KWALIFIKOWANE CENTRUM CERTYFIKACJI „CENCERT”

Polityka znakowania czasem i innych kwalifikowanych usług certyfikacyjnych

Wersja: 1.1

Karta dokumentu:

Tytuł dokumentu	Polityka znakowania czasem i innych kwalifikowanych usług certyfikacyjnych
Właściciel dokumentu	ENIGMA Systemy Ochrony Informacji Sp. z o.o.
Wersja	1.1
Status dokumentu	Zatwierdzony
Data zatwierdzenia	17 października 2014 r.
Liczba stron	39

zatwierdzone przez:

Wersja	1. zatwierdzający
1.1	Paweł A. Luksic – prezes zarządu Jacek Pokraśniewicz – prokurent, dyrektor zarządzający

historia wersji

Wersja	Data	Komentarze
1.0	2012-04-04	Zmiany: 1) połączenie *Polityki kwalifikowanych znaczników czasu w. 2.0* oraz *Polityki poświadczeń ważności certyfikatów kwalifikowanych w. 2.0* w jeden dokument (zmiana formalna) 2) Usunięcie ograniczenia, że odpowiedzi OCSP mogą dotyczyć tylko certyfikatów; 3) W rozdz. 5.5. usunięcie wymogu zapisu archiwizowanych danych na nośnik magnetooptyczny (pozostawiono *nośnik jednokrotnego zapisu*), usunięto postanowienia dotyczące przeglądu kopii archiwalnych co 5 lat (wymagane jest przechowywanie danych przez 3 lata, więc wymaganie na przegląd co 5 lat jest nierealne) 4) Uporządkowanie zapisów dotyczących odpowiedzialności finansowej CCK
1.1	2014-10-16	Zmiana adresu Centralnego Punktu Rejestracji. Przegląd dokumentu, usunięcie nadmiernej szczegółowości.

Spis treści

1. Wstęp

1.1. Wprowadzenie

Niniejszy dokument stanowi politykę certyfikacji realizowaną przez Centrum Certyfikacji Kluczy ***CenCert*** prowadzone przez firmę ENIGMA Systemy Ochrony Informacji Sp. z o.o. w celu realizacji następujących kwalifikowanych usług certyfikacyjnych:

1) znakowanie czasem,
2) poświadczanie ważności certyfikatów (OCSP).

Centrum Certyfikacji Kluczy realizujące niniejszą politykę stanowi kwalifikowany podmiot świadczący usługi certyfikacyjne, zgodnie z *Ustawą z dnia 18 września 2001 r. o podpisie elektronicznym*.

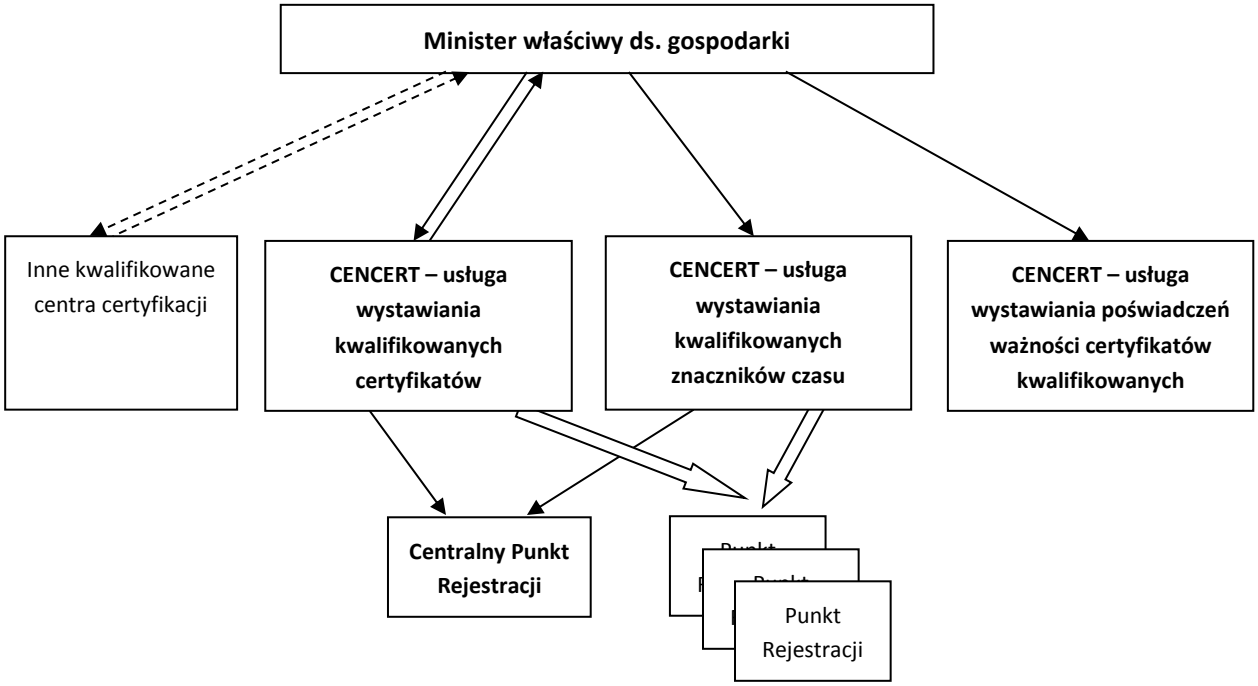
Struktura dokumentu została oparta na dokumencie RFC 3647 "*Internet X.509 Public Key Infrastructure Certification Policy and Certification Practices Framework*".

1.2. Identyfikator polityki certyfikacji

Nazwa polityki	Polityka znakowania czasem i innych kwalifikowanych usług certyfikacyjnych
Kwalifikator polityki	Brak
Numer OID (ang. *Object Identifier*)	1.2.616.1.113681.1.1.90.1.1
Data wprowadzenia	24 października 2014 r.
Data wygaśnięcia	Do odwołania

1.3. Opis systemu certyfikacji i uczestniczących w nim podmiotów

CCK CenCert, zgodnie z przepisami o podpisie elektronicznym, jest częścią krajowego systemu PKI obejmującego kwalifikowane podmioty certyfikacyjne. Rolę Nadrzędnego CCK (tzw. „*Root CA*") pełni Minister właściwy do spraw gospodarki lub podmiot, któremu Minister powierzył to zadanie.



CCK CenCert obsługuje Subskrybentów:

- W pełnym zakresie – poprzez Centralny Punkt Rejestracji (CPR), którego dane znajdują się w rozdziale 1.5.
- W zakresie wystawiania i unieważniania certyfikatów – poprzez Punkty Rejestracji (Punkty Obsługi Klientów), których dane znajdują się na stronach internetowych www.cencert.pl

CPR stanowi punkt kontaktowy dla wszelkich zapytań i wniosków związanych z działaniem CCK CenCert.

Subskrybentem usług certyfikacyjnych może być każda osoba fizyczna, prawna lub inna jednostka organizacyjna, przy czym do realizacji niektórych usług może być wymagane

zawarcie stosownej umowy. Nie jest wymagana umowa w przypadku usługi poświadczania ważności certyfikatów kwalifikowanych.

1.4. Zakres zastosowań

1.4.1 Usługa znakowania czasem

Zgodnie z przepisami o podpisie elektronicznym, kwalifikowane znaczniki czasu stanowią, w okresie ważności zaświadczenia certyfikacyjnego służącego do ich weryfikacji, dowód istnienia określonej treści (w szczególności: określonego podpisu elektronicznego) w danym czasie.

