Polityka Certyfikacji i Kodeks Postępowania Certyfikacyjnego Kwalifikowanej Usługi Zaufania Certum – certyfikat wydany w procesie podpisywania

Wersja 1.1

Ważny od: 27 lipca 2021 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 Kwalifikowanej Usługi Zaufania Certum – certyfikat wydany w procesie podpisywania" dalej zwana **Polityką CISP** 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. Niniejszy dokument pełni także rolę Polityki Certyfikacji dla każdego z rodzajów kwalifikowanych

certyfikatów oraz usługi wydawania **kwalifikowanych certyfikatów w procesie podpisywania**, obejmującym rejestrację **usługobiorców** oraz certyfikację kluczy publicznych.

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*,

- normami, o których mowa w Decyzji Wykonawczej Komisji (UE) 2016/650 z dnia 25 kwietnia 2016 r. ustanawiające normy dotyczące oceny bezpieczeństwa kwalifikowanych urządzeń do składania podpisu i pieczęci na podstawie art. 30 ust. 3 i art. 39 ust. 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym,

- usługa wymienione powyżej w punkcie 1, tj.: usługi wydawania kwalifikowanych certyfikatów w procesie podpisywania jest świadczona 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, zwanym dalej w treści niniejszego dokumentu *Rozporządzeniem eIDAS*.

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

Obszary zastosowań kwalifikowanych certyfikatów wydawanych w procesie podpisywania, wydawanych zgodnie z niniejszym dokumentem opisane są w rozdz. 1.4. Zakres stosowania certyfikatów i certyfikatów dostawcy usług zaufania, z kolei odpowiedzialność wynikająca ze stosowania ich przez Certum oraz użytkowników końcowych – w rozdz. 9.8. Ograniczenia odpowiedzialności.

Struktura i merytoryczna zawartość Polityki CISP są zgodne z zaleceniem RFC 3647 *Certificate Policy and Certification Practice Statement Framework*. Spełnia on również wymagania normy ETSI EN 319 411-1 *Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements* oraz wymagania normy ETSI EN 319 411-2 *Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates*.

Niniejszy dokument został utworzony przy założeniu, że czytelnik jest ogólnie zaznajomiony z pojęciami dotyczącymi certyfikatów dostawcy usług zaufania, certyfikatów, podpisów 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 CISP opisuje zakres działań jaki po stronie Certum, punktów rejestracji, subskrybentów i stron ufających musi zostać podjęty, aby spełniać najwyższe standardy prawne i normalizacyjne.

Zakres związany z przedmiotowym punktem zaadresowany został Polityce Głównej.

1.2. Nazwa dokumentu i jego identyfikacja

Niniejszemu dokumentowi przypisuje się nazwę własną o następującej postaci: **Polityka Certyfikacji i Kodeks Postępowania Certyfikacyjnego Kwalifikowanej Usługi Zaufania Certum – certyfikat wydany w procesie podpisywania** 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: 1.2.616.1.113527.2.4.1.0.3.1.1)[2]:

> **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-cisp(3) version(1) 1}**

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

1.3. Strony Polityki CISP

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:

- urzędów,
- Głównego Punktu Rejestracji (GPR),
- punktów rejestracji (PR),
- osób potwierdzających tożsamość,
- subskrybentów,
- stron ufających.

Istotnym elementem do podkreślenia jest fakt, że w ramach punktów rejestracji (PR) możliwe jest działanie tzw. **Biznesowych Punktów Potwierdzania Tożsamości**, w skrócie zwanych dalej BPPT oraz **Partnerów Biznesowych** (np. placówki bankowe czy leasingowe), których charakter,

[2] Identyfikatora dokumentu Polityki CISP nie należy mylić z identyfikatorem polityki certyfikacji (tzw. identyfikatorem OID), umieszczanym w treści wystawianego certyfikatu (patrz rozdz. 1.3.1.1).

zasięg i otwartość działania zależy od przyjętego modelu biznesowego między Certum a danym Partnerem Biznesowym.

1.3.1. Urzędy Usług Zaufania

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

1.3.1.1. Kwalifikowany urząd certyfikacji Certum QCA 2017

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

1.3.1.2. Kwalifikowany urząd elektronicznego znacznika czasu CERTUM QTSA oraz Certum QTST

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

1.3.1.3. Kwalifikowany urząd weryfikacji statusu certyfikatu CERTUM QOCSP

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

1.3.1.4. Kwalifikowana usługa walidacji kwalifikowanych podpisów elektronicznych i kwalifikowanych pieczęci elektronicznych CERTUM QDVCS oraz Certum QESValidationQ 2017

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

1.3.2. Główny Punkt Rejestracji, Punkty Rejestracji oraz Punkty Potwierdzania Tożsamości

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

Dodatkowo Biznesowe Punkty Potwierdzania Tożsamości oraz Partnerzy Biznesowi działają na zasadach określonych w Polityce Głównej.

1.3.3. Subskrybenci

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

1.3.4. Strony ufające

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

1.3.5. Inne Strony

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

1.4. Zakres stosowania certyfikatów i certyfikatów dostawcy usług zaufania

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

1.4.1. Typy certyfikatów i certyfikatów dostawcy usług zaufania oraz zalecane obszary ich zastosowania

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

1.4.1.1. Kwalifikowane certyfikaty

W ramach niniejszej Polityki CISP wydawane są kwalifikowane certyfikaty podpisu elektronicznego typu osobisty (uniwersalny).

Informacje o typach certyfikatów oraz ich zastosowaniach zaadresowane zostały w Polityce Głównej.

1.4.1.2. Certyfikaty dostawców usług zaufania

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

1.4.1.3. Elektroniczny znacznik czasu

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

1.4.1.4. Poświadczenia statusu certyfikatu

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

1.4.1.5. Poświadczenia walidacji

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

1.4.2. Nierekomendowane zastosowanie certyfikatów

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej

1.5. Administracja Kodeksem Postępowania Certyfikacyjnego

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

1.5.4. Procedura zatwierdzania Polityki Certyfikacji i Kodeksu Postępowania Certyfikacyjnego

Procedura zatwierdzania niniejszej Polityki CISP 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 CISP 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 CISP 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

Ogólne zasady weryfikacji tożsamości subskrybentów, którymi kieruje się Certum w zakresie wydawania certyfikatów kwalifikowanych określa Polityka Główna.

Niezmienne są natomiast zasady określające typy informacji, które umieszczone są w treści certyfikatu kwalifikowanego jak i środki, które należy przedsięwziąć w celu uzyskania pewności, iż informacje te są dokładne i wiarygodne w momencie wydawania certyfikatu.

Weryfikacja przeprowadzana jest **obligatoryjnie** podczas rejestracji subskrybenta, która w przypadku Polityki CISP jest powiązana z procesem biznesowym klienta.

3.1. Nadawanie nazw

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

3.1.1. Typy nazw

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

3.1.2. Konieczność używania nazw znaczących

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

Certyfikaty wydawane zgodnie z niniejszą Polityką CISP są wydawane w Kategorii I.

