Polityka Certyfikacji Niekwalifikowanych Usług CERTUM

Wersja 4.2

Data: 26 marca 2018

Status: archiwalny

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

Klauzula: Prawa Autorskie

Spis treści

1. Wstęp

Polityka Certyfikacji Niekwalifikowanych Usług CERTUM określa ogólne zasady świadczenia niekwalifikowanych usług certyfikacyjnych, stosowane przez CERTUM – Powszechne Centrum Certyfikacji (zwane dalej CERTUM) podczas procesu certyfikacji kluczy publicznych, usług Znacznika Czasu (*ang. TSA*), pozostałych systemów elektronicznej niezaprzeczalności oraz definiuje uczestników tego procesu, ich obowiązki i odpowiedzialność, typy certyfikatów, typy poświadczeń oraz obszary zastosowań. Szczegółowy opis wspomnianych zasad oraz procedury weryfikacji tożsamości subskrybentów przedstawione są z kolei w Kodeksie Postępowania Certyfikacyjnego Niekwalifikowanych Usług CERTUM. Znajomość natury, celu oraz roli Polityki Certyfikacji, jak również Kodeksu Postępowania Certyfikacyjnego jest szczególnie istotna z punktu widzenia subskrybenta oraz strony ufającej.

2. Certyfikaty

Certyfikat jest ciągiem danych (wiadomością), który zawiera co najmniej nazwę lub identyfikator urzędu wydającego certyfikaty, identyfikator subskrybenta, jego klucz publiczny, okres ważności certyfikatu, numer seryjny certyfikatu i jest podpisany przez pośredni urząd certyfikacji podległy jednemu z głównych urzędów: **Certum CA**, **Certum Trusted Network CA, Certum Trusted Network CA 2, Certum Elliptic Curve CA, Certum Trusted Root CA** oraz **Certum EC-384 CA**.

Każdy z urzędów **Certum CA**, **Certum Trusted Network CA, Certum Trusted Network CA 2, Certum Elliptic Curve CA, Certum Trusted Root CA, Certum EC-384 CA** wydając pośrednio certyfikat subskrybentowi potwierdza tożsamość subskrybenta lub inne dane, np. adres skrzynki poczty elektronicznej oraz fakt, iż będący w jego posiadaniu klucz publiczny w rzeczywistości należy do niego. Dzięki temu strona ufająca, po otrzymaniu podpisanej wiadomości jest w stanie zidentyfikować właściciela certyfikatu, który podpis ten złożył oraz ewentualnie rozliczyć go z działań, które podjął lub do których się zobowiązał.

CERTUM świadczy usługi certyfikacyjne zgodnie z wymogami *WebTrust*™ dla urzędów certyfikacji (patrz http://www.webtrust.org). Klucze urzędu certyfikacji chronione są sprzętowymi modułami kryptograficznymi. Urząd dysponuje zabezpieczeniami fizycznymi i proceduralnymi całego systemu. CERTUM wydaje certyfikaty w szeregu klasach o różnym poziomie wiarygodności. Wiarygodność certyfikatu zależy od przyjętej procedury weryfikacji tożsamości subskrybenta i wysiłku włożonego przez CERTUM w sprawdzenie danych przesłanych przez subskrybenta we wniosku rejestracyjnym. Im więcej informacji należy zweryfikować, a więc im bardziej procedura ta jest złożona, tym bardziej wiarygodny jest certyfikat. Klasa certyfikatu może być również uzależniona od poziomu bezpieczeństwa systemu operacyjnego lub serwisu usługowego przedstawionego do certyfikacji urządzenia bądź serwisu. Inżynierowie systemowi CERTUM mogą weryfikować stan techniczny i poziom bezpieczeństwa systemu informatycznego przed wydaniem certyfikatu o najwyższej klasie wiarygodności.

Subskrybent sam powinien zdecydować, jaki typ certyfikatu jest najodpowiedniejszy do jego potrzeb. Typy certyfikatów są dokładnie opisane w **Kodeksie Postępowania Certyfikacyjnego Niekwalifikowanych Usług CERTUM** oraz na stronach internetowych http://www.certum.pl. Informacje te są również dostępne za pośrednictwem poczty elektronicznej adresowanej do: info@certum.pl.

