Regulamin Kwalifikowanych Usług Certyfikacyjnych Certum PCC

Wersja 2.2

Data: 17 Październik 2016

Status: archiwalny

Asseco Data Systems S.A.
ul. Żwirki i Wigury 15
81-387 Gdynia
„Certum PCC - Powszechne Centrum Certyfikacji”
ul. Bajeczna 13
71-838 Szczecin
https://certum.pl

Spis treści

Rozdział I. Regulacje wstępne

§1 Przedmiot regulacji

1. Niniejszy dokument, zwany dalej „Regulaminem", reguluje podstawowe prawa i obowiązki stron umowy o świadczenie kwalifikowanych usług certyfikacyjnych.
2. Postanowienia Regulaminu dotyczą świadczenia usług certyfikacyjnych 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 certyfikacyjne są świadczone przez Asseco Data Systems S.A. z siedzibą w Gdyni przy ul. Żwirki i Wigury 15, 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, przez wyodrębnioną organizacyjnie komórkę Certum - Powszechne Centrum Certyfikacji (zwaną dalej CERTUM PCC).
2. Na podstawie decyzji 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 certyfikacyjne związane z podpisem elektronicznym.
3. Firma Asseco Data Systems S.A. (Spółka przejmująca) w ramach połączenia ze Spółką Unizeto Technologies S.A. (Spółka przejmowana), dokonanego na podstawie *art. 492 § 1 pkt 1 ustawy z dnia 15 września 2000 r. Kodeks spółek handlowych (t.j. Dz.U. z 2013 r. poz. 1030 z późn. zm., dalej "Ksh"),* polegającego na przeniesieniu całego majątku Spółki przejmowanej na Spółkę przejmującą, wstąpiła we wszelkie prawa i obowiązki Spółki Unizeto Technologies S.A. (sukcesja generalna - *art. 494 § 1 Ksh).*

   W związku z przeniesieniem całego majątki Spółki Unizeto Technologies S.A. na Spółkę Asseco Data Systems S.A. oświadczamy, że Spółka Asseco Data System S.A. zobowiązuje się do utrzymywania zaświadczenia certyfikacyjnego wydanego na Spółkę Unizeto Technologies S.A. do czasu wygaśnięcia ostatniego certyfikatu wydanego przez Spółkę Unizeto Technologies S.A. w ramach posiadanego zaświadczenia certyfikacyjnego.
4. CERTUM PCC wydaje kwalifikowane certyfikaty na podstawie złożonego przez Wnioskodawcę wniosku w formie elektronicznej o wydanie kwalifikowanego certyfikatu oraz umów subskrybenckich zawartych z poszczególnymi klientami w formie pisemnej.
5. Niniejszy Regulamin, Polityka Certyfikacji, Kodeks Postępowania Certyfikacyjnego oraz cennik są dostępne dla odbiorców usług certyfikacyjnych, na stronie internetowej CERTUM PCC oraz w punktach sieci Systemu Rejestracji CERTUM PCC.

§3 Słownik pojęć

Użyte w Regulaminie określenia oznaczają:

Certyfikat (certyfikat klucza publicznego) – elektroniczne zaświadczenie, wystawione przez podmiot świadczący usługi certyfikacyjne (centrum certyfikacji), które zawiera dane służące do weryfikacji podpisu elektronicznego. Certyfikat może być przypisany zarówno do osoby fizycznej jak i domeny, adresu IP lub urządzenia sieciowego itp. Podpisany przez wystawce. certyfikat zawiera m.in.: identyfikator wystawcy certyfikatu, identyfikator użytkownika, jego klucz publiczny, okres ważności i numer seryjny certyfikatu.

Dane służące do składania podpisu elektronicznego – niepowtarzalne dane, przyporządkowane konkretnej osobie, wykorzystywane do składania podpisu elektronicznego (klucz prywatny

certyfikatu). Muszą być szczególnie chronione. W razie ich ujawnienia należy unieważnić certyfikat.

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

Infrastruktura klucza publicznego (PKI) – jest to zbiór procedur, zasad oraz technik, które wspólnie wspomagają implementację i działanie kryptograficznych systemów klucza publicznego, opartych na certyfikatach. Infrastruktura Klucza Publicznego składa się z powiązanych ze sobą elementów infrastruktury sprzętowej, programowej, baz danych, sieci, procedur bezpieczeństwa oraz zobowiązań prawnych, które dzięki współpracy realizują oraz udostępniają usługi certyfikacyjne, jak również inne związane z tymi elementami usługi.

Klucz prywatny – jeden z dwóch kluczy, należących do pary kluczy asymetrycznych, znany tylko jego właścicielowi. W systemie podpisu asymetrycznego klucz prywatny służy do podpisywania. W systemie szyfrowania asymetrycznego klucz prywatny służy do deszyfrowania. Klucz prywatny musi być wyjątkowo starannie chroniony, aby uniknąć jego ujawnienia. Ujawnienie klucza może umożliwić jego użycie (wykonanie podpisu lub odszyfrowanie danych) przez niepowołane osoby. Z tego względu klucze prywatne dla certyfikatów o wyższej wiarygodności są zapisane na karcie mikroprocesorowej, skąd nie można ich skopiować.

Klucz publiczny – jeden z dwóch kluczy, należących do pary kluczy asymetrycznych, powszechnie dostępny, którego powiązanie z konkretną osobą lub firmą potwierdza certyfikat. W systemie podpisu asymetrycznego klucz publiczny służy do weryfikacji podpisu. W systemie szyfrowania asymetrycznego klucz publiczny służy do szyfrowania.

Kodeks Postępowania Certyfikacyjnego (KPC) – dokument opisujący szczegółowo proces certyfikacji klucza publicznego, uczestników tego procesu oraz określający obszary zastosowań uzyskanych w wyniku tego procesu certyfikatów, opublikowany w Internecie w repozytorium, pod adresem http://www.certum.pl/repozytorium.

Kwalifikowany Znacznik Czasu - usługa polegająca 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. Kwalifikowany Znacznik Czasu jest usługą datowania dokumentów i podpisów elektronicznych, która wywołuje skutki prawne daty pewnej w rozumieniu przepisów Kodeksu Cywilnego.

Lista certyfikatów unieważnionych (CRL, *ang. Certificate Revocation List*) – lista podpisana cyfrowo przez urząd certyfikacji, zawierająca numery seryjne zawieszonych i unieważnionych certyfikatów oraz daty i przyczyny ich zawieszenia lub unieważnienia, nazwę wydawcy CRL, datę publikacji listy, datę następnej planowanej publikacji listy CRL.

Odnowienie certyfikatu - Potwierdzenie ważności tego samego certyfikatu na następny okres. Certyfikat może zostać odnowiony tylko przed upływem jego okresu ważności przez urząd certyfikacji, który go wydał.

PIN (ang. Personal Identification Number) – jest to kod służący do uwierzytelnienia podmiotu i autoryzacji dostępu do komponentu technicznego lub magazynu danych w celu ich ochrony przed możliwością użycia przez podmioty nieuprawnione. Po trzykrotnym, błędnym następującym po sobie podaniu_następującym bezpośrednio po sobie, podaniu błędnego numeru PIN następuje blokada dostępu do komponentu technicznego lub magazynu danych.

Uwaga: Odblokowanie dostępu do komponentu technicznego, który znajduje się w stanie blokady, wymaga podania specjalnego numeru PUK. Z kolei odblokowanie dostępu do magazynu danych wymaga zwykle interwencji administratora magazynu i zmiany numeru PIN.

W komponencie technicznym może zostać wykorzystany mechanizm dodatkowego uwierzytelnienia za pomocą numeru PUK w celu wprowadzenia nowego numeru PIN.

Podpis elektroniczny – są to dane w postaci elektronicznej, które wraz z innymi danymi, do których zostały dołączone lub z którymi są logicznie powiązane, służą do identyfikacji osoby składającej podpis elektroniczny.

Polityka certyfikacji – dokument określający ogólne zasady stosowane podczas procesu certyfikacji kluczy publicznych. Definiuje uczestników procesu, ich obowiązki i odpowiedzialność, typy certyfikatów i ich dopuszczalne zastosowania oraz procedury weryfikacji tożsamości. Każdy urząd certyfikacji wydaje i stosuje własną politykę certyfikacji. Polityka jest publikowana w repozytorium internetowym. Każdej polityce certyfikacji przypisany jest jednoznaczny identyfikator obiektu.

Poświadczenie elektroniczne – dane w postaci elektronicznej, które wraz z innymi danymi, do których zostały dołączone lub logicznie z nimi powiązane, umożliwiają identyfikację podmiotu świadczącego usługi certyfikacyjne lub organu wydającego zaświadczenia certyfikacyjne spełniające wymagania określone w *Rozporządzeniem 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 *Ustawą z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. z 2016 r. poz. 1579).*

PUK (*ang. Personal Unblocking Key*) – to kod służący do odblokowania komponentu technicznego (najczęściej karty kryptograficznej) oraz zmiany kodu PIN. Numer PUK jest przydzielany do konkretnego komponentu technicznego w momencie wyodrębnienia na karcie potrzebnego profilu.

Punkt Rejestracji (PR) – placówka CERTUM – Powszechnego Centrum Certyfikacji, w której klient jest kompleksowo obsługiwany w zakresie świadczenia usług certyfikacyjnych. Główne zadania to:

- udzielanie informacji o możliwości zastosowania podpisu elektronicznego do użytku osobistego lub komercyjnego, o warunkach jego używania, skutkach, które wywołuje oraz o sposobie zakupu certyfikatu,
- przyjmowanie dokumentów Subskrybenta służących do potwierdzenia jego tożsamości, sprawdzenie autentyczności, sporządzenie z nich kopii oraz potwierdzenie zgodności z oryginałem,
- pomoc przy generowaniu dokumentów niezbędnych do wydania certyfikatu kwalifikowanego
- wydrukowanie i podpisanie dokumentów w wymaganej liczbie egzemplarzy,
- prezentowanie autorskich programów do podpisywania i weryfikacji podpisu (na życzenie klienta),
- prowadzenie sprzedaży kart oraz zestawów do składania bezpiecznego podpisu.
- przyjmowanie wniosków o wymianę karty kryptograficznej.
- przyjmowanie wniosków o unieważnienie certyfikatu.

