CENTRUM CERTYFIKACJI „CENCERT”

Polityka certyfikacji dla certyfikatów niekwalifikowanych powszechnych

Wersja: 1.3

Karta dokumentu:

Tytuł dokumentu	Polityka certyfikacji dla certyfikatów niekwalifikowanych powszechnych
Nazwa pliku	Polityka certyfikatów powszechnych
Właściciel dokumentu	ENIGMA Systemy Ochrony Informacji Sp. z o.o.
Wersja	1.3
Status dokumentu	zatwierdzony
Data zatwierdzenia	26 października 2017
Liczba stron	41

zatwierdzone przez:

Wersja	**zatwierdzający**
1.3	Jacek Pokraśniewicz, Dyrektor Pionu Utrzymania Usług CenCert

historia wersji

Wersja	**Data**	**Komentarze**
1.1	2016-11-08	Wersja po gruntownej aktualizacji
1.2	2017-09-20	Zmiana HSM oraz długości kluczy CA (do 4096)
1.3	2017-10-26	Zmiana w rozdz. 1.3, 7.1.2 – umożliwienie wystawiania certyfikatów dla podległych CA

Spis treści

1. Wstęp

1.1. Wprowadzenie

Niniejszy dokument stanowi politykę świadczenia usługi zaufania (politykę certyfikacji) polegającej na wydawaniu niekwalifikowanych certyfikatów kluczy publicznych. Usługa jest świadczona przez firmę ENIGMA Systemy Ochrony Informacji Sp. z o.o., pod nazwą handlową CenCert.

Odbiorcami usługi zaufania mogą być osoby fizyczne, osoby prawne oraz inne jednostki organizacyjne.

Centrum Certyfikacji Kluczy realizuje niniejszą politykę zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. (eIDAS), rozporządzeniami wykonawczymi Komisji Europejskiej wydanymi na podstawie eIDAS oraz prawem krajowym obowiązującym w Polsce.

Struktura niniejszego 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 certyfikacji dla certyfikatów niekwalifikowanych powszechnych
Kwalifikator polityki	Brak
Numer OID (ang. *Object Identifier*)	1.3.6.1.4.1.10214.99.1.2.1.1
Data wprowadzenia	20 września 2017
Data wygaśnięcia	Do odwołania

1.3. Opis systemu certyfikacji i uczestniczących w nim podmiotów

CenCert prowadzi niekwalifikowane centra certyfikacji (CA - *Certification Authority*) zgodnie z następującą strukturą:

- **rootCA**, CA wystawiające certyfikaty tylko dla innych niekwalifikowanych CA prowadzonych przez CenCert
- **CA „certyfikaty firmowe”** – CA wystawiające certyfikaty zgodnie z polityką „Polityka certyfikacji dla certyfikatów niekwalifikowanych firmowych”
- **CA „certyfikaty powszechne”** - CA wystawiające certyfikaty zgodnie z niniejszą polityką certyfikacji.

CA realizując niniejszą politykę certyfikacji, wystawia certyfikaty dla „użytkowników końcowych”, służące do realizacji usług informatycznych wymagających podpisu lub pieczęci elektronicznej, uwierzytelnienia i/lub szyfrowania.

W ramach niniejszej polityki mogą być wystawiane certyfikaty dla „podległych” (w sensie struktury PKI) podmiotów wystawiających certyfikaty.

CA obsługuje Subskrybentów w zakresie unieważnień certyfikatów, poprzez Centralny Punkt Rejestracji (CPR), którego dane znajdują się w rozdziale 1.5. Centralny Punkt Rejestracji realizuje usługi unieważniania w dni robocze, w godzinach 8-18.

1.4. Zakres zastosowań

Certyfikaty wystawiane zgodnie z niniejszą polityką certyfikacji mogą służyć do realizacji usług zgodnych z profilem danego certyfikatu.

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.

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

O ile w nowej wersji polityki nie będzie odmiennego postanowienia, wszystkie certyfikaty wystawione w okresie obowiązywania wcześniejszej wersji polityki certyfikacji, 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 CA CenCert jest:

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

Telefon kontaktowy:
+48 22 720 79 55 – czynny w dni robocze w godzinach 8-18
+48 666 028 044 – czynny w dni robocze w godzinach 8-18

Fax:
+48 22 720 79 55 – czynny całą dobę

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 CA CenCert.

Termin/akronim	**Opis**
CA	Centrum Certyfikacji Kluczy (Certification Authority) – jednostka organizacyjna, której zadaniem jest generowanie, dystrybucja i unieważnianie certyfikatów kluczy publicznych zgodnie z określonymi politykami certyfikacji.

Termin/akronim	Opis
CRL	Lista unieważnionych certyfikatów. Jest wystawiana, elektronicznie pieczętowana i publikowana przez CA.
DN	Identyfikator DN – *Distinguished Name* – Identyfikator podmiotu PKI według składni zdefiniowanej w normach serii X.500
HSM	*Hardware Security Module* – Sprzętowy moduł kryptograficzny – urządzenie posiadające funkcjonalność generowania kluczy kryptograficznych i wykorzystywania klucza prywatnego CA do generowania podpisów/poświadczeń elektronicznych.
Klucz prywatny	Dane służące do składania podpisu lub pieczęci elektronicznej (w tym w celu uwierzytelnienia) lub odszyfrowania danych, powiązane z certyfikatem służącym odpowiednio do weryfikacji podpisu/pieczęci lub zaszyfrowania.
Klucz publiczny	Dane umieszczane w certyfikacie, powiązane z kluczem prywatnym.
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
Subskrybent	Osoba (fizyczna lub prawna) uprawniona do dysponowania i dysponująca rzeczywiście kluczem prywatnym związanym z ważnym certyfikatem wystawionym przez CA CenCert.
Strona ufająca	Podmiot mający potrzebę weryfikacji certyfikatu wystawionego zgodnie z niniejszą polityką certyfikacji.
eIDAS	Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE

2. Zasady dystrybucji i publikacji informacji

CA publikuje, pod adresem www.cencert.pl, następujące informacje:

- Aktualne klucze publiczne CA (w postaci certyfikatów wystawionych przez rootCA).
- Aktualne listy CRL.
- Aktualną politykę certyfikacji, materiały marketingowe, komunikaty bieżące itd.