2.1. Certyfikaty DV (ang. Domain Validation)

Certyfikaty **DV** wydawane są w dwóch grupach. Jako nieodpłatne certyfikaty testowe o skróconym okresie ważności oraz standardowe certyfikaty o pełnym zakresie zastosowania. Certyfikaty z pierwszej grupy wydawane są przez pośrednie urzędy **Certum Level I CA, Certum Class 1 CA** oraz **Certum Class 1 CA SHA2** podczas gdy druga grupa certyfikatów wydawana jest przez **Certum Level II CA** oraz **Certum Domain Validation CA SHA2**.

Certyfikaty testowe **DV** przeznaczone są przede wszystkim do przeprowadzenia testów oprogramowania bądź urządzeń przed zakupem docelowego certyfikatu. Certyfikaty **DV** wydawane są do następujących rodzajów zastosowań: prowadzenia bezpiecznej korespondencji elektronicznej. oraz do zabezpieczania transmisji danych w oparciu o protokoły SSL i TLS.

Weryfikacja tożsamości subskrybenta jest prowadzona zgodnie z aktualną wersją dokumentu *Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates*, który dostępny jest na stronie: http://www.cabforum.org/.

CERTUM weryfikuje wszystkie dane przekazane przez podmiot w procesie certyfikacji. Weryfikacji podlegają: nazwa domeny – w przypadku certyfikatów SSL, nazwa powszechna – w przypadku certyfikatów poczty elektronicznej, adres skrzynki pocztowej oraz kraj. Szczegółowe wymagania odnośnie weryfikacji danych wnioskodawcy prezentowane są na stronach www.certum.pl oraz w **Kodeksie Postępowania Certyfikacyjnego Niekwalifikowanych Usług CERTUM**.

Na podstawie certyfikatów **DV** nie powinno się jednoznacznie potwierdzać tożsamości podmiotu.

W certyfikatach **DV**, przeznaczonych dla podmiotów końcowych umieszcza się identyfikator polityki, wg której wystawiany jest dany certyfikat.

Nazwa urzędu	**Identyfikator polityki**
Certum Level I CA	iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-certum(2) id-certum-level-I(1)
Certum Class 1 CA	iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-ctnca(5) id-ctn-certPolicy (1) id-certum-class-1(5)
Certum Class 1 CA SHA2	iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-ctnca(5) id-ctn-certPolicy (1) id-certum-class-1(5)
Certum Level II CA	iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-certum(2) id-certum-level-II(2)
Certum Domain Validation CA SHA2	{iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-ctnca(5)} id-ctn-certPolicy (1) id-certum-dv(3)

Za dane umieszczane w certyfikatach testowych wydawanych wg powyższych polityk, CERTUM nie ponosi odpowiedzialności finansowej ani nie daje żadnych gwarancji. Natomiast urzędy **Certum Level II CA** oraz **Certum Domain Validation CA SHA2** dają ograniczone gwarancje na wystawiane certyfikaty.

2.2. Certyfikaty OV (ang. Organization Validation)

Certyfikaty **OV** wydawane są przez pośrednie urzędy **Certum Level III CA**, **Certum Level IV CA** oraz **Certum Organization Validation CA SHA2**.

Certyfikaty **OV** przeznaczone są przede wszystkim do prowadzenia bezpiecznej korespondencji elektronicznej oraz do zabezpieczania transmisji danych w oparciu o protokoły SSL i TLS. Certyfikaty znajdują także zastosowanie w systemach transakcji finansowych prowadzonych w sieci globalnej oraz jako identyfikatory urzędów niezaprzeczalności elektronicznej.

Weryfikacja tożsamości subskrybenta jest prowadzona zgodnie z aktualną wersją dokumentu *Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates*, który dostępny jest na stronie: http://www.cabforum.org/.

CERTUM weryfikuje wszystkie dane przekazane przez podmiot w procesie certyfikacji. Szczegółowe wymagania odnośnie weryfikacji danych wnioskodawcy prezentowane są na stronach www.certum.pl oraz w **Kodeksie Postępowania Certyfikacyjnego Niekwalifikowanych Usług CERTUM**.

Na podstawie certyfikatów **OV** można jednoznacznie potwierdzić tożsamość podmiotu, autentyczność organizacji bądź wiarygodność zewnętrznego urzędu certyfikacji.

