Regulamin Kwalifikowanych Usług Zaufania Certum

Wersja 2.6
Ważny od: 8 lipca 2024 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

Elektronicznie podpisany przez
Asseco Data Systems S.A.
2024.07.05 12:23:24 +02:00

Spis treści

1. Przedmiot regulacji oraz zakres stosowania Regulaminu 3
2. Stosowana polityka usług zaufania 3
3. Świadczone usługi 3
3.1. Wydanie certyfikatu 3
3.2. Unieważnienie certyfikatu 4
3.3. Zawieszenie certyfikatu 4
4. Zakres stosowania certyfikatu 5
5. Obowiązki subskrybenta 5
6. Ograniczenia w użytkowaniu usługi 7
7. Informacje dla stron ufających 8
8. Okres przechowywania danych 10
9. Komunikacja subskrybenta z Certum 10
10. Wymagania techniczne 10
11. Dostępność usług 11
12. Podstawy prawne 11
13. Warunki zawarcia i rozwiązania umowy 13
14. Warunki rozstrzygania sporów, reklamacje 13
15. Ograniczenia odpowiedzialności 14
16. Audyty zgodności 15
17. Zmiany w Regulaminie 15
18. Słownik pojęć 15
Historia dokumentu 18

1. Przedmiot regulacji oraz zakres stosowania Regulaminu

Celem niniejszego Regulaminu Kwalifikowanych Usług Zaufania Certum (zwanego dalej **Regulaminem**) jest określenie szczegółowej regulacji stosunku prawnego między dostawcą kwalifikowanych usług zaufania – **Certum** i stroną, która subskrybuje usługę (zwana dalej **subskrybentem**). Świadczone przez Certum usługi zaufania obejmują:

a) usługę wydawania kwalifikowanych certyfikatów elektronicznego podpisu i pieczęci elektronicznej obejmującą: rejestrację i certyfikację, aktualizację kluczy (odnowienie certyfikatu), modyfikację danych w certyfikacie, unieważnienie lub zawieszenie certyfikatu,

b) usługę elektronicznego znacznika czasu,

c) usługę weryfikacji statusu certyfikatu,

d) usługę walidacji i konserwacji kwalifikowanych podpisów elektronicznych i kwalifikowanych pieczęci elektronicznych,

e) usługę rejestrowanego doręczenia elektronicznego.

2. Stosowana polityka usług zaufania

Świadczenie kwalifikowanych usług zaufania reguluje „Polityka Certyfikacji i Kodeks Postępowania Certyfikacyjnego Kwalifikowanych Usług Certum". Dokument dostępny jest na stronie internetowej urzędu certyfikacji Certum pod adresem: www.certum.pl.

3. Świadczone usługi

3.1. Wydanie certyfikatu

a) Certum wydaje certyfikat na podstawie wniosku, który stanowi potwierdzenie prawdziwości danych i zgodę subskrybenta na przyporządkowanie do niego tych danych w certyfikacie wydanym na podstawie tego wniosku.

b) Subskrybent może wnioskować samodzielnie o nowy certyfikat za pośrednictwem indywidualnego konta w serwisie panel.certum.pl.

Uwaga: Nie ma możliwości zmiany nazwy konta, tj. adresu e-mail, na który założone zostało konto w serwisie panel.certum.pl. Jedynym wyjątkiem jest założenie nowego konta w procesie odnawiania certyfikatu.

c) Certyfikat stanowi zaświadczenie elektroniczne, które zawiera dane identyfikacyjne subskrybenta, atrybuty oraz dane służące do sprawdzenia autentyczności podpisu elektronicznego (pieczęci elektronicznej) złożonych za pomocą danych zawartych:

- na karcie cryptoCertum, której subskrybent jest jedynym użytkownikiem i wyłącznie on zna kod PIN i PUK umożliwiający jej użycie w celu złożenia podpisu elektronicznego (pieczęci elektronicznej),
- w komponencie SimplySign, nad którym jedynie subskrybent ma kontrolę poprzez dysponowanie unikatowym środkiem uwierzytelniającym, za którego pomocą subskrybent będzie identyfikowany i logowany w usłudze SimplySign oraz nadany

przez siebie i znany tylko jemu kod PIN i PUK, który bezpośrednio pozwala na użycie danych do składania podpisu (pieczęci) znajdujących się w SimplySign.

d) Subskrybenci usługi SimplySign mają dostęp do swoich certyfikatów za pośrednictwem indywidualnego konta w serwisie panel.certum.pl.

   Uwaga: Nie ma możliwości zmiany nazwy konta, tj. adresu e-mail, na który założone zostało konto w serwisie panel.certum.pl.

e) Certyfikat wydawany jest w terminie 7 dniu roboczych liczonych od daty złożenia poprawnie wypełnionego i zweryfikowanego wniosku.

f) Certyfikat zawiera datę ważności zgodnie ze złożonym wnioskiem, przy czym okres ważności nie może być dłuższy niż 3 lata i 60 dni.

g) Certum wysyła subskrybentowi informację o zbliżającej się dacie końca ważności certyfikatu. Wiadomość zostaje dostarczona na podany w procesie rejestracji adres e-mail kolejno na 60, 30, 14 i 7 dni przed końcem ważności certyfikatu.