CA nie publikuje certyfikatów Subskrybentów.

3. Identyfikacja i uwierzytelnienie

3.1. Identyfikatory wyróżniające

Nie dopuszcza się wystawiania certyfikatów zawierających identyfikatory w pełni „anonimowe". Identyfikator musi zawierać dane wskazujące na konkretną organizację, osobę fizyczną, stronę WWW i/lub adres email.

Dane Subskrybentów umieszczone w certyfikacie nie mogą wprowadzać w błąd.

CA nie sprawdza prawa do posługiwania się zastrzeżonymi znakami towarowymi, nie odpowiada za nieuprawnione wykorzystywanie znaków towarowych i nie jest stroną w przypadku tego typu sporów. W przypadku utraty przez Subskrybenta prawa do posługiwania się daną nazwą lub innym oznaczeniem zamieszczonym w certyfikacie, jest on zobowiązany do zgłoszenia tego faktu celem unieważnienia certyfikatu z powodu nieaktualności danych zawartych w certyfikacie.

CA wystawia certyfikaty identyfikujące:

- Osobę prawną lub inną jednostkę organizacyjną, albo
- Osobę fizyczną, albo
- Adres email.

Certyfikat identyfikujący osobę prawną lub inną jednostkę organizacyjną może zawierać również inne dane - dane osoby fizycznej, adres DNS lub email. Analogicznie zasady dotyczą certyfikatów identyfikujących osoby fizyczne. Zakres weryfikacji przez CA/RA treści poszczególnych pól identyfikatora DN zawierają rozdziały 3.2, 3.3.

3.1.1 Certyfikaty identyfikujące osoby prawne lub inne jednostki organizacyjne

Certyfikaty identyfikujące osobę prawną lub inną jednostkę organizacyjną muszą posiadać następujące pola identyfikatora DN:

- *Kraj* (Country Name) – kod kraju, w którym ma siedzibę subskrybent
- *Nazwa organizacji* (Organization Name) – oficjalna nazwa subskrybenta

Jeśli nazwa pole Nazwa organizacji nie wskazuje jednoznacznie na daną organizację (np. dla organizacji komercyjnych), certyfikat musi zawierać dodatkowo pole:

- *Numer seryjny* (Serial Number) – numer KRS lub NIP przysługujący organizacji, wpisywany w postaci:
    - „NTRPL-XXXXXXXXXX”, dla numeru KRS (National Trade Register)
    - „VATPL-XXXXXXXXXX”, dla numeru NIP

Jeśli organizacja nie posiada numerów NIP/KRS, jako dodatkowe dane identyfikujące można użyć adresu organizacji.

Identyfikator certyfikatu może zawierać dodatkowe pola, takie jak:

- *Adres* (streetAddress) – pełen adres siedziby organizacji lub adres wyodrębnionej jednostki organizacyjnej
- *Jednostka organizacyjna* (Organizational Unit Name) – nazwa jednostki organizacyjnej
- Email
- Nazwa powszechna (commonName)
- Adres DNS
- Imię (givenName)
- Nazwisko (surname)

3.1.2 Certyfikaty identyfikujące osoby fizyczne

Certyfikaty identyfikujące osoby fizyczne muszą posiadać następujące pola identyfikatora DN:

- *Kraj* (countryName) – kod kraju
- Imię (givenName)
- Nazwisko (surname)

Identyfikator certyfikatu może zawierać dodatkowe pola, takie jak:

- *Numer seryjny* (serialNumber) – nr dowodu osobistego, paszportu, NIP lub PESEL, w postaci:
    - „PASPL-XXXXXXX” – dla paszportu
    - „IDCPL-XXXXXXX” – dla dowodu osobistego
    - „PNOPL-XXXXXXX” – dla PESEL
    - „TINPL-XXXXXXX” – dla NIPu
- Email
- Nazwa DNS
- Nazwa powszechna (commonName) lub adres DNS

3.1.3 Certyfikaty identyfikujące adres DNS

Certyfikaty identyfikujące adres DNS muszą posiadać następujące pola identyfikatora DN:

- Adres DNS

Identyfikator certyfikatu może zawierać dodatkowe pola, takie jak:

- *Kraj* (countryName) – kod kraju
- Email

3.1.4 Certyfikaty identyfikujące adres email

Certyfikaty identyfikujące adres email muszą posiadać następujące pola identyfikatora DN:

- Email

3.2. Uwierzytelnienie Subskrybenta przy wystawieniu pierwszego certyfikatu

Konieczność weryfikacji przez RA/CA zawartości poszczególnych pól identyfikatora subskrybenta zależy od rodzaju certyfikatu:

- Certyfikaty identyfikujące osoby prawne lub inne jednostki organizacyjne. Weryfikacji przez CA/RA podlegają następujące pola identyfikatora: ***Kraj, Nazwa organizacji, Numer seryjny, Adres DNS***. Stosuje się następujące sposoby sprawdzenia poprawności:
    - poprzez sprawdzenie istnienia i poprawności danych organizacji w oficjalnych rejestrach i innych powszechnie dostępnych źródłach **oraz**
    - poprzez umowy lub zamówienie na certyfikaty, podpisane przez osobę uprawnioną w danej organizacji **oraz**
    - poprzez dostarczanie przez CA kluczy i/lub certyfikatów jedynie na adresy email w domenie danej organizacji lub adres poczty tradycyjnej organizacji,
    - poprzez weryfikację formalnych uprawnień do adresu DNS na podstawie dostępnych publicznie baz danych lub poprzez weryfikację faktycznej możliwości zarządzania domeną.
- Certyfikaty identyfikujące osoby fizyczne. Weryfikacji przez CA/RA podlegają następujące pola identyfikatora: ***Imię, Nazwisko, Adres DNS***. Stosuje się następujące sposoby sprawdzenia poprawności:
    - poprzez weryfikację tożsamości osoby na podstawie dokumentu tożsamości lub przelewu bankowego z jej konta bankowego na konto CA.
    - poprzez weryfikację formalnych uprawnień do adresu DNS na podstawie dostępnych publicznie baz danych lub poprzez weryfikację faktycznej możliwości zarządzania domeną.
- Certyfikaty identyfikujące adres Email. Weryfikacji przez CA/RA podlega ***Email***, poprzez weryfikację dostępu do skrzynki.

