Informacja o infrastrukturze klucza publicznego Certum

Wersja 1.6

Data: 01 Sierpnia 2017 r.

Status: aktualny

Asseco Data Systems S.A.
ul. Podolska 21
81-321 Gdynia
„Certum – Powszechne Centrum Certyfikacji”
ul. Bajeczna 13
71-838 Szczecin
https://certum.pl
https://certum.eu

Spis treści

1. Dane adresowe

Asseco Data Systems S.A.
ul. Podolska 21
81-321 Gdynia

Certum – Powszechne Centrum Certyfikacji
ul. Bajeczna 13
71-838 Szczecin
strona WWW: https://certum.pl

2. Rodzaje certyfikatów, zastosowanie i procedury weryfikacji

Typ certyfikatu

Niniejsza deklaracja dotyczy wyłącznie kwalifikowanych usług zaufania oraz elektronicznego znacznika czasu świadczonych przez Certum – Powszechne Centrum Certyfikacji, zwanego dalej CERTUM PCC.
W ramach usług kwalifikowanych działa kwalifikowany urząd certyfikacji **CERTUM QCA** oraz **Certum QCA 2017**, który wydaje kwalifikowane certyfikaty klucza publicznego elektronicznych podpisów i pieczęci, kwalifikowany urząd elektronicznego znacznika czasu **CERTUM QTSA** oraz **Certum QTST 2017**, który wystawia tokeny elektronicznego znacznika czasu, kwalifikowany urząd **CERTUM QDVCS** oraz **Certum QESValidationQ 2017**, który wystawia elektroniczne poświadczenia o ważności kwalifikowanego certyfikatu klucza publicznego, kwalifikowanego podpisu elektronicznego, kwalifikowanej pieczęci elektronicznej.
Profil oraz jakiekolwiek ograniczenia kwalifikowanego certyfikatu klucza publicznego elektronicznych podpisów i pieczęci wydanego przez **CERTUM QCA** oraz **Certum QCA 2017** są zgodne ze specyfikacją ETSI EN 319 412.
Profil oraz jakiekolwiek ograniczenia elektronicznego znacznika czasu wystawianego przez **CERTUM QTSA** oraz **Certum QTST 2017** są zgodne ze specyfikacją ETSI EN 319 422.
Usługa **CERTUM QDVCS** oraz **Certum QESValidationQ 2017** wystawia token walidacji, który ma strukturę zgodną z RFC 3029 (rozdział 9).

Weryfikacja

Certyfikat kwalifikowany wydawany jest osobie fizycznej na podstawie weryfikacji jej tożsamości. Weryfikacja osób fizycznych, może być realizowana w punkcie systemu rejestracji, przez notariusza lub osobę upoważnioną do potwierdzenia tożsamości właściciela certyfikatu.
Osoba ubiegająca się o certyfikat kwalifikowany musi stawić się do weryfikacji w bezpośrednim spotkaniu z osobą upoważnioną.
Potwierdzenie tożsamości właściciela certyfikatu oraz osoby występującej o pieczęć elektroniczną w imieniu podmiotu, realizowane jest na podstawie ważnych dokumentów:

- dowodu osobistego lub
- paszportu,

oraz dodatkowo, w przypadku gdy osoba fizyczna występuje o certyfikat w imieniu podmiotu lub w przypadku osoby fizycznej występującej o pieczęć elektroniczną w imieniu podmiotu:

- stosownego upoważnienia wystawionego przez daną organizację do reprezentowania jej interesów i umieszczenie danych organizacji w certyfikacie lub pieczęci elektronicznej,
- aktualnego wypisu z Krajowego Rejestru Sądowego lub wpisu z Centralnej Ewidencji i Informacji o Działalności Gospodarczej.

Weryfikacja odbiorców usług świadczonych przez urząd elektronicznego znacznika czasu oraz urząd walidacji odbywa się na podstawie podpisu elektronicznego, opcjonalnie przez osobę potwierdzającą tożsamość zgodnie z zasadami opisanymi przy weryfikacji osób ubiegających się o certyfikat kwalifikowany.

