainstalowaną i skonfigurowaną na urządzeniu lub w środowisku użytkownika portfela.

Lista statusowa - mechanizm udostępniony przez TSP do komunikowania statusu poświadczenia poprzez publikowanie informacji o statusie, czy poświadczania jest ważne lub unieważnione.

Strona Ufająca - osoba fizyczna lub prawna, która polega na identyfikacji elektronicznej lub usłudze zaufania.

Usługa Zaufania (lub Usługa EAA) - niekwalifikowana usługa zaufania świadczona przez Eurocert polegająca na wydawaniu elektronicznych poświadczeń atrybutów.

Regulamin - Regulamin usługi wydawania elektronicznych poświadczeń atrybutów.

1.4. Ogólne postanowienia dotyczące usługi

Usługa EAA jest świadczona jako niekwalifikowana usługa zaufania na podstawie niniejszej polityki oraz regulaminu usługi dostępnego na stronie TSP: https://eurocert.pl/category/dokumenty-pl/.

Każde EAA wskazuje TSP jako wydawcę elektronicznego poświadczenia atrybutu oraz właściwą politykę EAAP umożliwiającą jego interpretację i weryfikację.

TSP wdraża zewnętrzne zasady i schematy EAA w ramach usługi jako EAAP.

TSP może również definiować wewnętrzne zasady i schematy jako EAAP.

Wdrożenie nowego EAAP wymaga zatwierdzenia zgodnie z wewnętrznym procesem zatwierdzenia.

Strona Ufająca przed poleganiem na EAA powinna zweryfikować jego integralność, autentyczność, okres ważności, status oraz ograniczenia wynikające z właściwego EAAP.

1.5. Zarządzanie Polityką

1.5.1. Organizacja zarządzająca dokumentem

Dane organizacji 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

TSP jest zobowiązany do przetwarzania wyłącznie powiadomień przesłanych w języku polskim lub angielskim, powiadomienia przesłane w innych językach są pozostawiane bez rozpatrzenia.

1.5.3. Osoba lub organizacja odpowiedzialna za zgodność

Dostawca, jest odpowiedzialny za zgodność EAA z Polityką EAAP, do której się on odnosi i za dostarczenie usługi zgodnie z przepisami zawartymi w tym dokumencie.
Osobą odpowiedzialną za zgodność świadczonej usługi 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

1.5.4. Procedury zatwierdzania polityki

Przygotowanie, modyfikacja, zatwierdzanie i wydawanie nowej wersji Polityki odbywa się zgodnie z procesem opisanym szczegółowo w sekcji 9.5.

2. Obowiązki związane z publikowaniem i repozytorium

2.1. Repozytorium

EuroCert publikuje polityki i warunki umowne w elektronicznym repozytorium dostępnym na stronie internetowej EuroCert: https://eurocert.pl/category/dokumenty-pl/. Aktualne i historyczne wersje dokumentów są utrzymywane zgodnie z obowiązującym procesem publikacji.

Dla Usługi EAA TSP publikuje:

- aktualną i historyczne wersje niniejszej Polityki;
- regulamin świadczenia Usługi EAA;
- polityki EAAP lub publiczne informacje o obsługiwanych EAAP;
- certyfikaty i/lub dane służące do weryfikacji zabezpieczeń kryptograficznych EAA i list statusowych.

Listy statusowe wydanych i zarządzanych EAA publikowane są zgodnie z rozdziałem 7.4.

TSP powiadamia klienta o każdej zmianie polityki oraz regulaminu świadczenia usługi EAA.

Repozytorium jest dostępne przez całą dobę, 7 dni w tygodniu, z zastrzeżeniem planowanych okien serwisowych.

2.2. 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 uwierzytelnianie

3.1 Nadawanie nazw

3.1.1 Typy nazw

TSP stosuje nazwy i identyfikatory zgodnie z właściwą polityką poświadczenia.

W zależności od rodzaju poświadczenia stosowane mogą być w szczególności nazwy i identyfikatory:

- subskrybenta,
- podmiotu atrybutu,
- wystawcy poświadczenia,
- podmiotu, w imieniu którego EAA zostało wydane,
- atrybutów,

- właściwej polityki poświadczenia,
- inne wymagane przez właściwy format EAA.

Sposób kodowania nazw oraz identyfikatorów jest zgodny wymaganiami ETSI TS 119 472-1 [1].

3.1.2 Konieczność używania nazw znaczących

Nazwy i identyfikatory stosowane w EAA powinny mieć znaczenie właściwe dla celu danego poświadczenia oraz odpowiadać danym zweryfikowanym w ramach procesu jego wydania.

