signet

Centrum Certyfikacji

Polityka Certyfikacji

Certyfikaty dla serwerów i urządzeń

Klasa 2

Spis treści

1 Wstęp

Niniejsza Polityka Certyfikacji, dalej zwana Polityką, określa szczegółowe rozwiązania (techniczne i organizacyjne) wskazujące sposób, zakres oraz warunki tworzenia, stosowania i ochrony certyfikatów przeznaczonych do zabezpieczania serwerów i urządzeń firm, (zwanych dalej Firmami), które podpisały z Centrum Certyfikacji Signet umowę na świadczenie usług certyfikacyjnych objętych Polityką, dalej nazywaną Umową.

Usługi certyfikacyjne opisywane w Polityce są świadczone przez Centrum Certyfikacji Signet, prowadzone przez TP Internet Sp. z o.o. z siedzibą w Warszawie przy ul. Domaniewskiej 41, kod pocztowy 02-672, wpisaną do rejestru przedsiębiorców prowadzonego przez Sąd Rejonowy dla m. st. Warszawy XX Wydział Gospodarczy pod numerem KRS 00000-43165, nazywaną dalej w Polityce Centrum Certyfikacji Signet, bądź CC Signet.

1.1 Identyfikacja polityki

Nazwa polityki	Polityka Certyfikacji - Certyfikaty dla serwerów i urządzeń
Zastrzeżenie	Certyfikat wydany zgodnie z dokumentem „Polityka Certyfikacji – Certyfikaty dla serwerów i urządzeń". Nie jest certyfikatem w rozumieniu Ustawy z dn. 18.09.2001 r. o podpisie elektronicznym.
Wersja	1.0
Identyfikator polityki OID (ang. Object Identifier)	1.3.6.1.4.1.7999.2.200.10.13.1.0
Urząd realizujący Politykę	CC Signet – CA Klasa 2
Data wydania	27-09-2004
Data ważności	Do odwołania
Kodeks Postępowania Certyfikacyjnego dotyczący Polityki	KPC Centrum Certyfikacji Signet (CPS CC Signet) 1.3.6.1.4.1.7999.2.1.1.1.2

1.2 Historia zmian

Wersja	Data	Opis zmian
1.0	27-09-2004	Pierwsza wersja.

O ile nie podano inaczej, to wprowadzane zmiany mają zastosowanie do certyfikatów wydanych po dacie wydania danej wersji Polityki. W każdym certyfikacie wydanym przez Centrum Certyfikacji Signet znajduje się odnośnik do pełnego tekstu Polityki w wersji obowiązującej dla tego certyfikatu.

1.3 Odbiorcy usług oraz zastosowanie certyfikatów

Certyfikaty wydawane zgodnie z Polityką są przeznaczone do zabezpieczania urządzeń, stosowanych w Firmie. Odbiorcą usług, czyli posiadaczem certyfikatu wydawanego zgodnie z Polityką, jest osoba o adresie poczty elektronicznej

podanym we wniosku o wydanie certyfikatu. W szczególności, posiadaczem certyfikatu może być administrator serwera lub innego urządzenia.

W ramach Polityki wydawane są certyfikaty służące do:

- certyfikaty do uwierzytelniania serwerów WWW oraz zestawiania bezpiecznego połączenia w protokole SSL (dalej nazywane certyfikatami dla serwerów);
- certyfikaty do zestawiania połączeń w wirtualnych sieciach prywatnych (dalej nazywane certyfikatami dla VPNów);
- certyfikat do uwierzytelniania serwerów wykorzystywanych jako kontrolery domen (dalej nazywane certyfikatami dla kontrolerów domen).

1.4 Dane kontaktowe

W celu uzyskania dalszych informacji dotyczących usług Centrum Certyfikacji Signet prosimy o kontakt:

TP Internet Sp. z o.o.
Centrum Certyfikacji Signet
Budynek „Mercury"
ul. Domaniewska 41
02-672 Warszawa
tel. 0 801 30 20 21 (Contact Center)
E-mail: kontakt@signet.pl

2 Podstawowe Zasady Certyfikacji

2.1 Wydawane certyfikaty

W ramach Polityki Centrum Certyfikacji Signet wydaje roczne certyfikaty klasy 2 przeznaczone do:

W ramach Polityki Centrum Certyfikacji Signet wystawia certyfikaty klasy 2 służące do:

- uwierzytelnienia serwerów i zestawiania bezpiecznego połączenia w protokole SSL;
- zestawiania wirtualnych sieci prywatnych;
- uwierzytelniania kontrolerów domen.