3.1.3. Anonimowość subskrybenta

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

3.1.4. Zasady interpretacji różnych form nazw

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

3.1.5. Unikalność nazw

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

3.1.6. Rola znaków towarowych

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

3.2. Rejestracja i weryfikacja tożsamości

Rejestracja obejmuje szereg wewnętrznych procedur, które jeszcze przed wydaniem kwalifikowanego certyfikatu podpisu usługobiorcy mają na celu zgromadzenie przez punkt systemu rejestracji uwiarygodnionych danych o podmiocie, identyfikujących jego tożsamość oraz uprawnienia. Potwierdzenie tych danych realizowane może być zgodnie z art. 24.1) *Rozporządzenia eIDAS*.

Usługobiorca składa wniosek (Oświadczenie), które stanowi potwierdzenie prawdziwości jego danych i zgodę na przyporządkowanie do niego tych danych. Na podstawie tego wniosku Certum wydaje certyfikat.

Oświadczenie o wydanie nowego certyfikatu jest podpisywane przez operatora Punktu Potwierdzania Tożsamości z wykorzystaniem kwalifikowanego podpisu elektronicznego. Oświadczenie jest także podpisywane pieczęcią Certum. W powodzie podpisu znajduje się kod akceptacyjny, wprowadzony przez usługobiorcę.

Certyfikat stanowi zaświadczenie elektroniczne, które zawiera dane identyfikacyjne usługobiorcy oraz dane służące do sprawdzenia autentyczności podpisu elektronicznego. Podpis elektroniczny składany jest za pomocą danych zawartych (przechowywanych) w sprzętowym module kryptograficznym (HSM), nad użyciem których jedynie usługobiorca ma kontrolę poprzez wyłączną kontrolę nad telefonem komórkowym, na który otrzyma kod pozwalający użyć tych danych do złożenia podpisu.

Usługobiorca jest zobowiązany potwierdzić zapoznanie się z „Regulaminem kwalifikowanej usługi zaufania Certum – certyfikat wydany w procesie podpisywania" poprzez zaakceptowanie warunków świadczenia usługi zaufania.

3.2.1. Dowód posiadania klucza prywatnego

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

3.2.2. Uwierzytelnienie pełnomocnictw i innych atrybutów

Nie dotyczy.

3.2.3. Weryfikacja tożsamości osób fizycznych

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

3.2.3.1. Weryfikacja tożsamości przez upoważnionego przedstawiciela Certum

Potwierdzenie tożsamości usługobiorcy realizowane jest na podstawie ważnego dowodu osobistego lub paszportu za pośrednictwem Biznesowego Punktu Potwierdzania Tożsamości.

3.2.3.2. Weryfikacja tożsamości za pomocą systemu wideo-identyfikacji

Nie dotyczy.

3.2.3.3. Weryfikacja tożsamości przez notariusza

Nie dotyczy.

3.2.3.4. Weryfikacja tożsamości na podstawie kwalifikowanego podpisu elektronicznego

Nie dotyczy.

3.2.3.5. Weryfikacja tożsamości przy użyciu środka identyfikacji elektronicznej

Nie dotyczy.

3.2.4. Nieweryfikowane informacje usługobiorcy

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

3.2.5. Weryfikacja uprawnień

Nie dotyczy.

3.2.6. Kryteria współdziałania – kryteria interoperacyjne

Nie dotyczy.

3.3. Uwierzytelnienie w przypadku certyfikacji, aktualizacji kluczy lub modyfikacji danych w certyfikacie

Nie dotyczy.

3.3.1. Identyfikacja i uwierzytelnienie w przypadku standardowej aktualizacji kluczy

Nie dotyczy.

3.3.1.1. Certyfikacja i aktualizacja kluczy

Nie dotyczy

3.3.1.2. Modyfikacja danych w certyfikacie

Nie dotyczy.

3.3.2. Uwierzytelnienie w przypadku wydania certyfikatu po unieważnieniu

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

3.4. Uwierzytelnienie tożsamości usługobiorcy w przypadku unieważniania certyfikatu

Wniosek o unieważnienie certyfikatu może zostać złożony telefonicznie.

Weryfikacja tożsamości usługobiorcy oraz wniosku o unieważnienie certyfikatu przeprowadzana jest w Głównym Punkcie Rejestracji przez Inspektora ds. rejestracji.

Dokładny opis procedury unieważnienia certyfikatu jest zawarty w rodz. 4.9.3.

4. Wymagania funkcjonalne

Poniżej przedstawiono sposób realizacji usługi wydania certyfikatu w procesie podpisywania. Wydanie certyfikatu rozpoczyna się od złożenia przez usługobiorcę stosownego wniosku w systemie Biznesowego Punktu Potwierdzania Tożsamości. Składane wnioski powinny zawierać informacje, które są niezbędne do prawidłowego zidentyfikowania usługobiorcy oraz danych zawartych w składanym wniosku.

4.1. Składanie wniosków

4.1.1. Kto może składać wnioski o wydanie certyfikatu

Z wnioskami o wydanie certyfikatu może występować każda osoba fizyczna, która jest lub będzie podmiotem certyfikatu. Wniosek musi być uwierzytelniony przez uprawnionego przedstawiciela Certum, w tym przypadku operatora Biznesowego Punktu Potwierdzania Tożsamości.

Certum nie wydaje certyfikatów podmiotom wykonującym działalność gospodarczą w państwach, z którym prawo Rzeczpospolitej Polskiej zabrania prowadzenia wymiany handlowej.

4.1.2. Proces składania wniosków i związane z tym obowiązki

4.1.2.1. Wniosek o certyfikację

Wniosek o certyfikację składany jest przez usługobiorcę w Biznesowym Punkcie Potwierdzania Tożsamości. Do systemu wprowadzany jest przez operatora BPPT.

4.1.2.2. Wniosek o aktualizację kluczy lub modyfikację danych w certyfikacie

Nie dotyczy.

4.1.2.3. Wniosek o unieważnienie

Wniosek o unieważnienie certyfikatu składany jest przez usługobiorcę w trakcie rozmowy telefonicznej.

Wniosek musi być potwierdzony przez inspektora ds. rejestracji.

Zakres informacji, które należy podać w rozmowie jest następujący:

- Imię i nazwisko usługobiorcy,
- Numer telefonu usługobiorcy,
- Numer seryjny certyfikatu,

- Kod podpisujący.

O unieważnieniu certyfikatu usługobiorca jest informowany poprzez wiadomość tekstową SMS na numer telefonu podany we wniosku o wydanie certyfikatu.

4.2. Przetwarzanie wniosków

Po zweryfikowaniu tożsamości usługobiorcy zgodnie z rozdziałem 3.2 wysyłany jest wniosek certyfikacyjny do Certum celem wydania certyfikatu.

