Polityka i Kodeks Świadczenia Kwalifikowanej Usługi Zaufania Certum „Zarządzanie kwalifikowanymi urządzeniami do składania podpisu/pieczęci elektronicznej na odległość”

Wersja 1.0

Ważny od: 15 marca 2026 r.

Asseco Data Systems S.A.
ul. Jana z Kolna 11,
80-864 Gdańsk
www.assecods.pl
Certum

ul. Bajeczna 13
71-838 Szczecin
www.certum.pl
www.certum.eu

Klauzula: Prawa Autorskie

Spis treści

1 Wstęp

Polityka Certyfikacji i Kodeks Postępowania Certyfikacyjnego Kwalifikowanych Usług Zaufania Certum „Zarządzanie kwalifikowanymi urządzeniami do składania podpisu/pieczęci elektronicznej na odległość" dalej zwana **Polityką RQSCD** jest dokumentem bazującym i uzupełniającym „Politykę Certyfikacji i Kodeks Postępowania Certyfikacyjnego Kwalifikowanych Usług Certum" zwaną dalej **Polityką Główną,** która określa ogólne zasady stosowane przez Certum w trakcie świadczenia kwalifikowanych usług zaufania.

Powyższe usługi są świadczone zgodnie z:

- wdrożonym przez Asseco Data Systems S.A. Zintegrowanym Systemem Zarządzania, który obejmuje zwłaszcza wymagania standardów PN-EN ISO 9001:2009 oraz PN-ISO/IEC 27001:2014,

- wymaganiami wynikającymi z *Rozporządzenia Ministra Cyfryzacji z dnia 5 października 2016 r. w sprawie krajowej infrastruktury zaufania*,

- *Ustawą o usługach zaufania oraz identyfikacji elektronicznej z dnia 5 września 2016 r. (Dz.U. 2019 r. poz. 162) z późniejszymi zmianami*,

- usługi wymienione powyżej są świadczone zgodnie z wymaganiami Rozporządzenia Parlamentu Europejskiego i Rady (UE) NR 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE wraz z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2024/1183 z dnia 11 kwietnia 2024 r. w sprawie zmiany rozporządzenia (UE) nr 910/2014 w odniesieniu do ustanowienia europejskich ram tożsamości cyfrowej, zwanym dalej w treści niniejszego dokumentu *Rozporządzeniem eIDAS*,

- usługi wymienione powyżej są świadczone zgodnie z wymaganiami Rozporządzenia Wykonawczego Komisji (UE) 2025/1567 z dnia 29 lipca 2025 r. ustanawiającego zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do zarządzania kwalifikowanymi urządzeniami do składania podpisu elektronicznego na odległość i kwalifikowanymi urządzeniami do składania pieczęci elektronicznej na odległość jako kwalifikowanymi usługami zaufania.

Polityka Główna definiuje także uczestników tego procesu, ich obowiązki i odpowiedzialność, oraz obszary zastosowań. Znajomość natury, celu oraz roli Polityki Głównej jest szczególnie istotna z punktu widzenia **subskrybenta** oraz **strony ufającej**[1].

Struktura i merytoryczna zawartość Polityki RQSCD są zgodne z zaleceniem RFC 3647 *Certificate Policy and Certification Practice Statement Framework*. Spełnia ona również wymagania normy *ETSI TS 119 431-1 Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP services operating a remote QSCD / SCDev .*

Niniejszy dokument został utworzony przy założeniu, że czytelnik jest ogólnie zaznajomiony z pojęciami dotyczącymi certyfikatów dostawcy usług zaufania, certyfikatów, podpisów/pieczęci elektronicznych oraz Infrastruktury Klucza Publicznego (**PKI**).

[1] Odbiorca, który działa na podstawie zaufania do certyfikatu i podpisu cyfrowego.

*Obowiązujące pojęcia, terminy i ich znaczenie są określone w **Słowniku pojęć** na końcu tego dokumentu.*

1.1 Wprowadzenie

Polityka RQSCD opisuje zasady zarządzania usługami zarządzania kwalifikowanymi urządzeniami do składania podpisu lub pieczęci elektronicznej na odległość, aby spełniać najwyższe standardy prawne i normalizacyjne.