3.2. Unieważnienie certyfikatu

a) Certum unieważnia certyfikat na podstawie:
   - żądania unieważnienia zgłoszonego przez subskrybenta,
   - żądania uprawnionego podmiotu, którego dane zawarte są we wniosku certyfikacyjnym,
   - żądania uprawnionego podmiotu na podstawie wcześniej zawartej umowy, która dopuszcza taką możliwość,
   - stwierdzenia zagrożenia interesu prawnego lub faktycznego subskrybenta lub osób trzecich wynikającego z wykorzystywania certyfikatu, o czym niezwłocznie informuje subskrybenta.

b) Podmiot potwierdzający atrybut jest zobowiązany zgłosić żądanie unieważnienia certyfikatu w przypadku stwierdzenia niezgodności atrybutu ze stanem faktycznym.

c) Certum unieważnia certyfikat i publikuje jego status jako „unieważniony” w okresie nie dłuższym niż 24 godziny od skutecznego zgłoszenia żądania unieważnienia.

d) Nie można przywrócić ważności unieważnionemu certyfikatowi.

e) Unieważnienie certyfikatu jest równoznaczne z utratą ważności certyfikatu i skutkuje rozwiązaniem zawartej umowy.

f) Rozwiązanie umowy spowodowane unieważnieniem certyfikatu nie powoduje zwrotu kosztów poniesionych przez subskrybenta wynikających z przedmiotu umowy.

g) Podpis elektroniczny złożony w okresie po unieważnieniu certyfikatu nie wywołuje skutku prawnego.

h) Wniosek o unieważnienie certyfikatu może być złożony poprzez stronę panel.certum.pl lub uniewaznienia.certum.pl.

3.3. Zawieszenie certyfikatu

a) Certum zawiesza ważność certyfikatu w przypadku uzyskania uprawdopodobnionej informacji, wymagającej jednak dodatkowego sprawdzenia, o zagrożeniu interesu

prawnego lub faktycznego subskrybenta lub osób trzecich wynikającego z wykorzystywania certyfikatu.

b) Certum publikuje status certyfikatu jako „zawieszony" na listach CRL i niezwłocznie informuje Subskrybenta o tym fakcie.
c) W okresie zawieszenia ważności można anulować zawieszenie certyfikatu przywracając jego ważność, jeżeli przesłanki decydujące o zawieszeniu okazały się nieprawdziwe, w szczególności po potwierdzeniu tego faktu przez subskrybenta.
d) Jeżeli w ciągu 7 dni od daty zawieszenia certyfikatu nie nastąpi anulowanie zawieszenia, to status certyfikatu pozostaje „zawieszony".
e) Jeżeli certyfikat zmienił status z „zawieszony" na „unieważniony", to podpis elektroniczny złożony w okresie zawieszenia nie wywołuje skutku prawnego.
f) Po uchyleniu zawieszenia certyfikatu, skutek prawny podpisu elektronicznego weryfikowanego tym certyfikatem, złożonego w trakcie zawieszenia, następuje z chwila uchylenia tego zawieszenia.

4. Zakres stosowania certyfikatu

Certyfikat służy do weryfikacji (walidacji) podpisu elektronicznego lub pieczęci elektronicznej.

Kwalifikowany podpis elektroniczny wywołuje skutek prawny równoważny podpisowi własnoręcznemu subskrybenta. Kwalifikowana pieczęć elektroniczna wywołuje skutek prawny równoważny jej fizycznemu odpowiednikowi .

Certyfikat, w związku z umieszczeniem w nim atrybutu, nie nadaje subskrybentowi żadnych szczególnych ról, uprawnień i pełnomocnictw, poza wynikającymi wyłącznie z treści tego atrybutu.

5. Obowiązki subskrybenta

Poprzez akceptację warunków świadczenia usług zaufania subskrybent wyraża zgodę na przystąpienie do systemu usług zaufania na warunkach określonych w Regulaminie oraz Polityce Certyfikacji i Kodeksie Postępowania Certyfikacyjnego.

5.1. Subskrybent zobowiązany jest do:

a) przestrzegania warunków świadczenia usług określonych w Regulaminie oraz Polityce Certyfikacji i Kodeksie Postępowania Certyfikacyjnego,
b) dostarczenia prawdziwych i poprawnych informacji na każdym etapie współpracy,
c) dostarczenia dokumentów potwierdzających prawdziwość dostarczonych informacji,
d) sprawdzenia poprawności danych zawartych w certyfikacie w procesie akceptacji certyfikatu i w przypadku nie stwierdzenia nieprawidłowości – zaakceptowanie go, nieodrzucenie certyfikatu skutkuje jego akceptacją,
e) przystąpienia do procedury unieważnienia certyfikatu w przypadku:
   - stwierdzenia błędów danych zawartych w certyfikacie,
   - stwierdzenia wad certyfikatu,
   - zmiany danych zawartych w certyfikacie,

- utraty kontroli (lub podejrzenia utraty kontroli) nad danymi do składania podpisu elektronicznego;
- utraty karty cryptoCertum lub środków uwierzytelniających wykorzystywanych w usłudze SimplySign
- ujawnienia kodu PIN i PUK (do karty cryptoCertum lub usługi SimplySign).

f) zaprzestania natychmiastowego i trwałego korzystania z usługi SimplySign lub karty cryptoCertum w przypadku, gdy certyfikat jest unieważniony, zawieszonym lub minął jego termin ważności,

g) wykorzystywania certyfikatu podpisu i pieczęci i odpowiadających im danych tylko i wyłącznie do składania podpisu lub pieczęci i zgodnie z deklarowanym w certyfikacie przeznaczeniem, celami i ograniczeniami,

h) jeżeli subskrybent jest osobą fizyczną - zobowiązany jest do sprawowania wyłącznej kontroli i nieudostępniania swojej karty cryptoCertum lub komponentu SimplySign, na których przechowywane są dane do składania podpisu elektronicznego osobom trzecim oraz nieujawniania kodu PIN i PUK - dotyczy kwalifikowanych certyfikatów podpisu elektronicznego,

i) jeżeli subskrybent jest osobą prawną (dotyczy również organizacji niemających osobowości prawnej) - zobowiązany jest do sprawowania kontroli i nieudostępniania swojej karty cryptoCertum lub komponentu SimplySign, na których przechowywane są dane do składania pieczęci elektronicznej osobom trzecim oraz nieujawniania kodu PIN i PUK - dotyczy kwalifikowanych certyfikatów pieczęci elektronicznej.