Punkt Potwierdzania Tożsamości (PPT) – funkcjonuje u Partnerów Asseco Data Systems S.A.

Ich funkcją jest:

- udzielanie informacji o możliwości zastosowania podpisu elektronicznego do użytku osobistego lub komercyjnego, o warunkach jego używania, skutkach, które wywołuje oraz o sposobie zakupu certyfikatu,
- przyjmowanie dokumentów Subskrybenta służących weryfikacji i potwierdzenia tożsamości sporządzenie z nich kopii oraz potwierdzenie zgodności z oryginałem,
- pomoc w wypełnianiu dokumentów niezbędnych do wydanie certyfikatu kwalifikowanego
- wydrukowanie i podpisanie umów w wymaganej liczbie egzemplarzy,
- prezentowanie autorskich programów do podpisywania i weryfikacji podpisu (na życzenie klienta),
- prowadzenie sprzedaży kart oraz zestawów do składania bezpiecznego podpisu.

Repozytorium (podmiotu świadczącego usługi certyfikacyjne) – zbiór publicznie dostępnych katalogów elektronicznych zawierających wydane certyfikaty oraz dokumenty związane z funkcjonowaniem CERTUM PCC.

Strona ufająca (*ang. relying party*) – odbiorca, który otrzymał informację zawierającą certyfikat oraz podpis elektroniczny weryfikowany przy pomocy klucza publicznego umieszczonego w tym certyfikacie. Strona ta decyduje o uznaniu lub odrzuceniu podpisu na podstawie zaufania do certyfikatu o uznaniu lub odrzuceniu podpisu.

Zamawiający (płatnik) – osoba lub instytucja, która w imieniu subskrybenta finansuje usługi certyfikacyjne na rzecz swojego przedstawiciela − Subskrybenta. Zamawiający jest właścicielem certyfikatu i przysługuje mu prawo do jego unieważnienia.

Subskrybent (certyfikatu) –osoba fizyczna, odbiorca usług certyfikacyjnych, do której jest przypisany certyfikat klucza publicznego, działająca w imieniu własnym i na rzecz Zamawiającego, na podstawie załączonego do niniejszej umowy pełnomocnictwa.

System Rejestracji – zespół podmiotów funkcjonujących w procesie świadczenia kwalifikowanych usług certyfikacyjnych oraz zasad i procedur regulujących ich działanie.

Unieważnienie certyfikatów (ang. certificates revocation) – procedury odwołania ważności pary kluczy (wycofania certyfikatu) w przypadku, gdy zachodzi konieczność unieważnienia subskrybentowi dostępu do tej pary i użycia ich w operacjach podpisu elektronicznego. Unieważniony certyfikat umieszczony jest na liście certyfikatów unieważnionych (CRL)

CERTUM - Powszechne Centrum Certyfikacji (zwane dalej CERTUM PCC) – jednostka usługowa Asseco Data Systems S.A., świadcząca usługi certyfikacyjne w zakresie wydawania kwalifikowanych certyfikatów klucza publicznego oraz znakowania czasem zgodnych z *Rozporządzeniem 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 *Ustawą z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. z 2016 r. poz. 1579).*

Urząd certyfikacji – podmiot świadczący usługi certyfikacyjne, będący elementem składowym zaufanej trzeciej strony, zdolny do tworzenia, poświadczania i wydawania certyfikatów, zaświadczeń certyfikacyjnych oraz tokenów znacznika czasu i statusu certyfikatu – w przypadku niniejszego Regulaminu.

Użytkownik (certyfikatu, *ang. end entity*) – uprawniony podmiot, posługujący się certyfikatem jako Subskrybent lub strona ufająca, z wyłączeniem urzędu certyfikacji.

Weryfikacja statusu certyfikatów (*ang. validation of public key certificates*) – umożliwia określenie czy certyfikat jest ważny czy ijest unieważniony.

Wnioskodawca – określenie używane w stosunku do Subskrybenta w okresie pomiędzy chwilą gdy wystąpił z jakimkolwiek żądaniem (wnioskiem) do urzędu certyfikacji, a momentem ukończenia procedury wydawania certyfikatu.

X.500 – norma międzynarodowa określająca protokół dostępu do katalogu DAP (*ang. Directory Access Protocol*) oraz protokół usług katalogowych DSP (*ang. Directory Service Protocol*).

Zaufana Trzecia Strona – instytucja lub jej przedstawiciel, mający zaufanie podmiotu uwierzytelnionego i/lub podmiotu weryfikującego oraz innych podmiotów w zakresie działań związanych z zabezpieczeniem oraz z uwierzytelnianiem.

Zaświadczenie certyfikacyjne – elektroniczne zaświadczenie za pomocą którego dane służące do weryfikacji poświadczenia elektronicznego są przyporządkowane do podmiotu świadczącego usługi certyfikacyjne lub organu, zgodnie z *Rozporządzeniem 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 *Ustawą z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. z 2016 r. poz. 1579)*, i które umożliwiają identyfikację tego podmiotu lub organu.

Zawieszenie certyfikatu (ang. suspension) – szczególna forma unieważnienia certyfikatu (i związanej z nim pary kluczy), której wynikiem jest czasowy brak akceptacji certyfikatu w operacjach kryptograficznych (niezależnie od statusu tej operacji); zawieszony certyfikat umieszczany jest na liście certyfikatów unieważnionych (CRL).

Rozdział II. Umowy o świadczenie usług certyfikacyjnych w zakresie wydawania i unieważniania kwalifikowanego certyfikatu

§4 Czynności przygotowawcze

1. W celu otrzymania certyfikatu kwalifikowanego należy zakupić Zestaw CERTUM PCC do składania podpisu elektronicznego w sklepie internetowym CERTUM PCC, Punktach Rejestracji CERTUM PCC lub w Punktach Partnerskich.
2. Wynagrodzenie Asseco Data Systems S.A. z tytułu umów o świadczenie usług certyfikacyjnych jest określane na podstawie obowiązującego cennika.
3. Wysokość opłat za poszczególne rodzaje usług certyfikacyjnych jest opublikowana w cenniku, dostępnym pod adresem: www.certum.pl
4. Subskrybent może samodzielnie aktywować kartę kryptograficzną na stronie internetowej www.certum.pl, wypełniając jeden z dostępnych formularzy aktywacyjnych (stosownie do żądanego rodzaju certyfikatu którym, chce się posługiwać) lub skorzystać z pomocy operatora w jednym z Punktów Rejestracji CERTUM PCC lub Punktów Potwierdzenia Tożsamości. Usługa ta w Punktach Rejestracji jest bezpłatna.
5. Rodzaje certyfikatów kwalifikowanych:
   - Certyfikat osobisty (**uniwersalny**) – zawierający wyłącznie dane Subskrybenta (osoby fizycznej),
   - Certyfikat profesjonalny (**z dodatkowymi danymi**) - zawierający dane Subskrybenta (osoby fizycznej) oraz dodatkowe dane identyfikujące podmiot reprezentowany przez Subskrybenta.

I. Formularz aktywacji karty kryptograficznej w przypadku certyfikatu uniwersalnego składa się między innymi z następujących danych:

1) Numeru karty kryptograficznej, znajdującej się na rewersie karty kryptograficznej
2) Danych wnioskodawcy
3) Danych dotyczących dokumentu tożsamości wnioskodawcy
   - Nazwa dokumentu
   - Cechy (seria i numer)
   - Organ wydający
4) Danych kontaktowych wnioskodawcy
   - Adres poczty elektronicznej
   - Telefon
5) Nazwy powszechnie stosowanej
   - Nazwa identyfikująca wnioskodawcę (imię i nazwisko Subskrybenta)
6) Adresu do korespondencji
7) Wybór podmiotu lub osoby, która pomogła w zakupie zestawu i wypełnienie wniosku o wydanie certyfikatu kwalifikowanego

Dodatkowo

- Subskrybent decyduje, które dane mają być widoczne w certyfikacie:
  - numer NIP lub/i numer PESEL - istnieje konieczność zamieszczenia jednego z numerów

II. Formularz aktywacji karty kryptograficznej w przypadku certyfikatu z dodatkowymi danymi składa się z następujących danych:

1) Numeru karty kryptograficznej, znajdującej się na rewersie karty kryptograficznej
2) Danych wnioskodawcy
3) Danych dotyczących charakteru prawnego wnioskodawcy
   - W imieniu własnym (np. jako osoba fizyczna prowadząca indywidualną działalność gospodarczą)
   - Jako przedstawiciel osoby prawnej lub jednostki organizacyjnej nieposiadającej osobowości prawnej
   - Jako członek organu albo organ osoby prawnej lub jednostki organizacyjnej nieposiadającej osobowości prawnej
   - Jako organ władzy publicznej
4) Danych dotyczących dokumentu tożsamości wnioskodawcy
   - Nazwa dokumentu
   - Cechy (seria i numer)
   - Organ wydający
5) Danych kontaktowych wnioskodawcy
   - Adres poczty elektronicznej
   - Telefon
6) Danych podmiotu w imieniu którego będzie występował wnioskodawca
   - Nazwa reprezentowanego podmiotu
   - Nazwa skrócona
   - Nazwa jednostki organizacyjnej
   - Numer REGON
   - Numer NIP
   - Nr podstawy prawnej funkcjonowania
   - Dane organu rejestrowego
   - Osoba lub osoby upoważnione do reprezentowania danego podmiotu
7) Danych kontaktowych reprezentowanego podmiotu
   - Adres poczty elektronicznej
   - Telefon
8) Danych pocztowych reprezentowanego podmiotu
9) Nazwy powszechnie stosowanej czyli
   - Nazwy identyfikującej wnioskodawcę (imię i nazwisko Subskrybenta oraz nazwa skrócona podmiotu)
10) Stanowisko wnioskodawcy w reprezentowanym podmiocie
11) Adresu do korespondencji (taki sam jak adres reprezentowanego podmiotu lub inny do wyboru)
12) Wybór podmiotu lub osoby, która pomogła w zakupie zestawu i wypełnienie wniosku o wydanie certyfikatu kwalifikowanego

Dodatkowo

Subskrybent decyduje, które dane mają być widoczne w certyfikacie:

- numer NIP lub/i numer PESEL - istnieje konieczność zamieszczenia jednego z numerów

6. Przy wypełnianiu elektronicznego formularza aktywacyjnego Subskrybent wyraża w formie elektronicznego oświadczenia dobrowolną zgodę na:

   - przetwarzanie danych osobowych na potrzeby niezbędne do realizacji procesu certyfikacji oraz przesłania drogą elektroniczną na wskazany adres e-mail, dokumentów wypełnionych danymi Subskrybenta
   - otrzymywanie informacji o aktualnej ofercie Asseco Data Systems S.A. i przetwarzanie danych osobowych Subskrybenta w celach marketingowych

   Dane Subskrybenta są przetwarzane przez Asseco Data Systems S.A., z siedzibą w Gdyni przy ul. Żwirki i Wigury 15, zgodnie z *Ustawą o ochronie danych osobowych, (Dz.U. z 2016 poz. 922,*

tekst jednolity ustawy). Subskrybentom przysługuje prawo do wglądu i poprawienia przekazanych danych osobowych.