3.3. Uwierzytelnienie Subskrybenta przy wystawianiu kolejnych certyfikatów

W przypadku, gdy wystawia się nowy certyfikat do tych samych kluczy publicznych, przeprowadza się ponowną weryfikację następujących pól identyfikatora DN:

- Certyfikaty identyfikujące osoby prawne lub inne jednostki organizacyjne: ponownej weryfikacji przez CA/RA podlegają następujące pola: *Kraj, Nazwa organizacji, Numer seryjny, Adres DNS.* Stosuje się następujące sposoby sprawdzenia poprawności:
    - poprzez sprawdzenie istnienia i poprawności danych organizacji w oficjalnych rejestrach i innych powszechnie dostępnych źródłach.
    - poprzez weryfikację formalnych uprawnień do adresu DNS na podstawie dostępnych publicznie baz danych lub poprzez weryfikację faktycznej możliwości zarządzania domeną.
- Certyfikaty identyfikujące osoby fizyczne: ponownej weryfikacji przez CA/RA podlegają następujące pola: *Adres DNS.* Stosuje się następujące sposoby sprawdzenia poprawności:
    - poprzez weryfikację formalnych uprawnień do adresu DNS na podstawie dostępnych publicznie baz danych lub poprzez weryfikację faktycznej możliwości zarządzania domeną.
- Certyfikaty identyfikujące adres Email: CA/RA ponownie weryfikuje poprawność *Adresu email,* jak w rozdziale 3.2.

W przypadku wystawiania certyfikatu dla nowych kluczy subskrybenta, przeprowadza się ponowną weryfikację danych jak w rozdziale 3.2.

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

Sposób uwierzytelnienia subskrybenta przy zgłaszaniu unieważnienia certyfikatu zależy od rodzaju certyfikatu:

- Certyfikaty identyfikujące osoby prawne lub inne jednostki organizacyjne: unieważnienia dokonuje się na podstawie pisemnej dyspozycji (patrz Załącznik 2) podpisanej przez osobę upoważnioną w organizacji wskazanej w certyfikacie.

- Certyfikaty identyfikujące osoby fizyczne: unieważnienia dokonuje się na podstawie pisemnej dyspozycji (patrz Załącznik 2) podpisanej przez osobę wskazaną w certyfikacie.
- Certyfikaty identyfikujące adres Email: unieważnienia dokonuje się na podstawie pisemnej dyspozycji (patrz Załącznik 2) przysłanej z adresu mailowego wskazanego w certyfikacie, albo na podstawie pisemnej dyspozycji przysłanej w inny sposób, po potwierdzeniu dostępu do skrzynki mailowej.

Niezależnie od postanowień powyższych, w każdym przypadku wystarczające jest uwierzytelnienie poprzez pisemną dyspozycję podpisaną elektronicznie przy użyciu certyfikatu, który ma zostać unieważniony.

CA nie prowadzi usługi zawieszania ważności certyfikatów.

4. Cykl życia certyfikatu – wymagania operacyjne

4.1. Zgłoszenie certyfikacyjne

Certyfikat subskrybenta jest wystawiany na podstawie wniosku złożonego na formularzu NKW-PCP-F1A lub NKW-PCP-F1B (patrz Załącznik 1).

Jeśli klucze subskrybenta nie są generowane przez CA, wraz z wnioskiem NKW-PCP-F1A, Centralny Punkt Rejestracji przyjmuje klucz publiczny subskrybenta w formacie PKCS#10.

Wraz z wnioskiem NKW-PCP-F1B, Centralny Punkt Rejestracji przyjmuje plik w formacie CSV, zawierający szczegółowe parametry certyfikatów do wystawienia.

4.2. Przetwarzanie zgłoszeń certyfikacyjnych

Zgłoszenia certyfikacyjne w postaci wniosków NKW-PCP-F1A i/lub NKW-PCP-F1B, wraz z ewentualnymi załącznikami PKCVS#10 i/lub CSV, są weryfikowane przez Inspektora ds. rejestracji, a następnie po potwierdzeniu poprawności, wprowadzane do systemu informatycznego Cencert.

4.3. Wystawienie certyfikatu

System informatyczny Centrum Certyfikacji Kluczy wystawia certyfikat niezwłocznie po wydaniu dyspozycji przez Inspektora ds. rejestracji

4.4. Akceptacja certyfikatu

Do sprawdzenia i akceptacji certyfikatu zobowiązany jest Subskrybent niezwłocznie po otrzymaniu certyfikatu, a przed jego użyciem (w szczególności przed wykonaniem pierwszego podpisu elektronicznego weryfikowanego przy użyciu tego certyfikatu). W

przypadku nieprawdziwości danych zawartych w certyfikacie (w szczególności danych identyfikacyjnych Subskrybenta) Subskrybent jest zobowiązany do niezwłocznego poinformowania CA, zgodnie z procedurami obowiązującymi przy unieważnianiu certyfikatów, w celu unieważnienia certyfikatu i otrzymania nowego, zawierającego poprawne dane. Nie jest dozwolone posługiwanie się certyfikatem zawierającym nieprawdziwe dane.

4.5. Korzystanie z pary kluczy i certyfikatu

4.5.1 Korzystanie z certyfikatu

Certyfikaty Subskrybentów mogą być wykorzystywane zgodnie z przeznaczeniem, dla jakiego zostały wydane.

Jedynymi sposobami potwierdzenia przez oprogramowanie Strony ufającej ważności certyfikatu Subskrybenta jest sprawdzenie okresu ważności certyfikatu oraz sprawdzenie ważności certyfikatu na aktualnej liście CRL poświadczonej przez CA.

4.5.2 Korzystanie z klucza prywatnego

Klucz prywatny związany z certyfikatem Subskrybenta służy do celów określonych w certyfikacie oraz niniejszej polityce certyfikacji. Klucz ten musi być chroniony przed nieuprawnionych dostępem.

W przypadku powzięcia uzasadnionego podejrzenia, że dostęp do klucza prywatnego ma osoba nieupoważniona, Subskrybent powinien natychmiast unieważnić związany z tym kluczem certyfikat (a jeśli z kluczem było związane kilka certyfikatów – unieważnione powinny być wszystkie certyfikaty).