1.2 Nazwa dokumentu i jego identyfikacja

Niniejszemu dokumentowi przypisuje się nazwę własną o następującej postaci: **Polityka Świadczenia Kwalifikowanych Usług Zaufania Certum „Zarządzanie kwalifikowanymi urządzeniami do składania podpisu/pieczęci elektronicznej na odległość"** i jest on dostępny w postaci elektronicznej w serwisie internetowym urzędu certyfikacji dostępnym pod adresem www.certum.pl.

Z ww. dokumentem związany jest następujący zarejestrowany identyfikatory obiektu (OID: 1.2.616.1.113527.2.4.1.0.6.1.0):

> **id-cck-kpc-v1 OBJECT IDENTIFIER ::= { iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-cck(4) id-cck-certum-certPolicy(1) id-certPolicy-doc(0) id-ccert-kpc(pc)(6) version(1) 0}**

w którym dwie ostatnie wartości liczbowe odnoszą się do aktualnej wersji i podwersji tego dokumentu.

1.3 Deklaracja zgodności dla Polityk Usługi Podpisu Serwerowego

Asseco Data Systems SA jako dostawca kwalifikowanej usługi „**Zarządzania kwalifikowanymi urządzeniami do składania podpisu/pieczęci elektronicznej na odległość"** deklaruje zgodność z polityką EUSPv2:

itu-t(0) identified-organization(4) etsi(0) SIGNATURE CREATION SERVICE-policies(19431) ops (1) policy-identifiers(1) eu-remote-qscd-v2 (4)

1.4 Strony Polityki RQSCD

Polityka Główna reguluje wszystkie najważniejsze relacje zachodzące pomiędzy podmiotami wchodzącymi w skład Certum, jego zespołami doradczymi (w tym audytorami) oraz klientami (użytkownikami dostarczanych usług). W szczególności regulacje te dotyczą:

- usług zarządzania kwalifikowanymi urządzeniami do składania podpisu lub pieczęci elektronicznego na odległość,
- subskrybentów,
- stron ufających.

1.4.1 Subskrybenci

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

1.4.2 Strony ufające

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

1.4.3 Inne Strony

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

1.5 Administracja Kodeksem Postępowania Certyfikacyjnego

Administrowanie niniejszą Polityką RQSCD odbywa się na zasadach opisanych w Polityce Głównej.

1.5.1 Organizacja odpowiedzialna za administrowanie dokumentem

Asseco Data Systems S.A.
ul. Jana z Kolna 11,
80-864 Gdańsk
Polska
KRS: 0000421310 Sąd Rejonowy Gdańsk-Północ w Gdańsku

1.5.2 Kontakt

Asseco Data Systems S.A.
Certum
ul. Bajeczna 13
71-838 Szczecin
Polska
E-mail: infolinia@certum.pl
Numer telefonu: +48 91 4801 340

1.5.3 Podmioty określające aktualność zasad określonych w dokumencie

Ocena aktualności i przydatności niniejszej Polityki RQSCD odbywa się na zasadach opisanych w Polityce Głównej.

1.5.4 Procedura zatwierdzania Polityki Certyfikacji i Kodeksu Postępowania Certyfikacyjnego

Procedura zatwierdzania niniejszej Polityki RQSCD odbywa się na zasadach opisanych w Polityce Głównej.

1.6 Definicje i używane skróty

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej, a specyficzne definicje dla Polityki RQSCD znajdują się na końcu niniejszego dokumentu.

2 Odpowiedzialność za publikację i repozytorium

2.1 Repozytorium

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

2.2 Informacje publikowane w repozytorium

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

2.3 Częstotliwość publikacji

Częstotliwość publikacji niniejszej Polityki RQSCD odbywa się na tych samych zasadach jak częstotliwość publikacji Polityki Głównej które zostały opisane w Polityce Głównej w rodz. 2.3.

2.4 Kontrola dostępu do repozytorium

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

3 Identyfikacja i uwierzytelnienie

3.1 Środki eID lub powiązanie tożsamości

Zakres związany z przedmiotowym punktem zaadresowany został w rozdziale 3 Polityki Głównej.

Każdy podpisujący musi być prawidłowo uwierzytelniony i zidentyfikowany, aby móc wykonać dowolną operację przy użyciu klucza.

Potwierdzenie tożsamości osoby prawnej odbywa się w procesie rejestracji klienta w systemie rejestracji usług kwalifikowanych. Identyfikacja klienta odbywa się zgodnie z Art. 24.1 *Rozporządzenia eIDAS* i realizowana jest na wysokim poziomie bezpieczeństwa (Level of Assurance High) lub z dużą dozą pewności zdefiniowaną w Art. 24.1a(c) (High Level of Confidence) *Rozporządzenia eIDAS*.