7. Wysłane za pośrednictwem formularza internetowego informacje posłużą CERTUM PCC do automatycznego wygenerowania dokumentów formalnych wymaganych w procesie certyfikacyjnym. System automatycznie nadaje numer umowy, obejmujący każdy z dokumentów, przy każdorazowym wypełnieniu formularza aktywacyjnego karty kryptograficznej.
8. Wprowadzone do formularza elektronicznego dane, przed wysłaniem do CERTUM PCC należy zweryfikować. W przypadku wykrycia błędów należy ponownie wypełnić formularz aktywacyjny karty kryptograficznej. Subskrybent na podany w formularzu adres e-mail otrzymuje informację o złożeniu zamówienia wraz z numerem umowy oraz linkiem (https://status.certum.pl/wniosek/), za pośrednictwem którego pobiera ze strony WWW wygenerowane dokumenty certyfikacyjne w formacie PDF. W przypadku wielokrotnego wygenerowania dokumentów można je każdorazowo pobrać z systemu Certum PCC, logując się z przypisanym kolejnym numerem umowy.
9. Numer karty kryptograficznej wiązany jest z osobą Subskrybenta. W przypadku gdy zostanie wprowadzony numer karty kryptograficznej, który już wcześniej został powiązany z innym numerem PESEL, Subskrybent otrzymuje drogą elektroniczną informację o tym fakcie, a generowanie dokumentów dla danej karty kryptograficznej nie zostanie zrealizowane. W przypadku konieczności wygenerowania nowych dokumentów na numer karty kryptograficznej, który został już wcześniej przypisany do innej osoby, należy zgłosić zaistniałą sytuację infolinii.
10. System Certum PCC generuje automatycznie w zależności od wybranego formularza (rodzaj certyfikatu kwalifikowanego) dokumenty formalne, które Subskrybent zobowiązany jest wydrukować:
    - w przypadku certyfikatu uniwersalnego:
        - Umowa z Subskrybentem (2 egzemplarze)
        - Załącznik nr 1 - Wniosek o wydanie certyfikatu kwalifikowanego (2 egzemplarze)
        - Oświadczenie o potwierdzeniu tożsamości wnioskodawcy (1 egzemplarz)
        - Instrukcja postępowania (opcjonalnie)
    - w przypadku certyfikatu z dodatkowymi danymi:
        - Umowa z Subskrybentem (2 egzemplarze)
        - Załącznik nr 1 - Wniosek o wydanie certyfikatu kwalifikowanego (2 egzemplarze)
        - Oświadczenie o potwierdzeniu tożsamości wnioskodawcy (1 egzemplarz)
        - Pełnomocnictwo (1 egzemplarz)
        - Instrukcja postępowania (opcjonalnie)
11. Subskrybent jest zobowiązany do zapoznania się z treścią dokumentów formalnych i sprawdzenia poprawności wprowadzonych danych. W przypadku wykrycia błędów, w wygenerowanych dokumentach formalnych, należy ponownie wypełnić odpowiedni formularz aktywacyjny.
12. W przypadku wykrycia odręcznych poprawek lub modyfikacji w wygenerowanych automatycznie dokumentach formalnych CERTUM PCC zastrzega sobie prawo do odrzucenia dokumentów. Subskrybent jest powiadamiany o fakcie odrzucenia dokumentów i jego przyczynie.
13. Osoba upoważniona do reprezentacji podmiotu udziela pełnomocnictwa osobie, dla której ma zostać wydany certyfikat kwalifikowany. Pełnomocnictwo upoważnia do podpisania umowy z Asseco Data Systems S.A. (zwanej dalej „Umową z Subskrybentem) na świadczenie usług certyfikacyjnych, w tym na wydanie certyfikatu kwalifikowanego, którego użytkownikiem będzie upełnomocniona osoba. Pełnomocnictwo jest ważne od dnia umocowania do dnia jego odwołania.
14. Subskrybent zobowiązany jest do przygotowania pełnomocnictwa wg poniższych instrukcji:
    - uzyskania czytelnego podpisu(ów) lub skróconego podpisu(ów) wraz z pieczątką(ami) imienną na dokumencie, zgodnego z zasadami reprezentacji podmiotu,
    - umieszczenia pieczęci nagłówkowej podmiotu w lewym górnym rogu dokumentu,

- określenia miejscowości i daty wystawienia dokumentu w prawym górnym rogu dokumentu.

Pełnomocnictwo nie jest wymagane w przypadku gdy Subskrybent jest upoważniony do samodzielnej reprezentacji firmy / jednostki / instytucji (np. prezes zarządu, dyrektor, wójt, burmistrz, prezydent lub osoby prowadzące indywidualną działalność gospodarczą itp.). Konieczność przedłożenia pełnomocnictwa uzależniona jest od zapisanego w KRS/CEiDG lub akcie wyboru / mianowania na stanowisko lub pełnomocnictwie notarialnym, sposobu reprezentacji firmy, jednostki, instytucji.

15. Przed zawarciem umowy o świadczenie usług certyfikacyjnych z Subskrybentem, CERTUM PCC informuje o warunkach użycia kwalifikowanego certyfikatu, w tym o sposobie rozpatrywania skarg i sporów, a w szczególności o istotnych warunkach obejmujących:
    a) zakres i ograniczenia stosowania kwalifikowanego certyfikatu,
    b) skutki prawne składania podpisów elektronicznych weryfikowanych przy pomocy tego certyfikatu,
    c) informacje o systemie dobrowolnej rejestracji kwalifikowanych podmiotów świadczących usługi certyfikacyjne i ich znaczeniu.

    Wnioskodawca potwierdza fakt zapoznania się z warunkami użycia kwalifikowanego certyfikatu stosownym oświadczeniem (Załącznik nr 1 do Umowy z Subskrybentem).

16. Za prawdziwość danych podanych w formularzu o wydanie certyfikatu odpowiada Subskrybent.

17. Szczegółowe dane na temat dokumentów niezbędnych w procesie weryfikacji tożsamości Subskrybenta zawarte są w niniejszym Regulaminie Kwalifikowanych Usług Certyfikacyjnych CERTUM PCC oraz na stronie internetowej www.certum.pl .

18. Aktualna lista wymaganych dokumentów w przypadku certyfikatu uniwersalnego oraz certyfikatu z dodatkowymi danymi znajduje się na stronie internetowej www.certum.pl.

19. Subskrybent jest zobowiązany zapoznać się z niniejszym Regulaminem przed zawarciem umowy.

§5 Weryfikacja tożsamości

1. Zgodnie z zapisem w *Ustawie o usługach zaufania oraz identyfikacji elektronicznej* Art. 14 „Kwalifikowany dostawca usług zaufania, wydając kwalifikowany certyfikat podpisu elektronicznego, jest obowiązany: uzyskać od osoby ubiegającej się o certyfikat potwierdzenie przyporządkowania do niej danych służących do weryfikacji podpisu elektronicznego, które są zawarte w wydanym certyfikacie;" (Dz.U. 2016 r. Nr 1579).

2. Wnioskodawca wraz z wygenerowanym kompletem dokumentów potwierdza swoją tożsamość w jednym z dostępnych Punktów Sieci Systemu Rejestracji CERTUM PCC:
    - Punktach Rejestracji CERTUM PCC (usługa bezpłatna).
    - Punktach Potwierdzenia Tożsamości.

    CERTUM PCC dopuszcza przedstawienie notarialnego potwierdzenia tożsamości Subskrybentów.

3. Subskrybent jest zobowiązany do przedstawienia Operatorowi Punktu Sieci Systemu Rejestracji CERTUM PCC dokumentu pozwalającego stwierdzić jego tożsamość, którym może być:
    - ważny dowód osobisty lub paszport RP

    W przypadku obcokrajowców:
    - ważny paszport EU i/lub paszport zagraniczny
    - karta stałego pobytu na terytorium RP (obligatoryjnie, jeżeli posiada)

    CERTUM PCC wymaga kserokopii paszportu (obligatoryjnie w przypadku występowania znaków specjalnych - diakrytycznych) oraz kserokopii karty stałego pobytu na terytorium RP (jeżeli posiada).

4. Operator Punktu Sieci Systemu Rejestracji CERTUM PCC weryfikuje tożsamość Subskrybenta na podstawie przedstawionego dokumentu tożsamości. Weryfikuje poprawność przedłożonego kompletu dokumentów formalnych do wydania certyfikatu kwalifikowanego.

