REGULAMIN
Kwalifikowanych Usług Zaufania
dla umów zawieranych w formie elektronicznej

Wersja 1.0
Data: 22.10.2018
Status: aktualny

1. Słownik pojęć

Certyfikat – kwalifikowany certyfikat podpisu elektronicznego w rozumieniu rozporządzenia UE 910/2014, czyli poświadczenie elektroniczne wydane przez kwalifikowanego dostawcę usług zaufania, które jednoznacznie przyporządkowuje dane służące do walidacji podpisu elektronicznego do osoby fizycznej;

Subskrybent – osoba fizyczna wnioskująca o certyfikat lub dla której certyfikat został wydany;

Certum – kwalifikowany dostawca usługi zaufania, jaką jest wydawanie kwalifikowanego certyfikatu podpisu elektronicznego;

Podpis elektroniczny – kwalifikowany podpis elektroniczny w rozumieniu rozporządzenia UE 910/2014;

Karta cryptoCertum – komponent techniczny spełniający wymagania kwalifikowanego urządzenia do składania podpisu elektronicznego w rozumieniu rozporządzenia UE 910/2014;

Komponent SimplySign – dostępny zdalnie komponent techniczny spełniający wymagania kwalifikowanego urządzenia do składania podpisu elektronicznego w rozumieniu rozporządzenia UE 910/2014;

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

Aplikacja SimplySign – oprogramowanie na urządzeniu mobilnym, pozostające pod wyłączną kontrolą Subskrybenta, umożliwiająca korzystanie z usługi SimplySign;

Dane identyfikacyjne – dane jednoznacznie identyfikujące Subskrybenta, których prawdziwość można potwierdzić na podstawie dokumentu tożsamości Subskrybenta;

Atrybut – dodatkowa dana zawarta w certyfikacie, której prawdziwość, co do zasady potwierdza podmiot trzeci;

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;

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;

Rozporządzenie UE 910/2014 – 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.

2. Przedmiot regulacji oraz zakres stosowania Regulaminu

Niniejszy Regulamin określa prawa i obowiązki Subskrybenta oraz Certum dla umów o świadczenie kwalifikowanych usług zaufania zawieranych w formie elektronicznej, na zasadach określonych w rozdziale 14 Regulaminu, w odniesieniu do wnioskowania i wydania Certyfikatu oraz zarządzania nim.

3. Wydanie certyfikatu

3.1. 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.

3.2. Certyfikat stanowi zaświadczenie elektroniczne, które zawiera dane identyfikacyjne Subskrybenta, atrybuty oraz dane służące do sprawdzenia autentyczności podpisu elektronicznego złożonego 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,
- w komponencie SimplySign, nad którego użyciem jedynie Subskrybent ma kontrolę poprzez dysponowanie unikatowym środkiem identyfikacji, za którego pomocą Subskrybent będzie identyfikowany i logowany w usłudze SimplySign oraz nadany przez siebie i znany tylko jemy kod PIN i PUK, który bezpośrednio pozwala na użycie danych do składania podpisu znajdujących się w SimplySign.

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

3.4. Certyfikat zawiera datę ważności zgodnie ze złożonym wnioskiem, przy czym okres ważności nie może być dłuższy niż 3 lata.

3.5. 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.

4. Zakres stosowania certyfikatu

4.1 Certyfikat służy do weryfikacji (walidacji) podpisu elektronicznego, który wywołuje skutek prawny równoważny podpisowi własnoręcznemu Subskrybenta i jako taki uznawany jest na terenie wszystkich państw członkowskich Unii Europejskiej..

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

5 Unieważnienie certyfikatu

5.1 Certum unieważnia certyfikat na podstawie:
- żądania unieważnienia zgłoszonego przez Subskrybenta;
- żądanie unieważnienia zgłoszonego przez podmiot potwierdzający atrybut;
- powzięcia informacji o zagrożeniu interesu prawnego lub faktycznego Subskrybenta lub osób trzecich wynikającego z wykorzystywania certyfikatu, o czym niezwłocznie informuje Subskrybenta.

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

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

5.4 Nie można przywrócić ważności unieważnionemu certyfikatowi.
5.5 Podpis elektroniczny złożony w okresie po unieważnienia certyfikatu nie wywołuje skutku prawnego.