5.2. Subskrybent oświadcza, że:

a) przed podpisaniem wniosku zapoznał się i akceptuje niniejszy Regulamin,

b) zapoznał się z klauzulą informacyjną RODO (patrz rozdz. 12),

c) wszystkie dostarczone informacje są zgodne z prawdą,

d) ponosi odpowiedzialność za szkody wynikające z podania nieprawdziwych lub fałszywych danych, za skutki nieprawidłowego użycia certyfikatów lub danych do składania podpisu lub pieczęci,

e) jest świadomy, że certyfikat, co do zasady, jest dostępny publicznie,

f) jest świadomy, że podpis elektroniczny składany na dokumentach uwidacznia dane osobowe subskrybenta w zakresie: imię, nazwisko oraz pozostałe dane wskazane do umieszczenia w treści certyfikatu. Ponadto potwierdza, że oświadczenia woli, na których subskrybent złożył podpis elektroniczny, mogą być zgodnie z decyzją subskrybenta, dostępne bez ograniczenia bez względu na lokalizację. Na obieg tak podpisanych dokumentów nie ma wpływu Asseco Data Systems S.A., kwalifikowany dostawca usług zaufania;

g) jest świadomy, że środowisko, w ramach którego odbywają się operacje kryptograficzne z wykorzystaniem danych służących do składania podpisu elektronicznego (pieczęci elektronicznej), zarządzane jest przez kwalifikowanego dostawcę usług zaufania, jakim jest Asseco Data Systems S.A – dotyczy subskrybentów usługi SimplySign.

5.3. Subskrybent wyraża zgodę:

a) na obowiązki subskrybenta, wymienione w rozdz.5,
b) na korzystanie z karty cryptoCertum lub z komponentu SimplySign w celu składania podpisów lub pieczęci,
c) na przechowywanie przez Certum informacji związanych z wydanymi certyfikatami przez wymagany prawem okres 20 lat,
d) na tworzenie przez Certum kopii zapasowych danych służących do składania podpisu elektronicznego (pieczęci elektronicznej) w celu zapewnienia minimum niezbędnego do zapewnienia ciągłości usługi SimplySign,
e) na umieszczenie przez Certum w certyfikacie danych służących do weryfikacji podpisu elektronicznego (pieczęci elektronicznej) oraz na stosowanie tych danych do weryfikacji jego podpisu elektronicznego (pieczęci elektronicznej).

5.4. Subskrybent, pobierający token znacznika czasu, powinien zweryfikować pieczęć elektroniczną urzędu oraz sprawdzić listę CRL pod kątem unieważnienia certyfikatu urzędu.

5.5. Certum udostępnia usługę OCSP weryfikacji certyfikatów kwalifikowanych w trybie on-line. Usługa umożliwia uzyskanie informacji o unieważnieniu certyfikatu także poza okresem jego ważności.

5.6. Usługobiorca kwalifikowanej usługi rejestrowanego doręczenia elektronicznego zobowiązany jest do:

- przestrzegania warunków świadczenia usługi rejestrowanego doręczenia elektronicznego świadczonej przez Asseco Data Systems S.A.,
- dostarczenia obsługującemu go punktowi sieci Systemu Rejestracji prawdziwych i poprawnych informacji na każdym etapie współpracy,
- dostarczenia dokumentów potwierdzających prawdziwość danych zawartych we wniosku w celu wypełnienia określonych w „Polityce Certyfikacji i Kodeksie Postępowania Certyfikacyjnego Kwalifikowanych Usług Certum oraz w Polityce" i „Kodeksie Kwalifikowanej Usługi Certum – rejestrowanego doręczenia elektronicznego eDoręczenia" wymagań procesu rejestracji,
- niezwłocznego poinformowania Certum o jakichkolwiek błędach lub o zmianach danych,
- korzystania z usługi rejestrowanego doręczenia elektronicznego wyłącznie w celach zgodnych z prawem.

6. Ograniczenia w użytkowaniu usługi

6.1. Subskrybent nie korzysta z usługi w celu dostarczania treści o charakterze bezprawnym, obraźliwym, treści nieprawdziwych lub mogących wprowadzić w błąd, treści zawierających wirusy lub treści, które mogą wywołać zakłócenia lub uszkodzenia systemów komputerowych.

6.2. Usługa SimplySign nie jest skierowana do zastosowań M2M (machine-to-machine) oraz masowego podpisywania lub pieczętowania dokumentów elektronicznych. W ramach tej usługi subskrybentowi przysługuje liczba podpisów lub pieczęci na poziomie 5000 w ciągu

miesiąca. Powyżej tej wartości usługodawca ma prawo ograniczyć wydajność usługi, np. do 100 podpisów i pieczęci na dzień.

6.3. Certum nie wydaje certyfikatów osobom niepełnoletnim (poniżej 18 roku życia).

7. Informacje dla stron ufających

7.1. Stroną ufającą, korzystającą z usług Certum jest dowolny podmiot, który podejmuje decyzję o akceptacji kwalifikowanego certyfikatu podpisu lub pieczęci elektronicznej, usługi znacznika czasu, usługi walidacji kwalifikowanych podpisów i pieczęci elektronicznych (w szczególności w powiązaniu z dokumentem) lub usługi eDoręczenia, która może być w jakikolwiek sposób uzależniona od:

a) ważności powiązania pomiędzy tożsamością subskrybenta a należącym do niego kluczem publicznym, potwierdzonym certyfikatem przez kwalifikowany urząd certyfikacji, lub

b) powiązania podpisu lub pieczęci elektronicznej z tokenem elektronicznego znacznika czasu, wydanym przez kwalifikowany urząd elektronicznego znacznika czasu, lub

c) potwierdzenia aktualnego statusu certyfikatu wystawionego przez kwalifikowany urząd weryfikacji statusu certyfikatu, lub

d) tokena walidacji wystawionego przez kwalifikowaną usługę,

e) dowodów usługi eDelivery.