4.6. Wymiana certyfikatu bez zmiany kluczy

Dopuszcza się wymianę ważnego certyfikatu bez zmiany klucza prywatnego Subskrybenta.

Nie ma możliwości wymiany certyfikatu unieważnionego. W takim przypadku należy postępować według zasad przewidzianych przy wydawaniu pierwszego certyfikatu.

Wymiana certyfikatu następuje z inicjatywy subskrybenta.

4.7. Wymiana certyfikatu połączona z wymianą pary kluczy

Wymiana certyfikatu następuje z inicjatywy subskrybenta.

Obowiązują zasady jak przy wydawaniu pierwszego certyfikatu.

4.8. Zmiana treści certyfikatu

Zmiana treści certyfikatu wymaga wystawienia nowego certyfikatu, zawierającego nową treść. Dotychczasowy certyfikat – o ile dane w nim zawarte stały się nieaktualne i zawierają nieprawdziwe informacje o subskrybencie – jest unieważniany.

Za zgłoszenie potrzeby aktualizacji danych zawartych w certyfikacie oraz za określenie, czy zmiana danych pociąga za sobą konieczność unieważnienia certyfikatu dotychczasowego, odpowiedzialny jest Subskrybent.

4.9. Unieważnienie i zawieszenie certyfikatu

Podmiotem uprawnionym do unieważnienia certyfikatu jest:

- Subskrybent,
- Centrum Certyfikacji Kluczy.

Subskrybent ma prawo unieważnić certyfikat w dowolnym czasie (lecz w okresie ważności certyfikatu) z dowolnej przyczyny. Kod powodu unieważnienia, jeśli został podany, umieszczany jest na liście CRL.

Subskrybent jest zobowiązany do niezwłocznego unieważnienia certyfikatu w następujących przypadkach:

- Gdy dostęp do klucza prywatnego związanego z certyfikatem ma (lub istnieje istotne zagrożenie, że może mieć) nieuprawniona osoba,
- Gdy dane zawarte w certyfikacie są nieprawidłowe (w tym nieprawdziwe albo nieaktualne).

CA ma prawo do unieważnienia certyfikatu jedynie w uzasadnionych przypadkach. W szczególności dotyczy to sytuacji:

- stwierdzenia nieprawidłowości danych zawartych w certyfikacie;
- stwierdzenia kompromitacji klucza prywatnego związanego z certyfikatem;
- nieotrzymania płatności z tytułu wystawienia certyfikatu, po uprzednim wezwaniu subskrybenta do uregulowania zapłaty.

4.10. Usługi informowania o statusie certyfikatów

Jedyną formą informowania o statusie certyfikatu jest lista CRL.

Lista CRL jest publikowana co najmniej raz dziennie.

4.11. Zakończenie umowy certyfikacyjnej

Umowa certyfikacyjna, zawarta w sposób domniemany pomiędzy Centrum Certyfikacji Kluczy a Subskrybentem, dotycząca wystawienia certyfikatu, kończy się wraz z upłynięciem terminu ważności określonego w certyfikacie.

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

CA jest umiejscowione w pomieszczeniach użytkowanych przez firmę ENIGMA Systemy Ochrony Informacji Sp. z o.o.

Serwery CA 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.

5.2. Zabezpieczenia proceduralne

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

Nazwa funkcji w CA	**Rodzaj obowiązków**
Administrator CA	Konfigurowanie systemu CA w zakresie polityki Centrum Certyfikacji Kluczy, nadawania uprawnień do systemu CA. Zarządzanie kluczami CA
Operator Systemu	Stała obsługa systemu teleinformatycznego, w tym wykonywanie kopii zapasowych, nadawanie uprawnień Inspektorom ds. rejestracji w systemie CA
Inspektor ds. rejestracji	Weryfikacja tożsamości Subskrybentów, podpisywanie zgłoszeń certyfikacyjnych, unieważnianie, zawieszanie i uchylanie zawieszenia certyfikatów, tworzenie listy CRL

Nazwa funkcji w CA	Rodzaj obowiązków
Inspektor ds. audytu	Analizowanie zapisy rejestrów zdarzeń mających miejsce w systemach teleinformatycznych wykorzystywanych przy świadczeniu usług certyfikacyjnych
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 byli skazani prawomocnym wyrokiem za przestępstwo przeciwko wiarygodności dokumentów, obrotowi gospodarczemu, obrotowi pieniędzmi i papierami wartościowymi, przestępstwo skarbowe, przestępstwa określone w ustawie o podpisie elektronicznym lub ustawie o usługach zaufania i identyfikacji elektronicznej,
- 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 przeszkoleni w zakresie przepisów prawa, procedur i regulaminy pracy obowiązujące w RA/CA oraz omówienie możliwej odpowiedzialności karnej w zakresie związanym z świadczeniem usług certyfikacyjnych.

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

Odpowiedzialność personelu CA 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 obowiązujących przepisach.

5.4. Procedury tworzenia logów audytowych

Centrum Certyfikacji Kluczy zapewnia rejestrowanie wszelkich istotnych zdarzeń związanych z realizacją świadczonych przez CA usług certyfikacyjnych.

Poza systemem automatycznego generowania logów przechowywane są zapisy o instalacji nowego oprogramowania lub o aktualizacjach.

Logi są zabezpieczone przed modyfikacją.

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:

- wszystkie certyfikaty i zaświadczenia certyfikacyjne wystawione w poprzednim roku,
- wszystkie listy CRL wystawione w poprzednim roku,
- rejestry zdarzeń.

Okres przechowywania kopii archiwalnych wynosi 11 lat.

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

Archiwizowane dane są podpisywane elektroniczne oraz oznaczane kwalifikowanym znacznikiem czasu i w tej postaci archiwizowane.

Archiwizacja zapisów jest wykonywana przez Operatora systemu, w obecności co najmniej Administratora CA, pod bezpośrednim nadzorem Inspektora ds. bezpieczeństwa.

Archiwizacja zapisów jest wykonywana na nośnikach jednokrotnego zapisu. Nośniki oznaczane są w sposób jednoznacznie identyfikujący rodzaj i zakres zapisanych informacji oraz są podpisywane i oznaczone datą przez osoby wykonujące i nadzorujące archiwizację.