1.4.2 Usługa poświadczania ważności certyfikatów

Poświadczenia elektroniczne wystawiane zgodnie z niniejszą polityką certyfikacji określają status danego certyfikatu, wystawionego przez CCK CenCert zgodnie z odpowiednią polityką certyfikacji, na moment określony w poświadczeniu.

W szczególności poświadczenia elektroniczne potwierdzające status certyfikatu jako ‘ważny’ stanowią dowód, na równi z listą CRL, ważności danego certyfikatu w określonym momencie (tzn. że certyfikat nie został unieważniony ani zawieszony).

1.5. Zasady administrowania polityką certyfikacji

Podmiotem uprawnionym do administrowania polityką certyfikacji, w tym zatwierdzania, zatwierdzania zmian itd., jest firma ENIGMA Systemy Ochrony Informacji Sp. z o.o., reprezentowana przez przedstawicieli upoważnionych zgodnie z wpisem KRS lub na podstawie osobnego upoważnienia.

Wszelkie zmiany niniejszej polityki certyfikacji, z wyjątkiem takich, które naprawiają oczywiste błędy redakcyjne lub stylistyczne, wymagają nadania nowego numeru wersji.

Wszystkie *tokeny* wystawione w okresie obowiązywania wcześniejszej wersji polityki certyfikacji i nadal ważne w chwili zatwierdzenia nowej wersji, zachowują swoją ważność i podlegają postanowieniom tej wersji polityki certyfikacji, zgodnie z którą zostały wystawione.

Punktem kontaktowym dla obsługi wszelkich spraw związanych z realizacją niniejszej polityki certyfikacji przez CCK CenCert jest:

Centralny Punkt Rejestracji
Centrum Certyfikacji Kluczy *CenCert*
ENIGMA Systemy Ochrony Informacji Sp. z o.o.
03-301 Warszawa
ul. Jagiellońska 78

Telefony kontaktowe i numer faksu są publikowane na stronie www.cencert.pl.

1.6. Słownik używanych terminów i akronimów

W niniejszym dokumencie następujące sformułowania użyte będą w wymienionym poniżej znaczeniu. Należy zwrócić uwagę, że opisy tu umieszczone nie są ogólnymi definicjami danego terminu, lecz wyjaśniają znaczenie danego terminu lub akronimu w kontekście używanym w CCK CenCert.

Termin/akronim	Opis
CCK	Centrum Certyfikacji Kluczy – jednostka organizacyjna, której zadaniem jest generowanie, dystrybucja i unieważnianie certyfikatów kluczy publicznych zgodnie z określoną polityką certyfikacji. Jeśli w jednym miejscu, przy wykorzystaniu wspólnych lub częściowo wspólnych zasobów technicznych i ludzkich, realizuje się kilka polityk certyfikacji, wystawiając certyfikaty podpisywane różnymi kluczami prywatnymi i certyfikaty te zawierają różne dane w polu *wystawca certyfikatu* (różne identyfikatory DN), mówimy o oddzielnych Centrach Certyfikacji Kluczy.
CRL	Lista unieważnionych certyfikatów. Jest wystawiana, poświadczana elektronicznie i publikowana przez CCK.
DN	Identyfikator DN – *Distinguished Name* – Identyfikator podmiotu PKI według składni zdefiniowanej w normach serii X.500

Termin/akronim	Opis
HSM	*Hardware Security Module* – Sprzętowy moduł kryptograficzny – urządzenie posiadające funkcjonalność generowania kluczy kryptograficznych i wykorzystywania klucza prywatnego CCK do generowania podpisów/poświadczeń elektronicznych. Urządzenia HSM pozwalają na użycie klucza prywatnego przez uprawnioną osobę/osoby lecz nie pozwalają na pobranie klucza prywatnego z urządzenia lub skopiowanie go, nawet przez osobę mającą uprawnienia dostępu do klucza.
Klucz prywatny	1) Dane służące do składania podpisu kwalifikowanego przez Subskrybenta 2) Dane służące do składania poświadczenia elektronicznego przez Centrum Certyfikacji Kluczy lub odpowiedniego ministra lub podmiot wskazany zgodnie z zapisami art. 23. Ust. 3 do 5 Ustawy
Klucz publiczny	Dane służące do weryfikacji podpisu elektronicznego, umieszczane w certyfikacie lub zaświadczeniu certyfikacyjnym
OSCP	*Online Certificate Status Protocol* - protokół i nazwa usługi PKI służącej do informowania o statusie konkretnych certyfikatów, o które pyta usługobiorca (czy certyfikat jest ważny, czy unieważniony)
PKI	*Public Key Infrastructure* – infrastruktura klucza publicznego – system obejmujący Centra Certyfikacji Kluczy, Punkty Rejestracji oraz użytkowników końcowych, służący do dystrybucji certyfikatów klucza publicznego oraz zapewnienia możliwości ich wiarygodnej weryfikacji
Podpis kwalifikowany	Bezpieczny podpis elektroniczny weryfikowany przy użyciu ważnego kwalifikowanego certyfikatu - zgodnie z definicją określoną w Ustawie
Rozporządzenie	Rozporządzenie Rady Ministrów z dnia 7 sierpnia 2002 r. w sprawie określenia warunków technicznych i organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego (Dz.U. z 2002r. nr 128 poz. 1094).
Subskrybent	Osoba korzystająca z kwalifikowanych usług certyfikacyjnych świadczonych przez CCK CenCert
Ustawa	Ustawa z dnia 18 września 2001 r. o podpisie elektronicznym. (Dz. U. z 2001r. nr 130 poz. 1450)

Termin/akronim	Opis
Token	(definicja specyficzna dla niniejszej polityki certyfikacji) – Dane wytworzone jako wynik realizacji danej usługi certyfikacyjnej, zawierające poświadczenie elektroniczne CCK, weryfikowane przy użyciu zaświadczenia certyfikacyjnego wystawionego przez ministra właściwego ds. gospodarki. Tokenem w tym rozumieniu jest np. znacznik czasu (wynik realizacji usługi znakowania czasem), jak też odpowiedź protokołu OCSP (jako wynik realizacji usługi poświadczania ważności).

Znaczenie terminów użytych w niniejszej polityce certyfikacji, o ile nie są one zdefiniowane powyżej, są zgodne ze znaczeniem określonym w Ustawie.

2. Zasady dystrybucji i publikacji informacji

CCK publikuje następujące informacje:

- Aktualną politykę certyfikacji, materiały marketingowe, komunikaty bieżące itd.

Powyższe informacje dostępne są w repozytorium dostępnym za pomocą protokołu HTTP/HTTPS. Protokół HTTPS zapewnia uwierzytelnienie serwera WWW, na którym znajduje się repozytorium, z poziomu popularnych przeglądarek internetowych.

Adres serwera www CCK CenCert to: www.cencert.pl

3. Identyfikacja i uwierzytelnienie

Niniejszy rozdział opisuje zasady identyfikacji i uwierzytelnienia stosowane przez CCK w trakcie realizacji usług – jeśli dana usługa tego wymaga.

3.1. Struktura nazw przydzielanych Subskrybentom

Nie dotyczy.

3.2. Uwierzytelnienie Subskrybenta przy pierwszej realizacji usługi

3.2.1 Usługa znakowania czasem

Uwierzytelnienie Subskrybenta dokonywane jest na podstawie podpisu elektronicznego złożonego pod żądaniem o wystawienie znacznika czasu.