4.2.1. Realizacja funkcji identyfikacji i uwierzytelnienia

Funkcje identyfikacji i uwierzytelniania wszystkich wymaganych danych usługobiorcy są realizowane przez Główny Punkt Rejestracji oraz współpracujące Biznesowe Punkty Potwierdzania Tożsamości zgodnie z warunkami określonymi w rozdz. 1.3.2.

4.2.2. Przyjęcie lub odrzucenie wniosku

4.2.2.1. Procedura przyjęcia wniosku

Biznesowy Punkt Potwierdzania Tożsamości przyjmuje i weryfikuje wniosek o wydanie certyfikatu i przekazuje go do Głównego Punktu Rejestracji.

4.2.2.2. Odmowa wydania certyfikatu

Certum może odmówić wydania certyfikatu dowolnemu usługobiorcy bez zaciągania jakichkolwiek zobowiązań lub narażania się na jakąkolwiek odpowiedzialność, które powstać mogą wskutek poniesionych przez usługobiorcę (w wyniku odmowy) strat lub kosztów. Certum zwraca w takim przypadku usługobiorcy wniesioną przez niego opłatę za wydanie certyfikatu (jeśli dokonał stosownej przedpłaty), chyba że usługobiorca w oświadczeniu o wydanie certyfikatu umieścił sfałszowane lub nieprawdziwe dane.

Odmowa wydania certyfikatu może nastąpić w następujących przypadkach:

- wygasła sesja, podczas której miało nastąpić wydanie certyfikatu w procesie podpisywania,
- usługobiorca po raz trzeci wprowadził błędny kod autoryzujący podpis,
- stwierdzono niezgodność danych w oświadczeniu ze stanem faktycznym,
- stwierdzono naruszenie zobowiązań przez Partnera Biznesowego wynikających z nieprzestrzegania procedur Certum.

Odmowa wydania certyfikatu – gdy trafiają do Certum dane, na podstawie których generowane jest oświadczenie:

- stwierdzenie niezgodności danych w oświadczeniu ze stanem faktycznym,
- stwierdzenie naruszenia zobowiązań “partnera” wynikających z nieprzestrzegania procedur Certum.

4.2.3. Okres oczekiwania na wydanie certyfikatu

Certyfikat wydawany jest natychmiast od momentu złożenia poprawnie wypełnionego i zweryfikowanego wniosku.

4.3. Wydanie certyfikatu

Usługobiorca akceptuje wydanie certyfikatu poprzez użycie kodu akceptacyjnego.

4.3.1. Działania urzędu podczas wydania certyfikatu

Urząd certyfikacji weryfikuje wniosek i po stwierdzeniu jego poprawności wydaje certyfikat.

Każdy certyfikat wydawany jest w zamkniętej strefie wewnętrznej Asseco Data Systems S.A., do której nie ma dostępu z sieci globalnej.

4.3.2. Powiadomienie usługobiorcy o wydaniu certyfikatu

Operator Biznesowego Punktu Potwierdzania Tożsamości obsługujący wniosek informuje usługobiorcę o wydaniu certyfikatu niezwłocznie po jego wydaniu.

Moment złożenia jednorazowego podpisu, dla którego wydano certyfikat w procesie podpisywania, jest momentem, w którym usługobiorca otrzymuje swój certyfikat. Przerwanie procesu podpisywania skutkuje nieudostępnieniem certyfikatu usługobiorcy.

4.3.3. Akceptacja certyfikatu

Akceptacja certyfikatu realizowana jest w ramach procesu biznesowego w którym usługobiorca uczestniczy, poprzez weryfikację i akceptację danych (imię, nazwisko, numer dokumentu tożsamości) oraz podpisanie Oświadczenia z danymi usługobiorcy, które zostaną zamieszczone w certyfikacie, za których dokładne odzwierciedlenie w generowanym certyfikacie odpowiada Certum. Pozostałe informacje będące częścią certyfikatu są informacjami technicznymi, za które odpowiada Certum.

Akceptacja certyfikatu jest także jednoznaczna z oświadczeniem usługobiorcy, że zanim użył klucza publicznego zawartego w certyfikacie lub komplementarnego z nim klucza prywatnego w dowolnej operacji kryptograficznej, to dokładnie zapoznał się warunkami świadczenia przez Asseco Data Systems S.A. usługi zaufania zawartej w trakcie procedury rejestracji w punkcie systemu rejestracji.

4.3.4. Publikacja certyfikatu

Nie dotyczy.

4.3.5. Informowanie o wydaniu certyfikatu innych podmiotów

Nie dotyczy.

4.4. Stosowanie kluczy oraz certyfikatów

4.4.1. Stosowanie kluczy oraz certyfikatów usługobiorców

Usługobiorcy są zobowiązani do używania kluczy prywatnych i certyfikatów:

- zgodnie z ich zastosowaniem, określonym w niniejszej Polityce CISP i zgodnym z treścią certyfikatu (pól **keyUsage** oraz **extendedKeyUsage**, patrz rozdz. 7.1),
- zgodnie z treścią zaakceptowanych przez usługobiorcę warunków świadczenia przez Asseco Data Systems S.A. usług zaufania,

- tylko w okresie ich ważności,
- tylko do momentu unieważnienia certyfikatu.

Certum weryfikuje czy certyfikat, który jest powiązany z kluczem prywatnym usługobiorcy jest ważny w momencie składania podpisu.

4.4.2. Stosowanie kluczy oraz certyfikatów przez strony ufające

Strony ufające są zobowiązane do używania kluczy publicznych i certyfikatów:

- zgodnie z ich zastosowaniem, określonym w niniejszej Polityce CISP i zgodnym z treścią certyfikatu (pól **keyUsage** oraz **extendedKeyUsage**, patrz rozdz. 7.1),
- tylko po zweryfikowaniu ich statusu.

4.5. Recertyfikacja

Nie dotyczy.

4.5.1. Okoliczności recertyfikacji certyfikatu

Nie dotyczy.

4.5.2. Kto może wnioskować o recertyfikację certyfikatu

Nie dotyczy.

4.5.3. Przetwarzanie wniosku o recertyfikację

Nie dotyczy.

4.5.4. Powiadomienie subskrybenta o wydaniu nowego certyfikatu

Nie dotyczy.

4.5.5. Postępowanie w przypadku akceptacji recertyfikacji certyfikatu

Nie dotyczy.

4.5.6. Publikacja recertyfikacji certyfikatu

Nie dotyczy.

4.5.7. Powiadomienie o wydaniu certyfikatu innych podmiotów

Nie dotyczy.

4.6. Certyfikacja i aktualizacja kluczy

Nie dotyczy.

4.6.1. Przesłanki w przypadku certyfikacji i aktualizacji kluczy

Nie dotyczy.

4.6.2. Kto może wnioskować o nowy klucz publiczny

Nie dotyczy.

4.6.3. Przetwarzanie wniosku o certyfikację, aktualizację kluczy

Nie dotyczy.