W wyniku realizacji procedury archiwizacji powstają dwa identyczne nośniki. Jeden z nich jest przechowywany w centrum podstawowym CA, drugi w centrum zapasowym.

5.6. Wymiana pary kluczy Centrum Certyfikacji Kluczy

Wygenerowanie i wymiana pary kluczy Centrum Certyfikacji Kluczy może następować w planowych terminach lub wcześniej na podstawie decyzji Dyrektora Pionu Utrzymania Usług CenCert.

Planowa wymiana pary kluczy CA następuje nie wcześniej niż po 5 latach i nie później niż po 6 latach od daty wygenerowania aktualnego zaświadczenia certyfikacyjnego.

Procedura wymiany pary kluczy polega na:

- Wygenerowaniu nowej pary kluczy CA i samo-podpisanego zaświadczenia certyfikacyjnego.
- Wykonaniu operacji „przełączenia” kluczy w oprogramowaniu CA, co powoduje, że wszystkie nowe certyfikaty, listy CRL i zaświadczenia certyfikacyjne wystawiane są już przy użyciu nowego klucza CA. Przy „przełączeniu” kluczy następuje także wygenerowanie zakładkowych zaświadczeń certyfikacyjnych kluczy CA.
- Umieszczeniu nowego samo-podpisanego zaświadczenia certyfikacyjnego oraz zakładkowych zaświadczeń certyfikacyjnych w repozytorium CA.

Alternatywnie, wymiana kluczy może być zrealizowana poprzez utworzenie nowej struktury PKI (przydzielenie nowego DNa dla CA).

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

5.7.1 Utrata poufności klucza prywatnego CA

Procedury obowiązujące w wypadku utraty poufności klucza prywatnego CA należy zastosować również wtedy, gdy istnieje uzasadnione podejrzenie zajścia takiego zdarzenia.

Po stwierdzeniu utraty poufności klucza CA, podejmuje się następujące działania:

1. Zarząd firmy, po pozytywnym zweryfikowaniu zgłoszenia (tzn. że zdarzenie takie rzeczywiście zaszło) podejmuje decyzję o nadaniu sprawie biegu.
2. Skompromitowany klucz prywatny CA, jak również wszelkie zaświadczenia certyfikacyjne zawierające odpowiadający mu klucz publiczny zostają wycofane z repozytorium CA.
3. Najszybciej jak to jest możliwe o zaistniałej sytuacji oraz o planie dalszego działania informowani są subskrybenci.
4. Dyrektor Pionu Usług Utrzymaniowych podejmuje decyzje powodujące zabezpieczenie wszelkich śladów mogących prowadzić do wyjaśnienia przyczyny zdarzenia oraz ustalenie osób winnych. Personel CA współpracuje z organami ścigania, w przypadku ewentualnego śledztwa, udostępniając na podstawie odpowiednich przepisów wymagane informacje. Udostępnieniu nie podlegają: klucz prywatny CA oraz klucze prywatne Subskrybentów.
5. Zarząd powołuje komisję, która ma zbadać przyczyny zaistnienia zdarzenia oraz zaproponować ewentualne działania korygujące.
6. Najszybciej, jak to jest możliwe, CA generuje nową parę kluczy CA do podpisywania certyfikatów i list CRL – stosując procedury obowiązujące przy generowaniu klucza CA. CA generuje także niezbędne klucze infrastruktury.
7. CA wznawia normalną działalność. O ile identyfikator DN Centrum Certyfikacji Kluczy nie uległ zmianie, CA generuje listy CRL w taki sposób, że lista unieważnień zawiera także numery wszystkich certyfikatów poświadczonych kluczem CA, który utracił poufność – każdy certyfikat aż do następnej listy CRL po upłynięciu okresu ważności certyfikatu.
8. Jeśli integralność bazy danych certyfikatów nie budzi wątpliwości i jest to technicznie możliwe, Dyrektor Pionu Usług Utrzymaniowych podejmuje decyzję o ponownym wystawieniu certyfikatów na te same klucze Subskrybentów i tym samym końcu okresu ważności. Nowe certyfikaty będą udostępniane subskrybentom.
9. Nowe certyfikaty wystawiane zgodnie z pkt. 8, są wystawiane nieodpłatnie.

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 jest klucz CA do poświadczania certyfikatów i list CRL oraz klucze infrastruktury niezbędne do funkcjonowania CA.

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

Oba centra są zabezpieczone przed zanikiem zasilania, pożarem, zalaniem. Centrum Podstawowe jest ponadto zabezpieczone przed utratą jednej linii telekomunikacyjnej, jednej linii zasilającej oraz awarią pojedynczego komputera, urządzenia lub dysku.

CA posiada udokumentowane oraz okresowo testowane procedury przewidujące działania na wypadek konieczności przełączenia przetwarzania na Centrum Zapasowe, zarówno w przypadku planowego, jak i nagłego przełączenia.

5.7.2.2 Wyłączenie Centralnego Punktu Rejestracji

W przypadku katastrofy powodującej wyłączenie Centralnego Punktu Rejestracji, personel CA niezwłocznie uruchamia Zastępczy Centralny Punkt Rejestracji, obsługujący Subskrybentów w zakresie unieważnienia, zawieszenia i uchylenia zawieszenia certyfikatu.

Centrum Certyfikacji Kluczy niezwłocznie informuje Subskrybentów, za pośrednictwem stron WWW o zaistniałej sytuacji, przekazując w razie potrzeby nowe numery telefonów i faksu.

5.7.2.3 Wyłączenie repozytorium CA i/lub serwera usług OCSP

W przypadku katastrofy polegającej na wyłączeniu działania repozytorium CA, o ile analogiczna usługa nie jest świadczona przez Centrum Zapasowe, personel CA podejmuje wysiłki w celu jak najszybszego przywrócenia działania tych usług.

Brak możliwości pobrania nowej listy CRL z jakiegokolwiek powodu nie może być w żadnym wypadku interpretowany jako potwierdzenie ważności jakiegokolwiek certyfikatu.

5.8. Zakończenie działalności CA

Decyzję o zakończeniu działalności CA podejmuje Zarząd Spółki.

O planowanym zakończeniu działalności informowani są subskrybenci z wyprzedzeniem co najmniej 6 miesięcy.

Po zakończeniu działalności klucz prywatny CA jest niszczony.