Dostawca usługi nie stosuje wartości fikcyjnych lub pozbawionych znaczenia, jeżeli ich użycie mogłoby prowadzić do niejednoznacznej lub błędnej interpretacji danych zawartych w EAA.

Każde wydane poświadczenie atrybutu jednoznacznie wskazuje właściwą politykę poświadczenia, zgodnie z którą zostało wydane, a zakres danych identyfikacyjnych oraz sposób ich prezentacji są określane przez tę politykę poświadczenia.

3.1.3 Prywatność danych

Zakres danych wykorzystywanych do wydania EAA jest ograniczony do informacji niezbędnych do realizacji celu określonego we właściwej polityce poświadczenia.
Dostawca usługi stosuje zasadę minimalizacji danych zarówno w odniesieniu do danych zawartych w EAA, jak i dowodów oraz informacji przetwarzanych w ramach procesu jego wydania i obsługi cyklu życia.
W zakresie przewidzianym przez właściwy format i politykę poświadczenia, dostawca usługi stosuje mechanizmy wspierające ochronę prywatności, w szczególności:

- mechanizmy selektywnego ujawniania atrybutów;
- mechanizmy ograniczające możliwość nieuzasadnionego korelowania różnych prezentacji poświadczeń;
- rozwiązania ograniczające możliwość śledzenia wykorzystania EAA przez dostawcę usługi lub inne podmioty.

3.1.4 Zasady interpretacji różnych form nazw

Znaczenie i sposób interpretacji nazw, identyfikatorów oraz pseudonimów zawartych w EAA wynikają z właściwej polityki poświadczenia.
W przypadku występowania różnych reprezentacji tej samej nazwy lub identyfikatora, w szczególności wynikających z zastosowania różnych alfabetów, transliteracji, wersji językowych, nazw urzędowych lub pseudonimów, właściwa polityka poświadczenia określa zasady ich stosowania i interpretacji.
Jeżeli sama nazwa nie pozwala jednoznacznie zidentyfikować podmiotu atrybutu, identyfikacja odbywa się z wykorzystaniem dodatkowego identyfikatora określonego we właściwej polityce poświadczenia.

3.2. Metody potwierdzenia tożsamości

W zależności od EAAP, EuroCert może wykorzystywać m.in.:

- wcześniej zweryfikowaną relację z TSP,
- PID z EUDI Wallet,
- notyfikowane i krajowe środki eID,
- inne metody określone w EAAP.

Wcześniejszy wynik identyfikacji może zostać ponownie wykorzystany tylko wtedy, gdy zezwala na to EAAP i wynik pozostaje odpowiedni, aktualny i wiarygodny dla danego celu.

3.3. Reprezentacja i działanie w imieniu innego podmiotu

Jeżeli EAAP dopuszcza wydanie EAA osobie działającej w imieniu innej osoby lub podmiotu, TSP określa sposób potwierdzenia umocowania.

3.4. Powiązanie z portfelem i kontrola kryptograficzna

Jeżeli EAA jest wydawane do jednostki portfela, będącej pod kontrolą i powiązanej z Subskrybentem, w ramach procesu wydania EAA, TSP weryfikuje wymagane informacje potwierdzające autentyczność i ważność jednostki portfela.

3.5. Identyfikacja i uwierzytelnianie żądań unieważnienia

Subskrybent lub Posiadacz EAA może wystąpić o jego unieważnienie. Wniosek o unieważnienie należy przesłać za pośrednictwem wiadomości e-maila na adres uniewaznienia@eurocert.pl

Po złożeniu wniosku o unieważnienie, Subskrybent lub Posiadacz EAA otrzyma wiadomość e-mail potwierdzającą otrzymanie wniosku.

TSP może przyjmować automatyczne żądania unieważnienia od źródeł danych.

Jeśli poświadczenie nadal jest ważne w momencie składania wniosku, TSP uwierzytelni osobę składającą wniosek o unieważnienie, aby upewnić się, że osoba składająca wniosek jest Subskrybentem lub Posiadaczem EAA.

4. Wymagania operacyjne dotyczące cyklu życia EAA

4.1. Wniosek o wydanie EAA

Każdy proces wydania EAA jest inicjowany żądaniem wskazującym co najmniej typ EAA lub dane umożliwiające jednoznaczne wybranie właściwego EAAP.

4.2. Przetwarzanie wniosku

Przetwarzanie wniosku obejmuje co najmniej: ustalenie właściwego EAAP, potwierdzenie uprawnienia wnioskującego, zebranie wymaganych danych i oświadczeń, potwierdzenie warunków korzystania z usługi.