4.6.4. Powiadomienie subskrybenta o wydaniu nowego certyfikatu

Nie dotyczy.

4.6.5. Potwierdzenie akceptacji nowego certyfikatu

Nie dotyczy.

4.6.6. Publikacja nowego certyfikatu

Nie dotyczy.

4.6.7. Powiadomienie o wydaniu certyfikatu innych podmiotów

Nie dotyczy.

4.7. Modyfikacja danych w certyfikacie

Nie dotyczy.

4.7.1. Okoliczności modyfikacji danych w certyfikacie

Nie dotyczy.

4.7.2. Kto może wnioskować o modyfikację danych w certyfikacie

Nie dotyczy.

4.7.3. Przetwarzanie wniosku o modyfikację danych w certyfikacie

Nie dotyczy.

4.7.4. Powiadomienie subskrybenta o wydaniu nowego certyfikatu

Nie dotyczy.

4.7.5. Potwierdzenie akceptacji zmodyfikowanych danych w certyfikacie

Nie dotyczy.

4.7.6. Publikacja certyfikatu ze zmodyfikowanymi danymi

Nie dotyczy.

4.7.7. Powiadomienie o wydaniu certyfikatu innych podmiotów

Nie dotyczy.

4.8. Unieważnienie i zawieszenie certyfikatu

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

Certum nie stosuje procedury zawieszenia certyfikatu dla certyfikatu wydanego w procesie podpisywania.

4.8.1. Okoliczności unieważnienia certyfikatu

W przypadku certyfikatów wydawanych zgodnie z Polityką CISP, wydane certyfikaty można unieważnić w dwóch przypadkach:

- gdy usługobiorca rezygnuje z podpisania dokumentów, które miał podpisać z wykorzystaniem usługi wydawania kwalifikowanych certyfikatów w procesie podpisywania;
- gdy podczas weryfikacji zawartości wydanego certyfikatu usługobiorca stwierdzi, że certyfikat zawiera nieprawidłowe dane.

4.8.2. Kto może żądać unieważnienia certyfikatu

Z żądaniem unieważnienia certyfikatu może wystąpić:

- usługobiorca, którego dane znajdują się w certyfikacie,
- autoryzowany przedstawiciel urzędu certyfikacji (w przypadku Certum rolę taką pełni Inspektor ds. Bezpieczeństwa),
- minister właściwy ds. informatyzacji.

4.8.3. Procedura unieważniania certyfikatu

Wniosek o unieważnienie certyfikatu może zostać złożony telefonicznie.

Usługobiorca dzwoniąc pod numer: +48 91 4801 360 składa wniosek o unieważnienie certyfikatu. Aby wniosek został skutecznie złożony, usługobiorca musi przekazać następujące dane:

- imię i nazwisko usługobiorcy,
- numer telefonu usługobiorcy (który podał we wniosku o wydanie certyfikatu),
- kod podpisujący,
- numer seryjny certyfikatu.

Inspektor ds. rejestracji, który odebrał wniosek o unieważnienie, weryfikuje wniosek. W przypadku pozytywnej weryfikacji, unieważnia certyfikat w ciągu 24 godzin od momentu przyjęcia wniosku. Informacja o unieważnionym certyfikacie jest dostępna w usłudze OCSP.

W przypadku negatywnej weryfikacji, certyfikat nie zostanie unieważniony.

Unieważniany certyfikat i komplementarny z nim klucz prywatny, przechowywane w sprzętowym module kryptograficznym HSM są w sposób nieodwracalny usunięte z tego nośnika. Operacja dokonywana jest automatycznie w trakcie realizacji zaakceptowanego przez Inspektora ds. rejestracji wniosku o unieważnienie certyfikatu.

4.8.4. Dopuszczalne okresy zwłoki w unieważnieniu certyfikatu

Certum gwarantuje, że maksymalne okresy zwłoki w przetwarzaniu wniosków o unieważnienie certyfikatów wynoszą 24 godziny.

4.8.5. Maksymalny dopuszczalny czas przetwarzania wniosku o unieważnienie

Wniosek o unieważnienie certyfikatu przetwarzany jest przez Certum w ciągu 24 godzin od momentu jego przyjęcia.

4.8.6. Obowiązek sprawdzania unieważnień przez stronę ufającą

Strona ufająca otrzymująca podpisany przez usługobiorcę dokument elektroniczny, zobowiązana jest do sprawdzenia w usłudze OCSP czy certyfikat klucza publicznego odpowiadający kluczowi prywatnemu, przy pomocy którego usługobiorca zrealizował podpis, nie został unieważniony.

Certum gwarantuje nieprzerwany dostęp do informacji o statusie certyfikatu w reżimie 24/7 (24 godziny / 7 dni w tygodniu).

4.8.7. Częstotliwość publikowania list CRL

Dla certyfikatów wydanych zgodnie z tą Polityką Certum nie publikuje list CRL.

4.8.8. Maksymalne opóźnienie w publikowaniu CRL

Nie dotyczy.

4.8.9. Dostępność weryfikacji unieważnień/statusu certyfikatu w trybie on-line

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

Dla certyfikatów wydanych zgodnie z tą polityką Certum nie publikuje list CRL.

4.8.10. Wymagania sprawdzania unieważnień w trybie on-line

Na stronę ufającą nie nakłada się obowiązku weryfikacji statusu certyfikatu w trybie on-line, realizowanej w oparciu o usługi i mechanizmy przedstawione w rozdz. 4.8.9. Dostępność weryfikacji unieważnień/statusu certyfikatu w trybie on-lineZaleca się jednak korzystanie z tej możliwości wtedy, gdy ryzyko zaakceptowania nieważnego lub sfałszowanego podpisu jest wysokie.

4.8.11. Inne dostępne formy ogłaszania unieważnień certyfikatów

Nie dotyczy.

4.8.12. Specjalne obowiązki w przypadku naruszenia ochrony aktualizacji kluczy

Nie dotyczy.

4.8.13. Okoliczności zawieszenia certyfikatu

Ta polityka nie dopuszcza zawieszania certyfikatu.

4.8.14. Kto może żądać zawieszenia certyfikatu

Nie dotyczy.

4.8.15. Procedura zawieszenia i odwieszania certyfikatu

Nie dotyczy.

4.8.16. Gwarantowany czas zawieszenia certyfikatu

Nie dotyczy.

4.8.17. Unieważnienie lub zawieszenie certyfikatu dostawcy usług zaufania urzędu certyfikacji

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

4.9. Pozostałe usługi

4.9.1. Charakterystyki operacyjne

4.9.1.1. Usługa znakowania czasem

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

4.9.1.2. Usługa walidacji kwalifikowanych podpisów elektronicznych i kwalifikowanych pieczęci elektronicznych

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

4.9.2. Dostępność usług

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

4.9.3. Funkcje opcjonalne

Nie dotyczy.

4.10. Zakończenie subskrypcji

Nie dotyczy.