Zastosowanie

Kwalifikowane certyfikaty wystawione przez kwalifikowany urząd certyfikacji **CERTUM QCA** oraz **Certum QCA 2017** muszą być używane zgodnie z wymaganiami Ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. z 2016 r. poz. 1579). Oznacza to, że mogą być stosowane wyłącznie do weryfikowania bezpiecznych podpisów, które są niezaprzeczalnym dowodem złożenia aktu woli i powiązania z podpisywaną informacją o różnym poziomie wrażliwości.
Kwalifikowane certyfikaty wystawione przez kwalifikowany urząd certyfikacji **CERTUM QCA** oraz **Certum QCA 2017** pozostają w zgodności z postanowieniami *Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylająca dyrektywę 1999/93/WE.*
Urząd elektronicznego znacznika czasu **CERTUM QTSA** oraz **Certum QTST 2017** wystawia tokeny elektronicznego znacznika czasu, które wywołują w szczególności skutki prawne daty pewnej w rozumieniu przepisów Kodeksu cywilnego (Art.81, §2 pkt.3). Głównym zastosowaniem elektronicznych znaczników czasu jest oznaczanie czasem kwalifikowanych podpisów elektronicznych w przypadku ich długookresowej ważności. Elektroniczne znaczniki czasu wystawiane przez urząd **CERTUM QTSA** oraz **Certum QTST 2017** mogą być używane także w dowolnych innych przypadkach, wymagających porównywalnej jakości takiej usługi.
Usługa kwalifikowanego elektronicznego znacznika czasu 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 eIDAS.*

Usługa walidacji kwalifikowanych podpisów elektronicznych i kwalifikowanych pieczęci elektronicznych **CERTUM QDVCS** oraz **Certum QESValidationQ 2017** wystawia elektroniczne poświadczenia o ważności kwalifikowanego certyfikatu klucza publicznego, kwalifikowanego podpisu elektronicznego, kwalifikowanej pieczęci elektronicznej.
Kwalifikowana usługa walidacji kwalifikowanych podpisów elektronicznych i kwalifikowanych pieczęci elektronicznych 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 eIDAS.*

3. Ograniczenia odpowiedzialności

Odpowiedzialność finansowa Asseco Data Systems S.A., w imieniu której CERTUM PCC świadczy kwalifikowane usługi, w stosunku do jednego zdarzenia wynosi równowartość w złotych 250.000 Euro, ale nie więcej niż 1.000.000 Euro w odniesieniu do wszystkich takich

zdarzeń. Odpowiedzialność finansowa dotyczy okresów 12-miesięcznych zgodnych z rokiem kalendarzowym.

W celu nadzoru nad sprawnym działaniem systemu CERTUM PCC, rozliczania użytkowników oraz personelu z ich działań, rejestrowane są wszystkie zdarzenia występujące w systemach CERTUM PCC, które mają istotny wpływ na bezpieczeństwo funkcjonowania CERTUM PCC. Rejestrowane zdarzenia obejmują między innymi: czynności związane z rejestracją, certyfikacją, aktualizacją, unieważnianiem i zawieszaniem certyfikatów, wystawianiem znacznika czasu, walidacją danych, weryfikacją statusu certyfikatu a także generowanie kluczy dla potrzeb urzędów CERTUM PCC oraz wszystkie zdarzenia występujące w systemie, które maja istotny wpływ na bezpieczeństwo funkcjonowania CERTUM PCC.

4. Zobowiązania Subskrybenta

Poprzez własnoręczne podpisanie wniosku o wydanie certyfikatu oraz zawarcie umowy na świadczenie usług certyfikacyjnych subskrybent wyraża zgodę na przystąpienie do systemu certyfikacji na warunkach określonych w Umowie, Polityce Certyfikacji i Kodeksie Postępowania Certyfikacyjnego oraz Regulaminie Kwalifikowanych Usług Zaufania CERTUM PCC.