5. Subskrybent, w obecności Operatora Punktu Rejestracji CERTUM PCC lub Punktu Potwierdzenia Tożsamości CERTUM PCC, podpisuje dokumenty formalne (Załącznik nr 1 do Umowy z Subskrybentem oraz Umowę z Subskrybentem). W przypadku notarialnego potwierdzenia tożsamości, CERTUM PCC wymaga wyłącznie poświadczenia podpisu na jednym egzemplarzu

Załącznika nr 1 do Umowy z Subskrybentem, pozostałe dokumenty (drugi egzemplarz Załącznika nr 1 do Umowy z Subskrybentem oraz dwa egzemplarze Umowy z Subskrybentem) Subskrybent zobowiązany jest podpisać własnoręcznie bez notarialnego poświadczenia podpisu.

6. Operator Punktu Rejestracji CERTUM PCC przekazuje komplet wymaganych dokumentów Subskrybenta do CERTUM PCC. Są to: Umowa z Subskrybentem, Załącznik nr 1 oraz Oświadczenie o potwierdzeniu tożsamości Subskrybenta a także Pełnomocnictwo wraz z dokumentami określającymi zasady reprezentacji, na adres:

   CERTUM PCC – Powszechne Centrum Certyfikacji
   ul. Bajeczna 13
   71-838 Szczecin

7. W przypadku weryfikacji tożsamości przez Punkt Potwierdzenia Tożsamości, Subskrybent przekazuje Umowę z Subskrybentem (2 egzemplarze), Załącznik nr 1 (2 egzemplarze) oraz Oświadczenie o potwierdzeniu tożsamości Subsrybenta (1 egzemplarz) a także Pełnomocnictwo (1 egzemplarz) wraz z dokumentami określającymi zasady reprezentacji (tylko w przypadku certyfikatu z dodatkowymi danymi), na adres:

   CERTUM PCC – Powszechne Centrum Certyfikacji
   ul. Bajeczna 13
   71-838 Szczecin

8. W przypadku notarialnego poświadczenia podpisu Subskrybenta na Załączniku numer 1, dokonanego przez notariusza, należy przesłać Umowę z Subskrybentem (2 egzemplarze) wraz z Załącznikiem nr 1 (2 egzemplarze, w tym jeden egzemplarz z notarialnym poświadczeniem podpisu), Pełnomocnictwo (1 egzemplarz) oraz dokumenty określające zasady reprezentacji (tylko w przypadku certyfikatu z dodatkowymi danymi) na adres:

   CERTUM PCC – Powszechne Centrum Certyfikacji
   ul. Bajeczna 13
   71-838 Szczecin

9. Certyfikat kwalifikowany będzie wydany tylko po otrzymaniu przez CERTUM PCC pełnego kompletu dokumentów formalnych, wymaganych do wydania certyfikatu kwalifikowanego o tym samym numerze umowy oraz kompletu wymaganych dokumentów podmiotu (wyłącznie w przypadku certyfikatu z dodatkowymi danymi). W przypadku niedostarczenia wymaganego kompletu dokumentów formalnych, dostarczenia dokumentów o różnym numerze umowy lub niedostarczenia wymaganego kompletu dokumentów podmiotu (wyłącznie w przypadku certyfikatu z dodatkowymi danymi) CERTUM PCC zastrzega sobie prawo do ich odesłania do Subskrybenta w terminie 3 miesięcy od daty wpłynięcia. Aktualna lista wymaganych dokumentów reprezentowanego podmiotu w przypadku certyfikatów z dodatkowymi danymi znajduje się na stronie internetowej www.certum.pl.

§6 Pobranie certyfikatu kwalifikowanego na kartę kryptograficzną

1. Po pozytywnej weryfikacji kompletu dokumentów Subskrybenta, CERTUM PCC wydaje certyfikat kwalifikowany.

2. Subskrybent otrzymuje na adres e-mail, podany w elektronicznym formularzu aktywacji karty, informację o wydaniu przez CERTUM PCC certyfikatu kwalifikowanego.

3. W wiadomości elektronicznej Subskrybent otrzymuje unikalny TELEKOD przypisany do:
   - umowy na podstawie której został wydany certyfikat kwalifikowany,
   - danych osobowych Subskrybenta,
   - numeru karty kryptograficznej.

   Subskrybent otrzymuje link do strony, zabezpieczonej protokołem SSL, za pośrednictwem której pobiera certyfikat kwalifikowany.

4. CERTUM PCC zaleca automatyczną instalację certyfikatu kwalifikowanego na karcie kryptograficznej, odbywającą się w 2 krokach:
   - Krok 1 - Nadanie kodu PIN.

- Krok 2 - Akceptacja certyfikatu.

Istnieje możliwość ręcznej instalacji certyfikatu kwalifikowanego na karcie kryptograficznej z wykorzystaniem oprogramowania proCertum CardManager dostępnego na stronie www.certum.pl

5. Subskrybent zobowiązany jest do zapoznania się z informacjami dotyczącymi kodów PUK i PIN, podanymi w procesie pobrania certyfikatu. W szczególności Subskrybent zobowiązany jest:
   - zapisać przypisany do karty kryptograficznej kod PUK i przechowywać go w bezpiecznym miejscu
   - nadać kod PIN do karty kryptograficznej i przechowywać go w bezpiecznym miejscu

Uwaga: po zainstalowaniu certyfikatu, zalecane jest ustanowienie nowego kodu PUK za pośrednictwem oprogramowania proCertumCardManager (aplikacja do pobrania na stronie www.certum.pl)

6. Trzykrotne błędne podanie kodu PIN podczas składania kwalifikowanego podpisu elektronicznego blokuje kod PIN karty kryptograficznej. Do odblokowania kodu PIN w aplikacji proCertumCardManager wymagany jest kod PUK.
7. Trzykrotne błędne podanie kodu PUK podczas odblokowania kodu PIN trwale blokuje kartę kryptograficzną. Szczegółowych informacji w zakresie wymiany karty kryptograficznej udziela Infolinia oraz Punkty Rejestracji CERTUM PCC.
8. Subskrybent zobowiązany jest zweryfikować poprawność swoich danych osobowych oraz danych podmiotu (obecnych wyłącznie w certyfikacie z dodatkowymi danymi), zawartych w wydanym certyfikacie kwalifikowanym oraz zaakceptować otrzymany certyfikat kwalifikowany w Oświadczeniu o akceptacji certyfikatu.
9. Akceptacja Subskrybenta równoznaczna jest z przyjęciem przez CERTUM PCC informacji o poprawności wydanego certyfikatu kwalifikowanego. Dane zawarte w wydanym certyfikacie kwalifikowanym po akceptacji mogą zostać zmienione wyłącznie poprzez ponowne wydanie certyfikatu kwalifikowanego.
10. W przypadku wykrycia błędów w danych osobowych Subskrybenta lub danych podmiotu (obecnych wyłącznie w certyfikacie z dodatkowymi danymi), Subskrybent zobowiązany jest powiadomić o tym fakcie CERTUM PCC w Oświadczeniu o akceptacji certyfikatu, podając przyczynę. Decyzja może być zmieniona tylko gdy zostanie podjęta decyzja o braku akceptacji certyfikatu.
11. W przypadku wykrycia błędów w danych osobowych Subskrybenta lub danych podmiotu w certyfikacie z dodatkowymi danymi po jego akceptacji należy problem zgłosić na Infolinię.
12. Szczegółowe informacje na temat procesu pobrania certyfikatu kwalifikowanego na kartę kryptograficzną znajdują się na stronie internetowej: www.certum.pl

§7 Zawarcie umowy

1. W CERTUM PCC funkcjonują dwa rodzaje umów zawieranych pomiędzy Subskrybentem a Asseco Data Systems S.A.:
   - umowa zawierana pomiędzy Asseco Data Systems S.A. a Subskrybentem indywidualnym tzn. występującym w imieniu własnym,
   - umowa zawierana pomiędzy Asseco Data Systems S.A. a Subskrybentem, występującym w imieniu Zamawiającego (czyli osoby fizycznej, prawnej, jednostki organizacyjnej nieposiadającej osobowości prawnej, organu władzy publicznej).
2. Przez zawarcie umowy, Asseco Data Systems S.A. zobowiązuje się do:
   - wydania certyfikatu kwalifikowanego zgodnie z danymi określonymi we wniosku o wydanie kwalifikowanego certyfikatu, stanowiącym integralną część Umowy (załącznik nr 1) w terminie 7 dni roboczych od daty wpłynięcia do CERTUM PCC kompletu wymaganych i poprawnie wypełnionych dokumentów. Za datę podpisania umowy uznaje się dzień jej wpłynięcia do siedziby Asseco Data Systems S.A.

- świadczenia usług zgodnie z warunkami określonymi w Rozporządzeniu 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, Ustawą z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. z 2016 r. poz. 1579), Regulaminem oraz postanowieniami Polityki Certyfikacji i Kodeksu Postępowania Certyfikacyjnego
- powiadamiania drogą elektroniczną o konieczności odnowienia certyfikatu kwalifikowanego co najmniej 7 dni roboczych przed upływem terminu jego ważności.
- nieodpłatnego udostępniania Subskrybentom usługi kwalifikowanego znakowania czasem do wykorzystania wyłącznie w aplikacji SmartSign[1],
- odmowy wykonania usługi kwalifikowanego znakowania czasem w przypadku przekroczenia przez Subskrybenta limitu przyznanych mu znaczników czasu[2].

3. Czas trwania umowy z Subskrybentem jest tożsamy z okresem ważności certyfikatu wydanego na jej podstawie, tj.: maksymalnie na okres dwóch lat.
4. Rozpoczęcie świadczenia usług przez CERTUM PCC, będących przedmiotem zawartej Umowy, następuje nie później niż 7 dni roboczych po dostarczeniu kompletu wymaganych, poprawnych dokumentów do Asseco Data Systems S.A..

