Regulamin
Kwalifikowanych Usług Zaufania
CERTUM PCC

Wersja 1.1

Data: 01.08.2017

Status: archiwalny

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

Spis treści

§1 Przedmiot regulacji

1. Niniejszy dokument, zwany dalej „Regulaminem", reguluje podstawowe prawa i obowiązki stron umowy o świadczenie kwalifikowanych usług zaufania, świadczonych drogą elektroniczną w rozumieniu przepisów *Ustawy o świadczeniu usług drogą elektroniczną*, na które składają się następujące usługi:
   1) usługę wydawania kwalifikowanych certyfikatów elektronicznego podpisu i pieczęci elektronicznej obejmującą:
      a) rejestrację i certyfikację,
      b) aktualizację kluczy,
      c) modyfikację danych w certyfikacie,
      d) unieważnienie lub zawieszenie certyfikatu,
   2) usługę elektronicznego znacznika czasu,
   3) usługę weryfikacji statusu certyfikatu,
   4) usługę walidacji kwalifikowanych podpisów elektronicznych i kwalifikowanych pieczęci elektronicznych.
2. CERTUM PCC zastrzega sobie prawo zmian Regulaminu. Wszelkie zmiany Regulaminu wchodzą w życie w terminie nie krótszym niż 7 dni od daty ich publikacji na stronie internetowej http://www.certum.pl. O zmianach Regulaminu Subskrybenci zostaną także powiadomieni za pośrednictwem poczty elektronicznej (e-mail), nie później niż na 7 dni przed wejście w życie zmian Regulaminu.
3. Każdorazowom po wprowadzeniu zmian w Regulaminie nowa akutalnie obowiązująca wersja zostaje opublikowana w serwisie internetowym urzędu certyfikacji dostępnym pod adresem http://www.certum.pl, z oznaczeniem kolejnej wersji.
4. Strona CERTUM jest przystosowana dla osób niedowidzących, które chciałyby ubiegać się o certyfikat kwalifikowany podpisu elektronicznego. Istnieje możliwość dostosowania współczynnika kontrastu między tekstem a tłem oraz zmiany rozmiaru tekstu, co nie wpływa na funkcjonalność i czytelność strony WWW.
5. Postanowienia Regulaminu dotyczą świadczenia usług zaufania w rozumieniu *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* oraz *Ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. z 2016 r. poz. 1579).*

§2 Podmiot regulacji

1. Kwalifikowane usługi zaufania są świadczone przez Asseco Data Systems S.A. z siedzibą w Gdyni przy ul. Podolskiej 21 , wpisaną do rejestru przedsiębiorców prowadzonego przez Sąd Rejonowy Gdańsk-Północ, VIII Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS 0000421310, kapitał zakładowy 120 002 940,00 PLN (wpłacony w całości), przez wyodrębnioną organizacyjnie komórkę Certum – Powszechne Centrum Certyfikacji (zwaną dalej CERTUM).
2. Decyzję Ministra Rozwoju Nr 1/47610-16/16 z dnia 01 kwietnia 2016 roku firma Asseco Data Systems S.A. z siedzibą w Gdyni została wpisana pod numerem 14 do rejestru

kwalifikowanych podmiotów świadczących usługi zaufania związane z podpisem elektronicznym.

3. Niniejszy Regulamin, Polityka Certyfikacji i Kodeks Postępowania Certyfikacyjnego oraz cennik są dostępne dla odbiorców usług zaufania, na stronie internetowej CERTUM oraz w punktach sieci Systemu Rejestracji CERTUM.
4. CERTUM posiada plan zakończenia działalności, opracowany zgodnie z wymaganiami *Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014* oraz *Ustawy o usługach zaufania oraz identyfikacji elektronicznej,* który jest obowiązkowy dla dostawców usług zaufania. Opis postępowania w przypadku zakończenia działalności przedstawia Polityka Certyfikacji i Kodeks Postępowania Certyfikacyjnego Usług CERTUM, natomiast szczegółowy sposób postępowania określa plan zakończenia działalności Centrum Certyfikacji, stanowiący wewnętrzną procedurę CERTUM.