Wnioskowanie o dostęp do usługi i rejestracja klienta odbywają się w procesie rejestracji do usługi wydawania kwalifikowanego certyfikatu podpisu lub kwalifikowanego certyfikatu pieczęci.

Środek identyfikacji elektronicznej wydawany w ramach usługi IdP/CAS spełnia wymagania wysokiego poziomu bezpieczeństwa lub dużej dozy pewności zgodnie z Art. 24.1a *Rozporządzenia eIDAS* zarówno w zakresie poziomu wiarygodności danych jak i mechanizmów ich uwalniania.

Usługa w sposób jednoznaczny wiąże klucze do składania podpisu z identyfikatorem referencyjnym środka tożsamości elektronicznej identyfikującego klienta poprzez przypisanie mu karty kryptograficznej z tymi kluczami.

W ramach świadczenia usługi zarządzania kwalifikowanymi urządzeniami do składania podpisu/ pieczęci Certum stosuje:

- wewnętrzne usługi uwierzytelniania,
- zewnętrzne usługi uwierzytelniania wbudowane w schemat identyfikacji wykorzystywany przez Europejski Portfel Tożsamości Cyfrowej (mObywatel).

3.2 Powiązanie z certyfikatem

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

3.3 Wydawanie środków identyfikacji elektronicznej

Dane aktywujące podpis są ustalane samodzielnie przez subskrybenta dla certyfikatów długoterminowych.

Dane używane do uwolnienia środka identyfikacji elektronicznej oraz aktywacji klucza prywatnego są przekazywane w następujący sposób użytkownikowi:

- SEED (ziarno) generatora OTP – generowany przez Certum i przekazywany do aplikacji mobilnej SimplySign po uwierzytelnieniu użytkownika jego danymi;
- OTP generowane na podstawie SEEDa i czasu bieżącego według algorytmu SHA-2 i przekazywane do aplikacji w celu uwierzytelnienia się, przez użytkownika końcowego;

- PIN do aktywacji klucza – ustawiany wyłącznie przez klienta w procesie wnioskowania o kwalifikowany certyfikat podpisu lub pieczęci.

Aktywacja operacji złożenia podpisu certyfikatem wydawanym w procesie podpisywania realizowana jest przez usługobiorcę, który ma kontrolę nad całym procesem poprzez dysponowanie pod swoją wyłączną kontrolą telefonem komórkowym:

- poprzez PUSH notyfikację po uwierzytelnieniu w aplikacji mObywatel (oficjalna rządowa aplikacja mobilna, która pozwala na bezpieczne potwierdzanie tożsamości);
- na ten telefon drogą SMS-ową otrzyma kod autoryzujący użycie klucza prywatnego zawartego w sprzętowym module kryptograficznym do złożenia podpisu.

3.4 Pozostałe usługi

3.4.1 Charakterystyki operacyjne

3.4.1.1 Usługi dotyczące statusu certyfikatu

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

3.4.1.2 Usługa znakowania czasem

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

3.4.1.3 Usługa walidacji i konserwacji kwalifikowanych podpisów elektronicznych i kwalifikowanych pieczęci elektronicznych

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej oraz w Polityce walidacji i konserwacji kwalifikowanych podpisów elektronicznych i kwalifikowanych pieczęci elektronicznych.

3.4.1.4 Usługa kwalifikowanego doręczenia elektronicznego

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej oraz w Polityce usługi kwalifikowanego doręczenia elektronicznego.

3.4.2 Dostępność usług

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

3.4.3 Funkcje opcjonalne

Nie dotyczy.

3.5 Zakończenie subskrypcji

Nie dotyczy.

3.6 Deponowanie i odtwarzanie kluczy

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

3.6.1 Zasady i praktyki depozytu i odzyskiwania kluczy

Nie dotyczy.

3.6.2 Enkapsulacja klucza sesji, polityka i praktyki przywracania

Nie dotyczy.

4 Zabezpieczenia techniczne, organizacyjne i operacyjne

W rozdziale opisano ogólne wymagania w zakresie nadzoru nad zabezpieczeniami fizycznymi, organizacyjnymi oraz działaniami personelu, stosowanymi w Certum m.in. uwierzytelniania podmiotów, emisji certyfikatów usług zaufania, wykonania operacji związanych z generowaniem kluczy i ich wykorzystaniem oraz wykonywania kopii zapasowych.