§8 Rozwiązanie i wygaśnięcie umowy

1. Subskrybent może wypowiedzieć umowę za uprzednim pisemnym czternastodniowym wypowiedzeniem. W takim przypadku CERTUM PCC unieważnia certyfikat Subskrybenta z dniem końca okresu wypowiedzenia.
2. Asseco Data Systems S.A. może wypowiedzieć umowę w każdym czasie ze skutkiem natychmiastowym lub zaprzestać świadczenia usług w razie:
   - naruszenia przez Subskrybenta postanowień Regulaminu, Kodeksu Postępowania Certyfikacyjnego lub właściwej Polityki Certyfikacji,
   - podania przez Subskrybenta nieprawdziwych danych lub posługiwania się podrobionymi lub przerobionymi dokumentami przy zawieraniu lub w trakcie wykonywania Umowy.
3. Umowa zostaje zawarta na czas określony, za której termin wygaśnięcia uważa się termin ważności certyfikatu.
4. Umowa wygaśnie samoistnie w przypadku:
   - zakończenia działalności przez CERTUM PCC,
   - prawomocnego zakończenia postępowania likwidacyjnego albo upadłościowego CERTUM PCC,
   - śmierci Subskrybenta,
   - upłynięcia terminu ważności certyfikatu.

Jeśli umowa wygasła przed upływem terminu ważności certyfikatu, to CERTUM PCC unieważnia certyfikat kwalifikowany wydany na jej podstawie.

[1] Usługa obejmuje swoim zakresem możliwość pobrania do 5000 kwalifikowanych znaczniów czasu w okresie jednego miesiąca.

[2] W przypadku potrzeby wykorzystania kwalifikowanych znaczników czasu w innych aplikacjach lub w większej ich ilości należy zamówić jeden z dostępnych na stronie https://www.certum.pl/certum/cert,oferta_znaczniki_czasu.xml komercyjnych pakietów oferowanych przez CERTUM PCC.

Rozdział III. Zasady odpowiedzialności

§9 Zobowiązania i odpowiedzialność CERTUM PCC

1. CERTUM PCC gwarantuje, że*;*
   - swoją działalność komercyjną realizuje w oparciu o wiarygodny sprzęt i oprogramowanie tworzące system, który spełnia wymagania określone w CWA 14167-1 Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements,
   - działalność oraz świadczone usługi są zgodne z prawem i w szczególności nie naruszają praw autorskich i licencyjnych stron trzecich,
   - świadczone usługi są zgodne z powszechnie akceptowanymi normami i standardami, m.in. z zaleceniami X.509, PKCS#7, PKCS#10 i PKCS#12,
   - wystawiane certyfikaty nie zawierają żadnych nieprawdziwych danych, które byłyby znane lub które powstałyby w wyniku zaniedbań lub naruszenia procedur przez osoby zatwierdzające wnioski o wystawienie certyfikatów lub wystawiające te certyfikaty,
   - nazwy wyróżnione (DN) Subskrybentów umieszczane w certyfikatach są unikalne w domenie nazw CERTUM PCC,
   - zapewnia ochronę danych osobowych Subskrybenta zgodnie z *Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych oraz Rozporządzeniem MSWiA z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych z póź. zm.,*
   - nie kopiuje, ani nie przechowuje kluczy prywatnych swoich Subsrybentów, służących do składania podpisów elektronicznych.
   - zatrudnia pracowników posiadających wiedzę, kwalifikacje i doświadczenie odpowiednie do pełnienia funkcji związanych z usługami certyfikacyjnymi, w szczególności obejmujących dziedziny:
     a. automatycznego przetwarzania danych w sieciach i systemach teleinformatycznych,
     b. mechanizmów zabezpieczania sieci i systemów teleinformatycznych,
     c. kryptografii, podpisów elektronicznych i infrastruktury klucza publicznego,
     d. sprzętu i oprogramowania stosowanego do elektronicznego przetwarzania danych.
2. CERTUM PCC zobowiązuje się do :
   - publikowania aktualnych wersji Kodeksu Postępowania Certyfikacyjnego i Polityki Certyfikacji i Regulaminu w repozytorium,
   - prowadzenia listy zarejestrowanych punktów sieci Systemu Rejestracji,
   - udostępnienia odbiorcom usług certyfikacyjnych wykazu bezpiecznych urządzeń do składania i weryfikacji podpisów elektronicznych,
   - zachowania w tajemnicy informacji związanych ze świadczeniem usług certyfikacyjnych, których nieuprawnione ujawnienie mogłoby narazić na szkodę CERTUM PCC lub odbiorcę usług certyfikacyjnych przez okres 10 lat od ustania stosunków prawnych, o których mowa w art. 15 Ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. z 2016 r. poz. 1579), oraz do zachowanie w tajemnicy danych do składania podpisu elektronicznego lub pieczęci elektronicznej,
   - przechowywania dokumentów i danych, o których mowa w ust.1, przez 20 lat od dnia ich wytworzenia.

3. Autoryzowane przez CERTUM PCC punkty sieci Systemu Rejestracji zobowiązane są do:
   - podporządkowania się w całości zaleceniom CERTUM PCC,
   - świadczenia usług na zasadach jakie obowiązują w CERTUM PCC, tj.: świadczenia względem Subskrybentów usług certyfikacyjnych w zakresie weryfikacji tożsamości przy wydawaniu i unieważnianiu kwalifikowanych certyfikatów zgodnie z zasadami określonymi w Kodeksie Postępowania Certyfikacyjnego i Polityce Certyfikacji, procedurach wewnętrznych oraz w obowiązujących przepisach prawa i zasadach współżycia społecznego ze szczególnym uwzględnieniem dochowania należytej staranności,
   - przesyłania do CERTUM PCC potwierdzonych danych Subskrybenta,
   - poddawania się planowym audytom przeprowadzanym lub zlecanym przez CERTUM PCC.
4. CERTUM PCC nie ponosi odpowiedzialności za:
   - szkody wyrządzone osobom trzecim przy użyciu wystawionego kwalifikowanego certyfikatu chyba, że zostanie udowodnione, iż CERTUM PCC w sposób ewidentny naruszyło zasady niniejszego Regulaminu, Polityki Certyfikacji i Kodeksu Postępowania Certyfikacyjnego,
   - szkody wynikłe przy użyciu wydanego certyfikatu, dokonane z przekroczeniem zakresu czynności prawnych objętych umocowaniem zawartym w kwalifikowanym certyfikacie.
5. CERTUM PCC nie będzie dokonywać wpisów w „dodatkowych polach" certyfikatu, zawierających treści naruszające dobra osobiste osób trzecich, obowiązujące zasady współżycia społecznego oraz dobre obyczaje.

§10 Zobowiązania i odpowiedzialność Zamawiającego

1. Zamawiający oświadcza, że:
   - wyraża zgodę na przetwarzanie swoich danych osobowych zgodnie z ustawą z dn. 29.08.1997 r. O ochronie danych osobowych (*Dz.U. z 2016 poz. 922, tekst jednolity ustawy*) realizacji niniejszej umowy
   - wyraża zgodę na pokrycie kosztów wydania certyfikatu kwalifikowanego dla Subskrybenta na podstawie załączonego Pełnomocnictwa,
2. Zamawiający zobowiązany jest do:
   - Wypełnienia druku otrzymanego pisemnego pełnomocnictwa dla Subskrybenta, z którego jednoznacznie wynika:
     - dla kogo wystawione jest pełnomocnictwo,
     - zgoda na składanie podpisów elektronicznych przez Subskrybenta w imieniu i na rzecz Zamawiającego.
   - Zgłoszenia CERTUM PCC żądania unieważnienia certyfikatu w przypadkach przewidzianych ustawowo i w przypadku cofnięcia pełnomocnictwa.

§11 Zobowiązania i odpowiedzialność Subskrybenta

1. Podpisując umowę Subskrybent wyraża zgodę na przystąpienie do systemu certyfikacji na warunkach określonych w umowie oraz niniejszym Regulaminie Kwalifikowanych Usług Certyfikacyjnych oraz Polityce Certyfikacji CERTUM PCC.
2. Subskrybent zobowiązuje się do:
   - przestrzegania postanowień umowy podpisanej z 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 podanych we wniosku w elektronicznym formularzu, w celu wypełnienia określonych w Polityce Certyfikacji wymagań procesu rejestracji, unieważnienia i odnowienia certyfikatu,
- przechowywania danych, służących do składania kwalifikowanego podpisu elektronicznego w taki sposób, aby zapewnić ich należytą ochronę przed nieuprawnionym wykorzystaniem w okresie ważności wydanego certyfikatu,
- zabezpieczenia i ochrony dostępu do nośników na których przechowywane są hasła i klucze,
- zweryfikowania poprawności swoich danych osobowych oraz danych podmiotu (obecnych wyłącznie w certyfikacie z dodatkowymi danymi), zawartych w wydanym certyfikacie kwalifikowanym oraz zaakceptować otrzymany certyfikat kwalifikowany w Oświadczeniu o akceptacji certyfikatu,
- złożenia żądania unieważnienia certyfikatu kwalifikowanego w przypadkach:
    a. gdy w procesie akceptacji certyfikatu kwalifikowanego, Subskrybent stwierdza jego wadę,
    b. gdy dane służące do składania kwalifikowanego podpisu elektronicznego związane z danymi służącymi do weryfikacji podpisu elektronicznego zawartymi w certyfikacie zostały ujawnione,
    c. gdy nastąpiła jakakolwiek zmiana danych zawartych w wystawionym certyfikacie określonych w Regulaminie Usług Certyfikacyjnych lub Kodeksie Postępowania Certyfikacyjnego,
- używania swojej pary kluczy i kluczy publicznych innych odbiorców usług certyfikacyjnych wyłącznie w sposób zgodny z Polityką Certyfikacji i zapewnienia bezpieczeństwa i integralności własnych kluczy prywatnych, włączając w to:
    a. kontrolę i zabezpieczenie dostępu do urządzeń zawierających jego klucze prywatne,
    b. niezwłoczne informowanie GPR o wszelkich okolicznościach, w wyniku których jego klucz prywatny został ujawniony osobom trzecim lub w wyniku których Subskrybent może podejrzewać, że klucz prywatny mógł ulec ujawnieniu osobom trzecim,
- nie składania podpisu elektronicznego przy pomocy należącego do niego klucza prywatnego, jeżeli certyfikat ten jest przeterminowany (minął jego okres ważności), jest unieważniony lub zawieszony,
- nieprzechowywania karty kryptograficznej zawierającej klucz prywatny razem z osobistym numerem identyfikacyjnym (PIN),
- 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,
- nie udostępniania i nie przekazywania swoich kluczy prywatnych oraz używanych przez siebie haseł osobom trzecim,
- niezwłocznego przystąpienia do procedury unieważnienia certyfikatu, w przypadku naruszenia ochrony (lub podejrzenia naruszenia ochrony) swojego klucza prywatnego
- wykorzystywania certyfikatu klucza publicznego oraz odpowiadającego klucza prywatnego tylko zgodnie z deklarowanym w certyfikacie przeznaczeniem, celami i ograniczeniami określonymi w Kodeksie Postępowania Certyfikacyjnego.