Nie wymaga się, aby podpis pod żądaniem był weryfikowany przy użyciu kwalifikowanego certyfikatu. Wymaga się natomiast aby podpis ten był weryfikowany przy użyciu certyfikatu:

1) wystawionego przez Centrum Certyfikacji Kluczy zaakceptowane przez CCK CenCert dla celów, których dotyczy niniejszy rozdział lub
2) zarejestrowanego w CCK CenCert i wskazanego dla celów, których dotyczy niniejszy rozdział.

3.2.2 Usługa poświadczania ważności certyfikatów

Nie jest wymagane uwierzytelnienie strony żądającej poświadczenia ważności certyfikatu.

3.3. Uwierzytelnienie Subskrybenta przy powtórnej realizacji usługi

Jak w rozdziale 3.2.

3.4. Sposoby uwierzytelnienia Subskrybenta przy zgłaszaniu żądania unieważnienia, zawieszenia i uchylenia zawieszenia certyfikatu

Nie dotyczy.

4. Cykl życia– wymagania operacyjne

4.1. Żądanie realizacji usługi

4.1.1 Usługa znakowania czasem

Centrum Certyfikacji Kluczy wystawia znacznik czasu każdorazowo na podstawie żądania znakowania czasem. Żądanie powinno być podpisane przez Subskrybenta.

Podpis pod żądaniem znakowania czasem jest wymagany jedynie w celu rozliczeń z tytułu wykonania usługi. CCK zastrzega sobie możliwość wystawiania znaczników czasu na podstawie niepodpisywanych żądań znakowania czasem (np. przy stosowaniu innego typu określania uprawnień Subskrybentów do uzyskiwania znaczników czasu).

4.1.2 Usługa poświadczania ważności certyfikatów

Centrum Certyfikacji Kluczy wystawia poświadczenie określające status ważności danego certyfikatu jako odpowiedź na przesłane elektronicznie żądanie potwierdzenia statusu certyfikatu. Nie wymaga się aby żądanie było uwierzytelnione podpisem elektronicznym.

Centrum Certyfikacji Kluczy zastrzega sobie możliwość selektywnego odrzucania żądań bez ich przetwarzania w przypadku wykrycia lub podejrzenia ataku sieciowego z określonego adresu lub podsieci.

Żądanie potwierdzenia ważności certyfikatu może dotyczyć więcej niż jednego certyfikatu.

4.2. Przetwarzanie żądań realizacji usługi

System informatyczny Centrum Certyfikacji Kluczy niezwłocznie po odebraniu żądania weryfikuje poprawność żądania oraz uprawnienia Subskrybenta (w przypadku znakowania czasem). Żądanie jest automatycznie odrzucane w przypadku niepoprawnej składni, niemożności wykonania usług (np. gdy zawarte w żądaniu parametry usługi nie są realizowane przez CCK), a w przypadku usługi znakowania czasem, także w przypadku braku uprawnień Subskrybenta do otrzymania znacznika czasu.

4.3. Odpowiedź serwera CCK na żądanie realizacji usługi

4.3.1 Usługa znakowania czasem

Po poprawnej weryfikacji żądania znakowania czasem system informatyczny CCK niezwłocznie wystawia i odsyła Subskrybentowi (jako odpowiedź na żądanie, w ramach protokołu HTTP) kwalifikowany znacznik czasu, zawierający czas z momentu wystawienia znacznika. Poprawnie zweryfikowane żądania przetwarzane są w kolejności odebrania.

4.3.2 Usługa poświadczania ważności certyfikatów

Po poprawnej weryfikacji żądania potwierdzenia ważności certyfikatu system informatyczny CCK niezwłocznie wystawia i odsyła Subskrybentowi (jako odpowiedź na żądanie, w ramach protokołu HTTP) poświadczoną elektronicznie przez CCK odpowiedź zawierającą informację o statusie certyfikatu (lub certyfikatów, jeśli żądanie dotyczyło więcej niż jednego certyfikatu).

Odpowiedź zawiera informację, czy:

1. certyfikat jest ważny (tzn. nie jest unieważniony lub zawieszony)
2. certyfikat jest unieważniony bądź zawieszony
3. status certyfikatu nie jest znany.

4.4. Akceptacja odpowiedzi serwera CCK przez Subskrybenta

Nie dotyczy.

4.5. Korzystanie z *tokenu* powstałego w wyniku realizacji usługi

4.5.1 Usługa znakowania czasem

Kwalifikowany znacznik czasu, zgodnie z przepisami o podpisie elektronicznym, stanowi dowód istnienia określonych danych w momencie czasu określonym w znaczniku. Znakowanie czasem przez kwalifikowany podmiot świadczący usługi certyfikacyjne

wywołuje w szczególności skutki prawne daty pewnej w rozumieniu przepisów Kodeksu cywilnego.

Domniemania, o których mowa powyżej, są zachowane, o ile dany znacznik czasu jest weryfikowany przy użyciu ważnego zaświadczenia certyfikacyjnego wystawionego przez ministra właściwego ds. gospodarki. Zaświadczenie certyfikacyjne traci ważność w terminie w nim określonym (jest wystawiane na 5 lat) oraz w innych przypadkach gdy minister decyduje o unieważnieniu zaświadczenia (np. zakończenie działalności podmiotu świadczącego usługi certyfikacyjne).

W przypadku, gdy utrata domniemania istnienia określonych danych elektronicznych w określonym momencie może wyrządzić szkodę Subskrybentowi lub osobom trzecim, na osobie która potencjalnie może ponieść szkodę spoczywa zarządzanie ryzykiem i ewentualnie decyzja o konieczności zapewnienia innych dowodów potwierdzających istnienie określonych danych (np. innego kwalifikowanego znacznika czasu).

4.5.2 Usługa poświadczania ważności certyfikatów

Odpowiedź o statusie certyfikatu stanowi mechanizm dostarczania Subskrybentom informacji o zawieszeniach i unieważnieniach certyfikatów alternatywnych w stosunku do list CRL.

Poświadczona elektronicznie odpowiedź o statusie certyfikatu, zawierająca status certyfikatu określony jako „ważny”, stanowi dowód, że w danym momencie (określonym w odpowiedzi) dany certyfikat nie był unieważniony ani zawieszony.

Odpowiedź ta nie informuje jednak, czy dany certyfikat w tym momencie był w okresie ważności ani czy w ogóle taki certyfikat był przez CCK kiedykolwiek wystawiony. Zweryfikowanie poprawności certyfikatu (w szczególności czy jest prawidłowo poświadczony przez CCK) oraz jego okresu ważności musi być wykonywane przy weryfikacji podpisu elektronicznego niezależnie od uzyskania informacji o statusie certyfikatu.

4.6. Wymiana *tokenu*

Nie dotyczy.

4.7. Wymiana połączona z wymianą pary kluczy

Nie dotyczy.

4.8. Zmiana treści *tokenu*

Nie dotyczy.

4.9. Unieważnienie i zawieszenie *tokenu*

Nie dotyczy.

4.10. Usługi informowania o statusie *tokenu*

Nie dotyczy.

4.11. Zakończenie umowy certyfikacyjnej

Umowa certyfikacyjna pomiędzy Centrum Certyfikacji Kluczy a Subskrybentem, dotycząca realizacji usługi wystawiania znaczników czasu kończy się wraz z zakończeniem ważności odpowiedniego zaświadczenia certyfikacyjnego CenCert służącego do weryfikacji „tokenów" wystawionych w wyniku realizacji usług.

4.12. Powierzanie i odtwarzanie kluczy prywatnych

Centrum Certyfikacji Kluczy nie powierza swojego klucza prywatnego inny podmiotom.