§3 Stosowana polityka usług zaufania

1. Świadczenie kwalifikowanych usług zaufania reguluje Polityka Certyfikacji i Kodeks Postępowania Certyfikacyjnego Kwalifikowanych Usług CERTUM, który to dokument dostępny jest w serwisie internetowym urzędu certyfikacji CERTUM pod adresem:

   www.certum.pl

   Niniejszemu dokumentowi przypisano Identyfikator Obiektu:

   OID: 1.2.616.1.113527.2.4.1.0.1.5.1

2. Struktura i merytoryczna zawartość Polityki Certyfikacji i Kodeksu Postępowania Certyfikacyjnego są zgodne z zaleceniem RFC 3647 Certificate Policy and Certification Practice Statement Framework.. Spełnia on również wymagania rozdziału 5 i 6 normy ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.

§4 Ograniczenia w użytkowaniu usługi

1. Subskrybenci są zobowiązani do korzystania z usług CERTUM:
   1) zgodnie z ich zastosowaniem, określonym w Polityce Certyfikacji i Kodeksie Postępowania Certyfikacyjnego i zgodnym z treścią certyfikatu,
   2) zgodnie z treścią umowy zawartej pomiędzy subskrybentem a Asseco Data Systems S.A.,
   3) tylko w okresie ich ważności,
   4) tylko do momentu unieważnienia certyfikatu; w okresie zawieszenia certyfikatu subskrybent nie może używać klucza prywatnego.
2. Ograniczenia w stosowaniu usług zaufania:
   1) nie przechowywania karty kryptograficznej zawierającej klucz prywatny razem z osobistym numerem identyfikacyjnym (PIN),
   2) nie udostępniania i nie przekazywania swoich kluczy prywatnych oraz używanych przez siebie haseł osobom trzecim.

   Zabrania się używania certyfikatów CERTUM niezgodnie z zasadami określonymi w Polityce Certyfikacji i Kodeksie Postępowania Certyfikacyjnego.

§5 Obowiązki subskrybenta

1. Poprzez zawarcie umowy na świadczenie usług zaufania subskrybent wyraża zgodę na przystąpienie do systemu usług zaufania na warunkach określonych w Umowie, Polityce Certyfikacji i Kodeksie Postępowania Certyfikacyjnego.
2. Subskrybent zobowiązany jest do:
   1) przestrzegania postanowień umowy podpisanej z Asseco Data Systems S.A.,
   2) dostarczenia obsługującemu go punktowi sieci Systemu Rejestracji prawdziwych i poprawnych informacji na każdym etapie współpracy,
   3) dostarczenia dokumentów potwierdzających prawdziwość danych zawartych we wniosku w celu wypełnienia określonych w Polityce Certyfikacji i Kodeksie Postępowania Certyfikacyjnego wymagań procesu rejestracji, unieważnienia i odnowienia certyfikatu,
   4) niezwłocznego poinformowania CERTUM o jakichkolwiek błędach lub wadach w jego certyfikacie lub o zmianach danych w nim zawartych,
   5) używania swojej pary kluczy i kluczy publicznych innych odbiorców usług zaufania wyłącznie w sposób zgodny z Polityką Certyfikacji i Kodeksem Postępowania Certyfikacyjnego oraz zapewnienia bezpieczeństwa i integralności własnych kluczy prywatnych, włączając w to:
      a) kontrolę i zabezpieczenie dostępu do urządzeń zawierających jego klucze prywatne,
      b) niezwłoczne informowanie Głównego Punkt Rejestracji 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,
      c) niezwłocznego informowania urzędu certyfikacji o utracie karty z certyfikatem lub utracie kodu PIN,
   6) zabezpieczenia i ochrony dostępu do nośników, na których przechowywane są hasła i klucze,
   7) 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,
   8) w przypadku naruszenia ochrony (lub podejrzenia naruszenia ochrony) swojego klucza prywatnego niezwłocznie przystępuje do procedury unieważnienia certyfikatu,
   9) zaprzestania posługiwania się unieważnionym, zawieszonym lub nieważnym certyfikatem,
   10) wykorzystywania kwalifikowanego certyfikatu klucza publicznego i odpowiadającego mu klucza prywatnego tylko zgodnie z deklarowanym w certyfikacie przeznaczeniem, celami i ograniczeniami.
3. Subskrybent pobierający token znacznika czasu, powinien zweryfikować podpis cyfrowy urzędu oraz sprawdzić listę CRL, pod kątem unieważnienia certyfikatu urzędu.
4. CERTUM udostępnia usługę OCSP weryfikacji certyfikatów kwalifikowanych w trybie *on-line*. Usługa umożliwia uzyskanie informacji o unieważnieniu certyfikatu także poza okresem jego ważności. Wykorzystanie usługi OCSP daje możliwość częstszego pozyskania bardziej aktualnych informacji o statusie certyfikatu (w porównaniu z korzystaniem z list