3. Subskrybent ponosi również odpowiedzialność za działania niezgodne z warunkami świadczenia usług certyfikacyjnych określonymi w umowie oraz w niniejszym Regulaminie, a w szczególności za:

- niewłaściwe stosowanie i brak odpowiedniego zabezpieczania przez Subskrybenta i osoby trzecie kluczy lub wydanych certyfikatów,
- wadliwą instalację i niewłaściwe użytkowanie aplikacji do składania podpisu elektronicznego,
- straty wynikłe z nieodpowiedniej jakości sprzętu stosowane przez Subskrybenta i osoby trzecie,
- szkody wynikłe z podania przez Subskrybenta nieprawdziwych lub fałszywych danych oraz za skutki nieprawidłowego użycia certyfikatu.

§12 Zasady odpowiedzialności Strony ufającej

1. Strona ufająca odpowiada za sposób weryfikacji aktualnego statusu certyfikatu Subskrybenta każdorazowo, gdy chce użyć certyfikatu do zweryfikowania podpisu elektronicznego poprzez sprawdzenie listy certyfikatów zawieszonych i unieważnionych. Strona ufająca powinna wykorzystać informacje zawarte w certyfikacie, do określenia czy podpis elektroniczny został złożony zgodnie z jego deklarowanym przeznaczeniem i zasadami określonymi w Polityce Certyfikacji.

Rozdział IV. Zasady świadczenia usług certyfikacyjnych

§13 Potwierdzanie tożsamości Subskrybentów.

1. Potwierdzenie tożsamości Wnioskodawcy musi wykazać, że Wnioskodawca jest rzeczywiście tą osobą, która została wymieniona we wniosku i przedłożonych dokumentach.
2. Weryfikacje tożsamości i pełnomocnictwa przeprowadzane są w celu uzyskania pewności, że informacje przekazywane do CERTUM PCC w celu umieszczenia w certyfikacie, są prawidłowe i wiarygodne w momencie przyjmowania wniosku.
3. Uwierzytelnianie Subskrybenta może być realizowane w Punktach Sieci Systemu Rejestracji.
4. Weryfikacja przeprowadzana jest obligatoryjnie podczas rejestracji Subskrybenta oraz na żądanie CERTUM PCC w przypadku każdej innej usługi certyfikacyjnej.
5. W celu zweryfikowania tożsamości przyszłego Subskrybenta, dopuszczane jest zastosowanie usługi notarialnego poświadczenia podpisu, realizowanej przez dowolną Kancelarię Notarialną.
6. Potwierdzenie tożsamości jest ważne przez okres 3 miesięcy od jego uzyskania. Zasady dotyczące ważności potwierdzenia tożsamości dotyczą także poświadczenia podpisu.

§14 Nazwy podmiotów umieszczane w certyfikacie

1. CERTUM PCC gwarantuje unikalność nazwy wyróżnionej (DN), przydzielonej podmiotowi certyfikatu.
2. CERTUM PCC rezerwuje sobie prawo do podejmowania wszelkich decyzji dotyczących składni nazwy Subskrybenta i przydzielania mu wynikłych z tego nazw.
3. Subskrybent ma prawo w trybie przewidzianym w Kodeksie Postępowania Certyfikacyjnego CERTUM PCC odrzucić proponowaną nazwę DN.
4. W przypadku powstania sporu na tle reklamacji nazw, CERTUM PCC rezerwuje sobie prawo do odrzucenia wniosku Subskrybenta, bez ponoszenia jakiejkolwiek odpowiedzialności z tego tytułu.
5. Zabrania się używania we wnioskach nazw, które nie są własnością Subskrybenta lub Zamawiającego.
6. CERTUM PCC weryfikuje poprawną nazwę na podstawie dostarczonych przez Subskrybenta dokumentów zawierających dane podmiotu / instytucji (KRS, NIP, CEiDG).

7. Zabrania się używania we wnioskach nazw obraźliwych, wyrazów powszechnie uważanych za wulgarne w tym obcojęzycznych. CERTUM PCC ma prawo do odrzucenia takiego wniosku.

§15 Generowanie i przekazanie kluczy kryptograficznych

1. Para kluczy jest generowana przez CERTUM PCC na karcie kryptograficznej za pomocą bezpiecznego modułu kryptograficznego.
2. CERTUM PCC generuje klucze i w bezpieczny sposób dostarcza je wnioskodawcom razem z kartą kryptograficzną, na której są one zapisane.
3. Klucze stosowane do składania podpisów elektronicznych, których część publiczna w postaci certyfikatu potwierdzana jest przez CERTUM PCC, są generowane za pomocą sprzętowych modułów kryptograficznych.
4. CERTUM PCC po wygenerowaniu klucza publicznego poddaje go odpowiednim testom na zgodność z ograniczeniami nałożonymi przez Kodeks Postępowania Certyfikacyjnego.
5. Każdy Subskrybent, a także operatorzy Systemu Rejestracji przechowują swój klucz prywatny w sposób zapobiegający ich utracie, ujawnieniu lub nieautoryzowanemu użyciu.

§16 Wydanie certyfikatu

1. CERTUM PCC wydaje kwalifikowany certyfikat po otrzymaniu prawidłowo wypełnionego formularza z danymi do certyfikatu, identyfikacji i uwierzytelnieniu Wnioskodawcy oraz po podpisaniu z nim Umowy o świadczenie usług certyfikacyjnych i uregulowaniu należności.
2. Wnioskodawca ponosi odpowiedzialność za poprawność i prawdziwość informacji zawartych w formularzu. W granicach określonych Polityką Certyfikacji osoba potwierdzająca tożsamość wykonuje kontrolę zgodności informacji zawartych we wniosku z informacjami w dokumentach wnioskodawcy.
3. CERTUM PCC nie jest odpowiedzialne za monitorowanie, sprawdzanie i potwierdzanie poprawności i aktualności informacji zawartych w certyfikacie po jego wydaniu.
4. Szczegółowe zasady wydania certyfikatu są przedstawione w Polityce Certyfikacji, zgodnie z którą wystawiony ma być żądany certyfikat.

§17 Odnowienie certyfikatu

1. Subskrybent może wystąpić z wnioskiem o odnowienie certyfikatu, przed upływem jego ważności.
2. Odnowienie należy przeprowadzić za pośrednictwem strony www.certum.pl
3. Proces odnowienia realizowany jest drogą elektroniczną. W trakcie procesu odnowienia Subskrybent musi podpisać elektronicznie aneks do posiadanej Umowy z Subskrybentem, wykorzystując w tym procesie ważny certyfikat kwalifikowany, który będzie odnawiany.
4. W przypadku utraty ważności przez posiadany przez Subskrybenta certyfikat kwalifikowany istnieje możliwość zakupienia nowego certyfikatu kwalifikowanego dla posiadanego bezpiecznego urządzenia do składania bezpiecznego podpisu elektronicznego, dostarczonego przez CERTUM PCC.
5. Zasady odnowienia certyfikatu są przedstawione w Polityce Certyfikacji i Kodeksie Postępowania Certyfikacyjnego oraz informacjach zamieszczonych na stronie internetowej CERTUM PCC.

§18 Repozytorium

1. Repozytorium to centralna baza danych zawierająca certyfikaty oraz dokumenty ogólnodostępne związane z funkcjonowaniem CERTUM PCC.

2. Informacje opublikowane przez CERTUM PCC w repozytorium dostępne są pod adresem: http://www.certum.pl/certum/cert,wiedza_repozytorium_pl_en.xml.
3. W repozytorium opublikowane zostały m.in.:
   - Polityka Certyfikacji,
   - Kodeks Postępowania Certyfikacyjnego,
   - Regulamin Usług Certyfikacyjnych,
   - zaświadczenie certyfikacyjne CERTUM PCC,
   - listy certyfikatów unieważnionych (CRL),
   - informacje pomocnicze, np. ogłoszenia.
4. Repozytorium jest uaktualniane z częstotliwością właściwą dla poszczególnych grup informacji (Kodeks Postępowania Certyfikacyjnego, rozdz.4.8.9).