5. Zabezpieczenia organizacyjne, operacyjne i fizyczne

5.1. Zabezpieczenia fizyczne

Centrum Certyfikacji Kluczy jest umiejscowione w pomieszczeniach użytkowanych przez firmę ENIGMA Systemy Ochrony Informacji Sp. z o.o..

Serwery CCK znajdują się w klimatyzowanej serwerowni, wyposażonej w system ochrony przed zalaniem, pożarem oraz zanikami zasilania, a także system kontroli dostępu oraz system alarmowy włamania i napadu klasy SA3.

Dostęp do pomieszczenia serwerowni jest możliwy tylko dla upoważnionych osób, a każdorazowy fakt dostępu jest odnotowywany.

Centrum Certyfikacji Kluczy jest wyposażone w centrum zapasowe, umiejscowione w lokalizacji oddalonej od centrum podstawowego.

Wszelkie dane i urządzenia istotne dla bezpieczeństwa Centrum Certyfikacji Kluczy i usług przez nie świadczonych (w szczególności karty elektroniczne z elementami klucza prywatnego CCK, kody dostępu do urządzeń, kart i systemów, nośniki archiwizacyjne) są przechowywane w pomieszczeniach CCK o kontrolowanym dostępie, w zamkniętych szafach metalowych.

5.2. Zabezpieczenia proceduralne

W Centrum Certyfikacji Kluczy występują następujące funkcje mające bezpośredni wpływ na realizację usług certyfikacyjnych:

Nazwa funkcji w CCK	**Nazwa funkcji według przepisów o podpisie elektronicznym**	**Rodzaj obowiązków**

Nazwa funkcji w CCK	Nazwa funkcji według przepisów o podpisie elektronicznym	Rodzaj obowiązków
Administrator Systemu Informatycznego	Administrator Systemu	Instalowanie, konfigurowanie, zarządzenie systemem i siecią informatyczną
Operator Systemu	Operator Systemu	Stała obsługa systemu teleinformatycznego, w tym wykonywanie kopii zapasowych
Administrator CCK	Administrator Systemu	Konfigurowanie systemu CCK w zakresie polityki. Zarządzanie kluczami CCK
Inspektor ds. audytu	Inspektor ds. audytu	Analizowanie zapisów rejestrów zdarzeń mających miejsce w systemach teleinformatycznych wykorzystywanych przy świadczeniu usług certyfikacyjnych
Inspektor ds. bezpieczeństwa	Inspektor ds. bezpieczeństwa	Nadzór nad wdrożeniem i stosowaniem wszystkich procedur bezpiecznej eksploatacji systemów teleinformatycznych wykorzystywanych przy świadczeniu usług certyfikacyjnych

Funkcja Inspektora ds. bezpieczeństwa nie może być łączona z funkcją Administratora Systemu ani z funkcją Operatora Systemu. Funkcja Inspektora ds. audytu nie może być łączona z żadną z pozostałych wymienionych funkcji.

5.3. Zabezpieczenia osobowe

Wszystkie osoby pełniące co najmniej jedną z funkcji wymienionych w rozdz. 5.2 spełniają następujące wymagania:

- posiadają pełną zdolność do czynności prawnych,
- nie były skazane prawomocnym wyrokiem za przestępstwo przeciwko wiarygodności dokumentów, obrotowi gospodarczemu, obrotowi pieniędzmi i papierami

wartościowymi, przestępstwo skarbowe lub przestępstwa określone w Ustawie o podpisie elektronicznym,

- posiadają niezbędną dla pracy na danym stanowisku wiedzę i umiejętności w zakresie technologii realizacji usług certyfikacyjnych świadczonych przez Centrum Certyfikacji Kluczy.

Wszystkie osoby pełniące wymienione funkcje, przed dopuszczeniem do wykonywania obowiązków, są kierowane na szkolenie obejmujące swoim zakresem podstawy systemów PKI oraz materiał odpowiedni dla określonego stanowiska pracy, w tym procedury i regulaminy pracy obowiązujące w CCK CenCert oraz omówienie możliwej odpowiedzialności karnej w zakresie związanym z świadczeniem usług certyfikacyjnych. Szkolenie kończy się egzaminem, a do wykonywania obowiązków dopuszczane są tylko te osoby, które uzyskały wymaganą liczbę punktów.

Szkolenie każdej osoby pełniącej co najmniej jedną z wymienionych funkcji powtarzane jest co 5 lat lub, w razie potrzeby, częściej.

W przypadku gdy określoną funkcję pełni osoba niezatrudniona w firmie prowadzącej CCK na podstawie umowy o pracę, CCK zawiera w umowie z tą osobą lub z firmą, w której jest ona zatrudniona, możliwość dochodzenia przez CCK wszelkich strat, które ewentualnie może ponieść Centrum Certyfikacji Kluczy w wyniku nienależytego wykonywania przez daną osobę obowiązków wynikających z realizowanej przez nią funkcji lub w wyniku nieprzestrzegania obowiązujących przepisów prawa, jak też zasad i regulaminów obowiązujących w CCK.

W przypadku gdy określoną funkcję pełni osoba zatrudniona w firmie prowadzącej CCK na podstawie umowy o pracę, odpowiedzialność tej osoby regulowana jest obowiązującymi przepisami Kodeksu pracy.

Niezależnie od ewentualnej odpowiedzialności finansowej, osoby wykonujące nierzetelnie swoje obowiązki związane ze świadczeniem usług certyfikacyjnych lub nieprzestrzegające wymagań nałożonych przez przepisy o podpisie elektronicznym (w szczególności wymagań o poufności, wymagań w zakresie wystawiania i unieważniania certyfikatów) podlegają sankcjom karnym określonym w Ustawie o podpisie elektronicznym, do kary pozbawienia wolności do lat 5 włącznie.

5.4. Procedury tworzenia logów audytowych

Centrum Certyfikacji Kluczy zapewni rejestrowanie wszelkich istotnych zdarzeń związanych z realizacją świadczonych przez CCK usług certyfikacyjnych. System informatyczny CCK zapewnia automatyczne tworzenie logów audytowych w 2 miejscach:

- Log systemu operacyjnego – rejestruje w szczególności następujące zdarzenia:
  - rozpoczęcie i przerwanie funkcji rejestrujących zdarzenia,
  - istotne zdarzenia związane ze zmianami w środowisku systemu, w szczególności tworzenia kont i rodzaju przydzielanych uprawnień,
  - zmiany w konfiguracji funkcji rejestrujących zdarzenia, w tym w szczególności każdą modyfikację czasu systemowego,
  - czas tworzenia kopii zapasowych,
  - czas archiwizowania rejestrów zdarzeń,
  - zamykanie, otwieranie i ponowne uruchamianie po zamknięciu systemu,
- Log systemu CCK – rejestruje w szczególności następujące zdarzenia:
  - żądanie świadczenia usług certyfikacyjnych normalnie udostępnianych przez system lub usług niewykonywanych przez system, informacji o wykonaniu lub niewykonaniu usługi oraz o przyczynie jej niewykonania – w szczególności kompletny, podpisany przez Inspektora ds. rejestracji formularz zawierający polecenie wystawienia bądź unieważnienia certyfikatu,
  - istotne zdarzeń związanych ze zmianami w środowisku systemu CCK, w tym w podsystemie zarządzania kluczami i certyfikatami,
  - rozpoczęcie i przerwanie funkcji rejestrujących zdarzenia,
  - zamykanie, otwieranie i ponowne uruchamianie po zamknięciu systemu,
- Log urządzenia HSM – rejestruje w szczególności następujące zdarzenia:
  - rozpoczęcie i przerwanie funkcji rejestrujących zdarzenia,
  - istotne zdarzenia związane ze zmianami w środowisku systemu, w szczególności tworzenia kont i rodzaju przydzielanych uprawnień,
  - zmiany w konfiguracji funkcji rejestrujących zdarzenia, w tym w szczególności każdą modyfikację czasu systemowego,
  - negatywne wyniki testów generatora pseudolosowego

Poza systemem automatycznego generowania logów przechowywane są następujące zapisy:

- zapisy o instalacji nowego oprogramowania lub o aktualizacjach,
- wszystkie zgłoszenia unieważnienia kwalifikowanego certyfikatu oraz wszystkich wiadomości z tym związanych, a w szczególności wysłane i odebrane komunikaty o zgłoszeniach przesyłane w relacjach posiadacza kwalifikowanego certyfikatu z kwalifikowanym podmiotem świadczącym usługi certyfikacyjne;

Log systemu operacyjnego jest dostępny dla Administratora systemu i jest zabezpieczony przed modyfikacją przed osobami nieposiadającymi praw Administratora systemu za pomocą mechanizmów systemu.