7.2. Strona ufająca jest odpowiedzialna za weryfikację aktualnego statusu certyfikatu subskrybenta oraz innych otrzymanych od niego tokenów. Decyzję taką strona ufająca musi podjąć każdorazowo, gdy chce użyć certyfikatu i tokenów do zweryfikowania podpisu elektronicznego (pieczęci elektronicznej), jego ważności dowodowej lub ważności dowodowej obiektów danych. Informacje zawarte w certyfikacie strona ufająca powinna wykorzystać do określenia, czy certyfikat został użyty zgodnie z jego deklarowanym przeznaczeniem.

7.3. Niezależnie od rodzaju świadczonej przez Certum usługi strona ufająca zobowiązana jest do akceptacji poniższych warunków:

a) akceptacji warunków określonych w Regulaminie, Polityce Certyfikacji i Kodeksie Postępowania Certyfikacyjnego, Polityce walidacji kwalifikowanej usługi Certum QESValidationQ,

b) rzetelnej weryfikacji każdego podpisu elektronicznego (pieczęci elektronicznej) umieszczonego na dokumencie lub certyfikacie, tokenie znacznika czasu, w tokenie statusu certyfikatu, w tokenie walidacji, dowodów usługi eDelivery,

c) właściwego i poprawnego realizowania operacji kryptograficznej przy użyciu oprogramowania i sprzętu, których poziom bezpieczeństwa jest zgodny z poziomem wrażliwości przetwarzanej informacji i poziomu wiarygodności stosowanych certyfikatów,

d) uznania podpisu elektronicznego (pieczęci elektronicznej) za nieważny, jeśli nie można rozstrzygnąć, czy podpis (pieczęć) jest ważny lub uzyskany wynik weryfikacji jest negatywny,
e) zaufania tylko tym certyfikatom:
   - które używane są zgodne z deklarowanym przeznaczeniem oraz są odpowiednie do zastosowań w obszarach, które wcześniej określiła strona ufająca, np. w formie polityki podpisu,
   - których status został zweryfikowany, np. w oparciu o aktualne listy certyfikatów unieważnionych (CRL) lub przy zastosowaniu usługi OCSP, udostępnianej przez Certum,
f) określenia warunków, jakie musi spełniać certyfikat oraz podpis elektroniczny (pieczęć elektroniczna), aby został uznany przez tą stronę za ważny. Warunki te mogą zostać sformułowane np. w postaci odpowiedniej polityki podpisu i opublikowane.

7.4. Jeśli dokument lub podpis elektroniczny jest oznakowany czasem lub w jakikolwiek sposób powiązany z innymi tokenami, to w celu racjonalnego zbudowania zaufania do weryfikowanego tokena strona ufająca powinna dodatkowo:
   a) zweryfikować, czy token został prawidłowo poświadczony elektronicznie oraz czy klucz prywatny użyty przez kwalifikowany urząd elektronicznego znacznika czasu nie był ujawniony aż do momentu weryfikacji tokena (chyba, że zawarty w nich czas spełnia wymagania daty pewnej), status klucza prywatnego można zweryfikować w oparciu o weryfikację komplementarnego z nim klucza publicznego,
   b) sprawdzić ograniczenia w stosowaniu certyfikatów podpisu elektronicznego i pieczęci elektronicznej, tokenów elektronicznego znacznika czasu, tokenów weryfikacji statusu certyfikatów w trybie on-line, tokenów walidacji danych określonych w Polityce Certyfikacji i Kodeksie Postępowania Certyfikacyjnego, Regulaminie oraz w Polityce walidacji kwalifikowanego elektronicznego podpisu i pieczęci.

7.5. Gwarancje oraz odpowiedzialność Certum obowiązują tylko dla wydanego i zaakceptowanego przez subskrybenta certyfikatu.

7.6. Listy certyfikatów unieważnionych (CRL) wydawane są w określonych odstępach czasu lub każdorazowo po zawieszeniu lub unieważnieniu jednego z wydanych certyfikatów. Zawierają:
   - nazwę urzędu certyfikacji, który je wydał,
   - datę aktualnej i następnej publikacji,
   - numery seryjne, daty i przyczyny unieważnienia (lub zawieszenia) certyfikatów.

7.7. W przypadku formatów podpisu elektronicznego lub pieczęci elektronicznej, które nie są obsługiwane przez kwalifikowaną usługę walidacji i konserwacji, pojawi się komunikat, że żądanie nie może zostać przetworzone.

7.8. W przypadku, gdy kwalifikowana usługa walidacji i konserwacji nie jest w stanie zebrać i zweryfikować wszystkich danych walidacyjnych, zostanie dostarczony komunikat, że żądanie nie może zostać przetworzone.

7.9. W przypadku usługi kwalifikowanego doręczenia elektronicznego strona ufająca powinna dokonać:

- rzetelnej weryfikacji każdego poświadczenia które do niej dotrze w celu zweryfikowania poświadczenia strona ufająca powinna:
  a) sprawdzić, czy wszystkie certyfikaty dostawców usług zaufania wchodzące w skład ścieżki certyfikacji należą do urzędów certyfikacji oraz czy nadano im prawo poświadczania rejestrowanych doręczeń elektronicznych,
  b) określić datę oraz czas poświadczenia. Jest to możliwe za pomocą kwalifikowanego elektronicznego znacznika czasu umieszczonego w poświadczeniu.