W certyfikatach **OV**, przeznaczonych dla podmiotów końcowych umieszcza się identyfikator polityki, wg której wystawiany jest dany certyfikat:

Nazwa urzędu	**Identyfikator polityki**
Certum Level III CA	iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-certum(2) id-certum-level-III(3)
Certum Level IV CA	iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-certum(2) id-certum-level-IV(4)
Certum Organization Validation CA SHA2	iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-ctnca(5) id-ctn-certPolicy (1) id-certum-ov(2)
Certum Digital Identification CA SHA2	iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-ctnca(5)} id-ctn-certPolicy(1) id-certum-di(6) adobe(11) iso(1) member-body(2) pl(616) organization(1) idunizeto(113527) id-ccert(2) id-ctnca(5)} id-ctncertPolicy(1) id-certum-di(6) basicid(12) iso(1) member-body(2) pl(616) organization(1) idunizeto(113527) id-ccert(2) id-ctnca(5)} id-ctncertPolicy(1) id-certum-di(6) professionalid(13) iso(1) member-body(2) pl(616) organization(1) idunizeto(113527) id-ccert(2) id-ctnca(5)} id-ctncertPolicy(1) id-certum-di(6) enterpriseid(14)

Odpowiedzialność finansowa CERTUM za dane umieszczane w certyfikatach **OV** jest określona w **Kodeksie Postępowania Certyfikacyjnego Niekwalifikowanych Usług CERTUM** oraz na stronach http://www.certum.pl. Urzędy certyfikacji **Certum Level III CA**, **Certum Level IV CA**, **Certum Organization Validation CA SHA2** dają pełne gwarancje na wystawiane certyfikaty.

2.3. Certyfikaty EV (ang. Extended Validation)

Certyfikaty **EV** wydane są przez urzędy **Certum Extended Validation CA, Certum Extended Validation CA SHA2** oraz **Certum Extended Validation Code Signing CA SHA2** zapewniają najwyższy poziom zaufania do tożsamości subskrybenta, przy czym weryfikacja tożsamości subskrybenta w momencie wydawania certyfikatu jest prowadzona zgodnie z aktualną wersją dokumentów *Guidelines for the issuance and Management of Extended Validation Certificates, oraz Guidelines For The Issuance And Management Of Extended Validation Code Signing Certificates,* które dostępne są na stronie http://www.cabforum.org/.

Certyfikaty **EV SSL** wydawane przez urzędy **Certum Extended Validation CA** oraz **Certum Extended Validation CA SHA2** dedykowane są wyłącznie osobom prawnym oraz jednostkom organizacyjnym nieposiadającym osobowości prawnej oraz przeznaczone są do zabezpieczania transmisji danych w oparciu o protokoły SSL i TLS.

Certyfikaty **EV Code Signing** wydawane przez urząd **Certum Extended Validation Code Signing CA SHA2** dedykowane są wyłącznie osobom prawnym oraz jednostkom organizacyjnym nieposiadającym osobowości prawnej oraz przeznaczone są do zabezpieczania kodu sterownika lub aplikacji. Dodatkowo, klucze prywatne subskrybentów certyfikatów **EV Code Signing** muszą być chronione na nośnikach zewnętrznych.

CERTUM weryfikuje wszystkie dane przekazane przez podmiot w procesie certyfikacji. Szczegółowe wymagania odnośnie weryfikacji danych wnioskodawcy prezentowane są na stronach www.certum.pl oraz w **Kodeksie Postępowania Certyfikacyjnego Niekwalifikowanych Usług CERTUM**.

Na podstawie certyfikatów **EV** można jednoznacznie potwierdzić tożsamość podmiotu, autentyczność organizacji bądź wiarygodność zewnętrznego urzędu certyfikacji.

W certyfikatach **EV**, przeznaczonych dla podmiotów końcowych umieszcza się identyfikator polityki, wg której wystawiany jest dany certyfikat.

Nazwa urzędu	**Identyfikator polityki**
Certum Extended Validation CA	iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-ctnca(5) id-ctn-certPolicy (1) id-certum-ev(1)
Certum Extended Validation CA SHA2	iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-ctnca(5) id-ctn-certPolicy (1) id-certum-ev(1)
Certum Extended Validation Code Signing CA SHA2	iso(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) ev-code-signing-requirements(3) iso(1) member-body(2) pl(616) organization(1) idunizeto(113527) id-ccert(2) id-ctnca(5) id-ctncertPolicy (1) id-certum-evcs(7)

Odpowiedzialność finansowa CERTUM za dane umieszczane w certyfikatach wydawanych wg powyższej polityki jest określona w **Kodeksie Postępowania Certyfikacyjnego Niekwalifikowanych Usług CERTUM** oraz na stronach http://www.certum.pl. Urzędy certyfikacji **Certum Extended Validation CA** oraz **Certum Extended Validation CA SHA2** dają pełne gwarancje na wystawiane certyfikaty.