Log systemu CCK jest dostępny dla Inspektora ds. Audytu i jest zabezpieczony przed modyfikacją przed osobami nieposiadającymi praw Administratora systemu za pomocą mechanizmów systemu operacyjnego.

Logi systemu operacyjnego oraz systemu CCK są przeglądane w każdym dniu roboczym odpowiednio przez Administratora systemu oraz Inspektora ds. audytu.

Logi podlegają procedurom tworzenia kopii zapasowych oraz – w razie potrzeby – są archiwizowane.

Logi są przechowywane przez 3 lata od ostatniego wpisu.

5.5. Archiwizacja zapisów

Procedury archiwizacyjne wykonywane są raz w roku (na początku roku) i obejmują:

- rejestry zdarzeń – okres przechowywania kopii archiwalnej wynosi 3 lata.

Zarchiwizowane informacje są usuwane z systemu CCK, o ile były przechowywane w plikach (nie w bazie danych CCK). Zarchiwizowane informacje mogą być usunięte z bazy danych CCK, o ile jest to konieczne i nie zakłóci bieżącej pracy CCK.

5.6. Wymiana pary kluczy Centrum Certyfikacji Kluczy

Wygenerowanie i wymiana pary kluczy Centrum Certyfikacji Kluczy może następować w planowych terminach lub wcześniej.

Planowa wymiana pary kluczy CCK następuje nie wcześniej niż 1 rok i nie później niż 3 lata po otrzymaniu poprzedniego zaświadczenia certyfikacyjnego wystawionego w imieniu ministra właściwego ds. gospodarki.

Procedura wymiany pary kluczy polega na:

- Wygenerowaniu nowej pary kluczy.
- Zgłoszeniu nowego klucza publicznego w celu umieszczenia go w zaświadczeniu certyfikacyjnym wystawionym w imieniu ministra właściwego ds. gospodarki.
- Otrzymaniu nowego zaświadczenia certyfikacyjnego.
- Wykonaniu operacji „przełączenia" kluczy w oprogramowaniu CCK, co powoduje, że wszystkie nowe poświadczenia wystawiane są już przy użyciu nowego klucza CCK.

5.7. Utrata poufności klucza prywatnego CCK i działanie CCK w przypadku katastrof

5.7.1 Utrata poufności klucza prywatnego CCK

CCK posiada odpowiednie procedury obowiązujące w wypadku utraty poufności klucza prywatnego CCK lub uzasadnionego podejrzenia zajścia takiego zdarzenia.

Procedury te przewidują w szczególności:

1. Powiadomienie Subskrybentów oraz ministra ds. gospodarki o zaistniałej sytuacji oraz o planie dalszego działania.
2. Wytworzenie nowych kluczy CCK i zgłoszenie ich ministrowi ds. gospodarki, w celu wystawienia nowych zaświadczeń certyfikacyjnych.

5.7.2 Katastrofy

5.7.2.1 Wyłączenie Centrum Podstawowego

Centrum Certyfikacji Kluczy posiada dwie lokalizacje: Centrum Podstawowe i Centrum Zapasowe, w miejscach oddalonych od siebie.

W obu lokalizacjach przechowywany są klucze CCK do realizacji odpowiednich usług oraz klucze infrastruktury niezbędne do funkcjonowania CCK.

Zawartość baz danych CCK jest na bieżąco uaktualniana w Centrum Zapasowym, na podstawie zawartości bazy w Centrum Podstawowym.

Centrum podstawowe jest zabezpieczone przed zanikiem zasilania, utratą jednej linii komunikacyjnej, pożarem, zalaniem, awarią pojedynczego komputera, urządzenia lub dysku. Centrum zapasowe jest zabezpieczone przed zanikiem zasilania, pożarem, zalaniem lub awarią pojedynczego dysku.

W przypadku katastrofy, awarii sprzętu lub infrastruktury przekraczającej możliwości wynikające z zabezpieczeń stosowanych w centrum podstawowym, CCK przełącza swoją działalność na centrum zapasowe, zgodnie z posiadanymi procedurami.

5.8. Zakończenie działalności CCK

Decyzję o zakończeniu działalności CCK podejmuje Zarząd Spółki. Decyzja może dotyczyć rezygnacji ze świadczenia wszystkich usług objętych niniejszą Polityką lub niektórych z tych usług.

O ile to w danej sytuacji możliwe, zakończenie działalności w zakresie danej usługi powinno nastąpić nie wcześniej niż z dniem upływu ważności zaświadczenia certyfikacyjnego związanego z realizacją tej usługi. Nie oznacza to konieczności wydawania nowych „tokenów" do tego czasu – aktywne świadczenie danej usługi może być zakończone lub zawieszone wcześniej, zgodnie z umowami zawartymi z Subskrybentami.

O planowanym zakończeniu działalności w danym zakresie niezwłocznie informowany jest minister właściwy ds. gospodarki, z co najmniej 3-miesięcznym wyprzedzeniem. O planowanym zakończeniu działalności informowani są także Subskrybenci.

Po zakończeniu działalności klucz prywatny CCK służący do realizacji danej usługi jest niszczony.

W przypadku, gdyby CenCert zaprzestał realizacji wszystkich kwalifikowanych usług certyfikacyjnych, co wiązałoby się z utratą wpisu do rejestru kwalifikowanych podmiotów i o ile inny kwalifikowany podmiot certyfikacyjny nie przejąłby w takim przypadku działalności CCK - dokumenty i zapisy, co do których jest wymagana archiwizacja, będą przekazywane po zakończeniu działalności ministrowi ds. gospodarki lub podmiotowi przez niego wskazanemu.

6. Zabezpieczenia techniczne

6.1. Generowanie i instalowanie par kluczy

6.1.1 Generowanie par kluczy

Pary kluczy Centrum Certyfikacji Kluczy generowane są przez personel Centrum Certyfikacji Kluczy zgodnie z udokumentowaną procedurą. W toku wykonywania procedury generowania kluczy wymagana jest obecność co najmniej osób pełniących następujące funkcje:

1. Administrator systemu informatycznego
2. Administrator CCK
3. Inspektor ds. bezpieczeństwa.

Wymagana jest nieprzerwana obecność Inspektora ds. bezpieczeństwa od momentu wywołania procedury generowania kluczy na urządzeniu HSM do momentu zapakowania kart elektronicznych zawierających fragmenty klucza oraz innych poufnych danych powstałych przy generowaniu kluczy (jak kody PIN) w sposób zgodny z procedurą.