4.1 Zabezpieczenia fizyczne

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

4.1.1 Miejsce lokalizacji oraz budynek

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

4.1.2 Dostęp fizyczny

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

4.1.3 Zasilanie oraz klimatyzacja

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

4.1.4 Zagrożenie zalaniem

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

4.1.5 Ochrona przeciwpożarowa

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

4.1.6 Nośniki informacji

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

4.1.7 Niszczenie zbędnych nośników i informacji

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

4.1.8 Przechowywanie kopii bezpieczeństwa

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

4.2 Zabezpieczenia organizacyjne

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

4.2.1 Zaufane role

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

4.2.2 Liczba osób wymaganych do realizacji zadania

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

4.2.3 Identyfikacja oraz uwierzytelnianie ról

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

4.2.4 Role, które nie mogą być łączone

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

4.3 Nadzorowanie personelu

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

4.3.1 Kwalifikacje, doświadczenie oraz upoważnienia

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

4.3.2 Procedura weryfikacji personelu

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

4.3.3 Wymagania dotyczące przeszkolenia

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

4.3.4 Częstotliwość powtarzania szkoleń oraz wymagania

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

4.3.5 Częstotliwość rotacji stanowisk i jej kolejność

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

4.3.6 Sankcje z tytułu nieuprawnionych działań

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

4.3.7 Pracownicy kontraktowi

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

4.3.8 Dokumentacja przekazana personelowi

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

4.4 Rejestrowanie zdarzeń, zarządzanie incydentami bezpieczeństwa oraz audyty bezpieczeństwa

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

4.4.1 Typy rejestrowanych zdarzeń

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

4.4.2 Częstotliwość analizy zapisów rejestrowanych zdarzeń (logów)

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

4.4.3 Okres przechowywania zapisów rejestrowanych zdarzeń

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

4.4.4 Ochrona zapisów rejestrowanych zdarzeń

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

4.4.5 Procedury tworzenia kopii zapisów rejestrowanych zdarzeń

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

4.4.6 System gromadzenia danych na potrzeby audytu (wewnętrzny a zewnętrzny)

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

4.4.7 Powiadamianie podmiotów odpowiedzialnych za zaistniałe zdarzenie

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

4.4.8 Oszacowanie podatności na zagrożenia

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

4.5 Archiwizowanie danych

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

4.5.1 Rodzaje archiwizowanych danych

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

4.5.2 Okres przechowywania archiwum

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

4.5.3 Ochrona archiwum

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

4.5.4 Procedury tworzenia kopii zapasowych

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

4.5.5 Wymaganie znakowania archiwizowanych danych elektronicznym znacznikiem czasu

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

4.5.6 System gromadzenia danych archiwalnych (wewnętrzny a zewnętrzny)

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

4.5.7 Procedury dostępu oraz weryfikacji zarchiwizowanej informacji

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

4.6 Zmiana klucza

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

4.7 Naruszenie ochrony klucza i uruchamianie po awariach oraz klęskach żywiołowych

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

4.7.1 Procedury obsługi incydentów i reagowania na zagrożenia

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

4.7.2 Uszkodzenie zasobów obliczeniowych, oprogramowania i/lub danych

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

4.7.3 Ujawnienie lub podejrzenie ujawnienia kluczy prywatnych urzędu certyfikacji

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

4.7.4 Zapewnienie ciągłości działania po katastrofach

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

4.8 Zakończenie działalności lub przekazanie zadań przez urząd certyfikacji

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej

4.8.1 Wymagania związane z przekazaniem obowiązków

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

4.8.2 Postępowanie w przypadku zakończenia działalności

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5 Procedury bezpieczeństwa technicznego

Rozdział ten opisuje procedury tworzenia oraz zarządzania parami kluczy kryptograficznych Certum oraz użytkowników, wraz z towarzyszącymi temu uwarunkowaniami technicznymi.

5.1 Generowanie pary kluczy i jej instalowanie

5.1.1 Generowanie par kluczy

5.1.1.1 Środowisko oraz moduł kryptograficzny

Środowisko oraz moduł kryptograficzny do przechowywania kluczy prywatnych spełnia wymagania przedstawione w rozdziale 6.2.1 Polityki Głównej.