2.4. Certyfikaty podpisujące oprogramowanie (ang. Code Signing)

Certyfikaty **Code Signing** wydawane są przez pośrednie urzędy **Certum Code Signing CA** oraz **Certum Code Signing CA SHA2.**

Przeznaczenie certyfikatów wydawanych przez w/w urzędy certyfikacji jest ograniczone wyłącznie do zadań związanych z podpisywaniem kodu. Dodatkowo, klucze prywatne subskrybentów certyfikatów **Code Signing** muszą być chronione na nośnikach zewnętrznych.

Weryfikacja tożsamości subskrybenta jest prowadzona zgodnie z aktualną wersją dokumentu *Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates,* który dostępny jest na stronie: https://casecurity.org/resources/.

CERTUM weryfikuje wszystkie dane przekazane przez podmiot w procesie certyfikacji. Szczegółowe wymagania odnośnie weryfikacji danych wnioskodawcy prezentowane są na stronach www.certum.pl oraz w **Kodeksie Postępowania Certyfikacyjnego Niekwalifikowanych Usług CERTUM**.

Na podstawie certyfikatów wydawanych według powyższych polityk można jednoznacznie potwierdzić tożsamość podmiotu, autentyczność organizacji bądź wiarygodność zewnętrznego urzędu certyfikacji.

W certyfikatach **Code Signing**, przeznaczonych dla podmiotów końcowych umieszcza się identyfikator polityki, wg której wystawiany jest dany certyfikat.

Nazwa urzędu	**Identyfikator polityki**
Certum Code Signing CA	iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-ctnca(5) id-ctn-certPolicy (1) id-certum-code-signing(4)
Certum Code Signing CA SHA2	iso(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) code-signing-requirements(4) code-signing(1)

Odpowiedzialność finansowa CERTUM za dane umieszczane w certyfikatach **Code Signing** jest określona w **Kodeksie Postępowania Certyfikacyjnego Niekwalifikowanych Usług CERTUM** oraz na stronach http://www.certum.pl. Urządy certyfikacji **Certum Code Signing CA** daje pełne gwarancje na wystawiane certyfikaty.

2.5. Certyfikaty zewnętrznych urzędów certyfikacji

Certyfikaty dla zewnętrznych urzędów certyfikacji są emitowane przez operacyjne urzędy certyfikacji **Certum Global Services CA** oraz **Certum Global Services CA SHA2**. Podmioty końcowe, którym wydawane są certyfikaty urzędów certyfikowanych przez **Certum Global Services CA** oraz **Certum Global Services CA SHA2** podlegają pełnej weryfikacji prowadzonej przez pracowników Asseco Data Systems S.A.Certyfikaty wydawane są na okres 10 lat i wymagana jest przy nich sprzętowa ochrona kluczy. Identyfikatory polityk wyglądają następująco:

Nazwa urzędu	**Identyfikator polityki**
Certum Global Services CA	iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-certum(2) id-global-services(9)
Certum Global Services CA SHA2	{iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-ctnca(5)} id-ctn-certPolicy (1) id-global-services(9)

Odpowiedzialność finansowa CERTUM za dane umieszczane w certyfikatach wydawanych wg powyższych polityk jest określona w odrębnych umowach partnerskich.

3. Poświadczenie niezaprzeczalności

Poświadczenie niezaprzeczalności jest ciągiem danych (wiadomością) dostarczonych przez klienta do jednego z urzędów niezaprzeczalności elektronicznej, który zawiera co najmniej skrót kryptograficzny, numer seryjny certyfikatu, numer zgłoszenia, itp. oraz jest podpisany elektroniczne przez ten urząd. Urzędy niezaprzeczalności elektronicznej, świadczące usługi na rzecz swoich klientów są afiliowane przy **Certum CA, Certum Trusted Network CA** oraz **Certum Trusted Network CA 2.**