Jeżeli wymagany atrybut lub jego weryfikacja są niedostępne albo wynik jest sprzeczny z wymaganiami EAAP, TSP nie wydaje EAA.

4.3. Pozyskiwanie i walidacja atrybutów

TSP pozyskuje atrybuty ze źródła danych i jeżeli wymaga tego EAAP, waliduje atrybuty zgodnie z regułami właściwymi dla danego EAA.

TSP utrzymuje kontrolowaną listę źródeł danych. Dodanie nowego źródła wymaga oceny m.in. podstawy dostępu, wiarygodności i aktualności danych.

Jeżeli dane ze źródła są niedostępne, niepełne, sprzeczne albo nieaktualne, TSP nie wydaje EAA.

4.4. Wydanie EAA

TSP wydaje EAA po zakończeniu czynności wymaganych przez właściwy EAAP.

Każde EAA jest zabezpieczane kryptograficznie w sposób zapewniający integralność i autentyczność oraz umożliwiający identyfikację TSP jako wystawcy.

Dla wydawanych EAA stosuje się format danych SD-JWT VC.

Każde EAA jest wydawana na okres nie dłuższy niż 24 miesiące.

4.5. Dostarczenie EAA

EAA może zostać dostarczone do jednostki portfela lub udostępnione w postaci pliku możliwego do pobrania, zgodnie z EAAP.

TSP podejmuje środki pozwalające upewnić się, że EAA jest dostarczane do właściwego odbiorcy lub właściwej jednostki portfela w zakresie wymaganym przez EAAP.

Jeżeli proces dostarczenia nie może zostać zakończony w sposób zgodny z EAAP, TSP nie kończy procesu wydania o czym informuje Subskrybenta.

4.6. Weryfikacja EAA

TSP może udostępniać funkcję weryfikacji EAA wspierającą Strony Ufające. Funkcja ta może być wywoływana m.in. po zeskanowaniu kodu QR lub przekazaniu indywidualnego identyfikatora URL.
Weryfikacja obejmuje co najmniej: weryfikację zabezpieczenia kryptograficznego, identyfikację wystawcy, kontrolę okresu ważności, ustalenie właściwego EAAP oraz sprawdzenie statusu EAA.

4.7. Ponowne wydanie

O ile EAAP nie stanowi inaczej, ponowne wydanie EAA jest traktowane jako nowe wydanie wymagające ponownego wykonania weryfikacji wskazanych w EAAP.

4.8. Unieważnienie EAA

EAA może zostać unieważnione przed upływem okresu ważności w przypadkach określonych w odpowiednim EAAP.
TSP może również unieważnić EAA na podstawie wiarygodnej informacji o zdarzeniu wpływającym na jego wiarygodność lub możliwość bezpiecznego użycia, jeżeli właściwy EAAP przewiduje taki mechanizm.
Jeżeli EAA jest związane z jednostką portfela, informacja o unieważnieniu lub utracie ważności portfela może stanowić przesłankę unieważnienia EAA zgodnie z EAAP.
Unieważnienie jest ostateczne, a ponowne uzyskanie ważnego EAA wymaga nowego procesu wydania.
Zmiana statusu po potwierdzeniu podstawy do unieważnienia jest publikowana w terminie do 24 godzin od otrzymania zgłoszenia.

4.9. Usługa statusowa

TSP zapewnia informację o statusie EAA za pomocą mechanizmu określonego przez właściwy EAAP. Dla EAA wydawanych na okres ważności dłuższy niż 24 h, stosowany jest mechanizm Token Status List.
Każde EAA objęte Token Status List zawiera dane umożliwiające ustalenie właściwej listy i pozycji określającej ważność wskazanego EAA na tej liście. Polityka dopuszcza utrzymywanie wielu list, w tym odrębnych list per EAAP lub per część puli wydanych EAA.
TSP tworzy kolejne listy statusowe w sposób kontrolowany i utrzymuje rejestr aktywnych i zamkniętych list.

4.10. Zakończenie korzystania z EAA

Cykl życia konkretnego EAA kończy się z chwilą:

- upływu jego okresu ważności;
- jego unieważnienia.

Zakończenie cyklu życia EAA nie powoduje usunięcia dowodów związanych z jego wydaniem i obsługą.

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.

5.1. Fizyczne środki kontroli

TSP zapewnia kontrolę fizycznego dostępu do usług o znaczeniu krytycznym i minimalizuje fizyczne ryzyko dla aktywów związanych z tymi usługami.

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.

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.