4.11. Deponowanie i odtwarzanie kluczy

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

4.11.1. Zasady i praktyki depozytu i odzyskiwania kluczy

Nie dotyczy.

4.11.2. Enkapsulacja klucza sesji, polityka i praktyki przywracania

Nie dotyczy.

5. 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. podczas generowania kluczy, uwierzytelniania podmiotów, emisji certyfikatów, unieważniania certyfikatów i certyfikatów dostawcy usług zaufania audytu oraz wykonywania kopii zapasowych.

5.1. Zabezpieczenia fizyczne

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.1.1. Miejsce lokalizacji oraz budynek

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.1.2. Dostęp fizyczny

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.1.3. Zasilanie oraz klimatyzacja

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.1.4. Zagrożenie zalaniem

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.1.5. Ochrona przeciwpożarowa

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.1.6. Nośniki informacji

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.1.7. Niszczenie zbędnych nośników i informacji

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.1.8. Przechowywanie kopii bezpieczeństwa

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.1.9. Bezpieczeństwo punktów rejestracji

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.1.9.1. Miejsce lokalizacji oraz budynek

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.1.9.2. Dostęp fizyczny

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.1.9.3. Zasilanie oraz klimatyzacja

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.1.9.4. Zagrożenie wodne

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.1.9.5. Ochrona przeciwpożarowa

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.1.9.6. Nośniki informacji

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.1.9.7. Niszczenie informacji

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.1.9.8. Przechowywanie kopii bezpieczeństwa

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.1.10. Bezpieczeństwo subskrybenta

Za bezpieczeństwo danych aktywujących podpis odpowiada usługobiorca.

5.2. Zabezpieczenia organizacyjne

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.2.1. Zaufane role

5.2.1.1. Zaufane role w Certum

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.2.1.2. Zaufane role w punkcie systemu rejestracji

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.2.1.3. Zaufane role u subskrybenta

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.2.2. Liczba osób wymaganych do realizacji zadania

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.2.3. Identyfikacja oraz uwierzytelnianie ról

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.2.4. Role, które nie mogą być łączone

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.3. Nadzorowanie personelu

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.3.1. Kwalifikacje, doświadczenie oraz upoważnienia

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.3.2. Procedura weryfikacji personelu

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.3.3. Wymagania dotyczące przeszkolenia

Operatorzy BPPT muszą być przeszkoleni w zakresie procedury weryfikacji tożsamości oraz obsługi systemu wydawania certyfikatów w procesie podpisywania. Jeżeli Operator BPPT w swojej organizacji przechodził szkolenie w zakresie weryfikacji tożsamości i zakres szkolenia pokrywa w pełni zakres szkolenia przeprowadzanego przez Certum (np. szkolenia przeprowadzane przez banki dla swoich operatorów), nie jest potrzebne oddzielne szkolenie przeprowadzane przez Certum.

5.3.4. Częstotliwość powtarzania szkoleń oraz wymagania

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.3.5. Częstotliwość rotacji stanowisk i jej kolejność

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.3.6. Sankcje z tytułu nieuprawnionych działań

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.3.7. Pracownicy kontraktowi

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.3.8. Dokumentacja przekazana personelowi

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.4. Rejestrowanie zdarzeń, zarządzanie incydentami bezpieczeństwa oraz audyty bezpieczeństwa

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.4.1. Typy rejestrowanych zdarzeń

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.4.2. Częstotliwość analizy zapisów rejestrowanych zdarzeń (logów)

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.4.3. Okres przechowywania zapisów rejestrowanych zdarzeń

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.4.4. Ochrona zapisów rejestrowanych zdarzeń

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.4.5. Procedury tworzenia kopii zapisów rejestrowanych zdarzeń

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.4.6. System gromadzenia danych na potrzeby audytu (wewnętrzny a zewnętrzny)

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.4.7. Powiadamianie podmiotów odpowiedzialnych za zaistniałe zdarzenie

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.4.8. Oszacowanie podatności na zagrożenia

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.5. Archiwizowanie danych

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.5.1. Rodzaje archiwizowanych danych

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.5.2. Okres przechowywania archiwum

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.5.3. Ochrona archiwum

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.5.4. Procedury tworzenia kopii zapasowych

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.5.5. Wymaganie znakowania archiwizowanych danych elektronicznym znacznikiem czasu

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.5.6. System gromadzenia danych archiwalnych (wewnętrzny a zewnętrzny)

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.5.7. Procedury dostępu oraz weryfikacji zarchiwizowanej informacji

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.6. Zmiana klucza

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.7. Naruszenie ochrony klucza i uruchamianie po awariach oraz klęskach żywiołowych

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.7.1. Procedury obsługi incydentów i reagowania na zagrożenia

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.7.2. Uszkodzenie zasobów obliczeniowych, oprogramowania i/lub danych

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.7.3. Ujawnienie lub podejrzenie ujawnienia kluczy prywatnych urzędu certyfikacji

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.7.4. Zapewnienie ciągłości działania po katastrofach

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.8. Zakończenie działalności lub przekazanie zadań przez urząd certyfikacji

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej

5.8.1. Wymagania związane z przekazaniem obowiązków

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

5.8.2. Postępowanie w przypadku zakończenia działalności

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

6. Procedury bezpieczeństwa technicznego

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

6.1. Generowanie pary kluczy i jej instalowanie

6.1.1. Generowanie par kluczy

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

6.1.1.1. Generowanie klucza publicznego i prywatnego

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

6.1.1.1.1 Procedury generowania początkowych kluczy urzędu certyfikacji

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

6.1.1.1.2 Procedury aktualizacji kluczy urzędu certyfikacji

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

6.1.2. Przekazywanie klucza prywatnego użytkownikowi końcowemu

Klucze usługobiorców generowane są przez urząd certyfikacji w sprzętowym module kryptograficznym (HSM) i są udostępniane zdalnie usługobiorcy.

Certum umożliwia usługobiorcom 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.

Usługobiorcy kwalifikowanej usługi – certyfikat wydany w procesie podpisywania otrzymują dostęp do personalizowanych kart wirtualnych umieszczonych na sprzętowym module kryptograficznym. Personalizacja kart oznacza przygotowanie karty do użycia poprzez założenie struktury głównej karty, utworzenie profili, wygenerowanie unikalnego numeru karty. Tak utworzona karta pełni rolę bezpiecznego urządzenia, na którym będzie znajdował się certyfikat usługobiorcy. Proces personalizacji kart odbywa się w zabezpieczonym pomieszczeniu – do którego dostęp posiadają wyłącznie wskazani pracownicy spośród osób pełniących zaufane role – na kartach generowane są klucze kryptograficzne usługobiorców oraz numery identyfikacyjne kart, które automatycznie zapisywane są do bazy danych. Proces personalizacji kart odbywa się na urządzeniach nie podłączonych do sieci.