CRL). Subskrybent korzystając z kwalifikowanych usług zaufania zobowiązuje się do powstrzymania od wykorzystywania usług do dostarczania przez Subskrybenta treści o charakterze bezprawnym, obraźliwych, treści nieprawdziwych lub mogących wprowadzić w błąd, treści zawierających wirusy lub treści, które mogą wywołać zakłócenia lub uszkodzenia systemów komputerowych.

5. Po otrzymaniu certyfikatu subskrybent zobowiązany jest do sprawdzenia jego zawartości, w tym w szczególności poprawności zawartych w nim danych oraz komplementarności klucza publicznego z kluczem prywatnym. Jeśli subskrybent nie znajdzie w certyfikacie żadnych nieprawidłowości – może go zaakcetować (brak odmowy skutkuje akceptacją certyfikatu).

   Jeśli wydany certyfikat zawiera jakiekolwiek wady, subskrybent powinien niezwłocznie wystąpić z wnioskiem o jego unieważnienie.

   Wniosek o unieważnienie certyfikatu może być złożony przez upoważnione do tego osoby w Głównym Punkcie Rejestracji lub przekazany tam faksem, telefonicznie lub pocztą poleconą.

§6 Wymagania techniczne

W celu korzystanie z kwalifikowanych usług zaufania, Subskrybent musi dysponować urządzeniem końcowym umożliwiającym korzystanie z sieci Internetowej oraz dysponować oprogramowaniem umożliwiającym korzystanie z danych usług, które spełniają minimalne wymagania techniczne:

1) system operacyjny: Microsoft Windows, Mac OS, Android, iOS (CERTUM gwarantuje poprawne działanie usług dla tych wersji systemów operacyjnych, które są aktualnie wspierane przez producentów lub dystrybutorów),
2) przeglądarki internetowe: Mozilla Firefox, Internet Explorer, Google Chrom, Safari (posiadające w szczególności obsługę skryptów Java),
3) procesor: Pentium 800 MHz,
4) pamięć operacyjna: 256 MB RAM,
5) właściwe aplikacje umożliwiające korzystanie z Usług,
6) oprogramowanie, dostarczone Użytkownikowi przez CERTUM na etapie uruchamiania danej Usługi.

§7 Warunki zawierania i rozwiązywania umów

1. Warunki zawierania umów o świadczenie kwalifikowanych usług zaufania są określone w Polityce Certyfikacji i Kodeksie Postępowania Certyfikacyjnego.
2. Rozwiązanie umowy o świadczenie kwalifikowanych usług zaufania możliwe jest tylko w przypadku unieważnienia kwalifikowanego certyfikatu podpisu lub pieczęci elektronicznej, dokonanej na warunkach określonych w Polityce Certyfikacji i Kodeksie Postępowania Certyfikacyjnego.

§8 Informacje dla stron ufających

1. Stroną ufającą, korzystającą z usług CERTUM jest dowolny podmiot, który podejmuje decyzję o akceptacji kwalifikowanego certyfikatu podpisu czy pieczęci elektronicznej lub innego uwierzytelnionego poświadczenia elektronicznego, usługi znacznika czasu

lub usługi walidacji kwalifikowanych podpisów i pieczęci elektronicznych (w szczególności dokumentu elektronicznego), która może być w jakikolwiek sposób uzależniona od:

1) ważności lub aktualności powiązania pomiędzy tożsamością subskrybenta a należącym do niego kluczem publicznym, potwierdzonym certyfikatem przez kwalifikowany urząd certyfikacji, lub
2) powiązania podpisu lub pieczęci elektronicznej z tokenem elektronicznego znacznika czasu, wydanym przez kwalifikowany urząd elektronicznego znacznika czasu, lub
3) potwierdzenia aktualnego statusu certyfikatu wystawionego przez kwalifikowany urząd weryfikacji statusu certyfikatu, lub
4) tokena walidacji wystawionego przez kwalifikowaną usługę.