8. Okres przechowywania danych

Wszystkie dane dotyczące świadczenia kwalifikowanych usług zaufania w tym wszystkie zaakceptowane przez subskrybentów wnioski o świadczenie usług zaufania, są archiwizowane (w formie elektronicznej lub papierowej), przechowywane są przez okres 20 lat zgodnie z Ustawą o usługach zaufania oraz identyfikacji elektronicznej.

Zapisy rozmów wideo pozyskanych w procesie zdalnej weryfikacji tożsamości przechowywane są do 14 dni, po upływie tego czasu zapisy są niszczone.

9. Komunikacja subskrybenta z Certum

W przypadku unieważnienia, zawieszenia lub anulowania zawieszenia certyfikatu subskrybent otrzyma informację na adres swojej poczty elektronicznej lub swój telefon (wiadomość SMS) w zależności, który kontakt Subskrybent wskazał wnioskując o certyfikat lub uzgodnił to w inny sposób z Certum.

Informacje kontaktowe:

Nazwa:	Certum
Adres korespondencyjny:	ul. Bajeczna 13, 71-838 Szczecin
Infolinia:	infolinia@certum.pl, +48 4472850[1], 801 540 340[1], +48 91 4801 340[1]
Unieważnienie certyfikatu:	uniewaznienia.certum.pl
Strona WWW:	www.certum.pl
Reklamacje:	reklamacje@certum.pl, +48 91 4801 380[1]
Inspektor ochrony danych:	IOD@assecods.pl, tel. +48 42 675 63 60[1]

10. Wymagania techniczne

a) Certum prowadzi listę bezpiecznych urządzeń, która zawiera kwalifikowane urządzenia do składania podpisu elektronicznego (Qualified electronic Signature Creation Device, QSCD), jakimi są karty cryptoCertum oraz sprzętowy moduł kryptograficzny (HSM), na

[1] Stawka za minutę połączenia zgodnie z cennikiem operatora.

którym przechowywane są wirtualne karty subskrybentów usługi SimplySign w rozumieniu Rozporządzenia eIDAS. Lista jest dostępna na stronie internetowej www.certum.pl.

b) Certum posiada w ofercie czytniki do kart cryptoCertum oraz udostępnia sterowniki niezbędne do ich prawidłowego funkcjonowania na stronie internetowej www.certum.pl.

c) Usługa SimplySign jest dostępna za pośrednictwem urządzenia z systemem operacyjnym Android, iOS, Windows lub MAC OS.

11. Dostępność usług

11.1. Polityka bezpieczeństwa, realizowana przez Certum bierze pod uwagę następujące zagrożenia, mające wpływ na dostępność i ciągłość świadczonych usług:

a) fizyczne uszkodzenie systemu i sieci komputerowej Certum,

b) awarie oprogramowania, utratę dostępu do danych,

c) utratę istotnych z punktu widzenia interesów Certum usług sieciowych,

d) awaria tej części sieci internetowej, za pośrednictwem której Certum udostępnia swoje usługi.

11.2. Aby zapobiec lub ograniczyć skutki wymienionych zagrożeń, polityka bezpieczeństwa Certum obejmuje następujące zagadnienia:

a) Plan odtwarzania systemu po katastrofie – wszyscy subskrybenci oraz strony ufające są jak najszybciej i w sposób najbardziej odpowiedni do zaistniałej sytuacji powiadamiani o każdej poważnej awarii lub katastrofie, dotyczącej dowolnego komponentu systemu komputerowego i sieci. Plan obejmuje szereg procedur, które są realizowane w momencie, gdy dowolna część systemu ulegnie skompromitowaniu (uszkodzeniu, ujawnieniu, itp.).

b) Kontrolowanie zmian – instalacja uaktualnionych wersji oprogramowania w systemie docelowym możliwa jest tylko i wyłącznie po przeprowadzeniu na systemie modelowym intensywnych testów, wykonywanych według ściśle opracowanych procedur.

c) System zapasowy – w przypadku awarii uniemożliwiającej funkcjonowanie Certum w ciągu maksymalnie 24 godzin zostanie uruchomiony ośrodek zapasowy, który do czasu uruchomienia głównego ośrodka Certum przejmie jego podstawowe funkcje.

d) System tworzenia kopii zapasowych – system Certum korzysta z oprogramowania tworzącego kopie zapasowe z danych, które w każdej chwili umożliwiają ich odtworzenie oraz obsługę audytu.

12. Podstawy prawne

12.1. Podstawę prawną świadczonych przez Certum usług zaufania stanowią poniższe akty prawne:

a) Rozporządzenie eIDAS, które stanowi akt prawny w całości obowiązujący w systemie prawnym Polski oraz we wszystkich państwach Unii Europejskiej;

b) Ustawa o usługach zaufania oraz identyfikacji elektronicznej z dnia 5 września 2016 r. (Dz.U. z 2021 r. poz. 1797, z późn. zm.);
c) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylająca dyrektywę 2007/64/WE
d) Ustawa o świadczeniu usług drogą elektroniczną z dnia 18 lipca 2002 r. (tj. Dz.U. z 2017 r. poz. 1219).