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 w 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. Kopie zapasowe danych audytowych i archiwalnych są przechowywane osobno w różnych lokalizacjach. 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 TSP: osoba odpowiedzialna za usługę EAA, 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, którego 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 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 personel nie przypisany do ról zaufanych, realizujący obowiązki dotyczące EAA, który jest szkolony w zakresie usługi EAA i portfeli cyfrowych.

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.
Dostęp do systemów IT krytycznych dla Usługi EAA wymaga identyfikacji, uwierzytelnienia oraz upoważnienia odpowiadającego pełnionej roli.

Dane do identyfikacji i uwierzytelnienia są unieważniane niezwłocznie w przypadku ustania praw użytkownika.
W celu weryfikacji dostępu fizycznego TSP używa systemu kontroli dostępu opartego na karcie RFID, natomiast w celu kontroli dostępu logicznego – VPN z uwierzytelnieniem 2FA. Bez pomyślnego uwierzytelnienia nie można wykonać żadnego działania krytycznego pod względem bezpieczeństwa. Przestrzegana jest zasada wiedzy koniecznej. 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 nie może 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 dotycząca 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. 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 o rozporządzeniu eIDAS i ustawie o usługach zaufania oraz identyfikacji elektronicznej;
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.

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.
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 wdrożył 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) dowody z usługi EAA:
- dowody z pozyskania lub walidacji atrybutów,
- dane identyfikacyjne Posiadacza EAA, Subskrybenta oraz Podmiotu Atrybutu,
- dane z przetwarzania wniosku o wydanie poświadczenia,
- umowy z Subskrybentem,
- wnioski o wydanie i unieważnienie, decyzje, wykonane kontrole, czas wydania oraz identyfikator EAA,
- zdarzenia dostarczenia, przypisanie listy i pozycji statusowej, decyzja o unieważnieniu oraz jej publikacja.

c) 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.

d) 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).

e) zarządzanie kluczami:
- wszystkie istotne zdarzenia dotyczące kluczy wystawcy EAA i zabezpieczenia list statusowych, w tym generowanie, aktywacja, użycie administracyjne, rotacja, kopie, odtwarzanie i zniszczenie;
- wszystkie zdarzenia związane z zarządzaniem kluczami prywatnymi przechowywanymi w dowolnym celu przez TSP.

f) przepływy danych:
- wszelkie dane krytyczne pod względem bezpieczeństwa ręcznie wprowadzone do systemu;
- dodanie lub usunięcie użytkownika.

g) HSM:
- Instalacja HSM;
- odinstalowanie HSM;
- usuwanie lub niszczenie HSM;
- dostawa HSM;
- resetowanie HSM;
- wgrywanie kluczy i certyfikatów na HSM.

h) zmiana konfiguracji:
- sprzęt;
- oprogramowanie;

- system operacyjny;
- patch naprawczy;
- instalacja, aktualizacja, usunięcie oprogramowania w systemie TSP;
- zmiany profilu statusowego, tworzenie, publikacja i zamknięcie Token Status List;
- zmiany polityk EAAP.

i) 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.

j) 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 Polityki EAA;
   - usunięcie zegara systemu operacyjnego.

k) inne zdarzenia:
   - wyznaczenie osoby do roli bezpieczeństwa;
   - instalacja systemu operacyjnego;
   - uruchomienie systemu;
   - 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 regularnie analizy wygenerowanych logów.

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. W tym okresie zachowuje 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.

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 analizę podatności obejmującą wydawanie EAA, walidację atrybutów, interfejsy portfeli i źródeł danych, usługę statusową oraz funkcję weryfikacji. Analiza jest prowadzona po wykryciu istotnego zagrożenia i co najmniej raz w roku, z terminami działań określonymi w procedurze zarządzania podatnościami.

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 postaci elektronicznej są odpowiednio przygotowane przez TSP w celu bezpiecznego długoterminowego archiwizowania.
TSP zachowuje dowody niezbędne do wykazania prawidłowości świadczenia Usługi EAA i odtworzenia przebiegu istotnych zdarzeń.

Dowody mogą obejmować: dane wniosku o wydanie EAA, identyfikator EAAP i jego wersję, dane o źródle danych, wynik walidacji atrybutu, czas wydania, identyfikator EAA, zdarzenia dostarczenia, status i unieważnienie, działania ról zaufanych oraz informacje związane z obsługą reklamacji.

Archiwizacji podlegają również właściwe wersje Polityki, Deklaracji praktyk, EAAP, warunków usługi, umów i dowodów zatwierdzenia zmian. Zakres danych ogranicza się do informacji niezbędnych dla określonych celów.