6 Zawieszenie ważności Certyfikatu

6.1 Certum zawiesza ważność certyfikatu w przypadku powzięcia uprawdopodobnionej informacji, wymagającej jednak dodatkowego sprawdzenia, o zagrożeniu interesu prawnego lub faktycznego Subskrybenta lub osób trzecich wynikającego z wykorzystywania certyfikatu.
6.2 Certum publikuje status certyfikatu jako „zawieszony" na listach CRL i niezwłocznie informuje Subskrybenta o tym fakcie.
6.3 Okres zawieszenia może trwać maksymalnie 7 dni.
6.4 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.
6.5 Jeżeli w ciągu 7 dni od daty zawieszenia certyfikatu nie nastąpi anulowanie zawieszenia, to status certyfikatu zostanie zmieniony na „unieważniony".
6.6 Jeżeli certyfikat zmienił status z „zawieszony" na „unieważniony", to podpis elektroniczny złożony w okresie zawieszenia nie wywołuje skutku prawnego.
6.7 Po uchyleniu zawieszenia certyfikatu, skutek prawny podpisu elektronicznego weryfikowanego tym certyfikatem, złożonego w trakcie zawieszenia, następuje z chwila uchylenia tego zawieszenia.

7 Obowiązki Subskrybenta

7.1 Subskrybent zobowiązany jest do:
7.1.1 Dostarczenia prawdziwych informacji na każdym etapie współpracy;
7.1.2 Dostarczenia dokumentów potwierdzających prawdziwość dostarczonych informacji;
7.1.3 Sprawdzenia poprawności danych zawartych w certyfikacie w procesie akceptacji certyfikatu i w przypadku nie stwierdzenia nieprawidłowości – zaakceptowanie go. Brak odrzucenia certyfikatu skutkuje akceptacją.
7.1.4 Zapewnienia ochrony dostępu do karty cryptoCertum lub komponentu SimplySign, na których przechowywane są do danych do składania podpisu elektronicznego, w szczególności poprzez nieujawnianie kodu PIN i PUK osobom postronnym.
7.1.5 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 identyfikacji wykorzystywane w usłudze SimplySign
- ujawnienia kodu PIN i PUK (do karty cryptoCertum lub SimplySign).

7.1.6 Zaprzestania natychmiastowego i trwałego korzystania z usługi SimplySign lub karty cryptoCertum w przypadku, gdy certyfikat jest unieważniony, zawieszonym lub minął jego termin ważności;

7.1.7 Wykorzystywania certyfikatu i odpowiadających mu danych do składania podpisu tylko zgodnie z deklarowanym w certyfikacie przeznaczeniem, celami i ograniczeniami.

7.2 Subskrybent oświadcza, że:

7.2.1 Przed podpisaniem wniosku zapoznał się i akceptuje niniejszy Regulamin;

7.2.2 Zapoznał się z klauzulą informacyjną RODO (patrz rozdz. 13);

7.2.3 Wszystkie dostarczone informacje są zgodne z prawdą;

7.2.4 Ponosi odpowiedzialność za szkody wynikające z podania nieprawdziwych lub fałszywych danych oraz za skutki nieprawidłowego użycia certyfikatów;

7.2.5 Jest świadomy, że certyfikat, co do zasady, jest dostępny publicznie;

7.2.6 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 złożono podpis elektroniczny, mogą być zgodnie z decyzją Subskrybenta, dostępne bez ograniczenia w szczególności co do lokalizacji. Na obieg tak podpisanych dokumentów nie ma wpływu Asseco Data Systems S.A., kwalifikowany dostawca usług zaufania;

7.2.7 Jest świadomy, że środowisko, w ramach którego odbywają się operacje kryptograficzne z wykorzystaniem danych służących do składania podpisu elektronicznego, zarządzane jest przez kwalifikowanego dostawcę usług zaufania, jakim jest Asseco Data Systems S.A.

7.3 Subskrybent wyraża zgodę:

7.3.1 Na obowiązki Subskrybenta, wymienione w pkt. 7.1;

7.3.2 Na korzystanie z karty cryptoCertum lub z komponentu SimplySign w celu składania podpisów;

7.3.3 Na przechowywanie przez Certum informacji związanych z wydanymi certyfikatami przez wymagany prawem okres 20 lat;

7.3.4 Na tworzenie przez Certum kopii zapasowej danych służących do składania podpisu elektronicznego w celu zapewnienia minimum niezbędnego do zapewnienia ciągłości usługi SimplySign;

7.3.5 Na umieszczenie przez Certum w certyfikacie danych służących do weryfikacji podpisu elektronicznego oraz na stosowanie tych danych do weryfikacji jego podpisu elektronicznego.