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 dwóch upoważnionych osób spośród personelu CA, w tym osoby pełniącej rolę Inspektora ds. bezpieczeństwa.

Wymagana jest nieprzerwana obecność Inspektora ds. bezpieczeństwa od momentu wywołania procedury generowania kluczy na urządzeniu HSM do momentu zabezpieczenia wszystkich poufnych informacji.

Generowanie par kluczy Centrum Certyfikacji Kluczy odbywa się wewnątrz urządzenia HSM.

Klucze Inspektorów ds. Rejestracji są generowane samodzielnie przez inspektorów, na karcie elektronicznej, na której są następnie przechowywane i przetwarzane.

Klucze Subskrybentów są generowane samodzielnie przez Subskrybentów lub przez Centrum Certyfikacji Kluczy CenCert.

6.1.2 Dostarczenie klucza prywatnego Subskrybentowi

Jeśli klucze prywatne subskrybentów są generowane przez CA, sposób ich przekazania musi gwarantować poufność na odpowiednim poziomie.

Standardowo klucze są przekazywane w plikach PFX zabezpieczonych hasłem zapewniającym entropię 80 bitów (np. hasło typu „małe i duże litery i cyfry” o długości 14 znaków, hasło typu „duże litery i cyfry” o długości 16 znaków, hasło typu „duże litery” o długości 17 znaków).

6.1.3 Dostarczenie klucza publicznego Subskrybenta do Punktów Rejestracji

Klucz publiczny Subskrybenta może być dostarczany do CPR w postaci załącznika do zgłoszenia certyfikacyjnego zgodnego z normą PKCS#10.

6.1.4 Dostarczenie klucza publicznego CA

Klucz publiczny Centrum Certyfikacji Kluczy jest publikowany, w postaci certyfikatu wystawionego przez rootCA, w repozytorium CA na stronie WWW, którego dane znajdują się w rozdziale 2. Repozytorium jest dostępne także poprzez protokół HTTPS.

6.1.5 Rozmiary kluczy

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

Klucze Centrum Certyfikacji Kluczy mają długość 4096 bitów.

Klucze Subskrybentów mają standardowo długość 2048 bitów. W przypadku szczególnych wymagań Subskrybenta (np. wysokowydajne aplikacje podpisujące), klucze mogą mieć inne długości, jednak nie krótsze niż 1024 bity.

Klucze infrastruktury:

- klucze do ochrony komunikacji pomiędzy CA a punktami rejestracji mają długość co najmniej 1024 bity,
- klucze Inspektorów ds. rejestracji mają długość 2048 bitów.

6.1.6 Cel użycia klucza

Pole rozszerzenia *keyUsage* w certyfikatach zgodnych z Zaleceniem X.509:2000 określa zastosowanie (jedno lub kilka) klucza publicznego zawartego w certyfikacie.

Klucz prywatny Centrum Certyfikacji Kluczy może być wykorzystywany tylko do podpisywania certyfikatów, zaświadczeń certyfikacyjnych i list CRL zgodnie z niniejszą polityką certyfikacji. Odpowiadający mu klucz publiczny służy wyłącznie do weryfikowania certyfikatów, zaświadczeń certyfikacyjnych i list CRL. Autocertyfikaty mają ustawione odpowiednie wartości (*cRLSign* i *keyCertSign*) w polu rozszerzenia *keyUsage*.

Zawartość rozszerzenia *keyUsage* w certyfikatach Subskrybentów jest odpowiednia do celu, dla którego dane certyfikaty są wystawiane.

6.2. Ochrona kluczy prywatnych

CA używa do przetwarzania klucza prywatnego używanego do wystawiania certyfikatów urządzeń HSM posiadających certyfikat FIPS PUB 140 dla poziomu 3.

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

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

Klucze prywatne CA nie są archiwizowane.

Klucze prywatne Subskrybentów nie są archiwizowane.

Klucze prywatne Inspektorów ds. rejestracji nie są nigdy odczytywane z urządzeń w którym zostały wygenerowane.

Klucze prywatne Centrum Certyfikacji Kluczy są uaktywniane przez personel Centrum Certyfikacji Kluczy zgodnie z procedurami operacyjnymi. Aktywacja partycji z kluczami wymaga współdziałania co najmniej 2 upoważnionych osób.

Klucze prywatne Inspektorów ds. rejestracji są aktywowane przez włożenie karty elektronicznej do czytnika, uruchomienie oprogramowania Centaur PR odwołującego się do karty w celu uwierzytelniania operacji przed CA i wprowadzenie na klawiaturze stacji roboczej kodu PIN. Klucz jest aktywny do momenty wyjęcia karty z czytnika lub zakończenia działania oprogramowania Centaur PR.

Niszczenie kluczy prywatnych Inspektorów ds. rejestracji wykonywane jest przez posiadacza danej karty, poprzez logiczne usunięcie klucza z karty elektronicznej lub fizyczne zniszczenie karty.

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

Centrum Certyfikacji Kluczy nie nakłada formalnych wymagań na badania pod kątem ujawniającego ulotu elektromagnetycznego urządzeń lub pomieszczeń, w których są generowane i przetwarzane klucze CA, Inspektorów ds. rejestracji i Subskrybentów.

W systemie PKI którego dotyczy niniejsza polityka certyfikacji nie występują klucze infrastruktury służące do szyfrowania podpisywanych danych przez Subskrybentów, nie występują również klucze infrastruktury służące do szyfrowania kluczy prywatnych CA.

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.

Okres ważności kluczy prywatnych Subskrybentów nie jest ograniczony. Zaleca się jednak, aby klucze prywatne Subskrybentów, o długości 2048 bitów nie były używane dłużej niż przez 11 lat, a klucze o długości 1024 bitów - nie używane dłużej niż przez 2 lata.

Okres ważności certyfikatów kluczy publicznych Subskrybentów wynosi maksymalnie 2 lata dla kluczy RSA 1024 i 5 lat dla kluczy RSA 2048 i dłuższych.

Okres ważności par kluczy Inspektorów ds. rejestracji oraz certyfikatów tych kluczy jest nie dłuższy niż 5 lat.