5.5.2. Okres utrzymywania archiwum

Okresy przechowywania archiwum wynosi 8 lat od momentu utworzenia danych. Po upływie okresu dane są bezpiecznie usuwane lub anonimizowane, chyba że zgodne z prawem zabezpieczenie dowodów uzasadnia dalsze przechowanie.

5.5.3. Ochrona archiwum

Podczas przechowywania danych archiwalnych 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.

5.5.5. Wymagania dotyczące znakowania czasem zapisów

Wszystkie zapisy w elektronicznym dzienniku logów są opatrzone znacznikiem czasu z dokładnością co do sekundy.

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.

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 wystawcy EAA

TSP planuje rotację kluczy EAA i list statusowych przed końcem ich dopuszczalnego użycia. Zachowuje certyfikaty niezbędne do weryfikacji wcześniej wydanych EAA oraz list statusowych.

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

Usługa EAA jest objęta istniejącym procesem zarządzania podatnościami oraz incydentami EuroCert a także planem ciągłości działania.

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.
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.

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.

5.7.3. Kompromitacja klucza wystawcy EAA lub list statusowych

Po wykryciu lub uzasadnionym podejrzeniu kompromitacji TSP wstrzymuje użycie klucza, określa zakres dotkniętych EAA i list, zabezpiecza dowody, inicjuje wymagane unieważnienia oraz publikuje informacje umożliwiające Stronom Ufającym bezpieczną weryfikację. TSP unieważnia certyfikat powiązany z kluczem.

Wznowienie wydawania i publikacji statusu następuje po przywróceniu integralności systemu i bezpiecznej dystrybucji danych weryfikacyjnych. Ponowne wydanie EAA odbywa się zgodnie z właściwym EAAP; samo odtworzenie systemu nie przywraca ważności unieważnionych EAA.

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 Usługi EAA

TSP utrzymuje plan zakończenia usługi.
Przed zakończeniem świadczenia usługi zaufania, TSP powinien, jeśli dotyczy:

a) powiadomić wszystkich Subskrybentów Posiadaczy EAA, Podmiotów Atrybutów oraz inne podmioty, z którymi pozostaje w relacjach umownych,
b) unieważnić wszystkie nadal ważne wydane poświadczenia,
c) unieważnić wszystkie certyfikaty wykorzystywane do składania pieczęci elektronicznych,
d) bezpiecznie usunąć wszystkie klucze prywatne (w tym kopie zapasowe i wycofane klucze) w sposób uniemożliwiający ich odtworzenie,
e) wycofać upoważnienia wszystkich podwykonawców do realizacji wszelkich działań związanych z wydaniem poświadczeń.

6. Techniczne 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 przeznaczenie kluczy

Klucze kryptograficzne TSP są generowane, aktywowane, przechowywane, używane, rotowane, archiwizowane lub niszczone zgodnie z istniejącym modelem zarządzania kluczami i wymaganiami bezpieczeństwa EuroCert.

Dla Usługi EAA wykorzystywane są odrębne klucze przeznaczone do tego celu, nawet jeżeli korzystają z istniejącej infrastruktury kryptograficznej TSP.

Klucze prywatne wykorzystywane do zabezpieczania EAA oraz, jeżeli dotyczy, list statusowych są chronione w odpowiednim urządzeniu kryptograficznym i nie są eksportowane w postaci jawnej.

Generowanie i aktywacja kluczy wystawcy odbywa się w kontrolowanym środowisku i jest dokumentowana. Operacje krytyczne wymagają udziału co najmniej dwóch osób pełniących role zaufane zgodnie z sekcją 5.2.2.

Klucze Usługi EAA są odseparowane od kluczy innych usług EuroCert. Zastosowanie wspólnego lub odrębnego klucza dla EAA i list statusowych wymaga zatwierdzonej decyzji wynikającej z analizy ryzyka i profilu technicznego.

6.2. Ochrona i cykl życia kluczy prywatnych

Klucze prywatne wystawcy EAA i list statusowych są generowane, przechowywane i używane w module HSM o parametrach i certyfikacji odpowiednich do zatwierdzonego profilu. Klucze nie opuszczają urządzenia w postaci jawnej. Dostęp, aktywacja, kopie zapasowe, migracja i niszczenie podlegają rozdziałowi obowiązków, kontroli uprawnień i rejestrowaniu.

Kopie kluczy są chronione co najmniej na poziomie systemu produkcyjnego i mogą być odtwarzane wyłącznie przez upoważniony personel, zgodnie z kontrolowaną procedurą. Wycofanie klucza obejmuje jego dezaktywację i udokumentowane zniszczenie wszystkich kopii, po wykonaniu obowiązków związanych z ciągłością i statusem.