Subskrybent zobowiązany jest do:

- przestrzegania postanowień umowy podpisanej z Asseco Data Systems S.A.,
- dostarczenia urzędowi certyfikacji prawdziwych i poprawnych informacji na każdym etapie współpracy,
- dostarczenia dokumentów potwierdzających prawdziwość danych zawartych we wniosku certyfikacyjnym,
- niezwłocznego poinformowania CERTUM PCC o jakichkolwiek błędach lub wadach w jego certyfikacie lub o zmianach danych w nim zawartych,
- używania swojej pary kluczy i kluczy publicznych innych odbiorców usług certyfikacyjnych wyłącznie w sposób zgodny z Polityką Certyfikacji i Kodeksem Postępowania Certyfikacyjnego oraz zapewnienia bezpieczeństwa i integralności własnych kluczy prywatnych, włączając w to:
    - kontrolę i zabezpieczenie dostępu do urządzeń zawierających jego klucze prywatne,
    - niezwłocznego informowania urzędu certyfikacji o wszelkich okolicznościach, w wyniku których jego klucz prywatny został ujawniony osobom trzecim lub w wyniku których subskrybent może podejrzewać, że klucz prywatny mógł ulec ujawnieniu osobom trzecim,
    - niezwłocznego informowania urzędu certyfikacji o utracie karty z certyfikatem lub utracie kodu PIN,
- zabezpieczenia i ochrony dostępu do nośników, na których przechowywane są hasła i klucze,

- traktowania utraty lub ujawnienia (przekazanie innej nieupoważnionej do tego osobie) hasła na równi z utratą lub ujawnieniem (przekazaniem innej nieupoważnionej do tego osobie) klucza prywatnego,
- w przypadku naruszenia ochrony (lub podejrzenia naruszenia ochrony) swojego klucza prywatnego niezwłocznie przystępuje do procedury unieważnienia certyfikatu,
- zaprzestania posługiwania się unieważnionym, zawieszonym lub nieważnym certyfikatem,
- wykorzystywania certyfikatu kwalifikowanego i odpowiadającego mu klucza prywatnego tylko zgodnie z deklarowanym w certyfikacie przeznaczeniem, celami i ograniczeniami określonymi w niniejszym dokumencie.

Ograniczenia w stosowaniu podpisu elektronicznego:

- nie składania podpisu elektronicznego lub pieczęci elektronicznej przy pomocy należącego do niego klucza prywatnego, jeżeli certyfikat ten jest przeterminowany (minął jego okres ważności), jest unieważniony lub zawieszony,
- nie przechowywania karty kryptograficznej zawierającej klucz prywatny razem z osobistym numerem identyfikacyjnym (PIN),
- nie udostępniania i nie przekazywania swoich kluczy prywatnych oraz używanych przez siebie haseł osobom trzecim.

Subskrybent pobierający token znacznika czasu, powinien zweryfikować podpis cyfrowy urzędu oraz sprawdzić listę CRL, pod kątem unieważnienie certyfikatu urzędu.

5. Zobowiązania stron ufających

Stroną ufającą, korzystającą z usług CERTUM PCC jest dowolny podmiot, który akceptuje kwalifikowany podpis i pieczęć elektroniczną, która może być w jakikolwiek sposób uzależniona od:

- ważności lub aktualności powiązania pomiędzy tożsamością subskrybenta a należącym do niego kluczem publicznym, potwierdzonym certyfikatem przez kwalifikowany urząd certyfikacji **CERTUM QCA** oraz **Certum QCA 2017**, lub
- powiązania podpisu lub pieczęci elektronicznej z tokenem elektronicznego znacznika czasu, wydanym przez kwalifikowany urząd elektronicznego znacznika czasu **CERTUM QTSA** oraz **Certum QTST 2017**, lub
- aktualnego statusu certyfikatu wystawionego przez kwalifikowany urząd weryfikacji statusu certyfikatu **CERTUM QOCSP**,
- tokena walidacji wystawionego przez kwalifikowaną usługę **CERTUM QDVCS** oraz **Certum QESValidationQ 2017**.