Generowanie par kluczy Centrum Certyfikacji Kluczy odbywa się wewnątrz urządzenia HSM posiadającego co najmniej jeden z certyfikatów wymaganych przepisami o podpisie elektronicznym.

6.1.2 Dostarczenie klucza prywatnego Subskrybentowi

Nie dotyczy.

6.1.3 Dostarczenie klucza publicznego Subskrybenta do Punktów Rejestracji

Nie dotyczy.

6.1.4 Dostarczenie klucza publicznego CCK

Klucz publiczny Centrum Certyfikacji Kluczy jest dostępny w postaci zaświadczenia certyfikacyjnego poświadczonego przez ministra właściwego ds. gospodarki lub podmiot przez niego wskazany.

6.1.5 Rozmiary kluczy

Wszystkie klucze, o których mowa w niniejszym rozdziale, są kluczami algorytmu RSA.

Klucze Centrum Certyfikacji Kluczy mają długość 2048 bitów.

6.1.6 Cel użycia klucza

6.1.6.1 Usługa znakowania czasem

Klucz prywatny Centrum Certyfikacji Kluczy może być wykorzystywany tylko do poświadczania znaczników czasu.

6.1.6.2 Usługa poświadczania ważności certyfikatów

Klucz prywatny Centrum Certyfikacji Kluczy może być wykorzystywany tylko do poświadczania ważności certyfikatów.

6.2. Ochrona kluczy prywatnych

Urządzenia służące do generowania kluczy kryptograficznych oraz do generowania podpisów (przez Subskrybentów) lub poświadczeń elektronicznych (przez Centrum Certyfikacji Kluczy) muszą posiadać jeden z następujących certyfikatów:

1) ITSEC dla poziomu E3 z minimalną siłą mechanizmów zabezpieczających, określoną jako "wysoka", albo poziomu bezpieczniejszego lub

2) FIPS PUB 140 dla poziomu 3 albo bezpieczniejszego, lub

3) Common Criteria (norma ISO/IEC 15408) dla poziomu EAL4 albo bezpieczniejszego.

Klucz prywatny Centrum Certyfikacji Kluczy jest wytworzony i zapisane z użyciem mechanizmu podziału sekretów „*2 z m*”, przy czym *m* wynosi co najmniej 6 i nie więcej niż 8 (do użycia klucza CCK jest potrzebne posiadania dowolnych 2 fragmentów klucza, wszystkich fragmentów jest *m*).

Klucz prywatny CCK nie jest przekazywany (w tym powierzany) innym podmiotom.

Kopie zapasowe kluczy prywatnych (CCK, Inspektorów ds. rejestracji, Subskrybentów) nie są tworzone. Wyjątkiem mogą być kopie niektórych kluczy infrastruktury używanych wewnętrznie w CCK i przetwarzanych programowo – o ile takie klucze występują.

Klucze prywatne nie są archiwizowane.

Klucz prywatny CCK jest odczytywany z urządzenia HSM jedynie w postaci zaszyfrowanych fragmentów klucza, umożliwiającej wykorzystanie fragmentu jedynie wewnątrz urządzenia HSM, z zachowaniem wszystkich przewidzianych zabezpieczeń.

Klucze prywatne Centrum Certyfikacji Kluczy są uaktywniane przez personel Centrum Certyfikacji Kluczy zgodnie z procedurami operacyjnymi. Uaktywnienie klucza wymaga obecności co najmniej dwóch uprawnionych osób, w tym osoby pełniącej rolę Inspektora ds. bezpieczeństwa. Klucz jest aktywny do momentu wyłączenia urządzenia HSM.

Niszczenie kluczy prywatnych CCK wykonywane jest komisyjnie przez personel CCK zgodnie z udokumentowaną procedurą. Wymagana jest obecność co najmniej dwóch osób, w tym osoby pełniącej rolę Inspektora ds. bezpieczeństwa. Wymagana jest identyfikacja kart przed zniszczeniem. Z procedury niszczenia sporządza się protokół.

Centrum Certyfikacji Kluczy używa urządzeń HSM charakteryzujących się niskim poziomem emisji elektromagnetycznej, nie nakłada się jednak żadnych formalnych wymagań na badania pod kątem ujawniającego ulotu elektromagnetycznego urządzeń lub pomieszczeń, w których są generowane i przetwarzane klucze CCK, Inspektorów ds. rejestracji i Subskrybentów.

Klucze infrastruktury służące do szyfrowania kluczy prywatnych CCK są przechowywane na indywidualnych modułach kluczowych, chronionych kodami PIN i przydzielonych upoważnionym osobom. Fragmenty kluczy infrastruktury zapisane są na modułach kluczowych z wykorzystaniem procedury podziału sekretu.

6.3. Inne aspekty zarządzania parą kluczy

Klucze publiczne Centrum Certyfikacji Kluczy prowadzi długoterminową archiwizację swoich kluczy publicznych, na takich zasadach, jakim podlegają inne archiwowane dane.

6.4. Dane aktywujące

CCK przyjęło i przestrzega udokumentowanych procedur postępowania z wszelkimi danymi aktywującymi. Ogólne zasady, na których zbudowane są szczegółowe procedury są następujące:

1. Uaktywnienie klucza CCK wymaga obecności co najmniej dwóch osób, w tym Inspektora ds. bezpieczeństwa.
2. Administrator systemu informatycznego nie może posiadać żadnych danych aktywujących pozwalających na wykonywanie jakichkolwiek operacji w CCK.
3. Administrator CCK i Operator CCK nie mogą posiadać danych pozwalających na wykonywanie operacji w systemie operacyjnym lub w systemie baz danych z prawami administratora systemu lub bazy.
4. Wszelkie dane aktywujące powinny być zapamiętane przez osoby rutynowo je używające. Kopie tych danych oraz dane używane rzadko są zapisywane przez uprawnioną osobę, a następnie pakowane w nieprzezroczyste koperty. Koperta jest być podpisywana i opisywana (zawartość koperty, kto i kiedy pakował) przez osoby pakujące, w tym Inspektora ds. bezpieczeństwa, i zabezpieczona tak, jak przesyłki z materiałami niejawnymi. Tak zabezpieczona koperta jest przechowywana w metalowej szafie w Centrum Podstawowym i/lub Zapasowym, w pomieszczeniu o kontrolowanym dostępie. Dane aktywujące potrzebne – choćby potencjalnie – w obu lokalizacjach, są zapisywane w dwóch kopiach i przechowywane w obu lokalizacjach.
5. Jest prowadzony rejestr, w którym są odnotowywane przypadki składania danych aktywujących oraz fakt każdorazowego dostępu do tych danych.

6.5. Zabezpieczenia komputerów

Nie jest wymagane używanie przez CCK serwerów posiadających certyfikaty bezpieczeństwa na sprzęt lub oprogramowanie systemu operacyjnego.

CCK może przeprowadzać audyty, w tym testy penetracyjne, używanego systemu informatycznego w środowisku testowym. Wyniki audytów nie są publikowane.

Wszystkie operacje przewidziane do wykonania na komputerach i serwerach CCK można wykonać po uprzednim uwierzytelnieniu się i kontroli uprawnień. Wykonywane operacje są zapisywane w dziennikach zdarzeń i podlegają przeglądowi co najmniej w każdy dzień roboczy.

6.6. Zabezpieczenia związane z cyklem życia systemu informatycznego

W Centrum Certyfikacji Kluczy przyjęto udokumentowaną procedurę dokonywania modyfikacji lub zmian w systemie teleinformatycznym. W szczególności dotyczy to testów nowych wersji oprogramowania i/lub wykorzystania do tego celu istniejących baz danych. Zasady te gwarantują nieprzerwaną pracę systemu teleinformatycznego, integralność jego zasobów oraz zachowanie poufności danych.