Urząd niezaprzeczalności elektronicznej, wydając poświadczenia potwierdza fakt zaistnienia określonego zjawiska w przeszłości bądź obecnie. Zjawiskiem takim może być przedłożenie dokumentu elektronicznego, uczestnictwo w elektronicznej wymianie dokumentów, data złożenia podpisu elektronicznego itp. Strona ufająca na podstawie przedłożonych danych akceptuje poświadczenie i weryfikuje poprawność podpisu na bazie zaufania do głównych urzędów certyfikacji **Certum CA, Certum Trusted Network CA** oraz **Certum Trusted Network CA 2.**

3.1. Znaczniki czasu

Znaczniki czasu wydawane są przez pośredni urząd **Certum EV TSA SHA2**. Znaczniki czasu, jako poświadczenie niezaprzeczalności wydawane są dla osób indywidualnych oraz klientów komercyjnych. Znajdują zastosowanie przede wszystkim w procesach tworzenia podpisów elektronicznych, zawierania transakcji finansowych, archiwizowania danych, notaryzacji dokumentów elektronicznych, itp. Zasady funkcjonowania Urzędu Znacznika Czasu oraz dodatkowe informacje związane z tym systemem zostały opisane w oddzielnym dokumencie (patrz **Polityka Urzędu Znacznika Czasu**).

W żetonach (ang. token) znacznika czasu, umieszcza się identyfikator polityki, wg której wystawiany jest dany znacznik. Identyfikator tej polityki wygląda następująco:

Nazwa urzędu	**Identyfikator polityki**
Certum Time-Stamping Authority	iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-certum-tsa(5) 1 11

Odpowiedzialność finansowa CERTUM za datę i czas oraz dodatkowe informacje umieszczane w znacznikach czasu, wystawianych wg powyższej polityki jest określona w **Polityce Urzędu Znacznika Czasu**, **Kodeksie Postępowania Certyfikacyjnego Niekwalifikowanych Usług CERTUM** oraz na stronach http://www.certum.pl. Urząd **Certum EV TSA SHA2** daje pełne gwarancje na wystawiane znaczniki. Informacje dotyczące cennika umieszczone są na witrynie na stronach http://www.certum.pl.

3.2. Poświadczenia OCSP

Poświadczenia **OCSP** (*ang. Online Certificate Status Protocol*) wydawane są przez pośrednie urzędy **Certum Validation Service**. Każdy urząd certyfikacji CERTUM posiada własny, dedykowany urząd weryfikacji. Poświadczenia statusu certyfikatu wydawane są dla osób indywidualnych oraz dla klientów komercyjnych. Znajdują zastosowanie przede wszystkim w procesach weryfikacji certyfikatów. Usługi te są usługami publicznymi i stanowią alternatywę dla list **CRL** (listy z certyfikatami unieważnionymi). Zasady funkcjonowania urzędu **OCSP** oraz dodatkowe informacje zostały opisane w **Kodeksie Postępowania Certyfikacyjnego Niekwalifikowanych Usług CERTUM** oraz na stronach http://www.certum.pl. Identyfikator polityki wygląda następująco:

Nazwa urzędu	**Identyfikator polityki**
Certum Validation Service	iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-certum(2) id-certum-dvcs(6)

4. Gwarancje CERTUM

W zależności od wydanego typu certyfikatu CERTUM gwarantuje, że podejmuje stosowne kroki, mające na celu weryfikację informacji zawartej w certyfikatach (patrz rozdz. 9.6.1 Kodeku Postępowania Certyfikacyjnego Niekwalifikowanych Usług CERTUM). Weryfikacja tego typu jest szczególnie istotna dla strony ufającej, która jest odbiorcą informacji, poświadczanych przy wykorzystaniu certyfikatów wydanych przez CERTUM. Z tego powodu CERTUM odpowiada finansowo za wszelkie szkody wynikające z winy CERTUM. Zakres oraz wysokość odszkodowań zależy od wiarygodności certyfikatu subskrybenta i może obejmować zarówno subskrybenta, jak i stronę ufającą.

Gwarancje CERTUM mogą być obwarowane wieloma ograniczeniami. Znajomość tych ograniczeń jest potwierdzana przez subskrybenta w stosownym oświadczeniu (patrz Akceptacja certyfikatu). CERTUM gwarantuje unikalność podpisów elektronicznych subskrybentów.