12.2. Zgodnie z art. 13 ust. 1 i 2 ogólnego rozporządzenia o ochronie danych z dnia 27 kwietnia 2016 r., zwanego dalej „Rozporządzeniem", informujemy, że:
a) Administratorem danych osobowych jest Asseco Data Systems S.A.
b) Kontakt do Inspektora ochrony danych w Asseco Data Systems S.A. został podany w rozdziale 9.
c) Dane osobowe przetwarzane będą w celach niezbędnych do wykonania usługi, na podstawie art. 6 ust. 1 lit. b Rozporządzenia.
d) Wszystkie dane dotyczące świadczenia kwalifikowanych usług zaufania, w tym dane osobowe i wszystkie zaakceptowane przez Subskrybenta warunki świadczenia usług zaufania, są archiwizowane (w postaci elektronicznej lub papierowej) oraz przechowywane przez okres 20 lat zgodnie z art. 17 ust. 2 Ustawy o usługach zaufania oraz identyfikacji elektronicznej.
e) Subskrybent posiada prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia/zapomnienia (po wygaśnięciu obowiązku wynikającego z art. 17 ust. 2 Ustawy o usługach zaufania oraz identyfikacji elektronicznej), ograniczenia przetwarzania, prawo do przenoszenia danych, prawo wniesienia sprzeciwu, prawo do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem. Wszystkie powyższe prawa można zrealizować poprzez złożenie wniosku na stronie www.daneosobowe.assecods.pl.
f) Subskrybent ma prawo wniesienia skargi do Regulatora, gdy uzna, iż przetwarzanie jego danych osobowych narusza przepisy Rozporządzenia.
g) Podanie danych osobowych jest warunkiem świadczenia usług. Subskrybent jest zobowiązany do ich podania, a konsekwencją niepodania danych osobowych będzie niemożność przeprowadzenia procesu wydania certyfikatu.

12.3. Certum jest jednostką organizacyjną firmy Asseco Data Systems S.A. wpisaną do rejestru kwalifikowanych dostawców usług zaufania prowadzonego w imieniu ministra właściwego ds. informatyzacji przez Narodowy Bank Polski. Rejestr ten jest publikowany pod adresem internetowym: www.nccert.pl.

12.4. Sposób realizacji kwalifikowanych usług zaufania przez Certum określa szczegółowo „Polityka certyfikacji i kodeks postępowania certyfikacyjnego kwalifikowanych usług Certum" dostępna pod adresem internetowym: www.certum.pl.

12.5. W sprawach nieuregulowanych obowiązują właściwie przepisy powszechnie obowiązującego prawa.

13. Warunki zawarcia i rozwiązania umowy

13.1. Umowa o świadczenie kwalifikowanych usług zaufania zawarta zostaje poprzez złożenie przez subskrybenta wniosku o wydanie certyfikatu oraz potwierdzenie jego tożsamości, akceptację Regulaminu oraz Polityki Certyfikacji i Kodeksu Postępowania Certyfikacyjnego.

13.2. Każdy kolejny wniosek o wydanie certyfikatu wymaga ponownego potwierdzenia tożsamości subskrybenta.

13.3. Rezygnacja z usług zaufania możliwa jest tylko w przypadku unieważnienia kwalifikowanego certyfikatu podpisu elektronicznego (pieczęci elektronicznej), dokonana na warunkach określonych w Polityce Certyfikacji i Kodeksie Postępowania Certyfikacyjnego.

13.4. Certum zastrzega sobie prawo do odrzucenia wniosków certyfikacyjnych w następujących przypadkach:

a) identyfikator subskrybenta (nazwa DN) ubiegającego się o wydanie certyfikatu pokrywa się z identyfikatorem innego subskrybenta,
b) termin ważności dokumentu tożsamości wnioskodawcy, którego dane (numer i seria) zawarte są w certyfikacie jest krótszy od daty ważności certyfikatu,
c) uzasadnionego podejrzenia, że subskrybent sfałszował lub podał nieprawdziwe dane,
d) niedostarczenia przez wnioskodawcę kompletu wymaganych dokumentów, stanowiących załącznik do wniosku,
e) wykrycia poprawek lub modyfikacji w przesłanych dokumentach formalnych,
f) przekroczenia terminu ważności przesłanych dokumentów - za przedawnione uznaje się te dokumenty, których data wytworzenia przekroczyła termin 3 miesięcy,
g) przekroczenia terminu ważności wniosku o wydanie certyfikatu - za przedawnione uznaje się te wioski, których data wypełnienia przekroczyła termin 3 miesięcy,
h) innych, ważnych nie wymienionych powyżej przyczyn, po uprzednim uzgodnieniu odmowy z **inspektorem bezpieczeństwa**.

W przypadku niedostarczenia wymaganego kompletu dokumentów formalnych, wymaganego kompletu dokumentów podmiotu (w przypadku certyfikatów z danymi podmiotu) Certum zastrzega sobie prawo do ich odesłania w terminie 3 miesięcy od daty wpłynięcia.

14. Warunki rozstrzygania sporów, reklamacje

14.1. Przedmiotem rozstrzygania sporów, w tym reklamacji, mogą być jedynie rozbieżności bądź konflikty powstałe pomiędzy stronami w zakresie wydawania i unieważniania certyfikatu w oparciu o Regulamin i regulacje Polityki Certyfikacji i Kodeksu Postępowania Certyfikacyjnego.

14.2. Spory, reklamacje, bądź zażalenia powstałe na tle użytkowania certyfikatów tokenów znacznika czasu, wystawianych przez Certum tokenów weryfikacji statusu certyfikatów,

usługi walidacji i konserwacji, usługi eDoręczenia będą rozstrzygane na podstawie pisemnych informacji w drodze mediacji. Skargi należy kierować w formie pisemnej:

Za pośrednictwem poczty e-mail: lub	reklamacje@certum.pl
Listownie na adres:	Asseco Data Systems S.A., ul. Królowej Korony Polskiej 21 70-486 Szczecin, z dopiskiem „Reklamacja”.
Dodatkowy kontakt:	Telefon: +48 91 4801 380[2] Faks: +48 91 4801 223[2]

14.3. Skargi podlegają pisemnemu rozpatrzeniu w terminie 21 dni roboczych od dnia ich doręczenia. W przypadku braku rozstrzygnięcia sporu w terminie 45 dni roboczych od rozpoczęcia postępowania pojednawczego, stronom przysługuje prawo do wystąpienia na drogę sądową. Sądem właściwym do rozpoznania sprawy będzie Sąd Powszechny miejscowo właściwy dla pozwanego.