5.1.1.2 Algorytmy i długość kluczy

Klucze kryptograficzne są generowane w module kryptograficznym, spełniającym wymagania klasy FIPS 140-2 Level 3 lub wyżej, z użyciem algorytmu RSA, dla długości 3072 oraz 4094. Długość kluczy i stosowane algorytmy aktualizuje się zgodnie z normą ETSI TS 119 312 (zalecane rozmiary kluczy vs. czas) oraz wymaganiami z SOG-IS-CRYPTO oraz ECCG/ENISA w specyfikacji: „**Agreed Cryptographic Mechanisms**" (uzgodnione mechanizmy kryptograficzne).

5.1.1.3 Ochrona klucza

Realizowane zgodnie z opisem producenta HSM w zakresie przechowywania danych związanych z kluczami kryptograficznymi.

5.1.1.4 Inicjalizacja HSM

Inicjalizacja HSM jest realizowana zgodnie z procedurą Procedura zarządzania modułem HSM.

5.1.1.5 Generowanie klucza publicznego i prywatnego

Klucze prywatne (a także publiczne) mogą znajdować się w jednym z trzech podstawowych stanów (zgodnie z normą ISO/IEC 11770-1):

- w oczekiwaniu na aktywność (gotowy) – klucz został już wygenerowany, ale nie jest jeszcze dostępny do użytku (aktualna data certyfikatu powiązanego z tym kluczem jest mniejsza od daty początku okresu ważności certyfikatu), lub klucz, który nie został jeszcze powiązany z certyfikatem,
- aktywny – klucz może być używany w operacjach kryptograficznych (np. do realizacji podpisów lub pieczęci elektronicznych), zaś aktualna data zawiera się w okresie ważności powiązanego certyfikatu i certyfikat nie jest unieważniony,
- uśpiony – w tym stanie klucz może być stosowany tylko i wyłącznie w operacji deszyfrowania (subskrybent nie może używać klucza prywatnego do realizacji podpisu elektronicznego lub pieczęci) – certyfikat jest przeterminowany.

5.1.1.6 Procedury generowania początkowych kluczy urzędu certyfikacji

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.1.1.7 Procedury aktualizacji kluczy urzędu certyfikacji

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.1.2 Przekazywanie klucza prywatnego użytkownikowi końcowemu oraz metody aktywacji klucza prywatnego

Klucze subskrybentów generowane są przez urząd certyfikacji w sprzętowym module kryptograficznym (HSM) i są udostępniane zdalnie subskrybentowi z wykorzystaniem mechanizmów dostarczanych przez Certum.

Certum umożliwia subskrybentom korzystanie z kluczy wyłącznie w certyfikowanych urządzeniach wpisanych na listę certyfikowanych urządzeń do składania kwalifikowanych podpisów i kwalifikowanych pieczęci notyfikowanych zgodnie z art. 30 ust. 2, art. 39 ust. 2 oraz art. 39 ust. 3 Rozporządzenia eIDAS.

Subskrybenci kwalifikowanej usługi otrzymują dostęp do personalizowanych kart wirtualnych umieszczonych na sprzętowym module kryptograficznym. Personalizacja kart oznacza przygotowanie karty do użycia, tj. wygenerowanie unikalnego numeru karty oraz unikalnej pary

kluczy. Tak utworzona karta pełni rolę bezpiecznego urządzenia, na którym będzie znajdował się certyfikat subskrybenta.

Dane do aktywowania karty:

- ustalane samodzielnie przez subskrybenta w przypadku kart umieszczonych na urządzeniu HSM, subskrybent nadaje kod PIN i kod PUK po otrzymaniu certyfikatu związanego z parą kluczy na karcie,
- kod przesłany drogą SMS-ową potrzebny do złożenia podpisu elektronicznego udostępniany jest usługobiorcom niezależnie w procesie podpisu certyfikatami certyfikatów o krótkim terminie ważności (do 24 godzin włącznie) dla certyfikatów wydanych w procesie podpisywania,
- poprzez PUSH notyfikacje po uwierzytelnieniu w aplikacji mObywatel (oficjalna rządowa aplikacja mobilna, która pozwala na bezpieczne potwierdzanie tożsamości) dla wydawanych certyfikatów w procesie podpisu, o krótkim terminie ważności (do 24 godzin włącznie).