W szczególności procedura gwarantuje testowanie nowych wersji oprogramowania w środowisku testowym. Gwarantuje także, że do realizacji jakichkolwiek testów nie mogą być używane kluczy prywatne CCK służące do realizacji usług kwalifikowanych, chyba że zostaną wypełnione wszystkie zasady obowiązujące przy realizacji tych usług.

Oprogramowanie urządzenia HSM i oprogramowanie używane do obsługi CCK kontroluje swoją integralność przy każdym uruchomieniu. W przypadku błędu integralności urządzenie lub oprogramowanie odmawia dalszej pracy.

6.7. Zabezpieczenia sieci komputerowej

Serwery wykorzystywane przez CenCert do świadczenia usług certyfikacyjnych zgodnie z niniejszą polityka certyfikacji są połączone za pomocą logicznie wydzielonej, dwusegmentowej sieci wewnętrznej. Sieć ta spełnia następujące wymagania:

1) dostęp z zewnątrz do wewnętrznego segmentu sieci odbywa się tylko za pośrednictwem serwerów (lub serwera) „proxy" zlokalizowanych w strefie DMZ (pomiędzy urządzeniami firewall), przy czym wszystkie urządzenia zlokalizowane w strefie DMZ mogą się kontaktować bez konieczności użycia urządzenia firewall tylko między sobą, natomiast w przypadku transmisji informacji z segmentem sieci wewnętrznej muszą korzystać z wewnętrznego urządzenia firewall, a w przypadku transmisji z zewnętrzną siecią teleinformatyczną muszą korzystać z pośrednictwa zewnętrznego urządzenia firewall;

2) wewnętrzny segment sieci, w którym znajdują się serwery dokonujące poświadczeń elektronicznych, jest oddzielony od segmentu podłączonego do strefy DMZ, za pomocą urządzenia firewall, rozpoznającego dane przychodzące spoza sieci wewnętrznej na podstawie adresu i portu docelowego i rozsyłającego je do odpowiednich adresów w sieci wewnętrznej;

3) urządzenia firewall (zewnętrzne i wewnętrzne) posiadają certyfikaty ITSEC klasy co najmniej E3 oraz są skonfigurowane w taki sposób, że pozwalają na realizację wyłącznie tych protokołów i usług, które są niezbędne do realizacji usług certyfikacyjnych.

6.8. Oznaczanie czasu

Do wystawiania znaczników czasu oraz oznaczania czasem zapisów w logach oprogramowania stosuje się wskazanie bieżącego czasu pochodzące z zegarów wbudowanych w urządzenia lub stacje robocze.

Zegary stacji roboczych są synchronizowane protokołem NTP z czasem uniwersalnym za pośrednictwem znajdującego się w strukturze CCK, w strefie DMZ, atomowego zegara czasu UTC, synchronizowanego drogą satelitarną.

Zapewnia się synchronizację z czasem UTC zegarów stacji roboczych, służących do znakowania czasem, z dokładnością nie mniejszą niż 1s.

7. Profil znaczników czasu

7.1. Identyfikatory DN

7.1.1 Usługa znakowania czasem

Identyfikator DN Centrum Certyfikacji Kluczy

Kraj (countryName) = ***PL***
Nazwa organizacji (organizationName) = ***ENIGMA SOI Sp. z o.o.***
Nazwa powszechna (*commonName*) = ***CenCert Centrum Kwalifikowanych Znaczników Czasu***
Numer seryjny (serialNumber) **= *Nr wpisu:* 12**

7.1.2 Usługa poświadczania ważności certyfikatów

Identyfikator DN Centrum Certyfikacji Kluczy

Kraj (countryName) = ***PL***
Nazwa organizacji (organizationName) = ***ENIGMA SOI Sp. z o.o.***
Nazwa powszechna (*commonName*) = ***CenCert Poświadczenia Ważności Certyfikatów***
Numer seryjny (serialNumber) **= *Nr wpisu:* 12**

7.2. Profil żądań realizacji usługi

7.2.1 Usługa znakowania czasem

Akceptowane są żądania znakowania czasem zgodne z normą RFC 3161, podpisane elektronicznie w celu uwierzytelnienia zgodnie z normą PKCS#7. Do przesłania treści żądania znakowania czasem oraz pobrania znacznika czasu używany jest protokół HTTP.

Jeśli w żądaniu znakowania czasem (wg RFC 3161) występuje opcjonalny atrybut *ReqPolicy,* powinien zawierać identyfikator „{2 5 29 32 0}" (any policy) lub identyfikator niniejszej polityki certyfikacji. Opcjonalny atrybut *Extensions* może występować lecz nie jest przetwarzany przez system CCK.

Atrybut *Version* podpisu pod żądaniem (wg PKCS#7) powinien zawierać wartość „1". Atrybut *Certificates* powinien zawierać listę certyfikatów, składającą się wyłącznie z certyfikatu (zgodnego z X.509v3) klucza, którym został podpisany znacznik czasu. Atrybut *Lista CRL* nie musi występować (listy CRL są pobierane w inny sposób). Atrybut *SignerInfos* powinien zawierać listę podpisów, składającą się z dokładnie jednego podpisu. Opcjonalne atrybuty podpisu *SignedAttrs* i *UnsignedAttrs* nie są przetwarzane przez system CCK.

7.2.2 Usługa poświadczania ważności certyfikatów

Akceptowane są żądania zgodne z normą RFC 2560. Do przesłania treści żądania oraz pobrania odpowiedzi używany jest protokół HTTP.

7.3. Profil „tokenów" odsyłanych przez CCK w wyniku realizacji usługi

7.3.1 Usługa znakowania czasem

Odpowiedź serwera znakowania czasem jest zgodna z Time Stamp Response – TSR zdefiniowaną w dokumencie RFC 3161, za wyjątkiem sytuacji, gdy klient wysyła błędnie sformatowane żądanie.

7.3.2 Usługa poświadczania ważności certyfikatów

Odpowiedź serwera poświadczeń jest zgodna z normą RFC 2560.

Atrybut *certStatus* zawierający wartość „good" oznacza jedynie to, że certyfikat nie jest w danym momencie unieważniony ani zawieszony. Nie oznacza to, że certyfikat jest ważny ze względu na określony w nim okres ważności. W szczególności certyfikat który został

unieważniony lub zawieszony, w okresie ważności będzie określany jako „revoked”, natomiast po upływie jego okresu ważności może być oznaczony jako „good”.

Atrybut *thisUpdate* określa moment, na który jest ważna informacja o statusie certyfikatu.

Atrybut *producedAt* określa moment poświadczenia odpowiedzi o statusie ważności certyfikatu. Nie jest to równoznaczne z momentem, na który jest określony status certyfikatu.

8. Audyt

Centrum Certyfikacji Kluczy podlega regularnym audytom w ramach funkcjonującego w firmie Zintegrowanego Systemu Zarządzania, zgodnego z normami ISO 9001:2008 oraz ISO 27001.

Niezależnie od tego, w każdym dniu roboczym osoba pełniąca funkcję Inspektora ds. audytu przegląda rejestr zapisu zdarzeń w celu bieżącej kontroli działania CCK i punktów rejestracji.

Centrum Certyfikacji Kluczy podlega także kontrolom, prowadzonym zgodnie z przepisami o podpisie elektronicznym przez ministra właściwego ds. gospodarki.