14.4. W przypadku wystąpienia innych sporów będących konsekwencją użycia wydanego certyfikatu lub innych kwalifikowanych usług świadczonych przez Certum, Subskrybent zobowiązuje się pisemnie poinformować Certum o przedmiocie powstałego sporu.

15. Ograniczenia odpowiedzialności

15.1. Odpowiedzialność finansowa Asseco Data Systems S.A., w imieniu której Certum świadczy kwalifikowane usługi, w stosunku do jednego zdarzenia wynosi 250.000 EUR, ale nie więcej niż 1.000.000 EUR w odniesieniu do wszystkich takich zdarzeń (równowartość w złotych). Odpowiedzialność finansowa dotyczy okresów 12-miesięcznych zgodnych z rokiem kalendarzowym.

15.2. Certum nie ponosi odpowiedzialności finansowej wobec innych osób trzecich, niebędących subskrybentami usług Certum.

15.3. 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, modyfikacją danych w certyfikacie aktualizacją, unieważnianiem i zawieszaniem certyfikatów, a także generowanie danych do składania i weryfikacji pieczęci elektronicznych dla potrzeb urzędów Certum oraz wszystkie zdarzenia występujące w systemie, które maja istotny wpływ na bezpieczeństwo funkcjonowania Certum.

[2] Stawka za minutę połączenia zgodnie z cennikiem operatora.

16. Audyty zgodności

16.1. Kwalifikowane usługi zaufania świadczone przez Certum podlegają corocznemu badaniu zgodności z Rozporządzeniem eIDAS. Audyt certyfikujący przeprowadzany jest raz na dwa lata. Dodatkowy audyt utrzymaniowy przeprowadzany jest pomiędzy dwoma audytami certyfikującymi.

16.2. Certum przechodzi również audyt zgodności Zintegrowanego Systemu Zarządzania – Systemu Zarządzania Bezpieczeństwem Informacji oraz Systemu Zarządzania Jakością. Celem tego audytu jest określenie stopnia zgodności postępowania Certum lub wskazanych przez nią elementów z Zintegrowanym Systemem Zarządzania, który obejmuje wymagania standardów PN-EN ISO:9001:2015 oraz PN ISO/IEC 27001:2017, oraz deklaracjami i procedurami właściwymi dla Certum.

17. Zmiany w Regulaminie

Regulamin wchodzi w życie z dniem jego umieszczenia w postaci elektronicznej na stronie internetowej: www.certum.pl i obowiązuje przez czas nieokreślony.

17.1. Certum zastrzega sobie prawo zmiany niniejszego Regulaminu. Wszelkie zmiany Regulaminu zostaną zakomunikowane w sposób wyraźny na stronie internetowej podanej w rozdziale 17 i wchodzą w życie:

- z chwilą opublikowania;
- w stosunku do subskrybentów posiadających ważne certyfikaty z upływem co najmniej 7 dni od dnia opublikowania zmian Regulaminu z zastrzeżeniem ust. 3 poniżej.

17.2. Zmiana Regulaminu skutkująca zmniejszeniem lub ograniczeniem wcześniej nabytych przez subskrybenta praw, upoważnia subskrybenta do złożenia rezygnacji ze świadczonych usług w terminie 7 dni od dnia otrzymania informacji o wejściu w życie zmian w Regulaminie. W sytuacji określonej w zdaniu poprzednim, subskrybent zobowiązany jest do złożenia oświadczenia sporządzonego w formie pisemnej i wysłania go na adres Certum.

17.3. O powyższych zmianach Regulaminu subskrybenci zostaną także powiadomieni za pośrednictwem poczty elektronicznej (e-mail).

18. Słownik pojęć

Audyt – dokonanie niezależnego przeglądu i oceny działania systemu w celu przetestowania adekwatności środków nadzoru systemu, upewnienia się czy system działa zgodnie z ustaloną Polityką Certyfikacji i Kodeksem Postępowania Certyfikacyjnego i wynikającymi z niej procedurami operacyjnymi oraz w celu wykrycia przekłamań zabezpieczeń i zalecenia wskazanych zmian w środkach nadzorowania, polityce certyfikacji oraz procedurach.

Certum – kwalifikowany dostawca usług zaufania zajmujący się wydawaniem kwalifikowanych certyfikatów podpisów elektronicznych i pieczęci, znaczników czasu, weryfikacji statusu online i usługi walidacji i konserwacji;

Certyfikat – kwalifikowany certyfikat podpisu elektronicznego lub pieczęci elektronicznej w rozumieniu Rozporządzenia eIDAS;

Dane identyfikacyjne – dane jednoznacznie identyfikujące subskrybenta, których prawdziwość można potwierdzić na podstawie dokumentu tożsamości subskrybenta, jeżeli

subskrybent jest osobą prawną (dotyczy również organizacji niemających osobowości prawnej) jego dane weryfikowane są na podstawie dokumentów rejestrowych;

Dostawca usług zaufania (TSP, ang. Trust Service Provider) – oznacza osobę fizyczną lub prawną, która świadczy przynajmniej jedną usługę zaufania, jako kwalifikowany lub niekwalifikowany dostawca usług zaufania.

Dzień roboczy – dzień od poniedziałku do piątku z wyłączeniem sobót, niedziel i dni ustawowo wolnych od pracy określonych w ustawie z dnia 18 stycznia 1951 r. o dniach wolnych od pracy (tekst jednolity Dz.U. z 2015 r. poz. 90).

Karta cryptoCertum – komponent techniczny spełniający wymagania kwalifikowanego urządzenia do składania podpisu elektronicznego w rozumieniu Rozporządzenia eIDAS;

Kwalifikowany elektroniczny znacznik czasu – usługa polegającą na dołączaniu do danych w postaci elektronicznej logicznie powiązanych z danymi opatrzonymi podpisem lub poświadczeniem elektronicznym, oznaczenia czasu w chwili wykonania tej usługi oraz poświadczenia elektronicznego tak powstałych danych przez TSP świadczącego tę usługę.