Certum gwarantuje, że procedury stosowane w urzędzie certyfikacji w żadnym momencie po wygenerowaniu klucza prywatnego nie pozwalają na użycie go do realizacji podpisu elektronicznego ani też nie stwarzają warunków, które umożliwią zrealizowanie takiego podpisu innemu podmiotowi, poza właścicielem tego klucza.

Przerwanie procesu podpisywania po wydaniu certyfikatu w procesie podpisywania skutkuje usunięciem klucza prywatnego, co uniemożliwia złożenie podpisu z wykorzystaniem tego klucza.

Dla podpisu jednorazowego klucze prywatne usługobiorców są aktywowane dopiero po uwierzytelnieniu (podaniu kodu otrzymanego drogą SMS-ową lub push-notyfikacji) i tylko na czas wykonania podpisu elektronicznego z użyciem tego klucza. Po wykonaniu operacji klucz prywatny jest automatycznie usuwany ze sprzętowego modułu kryptograficznego.

Nie można użyć klucza prywatnego do podpisywania lub pieczętowania o ile certyfikat jest nieważny, odwołany lub zawieszony.

Klucze prywatne mogą być użyte wyłącznie za zgodą podpisującego po uruchomieniu metody aktywacji.

5.1.3 Przekazywanie klucza publicznego do urzędu certyfikacji

Nie dotyczy.

5.1.4 Przekazywanie klucza publicznego urzędu certyfikacji stronom ufającym

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.1.5 Zastosowania kluczy

Do tworzenia podpisów i pieczęci stosowane algorytmy to SHA-256, SHA-384, SHA-512. Przez cały okres certyfikatu podpisującego weryfikujemy stosowanie algorytmów rekomendowanych przez ETSI TS 119 312, SOG-IS-CRYPTO oraz ECCG/ENISA w specyfikacji: „Agreed Cryptographic Mechanisms" (uzgodnione mechanizmy kryptograficzne).

5.2 Ochrona klucza prywatnego

Klucze subskrybentów generowane i utrzymywane są w sprzętowym module kryptograficznym. Urząd certyfikacji (patrz rozdz. Generowanie par kluczy), który generuje parę kluczy w imieniu

subskrybenta, musi przekazać dostęp do pary kluczy w sposób bezpieczny oraz pouczyć usługobiorcę o zasadach ochrony klucza prywatnego (patrz rozdz. Przekazywanie klucza prywatnego użytkownikowi końcowemu).

5.2.1 Standard modułu kryptograficznego

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.2.2 Podział klucza prywatnego na części

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.2.2.1 Akceptacja sekretu współdzielonego przez posiadacza sekretu

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.2.2.2 Zabezpieczenie sekretu współdzielonego

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.2.2.3 Dostępność oraz usunięcie (przeniesienie) sekretu współdzielonego

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.2.2.4 Odpowiedzialność posiadacza sekretu współdzielonego

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.2.3 Deponowanie klucza prywatnego

Klucze prywatne subskrybentów są przechowywane na sprzętowym module kryptograficznym i są dostępne jedynie dla subskrybenta po uwierzytelnieniu (podanie PIN), a dla certyfikatów wydawanych w procesie podpisywania po wykorzystaniu kodu otrzymanego drogą SMS-ową, lub PUSH-notyfikacji w aplikacji mObywatel).

5.2.4 Kopie zapasowe klucza prywatnego

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.2.5 Archiwizowanie klucza prywatnego

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.2.6 Wprowadzanie klucza prywatnego do modułu kryptograficznego

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.2.7 Przechowywanie klucza prywatnego w module kryptograficznym

W zależności od typu modułu kryptograficznego klucze prywatne mogą być przechowywane w module w formie jawnej lub zaszyfrowanej. Niezależnie od formy przechowywania klucz prywatny nie jest dostępny z zewnątrz modułu kryptograficznego dla nieuprawnionych podmiotów.

5.2.8 Metody dezaktywacji klucza prywatnego

Nie dotyczy.

5.2.9 Metody niszczenia klucza prywatnego w usłudze zdalnego podpisu lub pieczęci

5.2.9.1 Usuwanie klucza do składania podpisu lub pieczęci

Po wygaśnięciu certyfikatu podpisu lub pieczęci klucze związane z tym certyfikatem są niszczone automatycznie przez usługę zdalnego podpisu lub pieczęci. Po unieważnieniu przez subskrybenta certyfikatu podpisu lub pieczęci klucze związane z tym certyfikatem są niszczone automatycznie przez usługę zdalnego podpisu lub pieczęci.
Subskrybent może zlecić zniszczenie swoich kluczy poprzez dostarczane oprogramowanie SimplySign Desktop dla Windows.