Dane do aktywowania karty, tj. kod przesłany drogą SMS-ową potrzebny do złożenia podpisu elektronicznego udostępniany jest usługobiorcom niezależnie od wydawanych certyfikatów.

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 skutkuje usunięciem klucza prywatnego, co uniemożliwia złożenie podpisu z wykorzystaniem tego klucza.

6.1.3. Przekazywanie klucza publicznego do urzędu certyfikacji

Nie dotyczy.

6.1.4. Przekazywanie klucza publicznego urzędu certyfikacji stronom ufającym

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

6.1.5. Długości kluczy

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

6.1.6. Parametry generowania klucza publicznego oraz weryfikacja jakości klucza

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

6.1.7. Zastosowania kluczy

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

6.1.8. Sprzętowe i/lub programowe generowanie kluczy

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

6.2. Ochrona klucza prywatnego

Klucze usługobiorców generowane i utrzymywane są w sprzętowym module kryptograficznym. Urząd certyfikacji (patrz rozdz. 6.1.1. Generowanie par kluczy), który generuje parę kluczy w

imieniu usługobiorcy, musi przekazać dostęp do pary kluczy w sposób bezpieczny oraz pouczyć usługobiorcę o zasadach ochrony klucza prywatnego (patrz rozdz. 6.1.2. Przekazywanie klucza prywatnego użytkownikowi końcowemu).

6.2.1. Standard modułu kryptograficznego

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

6.2.2. Podział klucza prywatnego na części

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

6.2.2.1. Akceptacja sekretu współdzielonego przez posiadacza sekretu

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

6.2.2.2. Zabezpieczenie sekretu współdzielonego

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

6.2.2.3. Dostępność oraz usunięcie (przeniesienie) sekretu współdzielonego

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

6.2.2.4. Odpowiedzialność posiadacza sekretu współdzielonego

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

6.2.3. Deponowanie klucza prywatnego

Klucze prywatne usługobiorców są przechowywane na sprzętowym module kryptograficznym i są dostępne jedynie dla usługobiorcy po wykorzystaniu kodu otrzymanego drogą SMS-ową, zgodnie z wewnętrzną procedurą Certum.

6.2.4. Kopie zapasowe klucza prywatnego

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

Certum nie przechowuje kopii kluczy prywatnych usługobiorców.

6.2.5. Archiwizowanie klucza prywatnego

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

6.2.6. Wprowadzanie klucza prywatnego do modułu kryptograficznego

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

6.2.7. 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.

6.2.8. Metody aktywacji klucza prywatnego

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

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

6.2.9. Metody dezaktywacji klucza prywatnego

Nie dotyczy.

6.2.10. Metody niszczenia klucza prywatnego

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

6.2.11. Ocena modułu kryptograficznego

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

6.3. Inne aspekty zarządzania kluczami

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

6.3.1. Archiwizacja kluczy publicznych

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

6.3.2. 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.

6.4. 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.

6.4.1. Generowanie danych aktywujących i ich instalowanie

Aktywacja złożenia podpisu realizowana jest przez usługobiorcę, który ma kontrolę nad całym procesem poprzez dysponowanie pod swoją wyłączną kontrolą telefonem komórkowym. Na ten telefon drogą SMS-wą otrzyma kod autoryzujący użycie klucza prywatnego zawartego w sprzętowym module kryptograficznym do złożenia podpisu.

6.4.2. Ochrona danych aktywujących

Pewność, że kod autoryzujący trafi do usługobiorcy jest zapewniona poprzez osobiste stawiennictwo usługobiorcy w BPPT i weryfikację tożsamości usługobiorcy realizowaną przez operatora BPPT.

6.4.3. Inne aspekty związane z danymi aktywującymi

Kod autoryzacyjny nie może ulec zmianie.

6.5. Zabezpieczenia systemu komputerowego

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

6.5.1. Wymagania techniczne dotyczące specyficznych zabezpieczeń systemów komputerowych

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

6.5.2. Ocena bezpieczeństwa systemów komputerowych

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

6.6. Kontrola techniczna

6.6.1. Nadzorowanie rozwoju systemu

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

6.6.2. Kontrola zarządzania bezpieczeństwem

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

6.6.3. Ocena cyklu życia zabezpieczeń

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

6.7. Zabezpieczenia sieci komputerowej

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

6.8. Znakowanie czasem

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

7. 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. W niniejszej Polityce zawarte zostały jedynie te elementy profilu certyfikatu wydawanego w procesie podpisywania, które są specyficzne dla tego profilu. Certyfikaty wydawane są przez urząd Certum QCA 2017.

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.*

7.1. Profile certyfikatu – Struktura certyfikatów i certyfikatów dostawcy usług zaufania

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

7.1.1. Treść certyfikatu i certyfikatu dostawcy usług zaufania

Treść certyfikatu dostawcy usług zaufania została przedstawiona w Polityce Głównej (rozdz. 7.1.1, Tab.15).

Tab.1. Profil podstawowych pól kwalifikowanego certyfikatu usługobiorcy wydanego w procesie podpisywania

Nazwa pola	Wartość lub ograniczenie wartości	
Version (wersja)	3	
Serial Number (numer seryjny)	Unikalne wartości we wszystkich certyfikatach wydawanych przez kwalifikowany urząd certyfikacji Certum QCA 2017.	
Signature Algorithm (algorytm podpisu)	SHA-512 z szyfrowaniem RSA *sha512WithRSAEncryption* (OID: 1.2.840.113549.1.1.13)	
Issuer (wystawca): Certum QCA 2017	Common Name (CN; Nazwa powszechna) =	Certum QCA 2017
	Organization (O; Organizacja) =	Asseco Data Systems S.A.
	Country (C; Kraj) =	PL
	Organization Identifier (2.5.4.97; Identyfikator organizacji) =	VATPL-5170359458
Subject (podmiot): Usługobiorca	Common Name (CN; Nazwa powszechna) =	Imię i nazwisko usługobiorcy
	Given Name (G; Imię) =	Imię usługobiorcy
	Surename (SN; Nazwisko) =	Nazwisko usługobiorcy
	Serial Number (Numer seryjny) =	Identyfikator dokumentu tożsamości usługobiorcy zapisany zgodnie z wymaganiami w ETSI EN 319 412-1 rozdział 5.1.3
	Country (C; Kraj) =	Kraj wydania dokumentu tożsamości usługobiorcy
Not before (ważny od; początek okresu ważności)	Podstawowy czas wg UTC (Universal Coordinate Time). Certum posiada własny zegar satelitarny, taktowany atomowym wzorcem sekundy (PPS). Stosowany w Certum zegar jest znany jako ogólnoświatowe wiarygodne źródło czasu klasy Stratum I.	
Not after (ważny do; koniec okresu ważności)		

Nazwa pola	Wartość lub ograniczenie wartości	
Subject Public Key Info (klucz publiczny podmiotu)	Algorytm	Szyfrowanie RSA *RSA encryption* (OID: 1.2.840.113549.1.1.1)
	Długość klucza	2048 bitów
	Wartość klucza publicznego	Wartość wyrażona w postaci ciągu bajtów
Signature (podpis certyfikatu)	Podpis certyfikatu jest generowany i kodowany: • zgodnie z polem "Algorytm podpisu", • przez Wystawcę w celu potwierdzenia związku klucza publicznego z Podmiotem.	