§19 Unieważnienie certyfikatu

1. Wniosek o unieważnienie certyfikatu kwalifikowanego jest udostępniony na stronie www.certum.pl. Wniosek o unieważnienie można przesłać faksem pod numer wskazany w instrukcji unieważnienia, bądź złożyć osobiście w Punkcie Rejestracji CERTUM PCC.
2. Wniosek o unieważnienie certyfikatu kwalifikowanego może złożyć:
   - Subskrybent – w przypadku certyfikatu uniwersalnego.
   - Zamawiający lub Subskrybent – w przypadku certyfikatu z dodatkowymi danymi.
   - Inna osoba - osoba upoważniona przez Subskrybenta na podstawie pełnomocnictwa notarialnego – w przypadku uzasadnionej przyczyny.
3. W przypadku unieważnienia certyfikatu kwalifikowanego przez Zamawiającego, zobowiązany jest on wraz ze złożonym wnioskiem o unieważnienie certyfikatu dostarczyć oficjalne pismo dotyczące cofnięcia pełnomocnictwa, udzielonego Subskrybentowi.
4. Wniosek o unieważnienie certyfikatu musi zawierać informacje zgodne z procedurą przedstawioną w Polityce Certyfikacji oraz Kodeksie Postępowania Certyfikacyjnego.
5. Wniosek o unieważnienie certyfikatu kwalifikowanego należy wypełnić czytelnie.
6. Wniosek może być uwierzytelniony:
   - przy pomocy podpisu odręcznego na oświadczeniu o potwierdzeniu tożsamości Operatora Punktu Rejestracji CERTUM PCC,
   - z użyciem telefonicznej procedury uwierzytelnienia osoby upoważnionej do unieważnienia przeprowadzonej przez CERTUM PCC.
7. Podstawową przyczyną unieważnienia certyfikatu jest samo podejrzenie utraty kontroli nad kluczem prywatnym, będącym w posiadaniu Subskrybenta certyfikatu kwalifikowanego lub też rażące naruszanie przez Subskrybenta zasad Polityki Certyfikacji lub Kodeksu Postępowania Certyfikacyjnego. Pozostałe przyczyny są opisane w Polityce Certyfikacji oraz Kodeksie Postępowania Certyfikacyjnego.
8. CERTUM PCC zapewnia możliwość zgłoszenia wniosku o unieważnienie certyfikatu przez całą dobę.
9. CERTUM PCC gwarantuje, zgodnie z Polityką Certyfikacji, że maksymalny czas przetwarzania wniosków o unieważnienie certyfikatu wynosi 1 godzinę od momentu odebrania zgłoszenia przez Główny Punkt Rejestracji.
10. Informacja o unieważnionym certyfikacie umieszczana jest niezwłocznie na liście CRL. Wszystkie listy CRL publikowane są nie rzadziej niż co 24 godziny i automatycznie w repozytorium Urzędu Certyfikacji.

11. CERTUM PCC w momencie unieważnienia certyfikatu kwalifikowanego powiadamia o tym fakcie Zamawiającego oraz/lub Subskrybenta w przeciągu 7 dni roboczych.
12. Unieważnienie certyfikatów nie ma wpływu na wcześniej zaciągnięte zobowiązania lub obowiązki wynikłe z przestrzegania Kodeksu Postępowania Certyfikacyjnego oraz Polityki Certyfikacji.
13. Unieważnienie certyfikatu nie może następować z mocą wsteczną.
14. Informacja o sposobie zgłoszenia żądania unieważnienia certyfikatu jest przekazywana Subskrybentowi najpóźniej w momencie przekazania wydanego kwalifikowanego certyfikatu. To znaczy że wraz z oświadczeniem o akceptacji certyfikatu dostaje instrukcję jak unieważnić certyfikat kwalifikowany
15. CERTUM PCC zastrzega możliwość wydania decyzji odmownej unieważnienia certyfikatu kwalifikowanego, kiedy ma wątpliwości co do przyczyny i okoliczności unieważnienia lub zgłaszającego unieważnienie wraz ze wskazaniem przyczyny odmowy.

§20 Zawieszenie i uchylenie zawieszenia certyfikatu

1. Wniosek o zawieszenie kwalifikowanego certyfikatu może składać wyłącznie uprawniony pracownik CERTUM PCC.
2. Podstawową przyczyną zawieszenia certyfikatu jest uznanie przez Główny Punkt Rejestracji niemożliwości potwierdzenia tożsamości instytucji żądającej unieważnienia certyfikatu. Pozostałe przyczyny są opisane w Kodeksie Postępowania Certyfikacyjnego oraz Polityce Certyfikacji.
3. Zawieszenie certyfikatu kwalifikowanego jest czasowe, zwykle do czasu wyjaśnienia wątpliwości, które były podstawą do zawieszenia.
4. Uchylenie zawieszenia certyfikatu odbywa się tylko i wyłącznie z inicjatywy Subskrybenta, po uprzednim uwierzytelnionym potwierdzeniu wniosku o uchylenie zawieszenia certyfikatu.
5. Główny Punkt Rejestracji CERTUM PCC rezerwuje sobie prawo odrzucenia wniosku Subskrybenta o uchylenie zawieszenia, jeśli tylko może to w jakikolwiek sposób naruszyć wiarygodność urzędu certyfikacji.
6. Jeśli certyfikat pozostaje w stanie zawieszenia dłużej niż 7 dni, zostanie automatycznie unieważniany przez CERTUM PCC bez możliwości anulowania tej operacji.
7. CERTUM PCC gwarantuje, zgodnie z Polityką Certyfikacji, że maksymalny czas przetwarzania wniosków o zawieszenie certyfikatu i publikacja nowej listy certyfikatów zawieszonych i unieważnionych wynosi 1 godzinę.
8. CERTUM PCC w momencie zawieszenia certyfikatu niezwłocznie informuje o tym fakcie Subskrybenta oraz Zamawiającego.
9. Zawieszenie certyfikatów nie ma wpływu na wcześniej zaciągnięte zobowiązania lub obowiązki wynikłe z przestrzegania Polityki Certyfikacji oraz Kodeksu Postępowania Certyfikacyjnego.
10. CERTUM PCC jest uprawnione do zawieszenia certyfikatu wydanego przez siebie, zgodnie z procedurami, Regulaminem Usług Certyfikacyjnych i Polityką Certyfikacji oraz obowiązującymi przepisami prawa.
11. Zawieszenie certyfikatu nie może następować z mocą wsteczną.
12. Informacja o sposobie zgłoszenia odwieszenia certyfikatu, podobnie jak unieważnienia certyfikatu, jest przekazywana Subskrybentowi najpóźniej w momencie przekazania kwalifikowanego certyfikatu.

§21 Powody unieważnienia i zawieszenia kwalifikowanego certyfikatu

1. CERTUM PCC unieważnia kwalifikowany certyfikat przed upływem okresu jego ważności, jeżeli:

a) certyfikat ten został wydany na podstawie nieprawdziwych lub nieaktualnych danych, to jest: imienia i nazwiska Subskrybenta, jak również nieprawidłowości lub nieaktualności danych wpisanych na żądanie Subskrybenta do certyfikatu,

b) CERTUM PCC nie dopełniło obowiązków, w szczególności certyfikat został wydany w sposób niedozwolony lub błędny wskutek:

- niedopełnienia istotnych warunków wymaganych do wydania certyfikatu,
- nieprawdziwości albo podejrzenia nieprawdziwości danych zawartych w certyfikacie,
- popełnienia błędów przy wprowadzaniu danych lub innych błędów w zakresie przetwarzania danych.

c) Subskrybent weryfikowany na podstawie tego certyfikatu nie dopełnił obowiązku przechowywania danych służących do składania podpisu elektronicznego (klucza prywatnego) w sposób zapewniający ich ochronę przed nieuprawnionym wykorzystaniem w okresie ważności certyfikatu służącego do weryfikacji tych podpisów, tj.:

- klucz prywatny został ujawniony osobom trzecim lub nieprawidłowo użyty w wyniku: utraty, kradzieży, uszkodzenia klucza prywatnego Subskrybenta lub innego rodzaju jego ujawnienia osobom trzecim,
- umyślnego nieprawidłowego użycia przez Subskrybenta kluczy i certyfikatów związanego z nieprzestrzeganiem przez niego wymogów techniczno-organizacyjnych określonych w Umowie, Regulaminie, Kodeksie Postępowania Certyfikacyjnego oraz Polityce Certyfikacji,

d) CERTUM PCC zaprzestanie świadczenia usług certyfikacyjnych, a jego prawa i obowiązki nie zostały przejęte przez inny kwalifikowany podmiot,

e) zażądał tego Subskrybent lub osoba trzecia wskazana w certyfikacie,

f) zażądał tego minister właściwy do spraw informatyzacji,

g) osoba składająca podpis elektroniczny utraciła pełną zdolność do czynności prawnych,

h) zostało unieważnione zaświadczenie certyfikacyjne CERTUM PCC,

i) w przypadku zgonu subskrybenta,

j) Subskrybent rezygnuje z umowy zawartej z CERTUM PCC,

k) nastąpiła kradzież lub uzasadnione podejrzenie kradzieży klucza prywatnego, lub nośnika na którym jest przechowywany,

l) nastąpiło zagubienie lub istnieje uzasadnione podejrzenie zagubienia klucza prywatnego, lub nośnika na którym jest przechowywany,

m) nastąpiło zniszczenie klucza prywatnego, lub nośnika na którym jest przechowywany.

2. W przypadku istnienia uzasadnionego podejrzenia, że istnieją przesłanki do unieważnienia kwalifikowanego certyfikatu, CERTUM PCC jest ma obowiązek niezwłocznie zawiesić certyfikat i podjąć działania niezbędne do wyjaśnienia tych wątpliwości.

3. Po upływie maksymalnego okresu zawieszenia, w przypadku niemożności wyjaśnienia wątpliwości, CERTUM PCC niezwłocznie unieważnia kwalifikowany certyfikat.

§22 Skutki zawieszenia i unieważnienia certyfikatu

1. Subskrybent, którego certyfikat został unieważniony zobowiązuje się do permamentnego usunięcia przyporządkowanej pary kluczy wraz z certyfikatem z posiadanego bezpiecznego urządzenia.

2. Skutkiem prawnym unieważnienia kwalifikowanego certyfikatu jest trwałe ustanie możliwości używania certyfikatu.

3. Unieważniony certyfikat publikowany jest na liście CRL.

4. Skutkiem prawnym zawieszenia certyfikatu jest czasowe ustanie możliwości używania certyfikatu.
5. Subskrybent, którego certyfikat został zawieszony, zobowiązuje się do złożenia w ustalonym terminie wniosku o uchylenie zawieszenia lub wniosku o unieważnienie certyfikatu.