6.4. Dane aktywujące

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

1. Uaktywnienie klucza CA wymaga obecności co najmniej dwóch osób, w tym Inspektora ds. bezpieczeństwa.
2. 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 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.
3. 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 CA serwerów posiadających certyfikaty bezpieczeństwa na sprzęt lub oprogramowanie systemu operacyjnego.

CA przeprowadza audyty, w tym testy penetracyjne, używanego systemu informatycznego. Wyniki audytów nie są publikowane.

Wszystkie operacje przewidziane do wykonania na komputerach i serwerach CA można wykonać po uprzednim uwierzytelnieniu się i kontroli uprawnień. Wykonywane operacje są zapisywane w dziennikach zdarzeń..

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 prac w środowisku testowym nie mogą być używane kluczy prywatne CA służące do podpisywania certyfikatów w środowisku produkcyjnym.

Oprogramowanie urządzenia HSM i oprogramowanie używane do obsługi CA 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 polityką 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;

6.8. Znakowanie czasem

6.8.1 Oznaczanie czasem w procesie wystawiania certyfikatów

Do oznaczania czasem certyfikatów, zaświadczeń certyfikacyjnych, list CRL oraz zapisów w logach urządzeń i oprogramowania stosuje się wskazanie bieżącego czasu pochodzące z zegarów wbudowanych w urządzenia lub stacje robocze.

Zegary stacji roboczych są synchronizowane protokołem NTP z czasem UTC(pl).

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

7. Profil certyfikatów i list CRL

Rozdział zawiera informacje o profilu certyfikatów kluczy publicznych i list CRL generowanych zgodnie z niniejszą polityką certyfikacji.

7.1. Profil certyfikatów i zaświadczeń

7.1.1 Identyfikatory DN

Identyfikator DN Centrum Certyfikacji Kluczy

Kraj (countryName) = ***PL***
Nazwa organizacji (organizationName) = ***ENIGMA SOI Sp. z o.o.***
Nazwa powszechna (*commonName*) = ***CenCert Centrum Certyfikatów Powszechnych 2017***

7.1.2 Profil certyfikatów

Centrum Certyfikacji Kluczy wystawia certyfikaty w formacie zgodnym z Zaleceniem X.509:2000, wersja 3. formatu.

Podpisy pod certyfikatami są realizowane przy użyciu funkcji sha512.

Rozszerzenia certyfikatu

Pole	**Opis/wartość**	**krytyczne ?**
Extensions		
AuthorityKeyIdentifier		NIE
keyIdentifier	skrót SHA-1 z klucza publicznego	
SubjectKeyIdentifier		NIE
subjectkeyIdentifier	skrót SHA-1 z klucza publicznego	
KeyUsage	Patrz opis poniżej	TAK
CertificatePolicies		NIE

Pole	Opis/wartość	krytyczne ?
PolicyInformation		
CertPolicyId	{1.3.6.1.4.1.10214.99.1.2.2.1}	
basicConstraints		TAK
crlDistributionPoints	http://crl.cencert.pl/nkw/powszechny_2017.crl	NIE

Mogą być także stosowane inne, krytyczne bądź niekrytyczne, rozszerzenia certyfikatów, w zależności od potrzeb.

KeyUsage, obowiązkowe rozszerzenia dodatkowe - Stosowane są następujące, rozłączne, zestawy parametrów:

- „podpis”:
  - keyUsage:
    - digitalSignature, contentCommitment
- „szyfrowanie”:
  - keyUsage:
    - keyEncipherment, dataEncipherment, keyAgreement
- „podpis, szyfrowanie”:
  - keyUsage:
    - digitalSignature, contentCommitment, keyEncipherment, dataEncipherment, keyAgreement
- “SSL”:
  - keyUsage:
    - digitalSignature, keyEncipherment
  - dodatkowo rozszerzenia:
    - Extended key usage
      - Uwierzytelnienie serwera (1.3.6.1.5.5.7.3.1)
      - Uwierzytelnienie klienta (1.3.6.1.5.5.7.3.2)
    - Typ cerytyfikatu Netscape
      - Uwierzytelnianie klienta SSL, Uwierzytelnianie serwera SSL (c0)

Certyfikaty kluczy Inspektorów ds. Rejestracji posiadają niekrytyczne rozszerzenie ExtKeyUsage {1.3.6.1.4.1.10214.2.1.1.2} świadczące o tym, że są to certyfikaty infrastruktury używane wyłącznie w ramach systemu CA i nie mogą być używane poza tym systemem.
Certyfikaty kluczy do ochrony komunikacji posiadają niekrytyczne rozszerzenie ExtKeyUsage {1.3.6.1.4.1.10214.2.1.1.3} świadczące o tym, że są to certyfikaty infrastruktury używane wyłącznie w ramach systemu CA i nie mogą być używane poza tym systemem.

7.1.3 Profil zaświadczeń certyfikacyjnych

Centrum Certyfikacji Kluczy wystawia autocertyfikaty i certyfikaty zakładkowe w formacie zgodnym z Zaleceniem X.509:2000, wersja 3. formatu.

Rozszerzenia

Pole	**Opis/wartość**	**krytyczne ?**
extensions		
AuthorityKeyIdentifier		NIE
keyIdentifier	skrót SHA-1 z klucza publicznego	
SubjectKeyIdentifier		NIE
SubjectKeyIdentifier		
KeyUsage	keyCertSign, cRLSign	TAK
CertificatePolicies		TAK
PolicyInformation		
CertPolicyId	{1.3.6.1.4.1.10214.99.1.2.1.1}	
basicConstraints		TAK
cA	True	
PathLenConstraint	*„0”* dla autocertyfikatów	

7.2. Profil list CRL

Centrum Certyfikacji Kluczy wystawia listy CRL w formacie zgodnym z Zaleceniem X.509:2000, wersja 2. formatu.

Rozszerzenia

Pole	**Opis/wartość**	**krytyczne ?**
extensions		
AuthorityKeyIdentifier		NIE
keyIdentifier	skrót SHA-1 z klucza publicznego	
cRLNumber	numer kolejny listy CRL wystawionej w CA	NIE

Listy CRL mogą zawierać również inne rozszerzenia, oznaczone jako niekrytyczne.

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.

9. Inne postanowienia

9.1. Opłaty

CA pobiera opłaty za świadczenie swoich usług.