6.3. Certyfikaty i okresy użycia

TSP publikuje i utrzymuje certyfikaty pieczęci elektronicznych służących do wydawania EAA i list statusowych w repozytorium.

Okres używania klucza prywatnego nie może przekraczać okresu ważności odpowiadającego mu certyfikatu ani okresu dopuszczonego dla zastosowanego algorytmu i długości klucza.

6.4. Dane aktywacyjne

Dane aktywacyjne kluczy TSP są tworzone i chronione zgodnie z zatwierdzonym profilem HSM, zasadą najmniejszych uprawnień i rozdziałem obowiązków. Dostęp do nich jest ograniczony do upoważnionego personelu; ujawnienie lub utrata uprawnień powoduje niezwłoczne działania zabezpieczające. Sposób aktywacji jest zgodny z wymaganiami certyfikowanego urządzenia HSM.

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 VPN;
- 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, ciągłością działania 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.
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 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) po jakichkolwiek istotnych zmianach w systemie lub sieci;

b) przynajmniej co trzy (3) miesiące;

c) w terminie wynikającym z oceny zagrożenia i procedury zarządzania podatnościami po uzyskaniu informacji o istotnym zagrożeniu.

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 techniczne EAA i informacje o statusie

7.1. Profil certyfikatu wydawcy EAA

EAA wydawane przez TSP są opatrywane kwalifikowaną pieczęcią elektroniczną dostawcy usługi. Certyfikat wykorzystywany do pieczętowania EAA spełnia wymagania profilu EAA określonego w ETSI TS 119 412-6 [2].

7.2 Format EAA

TSP wydaje EAA w formacie SD-JWT VC. Szczegółowy typ EAA, zakres atrybutów oraz właściwy schemat danych określa właściwa polityka poświadczenia.

7.3. Profil listy statusowej

Jeśli informacje o statusie danego poświadczenia są udostępniane za pomocą listy statusów, wydane poświadczenie zawiera odwołanie do listy statusów (URI) oraz informacje niezbędne do zlokalizowania odpowiedniego wpisu statusu dla danego poświadczenia w ramach listy statusów zgodnie z wymaganiami normy ETSI TS 119 472-1 [1].

Lista Statusów jest publikowana przez HTTPS w URI osadzonym w każdym poświadczeniu i pozostaje dostępna do daty wygaśnięcia określonej dla odpowiedniej listy statusów.

7.4. Publikacja i dostępność Token Status List

Token Status Lists są publikowane pod adresami URI zawartymi w odpowiednich EAA i zabezpieczane kryptograficznie przez TSP w sposób pozwalający stronie ufającej zweryfikować autentyczność i integralność listy.

8. Audyt zgodności i inne rodzaje oceny

EuroCert wykorzystuje istniejący system kontroli wewnętrznej i audytu. Zakres audytu obejmuje zgodność z prawem, normami technicznymi, dokumentacją usługi, bezpieczeństwem fizycznym, personelem, bezpieczeństwem IT i ochroną danych.

Zakres kontroli obejmuje usługę EAA, gdzie stosowanie normy ETSI TS 119 471 [3] dla usług niekwalifikowanych stanowi dobre praktyki.

Wynikiem kontroli jest poufny dokument dostępny tylko dla upoważnionych osób.
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.

8.1. Częstotliwość i okoliczności oceny

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

8.2. Kwalifikacje osoby dokonującej oceny

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

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 niniejszą polityką;
- adekwatność zastosowanych procesów;
- dokumentacja;
- bezpieczeństwo fizyczne;
- adekwatność personelu;
- bezpieczeństwo IT;
- zgodność z zasadami ochrony danych osobowych.

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. Inne postanowienia biznesowe i prawne

9.1. Zobowiązania uczestników

9.1.1. Obowiązki TSP

TSP świadczy Usługę EAA zgodnie z Polityką, właściwym EAAP, obowiązującymi warunkami świadczenia usługi oraz właściwymi przepisami.

TSP odpowiada za prawidłowe wykonanie procesu od momentu przyjęcia danych/żądania w zakresie określonym przez EAAP, w tym za prawidłowe zabezpieczenie EAA, zarządzanie statusem i prowadzenie dowodów.

TSP nie przedstawia danych samodeklarowanych jako danych niezależnie zweryfikowanych, jeżeli taka weryfikacja nie została wykonana.

9.1.2. Obowiązki źródła danych

Jeżeli EAA wykorzystuje zewnętrzne źródło danych, odpowiedzialność i obowiązki źródła są określane w umowie z TSP.