5. Akceptacja certyfikatu

Odpowiedzialność oraz gwarancje CERTUM stają się obowiązujące z chwilą zaakceptowania przez subskrybenta wydanego certyfikatu. Ogólne warunki oraz sposób akceptacji certyfikatu określone są w Kodeksie Postępowania Certyfikacyjnego Niekwalifikowanych Usług CERTUM, zaś szczegółowe – w oświadczeniu użytkownika danego typu certyfikatu.

6. Usługi certyfikacyjne

CERTUM w ramach swojej infrastruktury świadczy cztery podstawowe usług certyfikacyjne:

- rejestracja i wydanie certyfikatu,
- odnowienie certyfikatu,
- unieważnienie certyfikatu oraz,
- weryfikacja statusu certyfikatu.

Pozostałe usługi są usługami niezaprzeczalności, które mogą być świadczone niezależnie od CERTUM:

- oznaczanie wiarygodnym czasem (*ang. Time-Stamping Authority*),
- notariat elektroniczny (*ang. Notary Authority*),
- skarbiec elektroniczny (*ang. Electronic Vault*),
- kurier elektroniczny (*ang. Delivery Authority*),
- OCSP (*ang. Online Certificate Status Protocol*).

Rejestracja służy potwierdzeniu tożsamości subskrybenta i poprzedza zawsze wydanie certyfikatu (patrz rozdz. 4.1 i 4.3 Kodeksu Postępowania Certyfikacyjnego Niekwalifikowanych Usług CERTUM).

Odnowienie certyfikatu ma miejsce wtedy, gdy zarejestrowany subskrybent chce uzyskać certyfikat dla nowego klucza publicznego lub zmodyfikować niektóre dane zawarte w certyfikacie, np. adres poczty elektronicznej (patrz rozdz. 4.7 oraz 4.8 Kodeksu Postępowania Certyfikacyjnego Niekwalifikowanych Usług CERTUM).

Unieważnianie certyfikatu następuje zawsze wtedy, gdy klucz prywatny związany z kluczem publicznym, zawartym w certyfikacie lub nośnik, na którym jest przechowywany, zostanie ujawniony lub istnieje uzasadnione podejrzenie, że został ujawniony (patrz rozdz. 4.9 Kodeksu Postępowania Certyfikacyjnego Niekwalifikowanych Usług CERTUM).

Weryfikacja statusu certyfikatu polega na określeniu przez CERTUM, czy certyfikat jest prawomocnie wydany przez CERTUM, czy znajduje się na liście certyfikatów unieważnionych oraz czy nie minął jego okres ważności. Weryfikacji statusu certyfikatu dokonuje również OCSP (patrz rozdz. 4.9.9 Kodeksu Postępowania Certyfikacyjnego Niekwalifikowanych Usług CERTUM).

CERTUM wymaga, aby każda para kluczy (prywatny i publiczny) była generowana przez subskrybenta. CERTUM może zalecić narzędzia, które umożliwią wygenerowanie takiej pary kluczy. W szczególnych przypadkach CERTUM może wygenerować unikalną parę kluczy i dostarczyć ją do subskrybenta.

7. Strona ufająca

Strona ufająca jest zobowiązana do rzetelnej weryfikacji każdego podpisu cyfrowego umieszczonego na dokumencie (w tym także certyfikacie), który do niej dotrze. W procesie weryfikacji strona ufająca powinna korzystać z zasobów i procedur udostępnianych przez CERTUM. Dotyczy to m.in. obowiązku korzystania z publikowanych przez CERTUM list certyfikatów unieważnionych CRL oraz weryfikowania ścieżki certyfikacji (patrz rozdz. 9.6.4 Kodeksu Postępowania Certyfikacyjnego Niekwalifikowanych Usług CERTUM).

Każdy dokument z wykrytą wadą w podpisie cyfrowym lub wynikłymi z niego wątpliwości powinien zostać odrzucony, ewentualnie poddany innym procedurom wyjaśniającym jego ważność, np. weryfikacji notarialnej.

8. Subskrybent

Subskrybent zobowiązany do bezpiecznego przechowywania swojego klucza prywatnego, zapobiegającego lub utrudniającego jego ujawnienie osobom postronnym. W przypadku ujawnienia klucza lub podejrzenia, że fakt taki mógł mieć miejsce subskrybent musi tak szybko jak to jest możliwe poinformować o tym urząd, który był wystawcą certyfikatu. Informacja taka musi być przekazana w sposób, który nie budzi wątpliwości co do tożsamości subskrybenta.