Strona ufająca zobowiązana jest do:

- zweryfikowania, czy podpis elektroniczny lub pieczęć elektroniczna została zrealizowany za pomocą klucza prywatnego odpowiadającego kluczowi publicznemu zawartemu w certyfikacie kwalifikowanym subskrybenta lub urzędu certyfikacji,

- zweryfkowania, czy podpisana wiadomość (dokument) lub certyfikat nie zostały zmodyfikowane po złożeniu na nim podpisu,
- właściwego i prawidłowego realizowania operacji kryptograficznych przy użyciu oprogramowania i sprzętu, których poziom bezpieczeństwa jest zgodny z poziomem wrażliwości przetwarzanej informacji i poziomem wiarygodności stosowanych certyfikatów,
- uznania certyfikatu podpisu elektronicznego lub pieczęci za nieważny, jeśli przy użyciu posiadanego oprogramowania i sprzętu nie można rozstrzygnąć czy podpis elektroniczny lub certyfikat są ważne lub uzyskany wynik weryfikacji jest negatywny,
- zaufania tylko tym certyfikatom kwalifikowanym, które używane są zgodnie z deklarowanym przeznaczeniem oraz są odpowiednie do zastosowań w obszarach, które wcześniej określiła strona ufająca, a także tych, których status został zweryfikowany w oparciu o aktualne listy unieważnionych certyfikatów (CRL) lub usługę weryfikacji certyfikatów kwalifikowanych w trybie on-line (OCSP),
- zweryfikowania, czy token, poświadczenie zostały prawidłowo poświadczone elektronicznie oraz czy klucz prywatny użyty przez kwalifikowany urząd elektronicznego znacznika czasu **CERTUM QTSA** oraz **Certum QTST 2017**, kwalifikowaną usługę walidacji **CERTUM QDVCS** oraz **Certum QESValidationQ 2017** nie był ujawniony aż do momentu weryfikacji tokena, poświadczenia (chyba, że zawarty w nich czas spełnia wymagania daty pewnej); status klucza prywatnego można zweryfikować w oparciu o weryfikację komplementarnego z nim klucza publicznego,
- zweryfikowania czy czas w nich zawarty spełnia wymagania daty pewnej. Status klucza prywatnego może zostać zweryfikowany w oparciu o weryfikację uzupełniającego klucza publicznego.

6. Odpowiedzialność CERTUM PCC

CERTUM PCC nie ponosi odpowiedzialności za działania stron trzecich, subskrybentów oraz innych stron nie związanych z CERTUM PCC. W szczególności, urząd certyfikacji nie odpowiada:

- za szkody powstałe na skutek działania siły wyższej lub innych, za których wystąpienie nie ponosi odpowiedzialności, tj.: pożaru, powodzi, wichury, wojny, aktów terroru, epidemii oraz innych klęsk naturalnych lub spowodowanych przez człowieka,
- za szkody powstałe na skutek instalacji, użytkowania oraz zarządzania aplikacjami innymi niż dostarczone przez CERTUM PCC,
- za szkody powstałe na skutek niewłaściwego stosowania wydanych certyfikatów, przy czym przez słowo niewłaściwe należy rozumieć używanie certyfikatu przeterminowanego, unieważnionego lub zawieszonego,
- w przypadku podania przez subskrybenta fałszywych danych i – mimo zachowania przez CERTUM PCC należytej staranności – umieszczenie ich na jego wniosek

zarówno w bazach CERTUM PCC, jak też w wydanym mu certyfikacie kwalifikowanym.

7. Polityka Certyfikacji i Kodeks Postępowania Certyfikacyjnego, Umowy, Regulamin

CERTUM PCC publikuje w serwisie internetowym w repozytorium dostępnym pod adresem: http://www.certum.pl/m.in.: następujące dokumenty:

- Polityka Certyfikacji i Kodeks Postępowania Certyfikacyjnego Kwalifikowanych Usług CERTUM PCC,
- Regulamin Kwalifikowanych Usług Zaufania CERTUM PCC,
- wzory umów.