9.1.3. Obowiązki Subskrybenta oraz Posiadacza EAA

Subskrybent oraz Posiadacz EAA są odpowiedzialni za dostarczanie dokładnych i kompletnych informacji oraz za niezwłoczne informowanie TSP o wszelkich błędach, wadach lub zmianach wpływających na wydane poświadczenie lub dane stanowiące podstawę jego wydania.

Subskrybent oraz Posiadacz EAA są zobowiązania niezwłocznie powiadomić TSP o wszelkich znanych zmianach, nieścisłościach, błędach lub nieaktualnych informacjach dotyczących danych wykorzystywanych do wydania poświadczenia lub samego wydanego poświadczenia.

9.1.4. Obowiązki strony ufającej

Strony ufające są zobowiązane do zweryfikowania integralności, autentyczności i aktualnego statusu poświadczenia, a także okresu jego ważności oraz wszelkich ograniczeń wynikających z właściwego EAAP, przed poleganiem na tym poświadczeniu.

Strona Ufająca interpretuje atrybuty zgodnie z poziomem ich weryfikacji. EAA zawierające dane samodeklarowane nie powinno być traktowane jako równoważne poświadczeniu atrybutów potwierdzonych w źródle autentycznym.

9.2. Odpowiedzialność TSP

TSP nie ponosi odpowiedzialności za dokładność, kompletność ani aktualność danych pochodzących ze źródła danych, jeżeli ich nieprawidłowość wynika z działania lub zaniechania tego źródła i nie została spowodowana przez TSP.

Odpowiedzialność TSP obejmuje prawidłowe uwierzytelnienie źródła danych, bezpieczne pozyskanie danych oraz ich prawidłowe przetworzenie zgodnie z obowiązującymi przepisami i polityką EAAP.

O ile nie wskazano inaczej, wydane poświadczenie odzwierciedla dane dostępne w chwili jego wydania. TSP nie ponosi odpowiedzialności za nieuwzględnienie późniejszych zmian danych, jeżeli zmiany te nie zostały przekazane lub udostępnione przez źródło danych w czasie umożliwiającym ich uwzględnienie przed wydaniem poświadczenia.

TSP nie ponosi odpowiedzialności za szkody wynikające z wykorzystania usługi zaufania lub wydanego poświadczenia niezgodnie z ich przeznaczeniem, ograniczeniami wskazanymi w poświadczeniu lub polityce atrybutów EAAP.

TSP nie ponosi odpowiedzialności za sposób wykorzystania, przedstawienia lub interpretacji poświadczenia przez Subskrybentów, posiadacza EAA, Strony Ufające, chyba że szkoda wynika z niewykonania lub nienależytego wykonania obowiązków TSP wynikających z obowiązujących przepisów prawa.

TSP nie gwarantuje przydatności usługi zaufania do określonego celu, w tym do określonych celów biznesowych.

Powyższe ograniczenia odpowiedzialności stosuje się w zakresie dozwolonym przez obowiązujące przepisy prawa i nie wyłączają odpowiedzialności, której zgodnie z prawem nie można ograniczyć ani wyłączyć.

9.3. Prywatność i ochrona danych

TSP stosuje istniejące środki ochrony danych osobowych, poufności i integralności danych oraz ogranicza dostęp do danych do osób i podmiotów uprawnionych.

Każdy EAAP jest projektowany z uwzględnieniem minimalizacji danych. EAA powinno zawierać wyłącznie atrybuty potrzebne do zamierzonego celu.

TSP określa, jakie dane źródłowe i dowody są przechowywane po wydaniu EAA oraz przez jaki okres. Okresy retencji są udokumentowane i proporcjonalne do celu.

Funkcja weryfikacji oparta na QR jest projektowana w sposób ograniczający zbędne pozyskiwanie informacji o użyciu EAA.

9.4. Reklamacje i spory

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 EAA należy kierować na dane kontaktowe w wskazane w rozdziale 1.5.2

TSP potwierdza otrzymanie reklamacji lub skargi w terminie 3 dni roboczych od dnia jej otrzymania, korzystając z danych kontaktowych podanych przez zgłaszającego. TSP udziela odpowiedzi na papierze lub innym trwałym nośniku, w szczególności pocztą elektroniczną, w terminie 14 dni od dnia otrzymania reklamacji lub skargi.