9. Aktualizacja Polityki Certyfikacji

Polityka Certyfikacji CERTUM może podlegać okresowym modyfikacjom. Modyfikacje te zostaną udostępnione wszystkim subskrybentom, a ich ostateczny kształt zostanie zaakceptowany przez Zespół ds. Rozwoju PKI. Subskrybenci, którzy nie zaakceptują wprowadzonych modyfikacji muszą przysłać do CERTUM stosowne oświadczenie i zrezygnować z usług CERTUM.

10. Opłaty

Usługi certyfikacyjne świadczone przez CERTUM są odpłatne. Wysokość opłat uzależniona jest od poziomu wydawanego lub posiadanego certyfikatu oraz rodzaju żądanej usługi certyfikacyjnej i dostępna jest w cenniku na stronach http://www.certum.pl..

Historia dokumentu

Historia zmian dokumentu		
V 1.0	15 kwietnia 2000 r.	Szkic dokumentu do dyskusji
V 1.27	12 marca 2002 r.	Pełna wersja dokumentu. Dokument zatwierdzony
V 2.0	15 lipca 2002 r.	Szczegółowe zdefinie dokładnie typów certyfikatów i dodanie usług niezaprzeczalności.
V 2.1	01 lutego 2005 r.	Rozszerzenie polityki certyfikacji o świadczenie usług przez pośredni urząd Certum Partners.
V 2.2	09 maja 2005 r.	Zmiana formy prawnej spółki, przekształcenie Unizeto Sp. z o.o. w Unizeto Technologies S.A.
V 2.3	26 października 2005 r.	Zmiana nazwy własnej jednostki i logo z Unizeto CERTUM – Centrum Certyfikacji na CERTUM – Powszechne Centrum Certyfikacji
V 2.4	19 maja 2006 r.	Usunięcie informacji o poprzedniej formie prawnej firmy. Przeniesienie szczegółów dotyczących dokumentów wymaganych do wydania certyfikatu do osobnego dokumentu.
V 2.5	12 maja 2008 r.	Poprawki edytorskie, zachowanie spójności z Kodeksem Postępowania Certyfikacyjnego.
V 3.0	19 października 2009 r.	Rozszerzenie polityki certyfikacji o świadczenie usług przez urząd Certum Trusted Network CA
V 3.1	12 sierpnia 2010 r.	Aktualizacja wymagań dot. weryfikacji subskrybenta.
V 3.2	07 października 2011	Dodanie informacji o nownym certyfikacie Root, certyfikacjie pośrednim Code Signing CA oraz drobne zmiany dotyczące weryfikacji certyfikatów Level I.
V 3.3	19 kwietnia 2012	Aktualizacja logo CERTUM
V 3.4	01 czerwca 2015	Dodanie informacji o nowych urzędach pośrednich. Nowy podział klas wydawanych certyfikatów.
V 3.5	03 listopad 2015	Dodanie urzędu głównego Certum Trusted Network CA EC oraz urzędów pośrednich Certum Digital Identification CA SHA2 oraz Certum Extended Validation Code Signing CA SHA2.
V 3.6	01 kwietnia 2016	Przeniesienie własności z Unizeto Technologies S.A. na Asseco Data System S.A. Dodanie informacji o zobowiązaniu do utrzymywania zaświadczenia certyfikacyjnego wydanego dla Unizeto Technologies przez Asseco Data System S.A.
V 3.7	22 sierpień 2016	Aktualizacja informacji o nowym urzędzie znacznika czasu Certum EV TSA SHA2
V 3.8	01.02.2017	Aktualizacja polityki certyfikacji dla certyfikatów Code Signing. Uzupełnienie informacji o obowiązujące akty norrmatywne CA/Browser Forum.
V 3.9	01 sierpnia 2017	Zmiana adresu Asseco Data Systems S.A. Dodanie Identyfikatorów polityki certyfikacji.
V 4.0	11 sierpnia 2017	Dodanie Identyfikatorów polityki certyfikacji.
V 4.1	23 marca 2018	Zmiana nazwy urzędu Certum Trusted Network CA EC na Certum Elliptic Curve CA oraz dodanie urzędu Certum Trusted Root CA .
V 4.2	26 marca 2018	Dodanie urzędu Certum EC-384 CA