CA nie pobiera opłat za unieważnienie, zawieszenie bądź uchylenie zawieszenia certyfikatu, a także za dostęp do klucza publicznego CA oraz aktualnej listy unieważnionych certyfikatów.

9.2. Odpowiedzialność finansowa

Centrum Certyfikacji Kluczy CenCert odpowiada wyłącznie za szkody wynikające z przyczyn zawinionych przez CA CenCert.

Centrum Certyfikacji Kluczy CenCert nie odpowiada za utracone korzyści.

Maksymalna odpowiedzialność finansowa CA CenCert, niezależnie od przyczyny powstania szkody, jest ograniczona w stosunku rocznym do wysokości równej opłaty za dany certyfikat.

9.3. Poufność informacji

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

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

- Polityka certyfikacji w wersjach aktualnie obowiązujących,
- Klucz publiczny CA,
- Lista unieważnionych certyfikatów,
- Wystawione certyfikaty centrum certyfikacji (samo podpisane, zakładkowe),
- Informacje bieżące, przeznaczone do publikacji (takie jak bieżące komunikaty, dane kontaktowe CA).

9.4. Ochrona danych osobowych

Centrum Certyfikacji Kluczy przetwarza dane osobowe Subskrybentów w takim zakresie, w jakim dane te są umieszczane w certyfikacie.

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

Dane osobowe Subskrybentów nie są przekazywane innym podmiotom i są wykorzystywane przez CA jedynie do realizacji usług certyfikacyjnych, w tym ewentualnie do przypominania o kończącym się okresie ważności certyfikatu.

Subskrybenci są poinformowani o przysługujących im prawach w związku z przetwarzaniem przez CA ich danych osobowych poprzez zapisy strony WWW Centrum Certyfikacji Kluczy.

Dane osobowe są zbierane przez CA od samych Subskrybentów lub są przekazywane CA przez firmy/instytucje reprezentujące Subskrybentów. W przypadku przekazywania danych osobowych firmy/instytucje, są one odpowiedzialne za pozyskanie zgody Subskrybentów na przekazanie CA danych osobowych w celu wystawienia certyfikatu (o ile dane takie występują w certyfikacie), a także za poinformowanie Subskrybentów, że ich dane będą przetwarzane przez CA CenCert zgodnie z niniejszą Polityką certyfikacji.

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 CA.

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

CA nie odpowiada za szkody wynikłe z nieprawdziwości danych zawartych w certyfikacie, opisanych w polityce jako dane nieweryfikowane przez RA/CA (patrz rozdział 3.2).

Centrum Certyfikacji Kluczy nie odpowiada za skutki wykorzystania klucza lub certyfikatu Subskrybenta niezgodnie z polityką certyfikacji, zgodnie z którą został wystawiony. W szczególności Centrum Certyfikacji Kluczy nie ponosi żadnej odpowiedzialności za skutki nieprawidłowej, niezgodnej z niniejszą polityką certyfikacji i/lub obowiązującymi przepisami, weryfikacji jakiegokolwiek certyfikatu lub znacznika czasu.

Centrum Certyfikacji Kluczy nie odpowiada za skutki, które mogą wyniknąć z użycia oprogramowania lub sprzętu, który nie był dostarczony przez CA.

CA nie odpowiada za to, czy Subskrybent użył do generowania i/lub przetwarzania swojego klucza prywatnego właściwego, zabezpieczonego odpowiedniego dla danego zastosowania urządzenia.

9.9. Przenoszenie roszczeń odszkodowawczych

CA może ubezpieczać swoją działalność na zasadach ogólnych stosowanych w prowadzeniu działalności gospodarczej.

9.10. Przepisy przejściowe i okres obowiązywania polityki certyfikacji

Niniejsza polityka certyfikacji obowiązuje w stosunku do certyfikatów wystawionych zgodnie z nią do utraty ważności tych certyfikatów (z powodu zakończenia okresu ważności lub unieważnienia). Certyfikaty wykorzystywane w celach dochodzeniowych lub dowodowych po okresie ich ważności powinny być wykorzystywane zgodnie z polityką certyfikacji, w ramach której zostały wystawione.

W stosunku do nowo wystawianych certyfikatów stosuje się najnowszą obowiązującą politykę certyfikacji.

Certyfikaty wystawione wcześniej, na podstawie niezatwierdzonej wersji polityki certyfikacji, pozostają ważne do momentu unieważnienia lub upłynięcia okresu ich ważności.

Do kluczy CA utworzonych w okresie obowiązywania polityki w wersji 1.1 lub wcześniejszych (klucze wciąż używane do wystawiania list CRL) mają zastosowanie postanowienia rozdziałów: 6.1.5, 6.2, 7.1 polityki w wersji 1.1. (zamiast analogicznych rozdziałów niniejszej wersji).

Postanowienia rozdziałów 1.3, 1.5 (godziny pracy Centralnego Punktu Rejestracji) dotyczą także wszystkich wystawionych wcześniej certyfikatów.

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 Dyrektora Pionu Utrzymania Usług CenCert lub Zarządu spółki ENIGMA SOI Sp. z o.o.

9.14. Obowiązujące prawo

Działanie podsystemu certyfikacji podlega prawu europejskiemu oraz 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:

- Rozporządzeniu eIDAS i wydanych na jego podstawie rozporządzeniach wykonawczych.
- Ustawie z dnia 18 września 2001 r. o podpisie elektronicznym – do dnia uchylenia ustawy przez ustawę o usługach zaufania.
- Ustawie z dnia 29 sierpnia 1997 o ochronie danych osobowych (tekst jednolity Dz. U. Nr 101/2002 poz. 926, z późn. zm.)
- Ustawie z dnia 6 czerwca 1997 Kodeks karny (Dz. U. Nr 88/1997 poz. 553, z późn. zm.)
- Ustawie z dnia 4 lutego 1994 Prawo autorskie (Dz. U. Nr 24/1994 poz. 83, z późn. zm.)

9.16. Inne postanowienia

Załącznikami do polityki certyfikacji są:

- Formularz NKW-PCP-F1A – wniosek o wystawienie certyfikatu
- Formularz NKW-PCP-F1B – wniosek o wystawienie certyfikatów zgodnie z załączonym plikiem
- Formularz NKW-PCP-F2 – wniosek o unieważnienie certyfikatu