8 Ograniczenia w użytkowaniu usługi

8.1 Subskrybent jest zobowiązany do korzystania z karty cryptoCertum lub z usługi SimplySign wyłącznie osobiście zgodnie z przeznaczeniem i w celu określonym w certyfikacie i tylko w okresie jego ważności.

8.2 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.

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

9 Informacje dla stron ufających

9.1 Stroną ufającą, korzystającą z usług Certum, jest dowolny podmiot, który podejmuje decyzję o akceptacji certyfikatu (w szczególności dokumentu elektronicznego), która może być w jakikolwiek sposób uzależniona od ważności lub aktualności powiązania pomiędzy tożsamością Subskrybenta a będącymi w jego wyłącznej dyspozycji

danymi do składania podpisu elektronicznego, potwierdzonego certyfikatem przez Certum.

9.2 Strona ufająca jest odpowiedzialna za weryfikację aktualnego statusu certyfikatu Subskrybenta. Decyzję taką strona ufająca musi podjąć każdorazowo, gdy chce użyć certyfikatu do zweryfikowania podpisu elektronicznego, 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.

9.3 Strona ufająca zobowiązana jest do akceptacji poniższych warunków:

9.3.1 Rzetelnej weryfikacji każdego podpisu elektronicznego umieszczonego na dokumencie lub certyfikacie;

9.3.2 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;

9.3.3 Uznania podpisu elektronicznego za nieważny, jeśli nie można rozstrzygnąć, czy podpis jest ważny lub uzyskany wynik weryfikacji jest negatywny;

9.3.4 Zaufania tylko tym certyfikatom:

- które używane są zgodnie 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).

9.3.5 Określenia warunków, jakie musi spełniać certyfikat oraz podpis elektroniczny, aby został uznany przez tą stronę za ważny. Warunki te mogą zostać sformułowane np. w postaci odpowiedniej polityki podpisu i opublikowane.

9.4 Gwarancje oraz odpowiedzialność Certum i Subskrybenta obowiązują tylko dla wydanego i zaakceptowanego certyfikatu przez Subskrybenta;

9.5 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.

10 Komunikacja Subskrybenta z Certum

10.1 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.

10.2 Informacje kontaktowe:

10.2.1 Asseco Data Systems S.A.: ul. Podolska 21, 81-321 Gdynia, www.assecods.pl, kontakt@assecods.pl

10.2.2 Certum

- Adres korespondencyjny: ul. Bajeczna 13, 71-838 Szczecin
- Infolinia: infolinia@certum.pl, 801 540 340[1], +48 91 4801 340[1]
- Unieważnienie certyfikatu: +48 91 4801 360[1]

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

– Reklamacje: reklamacje@certum.pl, +48 91 4801 380[1] (patrz rozdz. 15)

10.2.3 Inspektor ochrony danych: IOD@assecods.pl, tel. +48 42 675 63 60[1]

11 Wymagania techniczne

11.1 Certum prowadzi listę bezpiecznych urządzeń, która zawiera kwalifikowane urządzenia do składania podpisu elektronicznego (Qualified electronic Signature Creation Device, QSCD), jakimi są karty cryptoCertum, w rozumieniu rozporządzenia UE 910/2014. Lista jest dostępna na stronie internetowej www.certum.pl.

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

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

12 Dostępność usług

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

12.1.1 Fizyczne uszkodzenie systemu i sieci komputerowej Certum;

12.1.2 Awarie oprogramowania, utratę dostępu do danych;

12.1.3 Utratę istotnych z punktu widzenia interesów Certum usług sieciowych;

12.1.4 Awaria tej części sieci internetowej, za pośrednictwem której Certum udostępnia swoje usługi.

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

12.2.1 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.).

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

12.2.3 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.

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

13 Podstawy prawne

13.1 Podstawę prawną świadczenia usługi wydawania certyfikatu i korzystania z niego stanowią poniższe akty prawne:

– Rozporządzenie UE 910/2014, które stanowi akt prawny w całości obowiązujący w systemie prawnym Polski oraz we wszystkich państwach Unii Europejskiej;

– Ustawa o usługach zaufania oraz identyfikacji elektronicznej z dnia 5 września 2016 r. (Dz.U. 2016 poz. 1579);

– Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (tj. Dz.U. z 2017 r. poz. 1219).

13.2 Zgodnie z art. 13 ust. 1 i 2 ogólnego rozporządzenia o ochronie danych z dnia 27 kwietnia 2016 r., zwanego dalej „Rozporządzeniem", informujemy, że:

13.2.1 Administratorem danych osobowych jest Asseco Data Systems S.A.

13.2.2 Kontakt do Inspektora ochrony danych w Asseco Data Systems S.A. został podany w rozdziale 11. Komunikacja Subskrybenta z Certum.