Zakończenie procesu podpisywania certyfikatem wydanym w procesie podpisywania skutkuje usunięciem klucza prywatnego, co uniemożliwia złożenie kolejnego podpisu z wykorzystaniem tego klucza.

Przerwanie procesu podpisywania po wydaniu certyfikatu wydawanego w procesie podpisywania skutkuje usunięciem klucza prywatnego, co uniemożliwia złożenie podpisu z wykorzystaniem tego klucza.

Niszczenie kluczy odbywa się jako autonomiczna operacja w jednej sesji i nie jest łączona z operacją podpisu lub pieczęci (oprócz kluczy certyfikatów wydawanych w procesie podpisywania).

5.2.9.2 Usuwanie klucza do składania podpisu lub pieczęcie poprzez usuwanie karty

Subskrybent może zawnioskować o zniszczenie jego karty z kilkoma kluczami poprzez zgłoszenie. Przy usuwaniu karty usuwane są wszystkie klucze znajdujące się na karcie.

5.2.9.3 Usuwanie klucza do składania podpisu lub pieczęcie poprzez niszczenie modułu kryptograficznego

Działanie po stronie usługi zdalnego podpisu lub pieczęci skutkuje usunięciem kluczy wszystkich subskrybentów rozmieszczonych na sprzętowym module HSM.

5.2.10 Ocena modułu kryptograficznego

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.3 Inne aspekty zarządzania kluczami

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.3.1 Archiwizacja kluczy publicznych

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.3.2 Okresy stosowania klucza publicznego i prywatnego

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

Okres ważności certyfikatu wydawanego w procesie podpisywania wynosi nie dłużej niż 1 dzień.

5.4 Dane aktywujące

Dane aktywujące podpis stosowane są do uaktywniania kluczy prywatnych stosowanych przez punkty rejestracji, urzędy certyfikacji oraz usługobiorców. Używane są na etapie uwierzytelnienia podmiotu i kontroli dostępu do klucza prywatnego.

5.4.1 Generowanie danych aktywujących i ich instalowanie

Dane aktywujące podpis są ustalane samodzielnie przez subskrybenta dla certyfikatów długookresowych.

Aktywacja złożenia podpisu certyfikatem wydawanym w procesie podpisywania realizowana jest przez usługobiorcę, który ma kontrolę nad całym procesem poprzez dysponowanie pod swoją wyłączną kontrolą telefonem komórkowym:

- poprzez PUSH notyfikacje po uwierzytelnieniu w aplikacji mObywatel (oficjalna rządowa aplikacja mobilna, która pozwala na bezpieczne potwierdzanie tożsamości),
- na ten telefon drogą SMS-wą otrzyma kod autoryzujący użycie klucza prywatnego zawartego w sprzętowym module kryptograficznym do złożenia podpisu.

5.4.2 Inne aspekty związane z danymi aktywującymi

Kod autoryzacyjny nie może ulec zmianie.

5.5 Zabezpieczenia systemu komputerowego

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.6 Kontrola techniczna

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.7 Zabezpieczenia sieci komputerowej

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.8 Znakowanie czasem

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

6 Profile certyfikatów i zaświadczeń certyfikacyjnych, list CRL, tokenów elektronicznego znacznika czasu

Wszystkie profile certyfikatów, certyfikatów dostawcy usług zaufania, tokenu statusu certyfikatu (token OCSP) zawarte są w Polityce Głównej. Certyfikaty wydawane są przez urząd Certum QCA 2017 oraz Certum QCA G3 R35.

Profil kwalifikowanych certyfikatów podpisu elektronicznego wydawanych w procesie podpisywania jest zgodny z formatami określonymi w normie ITU-T X.509 v3 oraz profilami zawartymi w ETSI EN 319 412 *Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1 – 5.*

7 Audyt zgodności i inne oceny

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

8 Inne kwestie biznesowe i prawne

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

Dodatkowo należy wskazać, że wszelkie kwestie biznesowe związane z wydawaniem certyfikatów (dotyczy certyfikatów, gdzie kluczy zarządzane zdalnie przez usługę) w momencie podpisywania regulowane są między Asseco Data Systems S.A. a BPPT lub Partnerem Biznesowym.

