



# Informacja o infrastrukturze klucza publicznego Certum QCA

Wersja 1.4

Data: 8 Marzec 2017 r.

Status: **aktualny**

**Asseco Data Systems S.A.**

ul. Żwirki i Wigury 15

81-387 Gdynia

„Certum - Powszechne Centrum Certyfikacji”

ul. Bajeczna 13

71-838 Szczecin

<https://certum.pl>

<https://certum.eu>

# Spis treści

1. DANE ADRESOWE .....	3
2. RODZAJE CERTYFIKATÓW, ZASTOSOWANIE I PROCEDURY WERYFIKACJI .....	3
3. OGRANICZENIA ODPOWIEDZIALNOŚCI .....	4
4. ZOBOWIĄZANIA SUBSKRYBENTA .....	4
5. ZOBOWIĄZANIA STRON UFAJĄCYCH .....	5
6. ODPOWIEDZIALNOŚĆ CERTUM .....	6
7. KODEKS POSTĘPOWANIA CERTYFIKACYJNEGO, POLITYKA CERTYFIKACJI, UMOWY. ....	7
8. POLITYKA PRYWATNOŚCI .....	7
9. ZWROT OPŁAT .....	7
10. PRAWO ORAZ ROZSTRZYGANIE SPORÓW. ....	7
11. AUDYT .....	7
12. IDENTYFIKACJA DOKUMENTU .....	8
13. PUNKTY REJSTRACJI ORAZ PUNKTY POTWIERDZANIA TOŻSAMOŚCI .....	8

## 1. Dane adresowe.

### Asseco Data Systems S.A.

ul. Żwirki i Wigury 15  
81-387 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 certyfikacyjnych świadczonych przez CERTUM.

W ramach usług kwalifikowanych działa kwalifikowany urząd certyfikacji CERTUM QCA, który wydaje kwalifikowane certyfikaty klucza publicznego elektronicznych podpisów i pieczęci.

Profil oraz jakiegokolwiek ograniczenia kwalifikowanego certyfikatu klucza publicznego elektronicznych podpisów i pieczęci wydanego przez CERTUM QCA są zgodne ze specyfikacją ETSI EN 319 412.

### 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.

### Zastosowanie

Kwalifikowane certyfikaty wystawione przez kwalifikowany urząd certyfikacji **CERTUM QCA** 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** 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.

### 3. Ograniczenia odpowiedzialności.

Odpowiedzialność finansowa Asseco Data Systems S.A., w imieniu której CERTUM 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, rozliczania użytkowników oraz personelu z ich działań, rejestrowane są wszystkie te zdarzenia występujące w systemie, które mają istotny wpływ na bezpieczeństwo funkcjonowania CERTUM. 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 oraz wszystkie zdarzenia występujące w systemie, które mają istotny wpływ na bezpieczeństwo funkcjonowania CERTUM.

### 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, Kodeksie Postępowania Certyfikacyjnego oraz Polityce Certyfikacji.

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 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 Kodeksem Postępowania certyfikacyjnego oraz Polityką Certyfikacji i zapewnienia bezpieczeństwa oraz 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,
- 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,
- zabezpieczenia i ochrony dostępu do nośników na których przechowywane są hasła i klucze,
- nie udostępniania i nie przekazywania swoich kluczy prywatnych oraz używanych przez siebie haseł osobom trzecim,
- niezwłocznie unieważnienia certyfikatu w przypadku naruszenia ochrony (lub podejrzenia naruszenia ochrony) swojego klucza prywatnego,
- wykorzystywania certyfikatu kwalifikowanego i odpowiadającego mu klucza prywatnego tylko zgodnie z deklarowanym w certyfikacie przeznaczeniem, celami i ograniczeniami określonymi w niniejszym dokumencie.

## 5. Zobowiązania stron ufających.

Stroną ufającą, korzystającą z usług CERTUM jest dowolny podmiot, który podejmuje decyzję o akceptacji kwalifikowanego podpisu elektronicznego, 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**, lub
- aktualnego statusu certyfikatu wystawionego przez kwalifikowany urząd weryfikacji statusu certyfikatu **CERTUM QOCSP**.

Strona ufająca zobowiązana jest do:

- zweryfikowania czy podpis elektroniczny został zrealizowany za pomocą klucza prywatnego odpowiadającego kluczowi publicznemu zawartemu w certyfikacie kwalifikowanym subskrybenta lub urzędu certyfikacji,
- zweryfikowania 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 podpisu elektronicznego lub certyfikatu 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).

## 6. Odpowiedzialność CERTUM.

CERTUM nie ponosi odpowiedzialności za działania stron trzecich, subskrybentów oraz innych stron nie związanych z CERTUM. 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,

- za szkody powstałe na skutek niewłaściwego stosowania wydanych certyfikatów, przy czym przez słowo niewłaściwe należy rozumieć używanie certyfikatu przeterminowanego, unieważnionego lub zawieszonoego,
- w przypadku podania przez subskrybenta fałszywych danych i - mimo zachowania przez CERTUM należytej staranności - umieszczenie ich na jego wnioski zarówno w bazach CERTUM, jak też w wydany mu certyfikacie kwalifikowanym.

## 7. Kodeks Postępowania Certyfikacyjnego, Polityka Certyfikacji, Umowy.

CERTUM publikuje w serwisie internetowym w repozytorium dostępnym pod adresem:

<http://www.certum.pl/> następujące dokumenty:

- Kodeks Postępowania Certyfikacyjnego Kwalifikowanych Usług CERTUM,
- Polityka Certyfikacji Kwalifikowanych Usług CERTUM,
- 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\\_informacie\\_prawne.xml](http://www.certum.pl/certum/cert,onas_informacie_prawne.xml).

## 9. Zwrot opłat.

CERTUM dokłada wszelkich starań, aby świadczone usługi były na najwyższym poziomie. W każdym innym przypadku subskrybent może żądać zwrotu wniesionej opłaty, jeżeli usługa certyfikacyjna była wykonana niezgodnie z zasadami wynikającymi z umowy, Kodeksu Postępowania Certyfikacyjnego i postanowień niniejszego dokumentu.

## 10. Prawo oraz Rozstrzygnięcie sporów.

Funkcjonowanie CERTUM oparte jest na zasadach zawartych w Kodeksie Postępowania Certyfikacyjnego oraz obowiązujących na terytorium Polski przepisach prawa.

Spory związane z kwalifikowanymi usługami certyfikacyjnymi świadczonymi przez CERTUM 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. Sędem właściwym do rozpoznania sprawy będzie Sąd Powszechny właściwy dla pozwanego.

W przypadku wystąpienia innych sporów będących konsekwencją użycia certyfikatu wydany lub innych kwalifikowanych usług świadczonych przez CERTUM, subskrybent zobowiązuje się pisemnie poinformować CERTUM o przedmiocie powstałego sporu.

## 11. Audyt.

Audyty sprawdzające prawidłowość i zgodność z uregulowaniami proceduralnymi i prawnymi (przede wszystkim zgodność z Kodeksem Postępowania Certyfikacyjnego i Polityką Certyfikacji) są wykonywane w zależności od potrzeb, ale nie rzadziej niż raz do roku, na podstawie art. 20 eIDAS.

Usługi świadczone przez CERTUM 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: 1.2.616.1.113527.2.4.1.0.2.1.4).

## 13. Punkty Rejestracji oraz Punkty Potwierdzania Tożsamości.

Punkty Rejestracji i Punkty Potwierdzania Tożsamości zajmują się rejestrowaniem subskrybentów oraz weryfikacją ich tożsamości. Lista akredytowanych przez CERTUM 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.