7.1.2. Numer wersji

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

7.1.3. Rozszerzenia a typy wydawanych certyfikatów lub certyfikatów dostawcy usług zaufania

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

7.1.3.1. Kwalifikowane certyfikaty

Tab.2. Pola rozszerzeń standardowych kwalifikowanego certyfikatu usługobiorcy wydanego w procesie podpisywania

Nazwa rozszerzenia	Wartość lub ograniczenie wartości	Status rozszerzenia
Authority Key Identifier (identyfikator klucza wydawcy certyfikatu)	Skrót SHA-1 z wartości klucza publicznego (OID: 2.5.29.35)	Niekrytyczne
Subject Key Identifier (identyfikator klucza podmiotu)	Skrót SHA-1 z wartości klucza publicznego (OID: 2.5.29.14)	Niekrytyczne
Basic Constraints (podstawowe ograniczenia)	Typ podmiotu=brak (użytkownik końcowy) Ograniczenie długości ścieżki certyfikacji=brak (OID: 2.5.29.19)	Krytyczne
Key Usage (użycie klucza)	Podpis cyfrowy (digital signature), bit 0 Zobowiązanie odnośnie treści (content commitment)[3], bit 1 (OID: 2.5.29.15)	Krytyczne
Subject Alternative Name (alternatywna nazwa podmiotu)	Inna nazwa = msisdn_uuid@simplysign.onthefly.pl[4] (OID: 1.2.616.1.113527.2.200.1)	Niekrytyczne
Authority Information Access (dostęp do informacji o urzędzie)	Protokół stanu certyfikatu online (OCSP) https://qca-2017.qocsp-certum.com (OID: 1.3.6.1.5.5.7.48.1) Urząd certyfikacji – wystawca https://repository.certum.pl/qca_2017.cer (OID: 1.3.6.1.5.5.7.48.2)	Niekrytyczne

[3] W standardzie ITU-T X.509 zmieniono nazwę tego bitu z „nonRepudiation” (niezaprzeczalność) na „contentCommitment” (zobowiązanie odnośnie treści).

[4] Wartość msisdn_uuid@simplysign.onthefly.pl nie jest rzeczywistym adresem e-mail. Jest to nazwa nadana usługobiorcy przez Certum, niezbędna do wydania certyfikatu w procesie podpisywania. Element "msisdn" to numer telefonu usługobiorcy, natomiast "uuid" to fragment unikalnego numeru transakcji wydania certyfikatu w procesie podpisywania.

Nazwa rozszerzenia	Wartość lub ograniczenie wartości	Status rozszerzenia
QC Statements (deklaracje wydawcy certyfikatu kwalifikowanego)	Oświadczenie, że certyfikat jest europejskim kwalifikowanym certyfikatem[5]: id-etsi-qcs-QcCompliance (OID: 0.4.0.1862.1.1) Oświadczenie, że klucz prywatny powiązany z certyfikatem umieszczony jest w kwalifikowanym urządzeniu do składania podpisów: id-etsi-qcs-QcSSCD (OID: 0.4.0.1862.1.4) Odniesienie do informacji o infrastrukturze klucza publicznego Certum QCA 2017: id-etsi-qcs-QcPDS (OID: 0.4.0.1862.1.5) EN: https://repository.certum.pl/PDS/Certum_QCA-PDS-CISP_EN.pdf PL: https://repository.certum.pl/PDS/Certum_QCA-PDS-CISP_PL.pdf Wskazanie, że certyfikat służy do składania podpisów: id-etsi-qct-esign (OID: 0.4.0.1862.1.6.1)	Niekrytyczne
Certificate Policies (polityka certyfikacji)	Polityka certyfikacji (OID: 2.5.29.32) 1.2.616.1.113527.2.4.1.15.1, 0.4.0.194112.1.2 (certyfikat kwalifikowany dla podpisu, HSM, krótkoterminowy, dla osoby fizycznej) Kwalifikator kwalifikowanej polityki certyfikacji https://www.certum.pl/repozytorium (OID: 1.3.6.1.5.5.7.2.1)	Krytyczne

7.1.3.2. Certyfikaty dostawcy usług zaufania

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

7.1.3.3. Wzajemne certyfikaty dostawców usług zaufania

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

[5] Jest to oświadczenie Asseco Data Systems S.A., że wydawane certyfikaty kwalifikowane są zgodne z wymaganiami Rozporządzenia eIDAS oraz Ustawy. Asseco Data Systems S.A. deklaruje dodatkowo w ten sposób zgodność wydawanych certyfikatów kwalifikowanych ze specyfikacją ETSI EN 319 422. Oświadczenie zawsze zawiera identyfikator obiektu o wartości: {itu-t(0) identified-organization(4) etsi(0) id-qc-profile(1862) 1 1}.

7.1.4. Typy stosowanego algorytmu tworzenia poświadczenia elektronicznego

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

7.1.5. Formy nazw

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

7.1.6. Ograniczenia nakładane na nazwy

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

7.1.7. Identyfikatory polityk certyfikacji

Urząd certyfikacji Certum QCA 2017 wydaje kwalifikowane certyfikaty w procesie podpisywania zgodne z polityką certyfikacji o identyfikatorze:

Certyfikaty kwalifikowane podpisu elektronicznego, HSM, krótkoterminowe - 1.2.616.1.113527.2.4.1.15.1

7.1.8. Stosowanie rozszerzenia określającego ograniczenia nakładane na politykę

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

7.1.9. Składnia i semantyka kwalifikatorów polityki

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

7.1.10. Przetwarzanie semantyki krytycznych rozszerzeń polityki certyfikacji

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

7.2. Profil listy certyfikatów unieważnionych (CRL)

Dla certyfikatów wydanych zgodnie z tą polityką Certum nie publikuje list CRL.

7.2.1. Numer wersji

Nie dotyczy.

7.2.2. Obsługiwane rozszerzenia dostępu do listy CRL

Nie dotyczy.

7.2.3. Unieważnienie kwalifikowanego certyfikatu lub certyfikatu dostawcy usług zaufania a listy CRL

Unieważnienie kwalifikowanego certyfikatu wydanego w procesie podpisywania - nie dotyczy.

Unieważnianie certyfikatów dostawcy usługi zaufania i umieszczanie ich na listach CRL zostało zaadresowane w Polityce Głównej.