8.1 Opłaty

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

8.2 Odpowiedzialność finansowa

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

8.3 Poufność informacji biznesowej

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

8.4 Prywatność informacji osobowych

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

8.5 Prawo do własności intelektualnej

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

8.6 Zobowiązania i gwarancje

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

8.7 Wyłączenie odpowiedzialności z tytułu gwarancji

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

8.8 Ograniczenia odpowiedzialności

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

8.9 Odszkodowania

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

8.10 Okres obowiązywania

Niniejsza Polityka i Kodeks Świadczenia Kwalifikowanej Usługi Zaufania Certum „Zarządzanie kwalifikowanymi urządzeniami do składania podpisu/pieczęci elektronicznej na odległość" obowiązuje od daty wskazującej początek jej ważności do momentu opublikowania kolejnej aktualnej wersji. Zainteresowane strony mogą nadsyłać komentarze do proponowanych zmian w ciągu 7 dni roboczych od daty ich ogłoszenia (w sposób przedstawiony w rozdz. 9.12 w Polityce Głównej). Po upływie tego terminu, jeśli nie ma istotnych zastrzeżeń odnośnie merytorycznej zawartości proponowanych zmian, nowa wersja Polityki i Kodeksu Świadczenia Kwalifikowanej Usługi Zaufania Certum „Zarządzanie kwalifikowanymi urządzeniami do składania podpisu/pieczęci elektronicznej na odległość" staje się aktualna z datą ważności w niej wskazaną.

Decyzję
o zatwierdzeniu nowej wersji Polityki podejmuje osoba zarządzająca Certum. Wszystkie zmiany wprowadzane w dokumencie odnotowywane są w Historii dokumentu.

8.11 Indywidualne powiadamianie i komunikowanie się z użytkownikami

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

8.12 Procedura wprowadzania zmian

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

8.13 Warunki rozstrzygania sporów, reklamacje

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

8.14 Prawa właściwe

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

8.15 Zgodność z obowiązującym prawem

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

8.16 Przepisy różne

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

8.17 Postanowienia dodatkowe

8.17.1 Inne Polityki Certum

Niniejsza Polityka jest dokumentem bazującym i uzupełniającym „Politykę Certyfikacji i Kodeks Postępowania Certyfikacyjnego Kwalifikowanych Usług Certum".

Certum świadczy również inne kwalifikowane usługi zakres związany z tymi usługami zaadresowany został w Polityce Głównej.

9 Historia dokumentu

Historia zmian dokumentu		
1.0	15 Marca 2026 r.	Opracowanie dokumentu.

10 Słownik pojęć

Biznesowy Punkt Potwierdzania Tożsamości (BPPT) – jego funkcją jest weryfikacja i potwierdzanie tożsamości usługobiorcy w procesie wydawania kwalifikowanych certyfikatów podpisu w procesie podpisywania dokumentów (zazwyczaj umów) na potrzeby realizacji usługi świadczonej przez organizację odpowiedzialną za Biznesowy Punkt Potwierdzania Tożsamości. BPPT to punkty działające w ramach punktów rejestracji (PR) obok grupy Punktów Potwierdzania Tożsamości (np. placówki bankowe czy leasingowe), których charakter, zasięg i otwartość działania zależy od przyjętego modelu biznesowego między Certum a danym Partnerem Biznesowym.

Wydanie certyfikatu w procesie podpisywania – W celu zrealizowania procesu biznesowego u Partnera Biznesowego, niezbędne jest podpisanie dokumentów przez strony – Partnera Biznesowego i jego klienta. W tym celu, na potrzeby podpisania dokumentu (lub paczki dokumentów) wydawany jest certyfikat o krótkim okresie ważności, powiązany z kluczem prywatnym, który zostanie użyty do złożenia podpisów tylko w ramach procedowanego procesu biznesowego. Nie będzie możliwe użycie tego klucza do podpisania innych dokumentów niż te przedstawione klientowi do zapoznania się i przeznaczone do podpisu w trakcie procesu podpisywania.

Kod autoryzujący podpis - kod przesłany drogą SMS-ową, którego wprowadzenie autoryzuje użycie klucza prywatnego zawartego w sprzętowym module kryptograficznym (HSM) do złożenia podpisu elektronicznego.

Kod akceptacyjny - kod przesłany drogą SMS-ową, którego wprowadzenie oznacza akceptację wydania certyfikatu zgodnie z informacjami zawartymi w Oświadczeniu.