Rozdział V. Kwalifikowany certyfikat

§23 Opis i zawartość kwalifikowanego certyfikatu

1. Kwalifikowany certyfikat jest elektronicznym zaświadczeniem, za pomocą którego dane służące do weryfikacji podpisu elektronicznego są przyporządkowane do osoby składającej podpis elektroniczny i które umożliwiają identyfikację tej osoby.
2. Profile kwalifikowanych certyfikatów są zgodne z formatami określonymi w normie ITU-T X.509 v3 oraz specyfikacją ETSI EN 319 411-2.
3. Kwalifikowany certyfikat jest ważny w okresie w nim wskazanym.
4. Maksymalny okres ważności kwalifikowanego certyfikatu wydanego przez CERTUM PCC wynosi 2 lata.
5. CERTUM PCC wydaje dwa podstawowe typy kwalifikowanych certyfikatów:
   - Certyfikat osobisty (**uniwersalny**) – zawierający wyłącznie dane Subskrybenta (osoby fizycznej),
   - Certyfikat profesjonalny (**z dodatkowymi danymi**) - zawierający dane Subskrybenta (osoby fizycznej) oraz dodatkowe dane identyfikujące podmiot reprezentowany przez Subskrybenta.
6. Kwalifikowane certyfikaty wystawiane są Subskrybentom (osobom fizycznym), którzy podpiszą umowę z Asseco Data Systems S.A. na świadczenie usług certyfikacyjnych i zaakceptują postanowienia Kodeksu Postępowania Certyfikacyjnego i Regulaminu Usług Certyfikacyjnych.
7. Kwalifikowany certyfikat powinien zawierać między innymi:
   a) numer certyfikatu,
   b) wskazanie, że certyfikat został wydany jako kwalifikowany certyfikat do stosowania zgodnie z określoną polityką certyfikacji,
   c) wskazanie CERTUM PCC jako podmiotu świadczącego usługi certyfikacyjne wydającego certyfikat,
   d) wskazanie państwa, w którym ma siedzibę Asseco Data Systems S.A.,
   e) numer pozycji, pod którym jest wpisane CERTUM PCC w rejestrze kwalifikowanych podmiotów świadczących usługi certyfikacyjne,
   f) imię i nazwisko Subskrybenta,,
   g) oznaczenie początku i końca okresu ważności certyfikatu,
   h) poświadczenie elektroniczne CERTUM PCC jako podmiotu świadczącego usługi certyfikacyjne, wydającego certyfikat,
   i) ograniczenia zakresu ważności certyfikatu, jeżeli przewiduje to określona polityka certyfikacji,
   j) o ile przewiduje to umowa, wskazanie, czy Subskrybent działa:
      - we własnym imieniu,
      - jako przedstawiciel innej osoby fizycznej, osoby prawnej albo jednostki organizacyjnej nieposiadającej osobowości prawnej,

- w charakterze członka organu albo organu osoby prawnej, albo jednostki organizacyjnej nieposiadającej osobowości prawnej,
- jako organ władzy publicznej.

Rozdział VI. Postanowienia końcowe

§24 Udostępnianie informacji

1. CERTUM PCC udostępnia za pośrednictwem repozytorium dokumenty i informacje:
   - Polityka Certyfikacji wraz z Kodeksem Postępowania Certyfikacyjnego i Regulamin Usług Certyfikacyjnych,
   - Zaświadczenia certyfikacyjne urzędów certyfikacji,
   - Listy certyfikatów unieważnionych (CRL),
   - Informacje pomocnicze, np. ogłoszenia.
2. W szczególności za informacje jawne uważa się te informacje, które umieszczane są w certyfikacie przez organy wydające certyfikaty zgodnie z opisem przedstawionym w rozdz.7 Kodeksu Postępowania Certyfikacyjnego. Przyjmuje się w tym przypadku zasadę, że Subskrybent występując z wnioskiem o wydanie certyfikatu jest świadom, jaka informacja umieszczana jest w certyfikacie i wyraża zgodę na jej upublicznienie.

§25 Rozpatrywanie skarg i zażaleń

1. Przedmiotem rozstrzygania skarg mogą być jedynie rozbieżności bądź konflikty powstałe pomiędzy stronami w zakresie wydawania i unieważniania kwalifikowanego certyfikatu w oparciu o regulacje Kodeksu Postępowania Certyfikacyjnego.
2. Skargi i zażalenia dotyczące świadczenia kwalifikowanych usług certyfikacyjnych rozpatrywane są zgodnie z obowiązującą w Asseco Data Systems S.A. procedurą obsługi reklamacji.
3. Skargi i zażalenia należy kierować do Centrum Obsługi Klienta na adres reklamacje@certum.pl.
4. W przypadku wystąpienia innych sporów będących konsekwencją użycia wydanego certyfikatu lub innych usług świadczonych przez CERTUM PCC, Subskrybent zobowiązuje się pisemnie poinformować CERTUM PCC o przedmiocie powstałego sporu.
5. Spory związane z usługami certyfikacyjnymi świadczonymi przez CERTUM PCC będą w pierwszej kolejności rozstrzygane na drodze postępowania pojednawczego.
6. W przypadku braku rozstrzygnięcia sporu w terminie 30 dni od rozpoczęcia postępowania pojednawczego, stronom przysługuje prawo do wystąpienia na drogę sądową. Sądem właściwym do rozpoznania sprawy będzie Sąd Powszechny właściwy dla pozwanego.

§26 Polityka prywatności

1. CERTUM PCC dokłada należytej staranności w zakresie ochrony prywatności Subskrybentów, Stron ufających oraz osób, na rzecz których wydawane są certyfikaty.
2. CERTUM PCC przetwarza dane osobowe w oparciu o zasady określone w *Ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych*.
3. Administratorem danych osobowych pozyskiwanych w ramach świadczenia kwalifikowanych usług certyfikacyjnych, jest Asseco Data Systems S.A.mające siedzibę w Gdyni przy ulicy Żwirki i Wigury 15.
4. Osoby, których dane osobowe są przetwarzane przez Asseco Data Systems S.A. są uprawnione do dostępu do treści swoich danych oraz ich poprawiania, za wyjątkiem danych umieszczanych w wydanym Subskrybentowi kwalifikowanym certyfikacie, z uwzględnieniem zasad przedstawionych w niniejszym Regulaminie. Zmiana danych umieszczanych w wydanym Subskrybentowi kwalifikowanym certyfikacie skutkuje unieważnieniem certyfikatu i wydaniem nowego.

§27 Prawo własności intelektualnej

1. Wszystkie używane przez CERTUM PCC znaki towarowe, handlowe, patenty, znaki graficzne, licencje i inne stanowią własność intelektualną ich prawnych właścicieli. CERTUM PCC zobowiązuje się do umieszczania odpowiednich (wymaganych przez właścicieli) uwag w tej dziedzinie.
2. Każda para kluczy, z którymi związany jest certyfikat klucza publicznego, wystawiony przez CERTUM PCC jest własnością podmiotu, określonego w polu *subject* certyfikatu.

§28 Podstawy prawne

1. Działalność urzędu certyfikacji CERTUM PCC polegająca na świadczeniu usług certyfikacyjnych opiera się na zasadach opisanych w niniejszym Regulaminie, zawieranej z Subskrybentami umowie o świadczenie usług certyfikacyjnych, Kodeksie Postępowania Certyfikacyjnego, Polityce Certyfikacji, obowiązujących aktualnie na terenie Rzeczypospolitej Polskiej przepisach prawnych, a w szczególności:
   - *Ustawie z dnia 23 kwietnia 1964 r. - Kodeks cywilny (Dz.U. 1964 Nr 16 poz.93 z późn. zm.)*,
   - *Ustawie z dnia 2 marca 2000 r. o ochronie niektórych praw konsumentów oraz o odpowiedzialności za szkodę wyrządzoną przez produkt niebezpieczny (Dz.U. 200 Nr 22 poz.271 z późn. zm.)*,
   - *Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2016 poz. 922, tekst jednolity ustawy),*
   - *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,*
   - *Ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. z 2016 r. poz. 1579)*

   oraz powszechnie obowiązujących zasadach współżycia społecznego.
2. Nieważność bądź nieskuteczność jakiegokolwiek postanowienia Regulaminu nie wpływa na ważność bądź skuteczność innych postanowień niniejszego Regulaminu.
3. Niniejszy Regulamin wiąże strony umów o świadczenie usług certyfikacyjnych oraz osoby fizyczne, na rzecz których wydawane są certyfikaty.
4. Wszelkie powiadomienia są ogłaszane zgodnie z wymaganiami właściwej Polityki Certyfikacji lub Umowy. Jeżeli Polityka Certyfikacji albo Umowa nie stanowią inaczej, specjalne potwierdzanie powiadomienia nie jest wymagane.
5. W przypadku rozbieżności bądź sprzeczności postanowień Regulaminu, Polityk Certyfikacji, Kodeksu Postępowania Certyfikacyjnego, Umów w ramach danego stosunku prawnego pierwszeństwo mają postanowienia:
   - w przypadku rozbieżności i sprzeczności postanowień Umowy z innymi postanowieniami – postanowienia zawarte w Umowie,
   - w przypadku rozbieżności i sprzeczności postanowień Polityki Certyfikacji z postanowieniami Regulaminu – postanowienia Polityki Certyfikacji.
6. Interpretacja Regulaminu dokonywana jest z zachowaniem dobrych obyczajów związanych ze świadczeniem usług certyfikacyjnych. Przy interpretacji Regulaminu strony mają na względzie międzynarodowy charakter usług certyfikacyjnych oraz zasadę działania w dobrej wierze.

§29 Zaprzestanie działalności

1. W przypadku zaprzestania świadczenia usług certyfikacyjnych przez CERTUM PCC, urząd certyfikacji dołoży wszelkich starań, by ograniczyć szkody odbiorców usług certyfikacyjnych z tym związane:
   - opublikowana zostanie z wymaganym wyprzedzeniem informacja o zakończeniu działalności,

- o fakcie tym za pośrednictwem uwierzytelnionej poczty elektronicznej zostaną powiadomieni wszyscy Subskrybenci CERTUM PCC.

§30 Zmiany Regulaminu

1. CERTUM PCC zastrzega sobie prawo zmian Regulaminu.
2. W przypadku wprowadzenia zmian w Regulaminie zostanie on opublikowany w Repozytorium CERTUM PCC na stronie www.certum.pl z oznaczeniem wersji.
3. Subskrybenta nie obowiązują zmiany Regulaminu wprowadzone po zawarciu umowy.