7.3. Profil tokena statusu certyfikatu (token OCSP)

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

7.3.1. Numer wersji

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

7.3.2. Obsługiwane rozszerzenia

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

7.4. Inne profile

7.4.1. Profil tokena elektronicznego znacznika czasu

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

7.4.2. Profil tokena walidacji podpisów elektronicznych i pieczęci elektronicznych

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

7.4.3. Profile tokenów weryfikacji statusu certyfikatów

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

8. Audyt zgodności i inne oceny

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

8.1. Częstotliwość i okoliczności audytu

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

8.2. Tożsamość/kwalifikacje audytora

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

8.3. Związek audytora z audytowaną jednostką

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

8.4. Zagadnienia obejmowane przez audyt

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

8.5. Podejmowane działania w celu usunięcia rozbieżności wykrytych podczas audytu

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

8.6. Informowanie o wynikach audytu

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9. 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 w momencie podpisywania regulowane są między Asseco Data Systems S.A. a BPPT lub Partnerem Biznesowym.

9.1. Opłaty

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.1.1. Opłaty za wydanie certyfikatu

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.1.2. Opłaty za dostęp do certyfikatów i certyfikatów dostawcy usług zaufania

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.1.2.1. Opłaty za znaczniki czasu, inne tokeny i poświadczenia

Nie dotyczy.

9.1.3. Opłaty za unieważnienie i informacje o statusie kwalifikowanego certyfikatu

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.1.4. Opłaty za inne usługi

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.1.5. Zwrot opłat

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.2. Odpowiedzialność finansowa

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.2.1. Zakres ubezpieczenia

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.2.2. Inne aktywa

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.2.3. Rozszerzony zakres gwarancji

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.3. Poufność informacji biznesowej

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.3.1. Zakres poufności informacji

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.3.2. Informacje znajdujące się poza zakresem poufności informacji

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.3.3. Obowiązek ochrony poufności informacji

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.4. Prywatność informacji osobowych

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.4.1. Polityka prywatności

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.4.2. Informacje uważane za prywatne

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.4.3. Informacja nieuważana za prywatną

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.4.4. Odpowiedzialność za ochronę informacji prywatnej

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.4.5. Zastrzeżenia i zezwolenie na użycie informacji prywatnej

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.4.6. Udostępnianie informacji zgodnie z nakazem sądowym lub administracyjnym

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.4.7. Inne okoliczności ujawniania informacji

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.5. Prawo do własności intelektualnej

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.5.1. Znak towarowy

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.6. Zobowiązania i gwarancje

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.6.1. Zobowiązania i gwarancje urzędu certyfikacji

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.6.1.1. Zobowiązania urzędu elektronicznego znacznika czasu

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.6.1.2. Zobowiązania urzędu weryfikacji statusu certyfikatu i walidacji danych

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.6.1.3. Zobowiązania repozytorium urzędu certyfikacji

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.6.2. Zobowiązania i gwarancje Punktów Rejestracji

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.6.3. Zobowiązania i gwarancje subskrybenta

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.6.4. Zobowiązania i gwarancje stron ufających

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.6.5. Zobowiązania i gwarancje innych użytkowników

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.7. Wyłączenie odpowiedzialności z tytułu gwarancji

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.8. Ograniczenia odpowiedzialności

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.8.1. Odpowiedzialność Certum

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.8.1.1. Odpowiedzialność urzędu certyfikacji Certum QCA 2017

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.8.1.2. Odpowiedzialność urzędu elektronicznego znacznika czasu

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.8.1.3. Odpowiedzialność urzędu weryfikacji statusu certyfikatów, urzędu walidacji danych

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.8.1.4. Odpowiedzialność repozytorium urzędu certyfikacji

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.8.1.5. Odpowiedzialność subskrybentów

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.8.1.6. Odpowiedzialność strony ufającej

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.9. Odszkodowania

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.9.1. Odszkodowanie z tytułu odpowiedzialności cywilnej subskrybenta

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.9.2. Odszkodowanie z tytułu odpowiedzialności cywilnej strony ufającej

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.10. Okres obowiązywania Polityki Certyfikacji i Kodeksu Postępowania Certyfikacyjnego oraz jego ważność

9.10.1. Okres obowiązywania

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.10.2. Wygaśnięcie ważności

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.10.3. Skutki wygaśnięcia ważności Polityki i Kodeksu i okres przejściowy

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.11. Indywidualne powiadamianie i komunikowanie się z użytkownikami

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.12. Procedura wprowadzania zmian

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.12.1. Procedura wnoszenia poprawek

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.12.1.1. Zmiany nie wymagające informowania

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.12.2. Mechanizm powiadamiania oraz okres oczekiwania na komentarze

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.12.2.1. Okres oczekiwania na komentarze

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.12.3. Okoliczności wymagające zdefiniowania nowego identyfikatora polityki

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.12.4. Dystrybucja nowej wersji Polityki Certyfikacji i Kodeksu Postępowania Certyfikacyjnego oraz Regulaminu Kwalifikowanych Usług Zaufania

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.12.5. Elementy nie publikowane w Polityce Certyfikacji i Kodeksie Postępowania Certyfikacyjnego

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.13. Warunki rozstrzygania sporów, reklamacje

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.14. Prawa właściwe

9.14.1. Ciągłość postanowień

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.14.2. Odniesienia do przepisów

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.15. Zgodność z obowiązującym prawem

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.16. Przepisy różne

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.16.1. Kompletność warunków umowy

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.16.2. Cesja praw

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.16.3. Rozłączność postanowień

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.16.4. Klauzula wykonalności

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.16.5. Siła wyższa

Zakres związany z przedmiotowym punktem zaadresowany został w Polityce Głównej.

9.17. Postanowienia dodatkowe

9.17.1 Inne Polityki Certum

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

Certum świadczy również kwalifikowane usługi walidacji i konserwacji opisane w „Polityce kwalifikowanej usługi walidacji i kwalifikowanej usługi konserwacji kwalifikowanych podpisów i pieczęci elektronicznych (Certum QESValidationQ).

10. Historia dokumentu

Historia zmian dokumentu		
1.0	30 Grudnia 2020 r.	Opracowanie dokumentu.
1.1	27 lipca 2021	Naniesie poprawek po uwagach audytowych zgodności z eIDAS, zmiana adresu siedziby Asseco Data Systems S.A. i inne poprawki edytorskie.

11. 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.

Polityka Certyfikacji i Kodeks Postępowania Certyfikacyjnego Kwalifikowanej Usługi Zaufania Certum – certyfikat wydany w procesie podpisywania (Polityka CISP) - niniejszy dokument bazujący i uzupełniający „Politykę Certyfikacji i Kodeks Postępowania Certyfikacyjnego Kwalifikowanych Usług Certum" zwaną Polityką Główną, która określa ogólne zasady stosowane przez Certum w trakcie świadczenia kwalifikowanych usług zaufania. Niniejszy dokument pełni także rolę Polityki Certyfikacji dla każdego z rodzajów kwalifikowanych certyfikatów oraz usługi wydawania kwalifikowanych certyfikatów w procesie podpisywania, obejmującym rejestrację usługobiorców oraz certyfikację kluczy publicznych.

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.