2. Strona ufająca jest odpowiedzialna za weryfikację aktualnego statusu certyfikatu subskrybenta oraz innych otrzymanych od niego tokenów i poświadczeń. Decyzję taką strona ufająca musi podjąć każdorazowo, gdy chce użyć certyfikatu, tokenów i poświadczeń do zweryfikowania podpisu elektronicznego, jego ważności dowodowej lub ważności dowodowej obiektów danych. Informacje zawarte w kwalifikowanym certyfikacie strona ufająca powinna wykorzystać do określenia czy certyfikat został użyty zgodnie z jego deklarowanym przeznaczeniem.
3. Niezależnie od rodzaju świadczonej przez CERTUM usługi strona ufająca zobowiązana jest do akceptacji warunków określonych w niniejszym dokumencie.
   1) Akceptacji warunków określonych w Polityce Certyfikacji i Kodeksie Postępowania Certyfikacyjnego, Polityka walidacji kwalifikowanej usługi CERTUM Certum QDVCS itp. Strona ufająca akceptuje ww. warunki w chwili pierwszego odwołania się do dowolnej usługi świadczonej przez CERTUM lub pierwszego zaakceptowania podpisu subskrybenta. Gwarancje oraz odpowiedzialność CERTUM lub subskrybenta obowiązują od momentu akceptacji wydanego certyfikatu przez subskrybenta,
   2) rzetelnej weryfikacji każdego podpisu lub poświadczenia elektronicznego umieszczonego na dokumencie lub certyfikacie, tokenie znacznika czasu, w tokenie statusu certyfikatu, w tokenie walidacji,
   3) 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,
   4) uznania podpisu cyfrowego za nieważny, jeśli przy użyciu posiadanego oprogramowania i sprzętu nie można rozstrzygnąć czy podpis cyfrowy jest ważny lub uzyskany wynik weryfikacji jest negatywny,
   5) zaufania tylko tym certyfikatom klucza publicznego:
      a) które używane są zgodnie z deklarowanym przeznaczeniem oraz są odpowiednie do zastosowań w obszarach, które wcześniej określiła strona ufająca, np. w formie polityki podpisu,
      b) których status został zweryfikowany w oparciu o aktualne listy certyfikatów unieważnionych lub przy zastosowaniu usługi OCSP, udostępnianej przez CERTUM,
   6) określenia warunków, jakie musi spełniać certyfikat klucza publicznego oraz podpis cyfrowy, aby został uznany przez tą stronę za ważny; warunki te mogą zostać sformułowane np. w postaci odpowiedniej polityki podpisu i opublikowane.

4. Jeśli dokument lub podpis elektroniczny jest oznakowany czasem lub w jakikolwiek sposób powiązany z innymi tokenami, poświadczeniami wystawianymi przez CERTUM, to w celu racjonalnego zbudowania zaufania do weryfikowanego tokena lub poświadczenia strona ufająca powinna dodatkowo:
   1) zweryfikować, czy token, poświadczenie zostały prawidłowo poświadczone elektronicznie oraz czy klucz prywatny użyty przez kwalifikowany urząd elektronicznego znacznika czasu 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,
   2) 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 określone w Polityce Certyfikacji i Kodeksie Postępowania Certyfikacyjnego oraz umowie zawartej z CERTUM.