Jeżeli rozpatrzenie sprawy wymaga dodatkowych informacji, TSP zwraca się do zgłaszającego o ich uzupełnienie. Nie powoduje to przedłużenia ustawowego terminu odpowiedzi ani wyłączenia skutków jego niedochowania.
Jeżeli zgłaszający nie zgadza się z odpowiedzią TSP, strony mogą podjąć dobrowolne konsultacje w celu polubownego rozwiązania sporu. Termin, sposób prowadzenia konsultacji oraz zakres udostępnianych informacji strony uzgadniają z zachowaniem zasad poufności i ochrony danych osobowych.
Złożenie reklamacji lub skargi ani udział w konsultacjach nie stanowią warunku dochodzenia roszczeń przed sądem i nie ograniczają prawa do skorzystania z dostępnych pozasądowych sposobów rozwiązywania sporów konsumenckich.
Spory rozstrzygają sądy właściwe zgodnie z obowiązującymi przepisami prawa. Postanowienia Polityki nie ograniczają uprawnień konsumentów ani innych osób objętych ochroną konsumencką.
Zgłoszenia dotyczące bezpieczeństwa Usługi oraz żądania unieważnienia EAA są obsługiwane zgodnie z właściwymi postanowieniami Polityki i EAAP, niezależnie od postępowania reklamacyjnego. Termin odpowiedzi na reklamację lub skargę nie przedłuża terminów realizacji tych czynności.

9.5. Zmiany

TSP zastrzega sobie prawo do zmiany niniejszego dokumentu w przypadku zmiany zasad normatywnych, wymogów bezpieczeństwa, warunków rynkowych lub innych okoliczności.

9.5.1. Procedura wprowadzania zmian

TSP ujawnia w swoich regulacjach publicznych wyłącznie te procedury, których znajomość nie zagraża bezpieczeństwu usług.
Wszystkie regulacje wewnętrzne (jawne i niejawne) są zatwierdzane zgodnie z Metodyką Zatwierdzania Regulacji przez Kierownika TSP. TSP dokonuje przeglądu polityki świadczenia usługi 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 zatwierdzoną politykę na swojej stronie internetowej co najmniej 14 dni przed planowanym wejściem w życie.

9.6. Prawo właściwe

TSP przez cały czas działa zgodnie z obowiązującymi przepisami prawa polskiego oraz prawa europejskiego. Prawo polskie jest prawem właściwym dla umów, regulacji i ich egzekwowania.

9.7. Zgodność z obowiązującym prawem

Obowiązujące przepisy:

- Rozporządzenie (UE) nr 910/2014 Parlamentu Europejskiego i Rady z dnia 23 lipca 2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE, zmienionej przez rozporządzenie (UE) 2024/1183 (OJ 28.08.2014, L 257/79) (eIDAS),
- Rozporządzenie (UE) 2016/679 Parlamentu Europejskiego i Rady z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych

i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (OJ L 119 z 4.5.2016, s. 1),

- ROZPORZĄDZENIE WYKONAWCZE KOMISJI (UE) 2025/2160 z dnia 27 października 2025 r. ustanawiające zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do norm referencyjnych, specyfikacji i procedur dotyczących zarządzania ryzykiem związanym ze świadczeniem niekwalifikowanych usług zaufania (OJ L, 2025/2160, 28.10.2025),
- Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej, Dz.U. z 2016 poz. 1579, z późn. zm.),
- Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. 2018 poz. 1560),
- ROZPORZĄDZENIE WYKONAWCZE KOMISJI (UE) 2024/2690 z dnia 17 października 2024 r. ustanawiające zasady stosowania dyrektywy (UE) 2022/2555 w odniesieniu do wymogów technicznych i metodycznych dotyczących środków zarządzania ryzykiem w cyberbezpieczeństwie oraz doprecyzowujące przypadki, w których incydent uznaje się za poważny w odniesieniu do dostawców usług DNS, rejestrów nazw TLD, dostawców usług chmurowych, dostawców usług ośrodka przetwarzania danych, dostawców sieci dostarczania treści, dostawców usług zarządzanych, dostawców usług zarządzanych w zakresie bezpieczeństwa, dostawców internetowych platform handlowych, wyszukiwarek internetowych i platform usług sieci społecznościowych oraz dostawców usług zaufania (OJ L 2690 z 18.10.2024),
- ETSI EN 319 401 v.3.2.1 Podpisy elektroniczne i infrastruktura zaufania (ESI); Ogólne wymagania polityki dla dostawców usług zaufania (ETSI EN 319 401).

Bibliografia

[1] Electronic Signatures and Trust Infrastructures (ESI); Profiles for Electronic Attestation of Attributes; Part 1: General requirements.

[2] Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles; Part 6: Certificate profile requirements for PID, Wallet, EAA, QEAA, and PSBEAA providers.

[3] Electronic Signatures and Trust Infrastructures (ESI); Policy and Security requirements for Providers of Electronic Attestation of Attributes Services.