13.2.3 Dane osobowe przetwarzane będą w celach niezbędnych do wykonania usługi, na podstawie art. 6 ust. 1 lit. b Rozporządzenia.

13.2.4 Wszystkie dane dotyczące świadczenia kwalifikowanych usług zaufania, w tym dane osobowe i wszystkie zaakceptowane przez Subskrybenta warunki świadczenia usług zaufania, są archiwizowane (w formie elektronicznej i papierowej) oraz przechowywane przez okres 20 lat zgodnie z art. 17 ust. 2 ustawy o usługach zaufania oraz identyfikacji elektronicznej.

13.2.5 Subskrybent posiada prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia/zapomnienia, 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. Realizację wszystkich powyższych praw można zrealizować poprzez wniosek złożony na stronie www.daneosobowe.assecods.pl.

13.2.6 Subskrybent ma prawo wniesienia skargi do Regulatora, gdy uzna, iż przetwarzanie jego danych osobowych narusza przepisy Rozporządzenia.

13.2.7 Podanie danych osobowych jest warunkiem świadczenia usług. Subskrybent jest zobowiązany do ich podania, a konsekwencją niepodania danych osobowych będzie niemożność przeprowadzenia procesu wydania certyfikatu.

13.3 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.

13.4 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.

13.5 W sprawach nieuregulowanych obowiązują właściwie przepisy powszechnie obowiązującego prawa.

14 Warunki zawarcia i rozwiązania umowy

14.1 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.

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

15 Warunki rozstrzygania sporów, reklamacje

15.1 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.

15.2 Spory, reklamacje, bądź zażalenia powstałe na tle użytkowania certyfikatów wystawianych przez Certum, będą rozstrzygane na podstawie pisemnych informacji w drodze mediacji. Skargi należy kierować w formie pisemnej:

- Za pośrednictwem poczty e-mail: reklamacje@certum.pl lub
- Listownie na adres: Asseco Data Systems S.A., ul. Bajeczna 13, 71-838 Szczecin, z dopiskiem „Reklamacja".

Dodatkowy kontakt:

- Telefon: +48 91 4801 380[2]
- Faks: +48 91 4801 223[2]

15.3 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.

15.4 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.

16 Ograniczenia odpowiedzialności

16.1 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.

16.2 Certum nie ponosi odpowiedzialności finansowej wobec innych osób trzecich, niebędących odbiorcami usług Certum.

16.3 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.

17 Audyty zgodności

17.1 Kwalifikowane usługi zaufania świadczone przez Certum podlegają corocznemu badaniu zgodności z rozporządzeniem UE 910/2014. Audyt certyfikujący dokonywany jest raz na dwa lata. Dodatkowo zaleca się, aby przynajmniej jeden audyt utrzymaniowy przeprowadzany był pomiędzy dwoma audytami certyfikującymi.

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

17.2 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:9001:2009 oraz PN ISO/IEC 27001:2007, oraz deklaracjami i procedurami właściwymi dla Certum.

18 Zmiany w Regulaminie

18.1 Regulamin wchodzi w życie z dniem jego umieszczenia w formie elektronicznej na stronie internetowej:
http://www.certum.pl/pl/cert_wiedza_regulamin_kwalifikowanych_uslug_zaufania/
i obowiązuje przez czas nieokreślony.

18.2 Asseco Data Systems S.A. zastrzega sobie prawo zmiany niniejszego Regulaminu. Wszelkie zmiany Regulaminu zostaną zakomunikowane w sposób wyraźny na stronie internetowej podanej w punkcie 17.1 i wchodzą w życie:

18.2.1 z chwilą opublikowania;

18.2.2 w stosunku do Subskrybentów posiadających ważne Certyfikaty z upływem co najmniej 7 dni od dnia opublikowania zmian Regulaminu z zastrzeżeniem ust. 3 poniżej.

18.3 Zmiana Regulaminu skutkująca zmniejszeniem lub ograniczeniem wcześniej nabytych przez Subskrybenta praw, upoważnia Subskrybenta to złożenia rezygnacji ze świadczonych usług w terminie 7 dni od dnia otrzymania informacji o wejściu w życie zmian Regulaminu. W sytuacji określonej w zdaniu poprzednim, Subskrybent zobowiązany jest do złożenia oświadczenia sporządzonego w formie pisemnej i wysłanego na adres siedziby Asseco Data Systems S.A.

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