§9 Okres przechowywania danych

Wszystkie dane dotyczące świadczenia kwalifikowanych usług zaufania w tym wszystkie umowy z subskrybentami, są archiwizowane (w formie elektronicznej i papierowej), przechowywane są przez okres 20 lat zgodnie z *Ustawą o usługach zaufania oraz identyfikacji elektronicznej z dnia 5 września 2016r.*

§10 Ograniczenia odpowiedzialności

1. 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.
2. CERTUM nie ponosi odpowiedzialności finansowej zdefiniowanej w niniejszym dokumencie wobec innych osób trzecich, niebędących odbiorcami usług CERTUM.
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 maja 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 maja istotny wpływ na bezpieczeństwo funkcjonowania CERTUM.

§11 Stosowany system prawny

1. Usługi świadczone są zgodnie z *Rozporządzeniem UE 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* oraz *Ustawy z dnia 05 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. z 2016 r. poz. 1579).*
2. Dane Subskrybenta są przetwarzane przez Asseco Data Systems S.A., zgodnie z *Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2016 r. poz. 922).*

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

3. Wszelkie spory sądowe będą rozstrzygane przez Sąd Powszechny miejscowo właściwy dla siedziby pozwanego.

§12 Warunki rozstrzygania sporów, reklamacje

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 regulacje Polityki Certyfikacji i Kodeksu Postępowania Certyfikacyjnego, oraz zawartych umów.
2. Spory, reklamacje, bądź zażalenia powstałe na tle użytkowania certyfikatów, zaświadczeń certyfikacyjnych, tokenów znacznika czasu, tokenów weryfikacji statusu certyfikatów, wystawianych przez CERTUM, będą rozstrzygane na podstawie pisemnych informacji w drodze mediacji. Skargi należy kierować w formie pisemnej na adres:

   Asseco Data Systems S.A.

   ul. Bajeczna 13

   71-838 Szczecin

3. Skargi podlegają pisemnemu rozpatrzeniu w terminie 21 dni od dnia ich doręczenia na adres wskazany w ust. 2 niniejszego paragrafu. 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 miejscowo właściwy dla pozwanego.
4. W przypadku wystąpienia innych sporów będących konsekwencją użycia certyfikatu wydanego lub innych kwalifikowanych usług świadczonych przez CERTUM, subskrybent zobowiązuje się pisemnie poinformować CERTUM o przedmiocie powstałego sporu.

§13 Audyty zgodności

1. Kwalifikowane usługi zaufania świadczone przez CERTUM podlegają corocznemu badaniu zgodności z eIDAS na podstawie art. 20 pkt.1 i 17.4. *Rozporządzenia Parlamentu Europejskiego i Rady UE nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym z dnia 23 czerwca 2014 roku, zastępującego Dyrektywę 1999/93/EC.* Zgodnie z postanowieniami rozdziału 7 normy ETSI EN 319 403 „Audyt zgodności dostawców usług zaufania" – regulującej zasady działania podmiotów potwierdzających zgodność dostawców usług zaufania – audyt certyfikujący dokonywany jest raz na dwa lata. Dodatkowo zaleca się aby przynajmniej jeden audyt utrzymaniowy przeprowadzany był pomiędzy dwoma audytami certyfikującymi.
2. Dodatkowo CERTUM przechodzi również audyt zgodności Zintegrowanego Systemu Zarządzania – Systemu Zarządzania Bezpieczeństwem Informacji oraz System Zarządzania Jakościa. Celem tego audytu jest określenie stopnia zgodności postępowania jednostki usługowej CERTUM lub wskazanych przez nią elementów z wdrożonym przez Asseco Data Systems S.A. 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.

§14 Informacje kontaktowe

Asseco Data Systems S.A.