8. Polityka Prywatności

Dane Subskrybenta są przetwarzane przez Asseco Data Systems S.A., zgodnie z Ustawą o ochronie danych osobowych (Dz.U. z 2016 poz. 922, tekst jednolity ustawy). Subskrybentom przysługuje prawo do wglądu i poprawienia przekazanych danych osobowych. Polityka Prywatności dostępna jest pod adresem:

http://www.certum.pl/certum/cert,onas_informacje_prawne.xml

9. Zwrot opłat

CERTUM PCC dokłada wszelkich starań, aby świadczone usługi były na najwyższym poziomie. Subskrybent może żądać zwrotu wniesionej opłaty, jeżeli usługa certyfikacyjna była wykonana niezgodnie z zasadami wynikającymi z umowy, Polityki Certyfikacji i Kodeksu Postępowania Certyfikacyjnego i postanowień niniejszego dokumentu.

10. Prawo oraz Rozstrzyganie sporów

Funkcjonowanie CERTUM PCC oparte jest na zasadach zawartych w Polityce Certyfikacji i Kodeksie Postępowania Certyfikacyjnego oraz obowiązujących na terytorium Polski przepisach prawa.
Spory związane z kwalifikowanymi usługami certyfikacyjnymi świadczonymi przez CERTUM PCC będą w pierwszej kolejności rozstrzygane na drodze postępowania pojednawczego.
W przypadku braku rozstrzygnięcia sporu w terminie 45 dni od rozpoczęcia postępowania pojednawczego, stronom przysługuje prawo do wystąpienia na drogę sądową. Sądem właściwym do rozpoznania sprawy będzie Sąd Powszechny właściwy dla pozwanego.
W przypadku wystąpienia innych sporów będących konsekwencją użycia certyfikatu wydanego lub innych kwalifikowanych usług świadczonych przez CERTUM PCC, subskrybent zobowiązuje się pisemnie poinformować CERTUM PCC o przedmiocie powstałego sporu.

11. Audyt

Audyty sprawdzające prawidłowość i zgodność z uregulowaniami proceduralnymi i prawnymi (przede wszystkim zgodność z Polityką Certyfikacji i Kodeksem Postępowania Certyfikacyjnego) są wykonywane na podstawie art. 20 eIDAS. Zaudytowane kwalifikowane usługi świadczone przez CERTUM PCC znajdują się na zaufanej liście – lista TSL (lista zawierająca informacje dotyczące kwalifikowanych dostawców usług zaufania, wraz z informacjami dotyczącymi świadczonych usług zaufania, zgodnie z przepisami Rozporządzenia eIDAS).
Usługi świadczone przez CERTUM PCC podlegają corocznemu audytowi w zakresie Zintegrowanego Systemu Zarządzania na zgodność z normami PN-EN ISO:9001:2009 oraz PN ISO/IEC 27001:2014.

12. Identyfikacja dokumentu

Z niniejszym dokumentem związany jest następujący zarejestrowany identyfikator obiektu (OID: 1.2.616.1.113527.2.4.1.0.2.1.6).

13. Punkty Rejestracji oraz Punkty Potwierdzania Tożsamości

Punkty Rejestracji i Punktry Potwierdzania Tożsamości zajmują się rejestrowaniem subskrybentów oraz weryfikacją ich tożsamości. Lista akredytowanych przez CERTUM PCC Punktów Rejestracji oraz Punktów Potwierdzania Tożsamości znajduje się na stronie:

https://sklep.certum.pl/partnersmap

Historia dokumentu

Historia zmian dokumentu		
1.0	25.02 2015.	Na podstawie wytycznych ETSI EN 319 411-2
1.1	01.04 2016	Przeniesienie własności z Unizeto Technologies S.A. na Asseco Data System S.A.
1.2	17.10.2016	Aktualizacja aktów prawnych.
1.3	13.12.2016	Aktualizacja dokumentacji i aktów prawnych.
1.4	08.032017	Dodanie informacji na temat pieczęci elektronicznej, usunięto informacje o zgodności z WebTrust.
1.5	26.04.2017	Dodanie informacji na temat elektronicznego znacznika czasu oraz walidacji.
1.6	01.08.2017	Zmiana w adresie Asseco Data Systems S.A.