9. Inne postanowienia

9.1. Opłaty

CCK pobiera opłaty za świadczenie swoich usług zgodnie z obowiązującym w danym momencie cennikiem usług certyfikacyjnych.

9.2. Odpowiedzialność finansowa

Centrum Certyfikacji Kluczy odpowiada za wszelkie szkody spowodowane niewykonaniem lub nienależytym wykonaniem swych obowiązków w zakresie świadczonych usług, chyba że niewykonanie lub nienależyte wykonanie tych obowiązków jest następstwem okoliczności, za które podmiot świadczący usługi certyfikacyjne nie ponosi odpowiedzialności i którym nie mógł zapobiec mimo dołożenia należytej staranności, z uwzględnieniem ograniczeń odpowiedzialności CCK określonych w rozdziale 9.8 poniżej.

9.3. Poufność informacji

Zasady ochrony poufności informacji związanych ze świadczeniem usług certyfikacyjnych określone są w Ustawie o podpisie elektronicznym, także w Ustawie o ochronie danych osobowych.

Centrum Certyfikacji Kluczy traktuje jako informacje poufne wszystkie informacje związane z realizowanymi przez siebie usługami poza informacjami następującymi:

- Polityka certyfikacji w wersjach aktualnie obowiązujących,
- Klucz publiczny CCK,
- Informacje bieżące, przeznaczone do publikacji (takie jak cennik usług, oferta handlowa, bieżące komunikaty, dane kontaktowe).

9.4. Ochrona danych osobowych

Centrum Certyfikacji Kluczy może przetwarzać dane osobowe Subskrybentów. Centrum Certyfikacji Kluczy zgłosiło zbiór danych osobowych zgodnie z obowiązującymi przepisami, a także wdrożyło i realizuje odpowiednie regulaminy zapewniające ochronę danych osobowych.

Subskrybenci są informowani przy podpisywaniu umowy o przetwarzaniu ich danych osobowych przez CCK oraz o przysługujących im w związku z tym prawach.

9.5. Zabezpieczenie własności intelektualnej

Firma ENIGMA Systemy Ochrony Informacji Sp. z o.o. ma pełne prawo do dysponowania majątkowymi prawami autorskimi odnoszącymi się do niniejszej polityki certyfikacji.

ENIGMA Systemy Ochrony Informacji Sp. z o.o. zezwala na wykorzystywanie polityki (w tym drukowanie i kopiowanie) przez Subskrybentów i innych odbiorców usług certyfikacyjnych, w celach związanych z wykorzystywaniem certyfikatów, odpowiedzi OCSP i znaczników czasu wystawianych przez CCK.

9.6. Udzielane gwarancje

Nie dotyczy

9.7. Zwolnienia z domyślnie udzielanych gwarancji

Centrum Certyfikacji Kluczy nie udziela Subskrybentom żadnych domyślnie udzielanych gwarancji, poza gwarancjami które mogą wynikać z obowiązujących przepisów.

Wszelkie gwarancje udzielane przez Centrum Certyfikacji Kluczy muszą być udzielane w formie pisemnej, pod rygorem nieważności.

9.8. Ograniczenia odpowiedzialności

Centrum Certyfikacji Kluczy Cencert nie odpowiada za szkody wynikające z:

- siły wyższej;
- innych przyczyn niezależnych od CCK Cencert, a w szczególności z powodu niefunkcjonowania lub nieprawidłowego funkcjonowania infrastruktury telekomunikacyjnej oraz sprzętu teleinformatycznego nieznajdującego się pod kontrolą CCK CenCert;
- utraty ważności zaświadczenia certyfikacyjnego służącego do weryfikacji wystawionych *tokenów* (w szczególności znaczników czasu);
- odmowy wydania znacznika czasu z powodu negatywnej weryfikacji uprawnień Subskrybenta do pobrania znacznika.
- odmowy realizacji usługi z powodu nieprawidłowego formatu lub niekompletnego żądania realizacji usługi;
- użycia, przez Subskrybenta lub osobę trzecią, znacznika czasu lub innych poświadczonych danych poza zakresem określonym w polityce certyfikacji;
- użycia, przez Subskrybenta lub osobę trzecią, oprogramowania lub sprzętu, który nie był dostarczony przez CCK Cencert lub nie znajduje się na Liście bezpiecznych urządzeń opublikowanej przez CCK Cencert;
- niewłaściwego użytkowania lub instalacji aplikacji lub sprzętu kryptograficznego stosowanego przez Subskrybenta lub osobę trzecią do obsługi znaczników czasu lub innych *tokenów* wystawianych przez CCK CenCert;
- niewystawienia *tokenu* w wyniku tymczasowego wstrzymania świadczenia danej usługi, np. na skutek awarii lub prac konserwacyjnych.
- zaprzestania świadczenia danej usługi.

Łączna odpowiedzialność finansowa ENIGMA SOI Sp. z o.o. z tytułu świadczenia przez CCK CenCert usług certyfikacyjnych nie może przekroczyć 1 000 000 EUR. Wysokość jednorazowego odszkodowania z tytułu użycia nieprawidłowego certyfikatu wydanego przez CCK Cencert nie może przekroczyć 250 000 EUR.

9.9. Przenoszenie roszczeń odszkodowawczych

Centrum Certyfikacji Kluczy zawarło umowę ubezpieczenia odpowiedzialności cywilnej za szkody wyrządzone odbiorcom usług certyfikacyjnych, zgodnie z Rozporządzeniem ministra finansów z dnia 16 grudnia 2003 r. w sprawie obowiązkowego ubezpieczenia

odpowiedzialności cywilnej kwalifikowanego podmiotu świadczącego usługi certyfikacyjne ubezpieczenia cywilnego.

9.10. Przepisy przejściowe i okres obowiązywania polityki certyfikacji

Niniejsza polityka certyfikacji obowiązuje w stosunku do *tokenów* wystawionych zgodnie z nią. *Tokeny* wykorzystywane w celach dochodzeniowych lub dowodowych po okresie ich ważności powinny być wykorzystywane zgodnie z polityką certyfikacji, w ramach której zostały wystawione.

9.11. Określanie trybu i adresów doręczania pism

Wszelkie pisma związane z działalnością Centrum Certyfikacji Kluczy powinny być dostarczane pod adresem Centralnego Punktu Rejestracji.

9.12. Zmiany w polityce certyfikacji

Zasady zarządzania polityką certyfikacji zostały opisane w rozdziale 1.5.

9.13. Rozstrzyganie sporów

We wszelkich sprawach dotyczących spraw związanych z niniejszą polityką certyfikacji można się zwracać do firmy ENIGMA SOI Sp. z o.o. pod adresem biuro@enigma.com.pl.

Skargi na działalność Centrum Certyfikacji Kluczy można także kierować, na zasadach określonych przez przepisy Kodeksu postępowania administracyjnego, do ministra właściwego do spraw gospodarki.

9.14. Obowiązujące prawo

Działanie podsystemu certyfikacji podlega prawu Rzeczpospolitej Polskiej.

9.15. Podstawy prawne

Zasady działania Centrum Certyfikacji Kluczy są zgodne z obowiązującym prawem, a w szczególności z przepisami zawartymi w następujących aktach prawnych:

- Ustawie z dnia 18 września 2001 r. o podpisie elektronicznym.
- Ustawie z dnia 29 sierpnia 1997 o ochronie danych osobowych.
- Ustawie z dnia 6 czerwca 1997 Kodeks karny.
- Ustawie z dnia 4 lutego 1994 Prawo autorskie.

9.16. Inne postanowienia

Nie występują.