ul. Podolska 21

81-321 Gdynia

Strona internetowa: https://www.assecods.pl

e-mail: kontakt@assecods.pl

Certum – Powszechne Centrum Certyfikacji

ul. Bajeczna 13

71-838 Szczecin

Strona internetowa: https://certum.pl

e-mail: infolinia@certum.pl

§15 Dostępność usług

1. Polityka bezpieczeństwa, realizowana przez CERTUM bierze pod uwagę następujące zagrożenia, mające wpływ na dostępność i ciągłość świadczonych usług:
   1) fizyczne uszkodzenie systemu i sieci komputerowej CERTUM,
   2) awarie oprogramowania, utratę dostępu do danych,
   3) utratę istotnych z Punktu widzenia interesów CERTUM usług sieciowych,
   4) awaria tej części sieci internetowej, za pośrednictwem której CERTUM udostępnia swoje usługi.
2. Aby zapobiec lub ograniczyć skutki wymienionych zagrożeń, polityka bezpieczeństwa CERTUM obejmuje następujące zagadnienia:
   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 odtwarzania systemu obejmuje szereg procedur, które są realizowane w momencie, gdy dowolna część systemu ulegnie skompromitowaniu (uszkodzeniu, ujawnieniu, itp.).
   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.
   3) System zapasowy. W przypadku awarii uniemożliwiającej funkcjonowanie CERTUM w ciągu maksymalnie 24 godzin zostanie uruchomiony ośrodek zapasowy, który przejmie do czasu uruchomienia głównego ośrodka CERTUM podstawowe funkcje urzędów certyfikacji.
   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.

§16 Słownik pojęć

Użyte w Regulaminie określenia oznaczają:

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 – Powszechne Centrum Certyfikacji (w skrócie: CERTUM lub CERTUM PCC) – jednostka usługowa Asseco Data Systems S.A., świadcząca niekwalifikowane i kwalifikowane usługi zaufania. Kwalifikowane usługi zaufania świadczy w zakresie wydawania kwalifikowanych certyfikatów klucza publicznego podpisu elektronicznego i pieczęci elektroniczej, znakowania czasem, weryfikowania statusu certyfikatów w trybie on-line, walidacji danych oraz poświadczania odbioru i przedłożenia, w szczególności zgodnie z *Ustawą z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz.U. 2016r. poz. 1579).*

Certyfikat (certyfikat klucza publicznego, PKC) – elektroniczne zaświadczenie, za pomocą którego dane służące do weryfikacji podpisu elektronicznego są przyporządkowane do osoby składającej podpis elektroniczny i które umożliwiają identyfikację tej osoby.

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.

Główny Punkt Rejestracji (GPR) – punkt rejestracji, który oprócz standardowych czynności akredytuje inne punkty rejestracji i może generować, w imieniu urzędu certyfikacji, pary kluczy, które poddawane są następnie procesowi certyfikacji.

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.

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 podmiot świadczący tę usługę.

Kwalifikowane usługi zaufania – usługi zaufania udostępniane przez kwalifikowany podmiot świadczący usługi zaufania.

Pieczęć elektroniczna – dane w postaci elektronicznej dodane do innych danych w postaci elektronicznej lub logicznie z nimi powiązane, aby zapewnić autentyczność pochodzenia oraz integralność powiązanych danych.

Polityka Certyfikacji i Kodeks Postępowania Certyfikacyjnego – dokument opisujący szczegółowo proces certyfikacji klucza publicznego, uczestników tego procesu,

ich obowiązki i odpowiedzialność, typy certyfikatów, procedury weryfikacji tożsamości używane przy ich wydawaniu oraz określający obszary zastosowań uzyskanych w jego wyniku certyfikatów, opublikowany w serwisie internetowym dostępnym pod adresem http://www.certum.pl.

Rozporządzeniem eIDAS – Rozporządzenia Parlamentu Europejskiego i Rady (UE) NR 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (Dz.Urz.UE.L Nr 257, str. 73).

Subskrybent – osoba fizyczna lub w przypadku pieczęci elektronicznej osoba prawna lub jednostka organizacyjna nie posiadająca osobowości prawnej, która jest podmiotem wymienionym lub zidentyfikowanym w wydanym certyfikacie, posiada klucz prywatny, który odpowiada kluczowi publicznemu zawartemu w certyfikacie oraz sama nie wydaje certyfikatów innym stronom. Subskrybent może być tożsamy z podmiotem, lub reprezentować innego subskrybenta. (patrz.: ETSI EN 319 411-1 5.4.2).

Umowa z subskrybentem – umowa zawierana jest pomiędzy Asseco Data Systems S.A. a subskrybentem zamawiającym certyfikat kwalifikowany osobisty do działania we własnym imieniu lub certyfikat kwalifikowany profesjonalny do wykonywania zadań w imieniu podmiotu reprezentowanego przez subskrybenta.

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

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

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.