Klucz prywatny – klucz pary kluczy asymetrycznych podmiotu, który jest stosowany jedynie przez ten podmiot. W przypadku systemu podpisu asymetrycznego klucz prywatny określa przekształcenie podpisu. W przypadku systemu szyfrowania asymetrycznego klucz prywatny określa przekształcenie deszyfrujące.

Klucz publiczny – klucz z pary kluczy asymetrycznych podmiotu, który może być uczyniony publicznym. W przypadku systemu podpisu asymetrycznego klucz publiczny określa przekształcenie weryfikujące. W przypadku systemu szyfrowania asymetrycznego klucz publiczny określa przekształcenie szyfrujące.

Komponent SimplySign – dostępny zdalnie komponent techniczny spełniający wymagania kwalifikowanego urządzenia do składania podpisu elektronicznego w rozumieniu Rozporządzenia eIDAS;

Lista certyfikatów unieważnionych (CRL) – lista zawierająca numery seryjne, daty i przyczyny unieważnienia (lub zawieszenia) certyfikatów. Zawiera także nazwę urzędu certyfikacji, który ją wydał oraz datę aktualnej i następnej publikacji. Lista wydawana jest w określonych odstępach czasu lub każdorazowo po zawieszeniu lub unieważnieniu jednego z wydanych certyfikatów;

Modyfikacja danych w certyfikacie - utworzenie nowego certyfikatu na podstawie certyfikatu, który jest aktualnie w posiadaniu subskrybenta, nie został unieważniony, zaś jego okres ważności nie minął. Nowy certyfikat posiada nowy klucz publiczny, nowy numer seryjny i różni się zawartością przynajmniej jednego z pozostałych pól certyfikatu.

PIN (ang. Personal Identification Number) – osobisty numer identyfikacyjny, kod zabezpieczający kartę kryptograficzną przed możliwością złożenia podpisu elektronicznego przez osoby niepowołane.

Podpis elektroniczny (pieczęć elektroniczna) – kwalifikowany podpis elektroniczny (pieczęć elektroniczna) w rozumieniu Rozporządzenia eIDAS;

Polityka Certyfikacji i Kodeks Postępowania Certyfikacyjnego – zestaw reguł określających w szczególności zasady świadczenia usługi zaufania, odpowiedzialność stron, dostępny w formie elektronicznej na stronie www.certum.pl;

PUK (ang. Personal Unblocking Key) – kod służący do odblokowania karty kryptograficznej oraz zmiany kodu PIN.

Rozporządzenie eIDAS – rozporządzenie 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 uchylające dyrektywę 1999/93/WE wraz z Rozporządzeniem Parlamentu Europejskiego I Rady (UE) 2024/1183 z dnia 11 kwietnia 2024 r. w sprawie zmiany rozporządzenia (UE) nr 910/2014 w odniesieniu do ustanowienia europejskich ram tożsamości cyfrowej.

Subskrybent – osoba fizyczna w przypadku podpisu elektronicznego lub osoba prawna w przypadku pieczęci elektronicznej wnioskująca o certyfikat lub dla której certyfikat został wydany. Subskrybentem jest również osoba fizyczna bądź osoba prawna lub jednostka nieposiadająca osobowości prawnej, która korzysta z usługi kwalifikowanego znacznika czasu, walidacji podpisu/pieczęci oraz konserwacji podpisu/pieczęci i rejestrowanego doręczenia elektronicznego eDoręczenia.

Usługa SimplySign – usługa polegająca na zarządzaniu infrastrukturą, w której znajduje się SimplySign, komponent będący pod kontrolą subskrybenta.

Ustawa o świadczeniu usług drogą elektroniczną – ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. z 2016 r. poz. 1030, z późn. zm.).

Ustawa o usługach zaufania oraz identyfikacji elektronicznej – Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz.U. z 2021 r. poz. 1797, z późn. zm.).

Historia dokumentu

Historia zmian dokumentu		
1.0	26 czerwca 2017 r.	Opracowanie dokumentu.
1.1	01sierpnia 2017 r.	Zmiana w adresie Asseco Data Systems S.A.
1.2	29 czerwca 2018	"Podpisanie umowy" zamieniono na "akceptację warunków świadczenia usług".
1.3	1 października 2018	Aktualizacja numeru OID przypisanego Polityce Certyfikacji i Kodeksowi Postępowania Certyfikacyjnego.
2.0	27 czerwca 2019 r.	Opracowanie dokumentu – połączenie „Regulaminu Kwalifikowanych Usług Zaufania Certum" i „Regulaminu Kwalifikowanych Usług Zaufania dla umów zawieranych w formie elektronicznej".
2.1	9 września 2020	Wprowadzenie poprawek edytorskich
2.2	30 Grudnia 2020	Wprowadzenie poprawek edytorskich
2.3	27 lipca 2021	Zmiana ścieżki składania wniosku o unieważnienie certyfikatu, zmiana adresu siedziby Asseco Data Systems S.A. i inne poprawki edytorskie.
2.4	1 czerwca 2022	Dodanie nowej kwalifikowanej usługi eDoręczenia *(Kwalifikowana usługa rejestrowanego doręczenia elektronicznego jest objęta na tę chwilę audytem zgodności z Rozporządzeniem eIDAS, po otrzymaniu wszystkich stosownych certyfikatów, zostanie udostępniona dla subskrybentów)*
2.5	26 luty 2024	Dodanie informacji o braku możliwości zmiany nazwy konta w serwisie panelu.certum.pl.
2.6	8 lipca 2024	Aktualizacja zapisów w związku z nowelizacją Rozporządzenia eIDAS.