Certyfikaty wydawane w ramach Polityki nie są certyfikatami w rozumieniu ustawy z dnia 18 września 2001 o podpisie elektronicznym (Dz. U. Nr 130, poz. 1450) i nie służą do weryfikacji podpisu elektronicznego.

Posiadaczem certyfikatu jest osoba lub osoby o adresie poczty elektronicznej podanym we wniosku o wydanie certyfikatu. W szczególności, posiadaczem certyfikatu może być administrator serwera lub innego urządzenia.

2.2 Obowiązki stron

2.2.1 Obowiązki posiadacza certyfikatu

Przed złożeniem wniosku o wydanie certyfikatu, przyszły posiadacz zobowiązany jest do zapoznania się z treścią Polityki i Regulaminem Usług Certyfikacyjnych. Złożenie wniosku oznacza akceptację warunków świadczenia usługi, w ramach której wydawane są certyfikaty objęte Polityką.

Posiadacz certyfikatu zobowiązany jest do bezpiecznego przechowywania klucza prywatnego, z którym jest skojarzony klucz publiczny umieszczony w jego certyfikacie.

W przypadku utraty kontroli nad kluczem prywatnym, skojarzonym z kluczem publicznym umieszczonym w certyfikacie, jego ujawnienia lub też uzasadnionego podejrzenia, iż fakt taki mógł mieć miejsce, posiadacz certyfikatu zobowiązuje się niezwłocznie powiadomić o tym wydawcę certyfikatu poprzez złożenie wniosku o unieważnienie tego certyfikatu.

Posiadacz certyfikatu jest odpowiedzialny za prawdziwość danych przekazywanych we wniosku o wydanie certyfikatu.

Posiadacz certyfikatu zobowiązuje się do informowania wydawcy certyfikatu o wszelkich zmianach informacji zawartych w jego certyfikacie lub podanych we wniosku o wydanie certyfikatu.

2.2.2 Obowiązki strony ufającej

Strona ufająca jest zobowiązana do pobrania w sposób bezpieczny certyfikatu Urzędu Certyfikacji (CA), który obdarzyła zaufaniem oraz zweryfikowania klucza publicznego tego urzędu. Metody udostępnienia certyfikatów urzędów certyfikacji oraz informacji niezbędnych dla weryfikacji ich poprawności opisane są w Kodeksie Postępowania Certyfikacyjnego.

W trakcie określania swojego zaufania wobec usługi bazującej na certyfikacie wydanym w ramach Polityki, obowiązkiem strony ufającej jest przeprowadzenie stosownej weryfikacji ważności certyfikatu. W procesie weryfikacji strona ufająca musi zweryfikować ścieżkę certyfikacji. Ścieżką certyfikacji jest uporządkowany ciąg certyfikatów urzędów certyfikacji i weryfikowanego certyfikatu, utworzony w ten sposób, że przy pomocy danych służących do weryfikacji poświadczenia elektronicznego i nazwy wydawcy pierwszego certyfikatu na ścieżce możliwe jest wykazanie, że dla każdych dwóch bezpośrednio po sobie występujących certyfikatów, poświadczenie elektroniczne zawarte w następnym z nich zostało sporządzone przy pomocy danych służących do składania poświadczenia elektronicznego związanych z poprzednim z nich; dane służące do weryfikacji pierwszego poświadczenia elektronicznego są dla weryfikującego punktem zaufania. W procesie weryfikacji strona ufająca powinna korzystać z zasobów i procedur udostępnianych przez CC Signet.

Kodeks Postępowania Certyfikacyjnego definiuje dostępne usługi i metody określania ważności certyfikatu dla każdej z klas certyfikatów. Strona ufająca jest zobowiązana co najmniej do korzystania z publikowanej przez CC Signet listy certyfikatów unieważnionych oraz weryfikowania ścieżki certyfikatów od Urzędu Certyfikacji, który obdarzyła zaufaniem do urzędu, który wydał certyfikat.

2.2.3 Obowiązki Centrum Certyfikacji Signet

Usługi certyfikacyjne są świadczone przez Centrum Certyfikacji Signet zgodnie z obowiązującymi na terenie Rzeczypospolitej Polskiej przepisami prawa.

Centrum Certyfikacji Signet zobowiązuje się do postępowania zgodnie z zapisami Polityki, a w szczególności do przeprowadzania procedur rejestracji, odnawiania i unieważniania certyfikatów zgodnie z zasadami opisanymi w Polityce, Regulaminie Usług Certyfikacyjnych oraz Umowie.

2.3 Odpowiedzialność Centrum Certyfikacji Signet

Centrum Certyfikacji Signet odpowiada za zgodność informacji zawartych w certyfikacie z informacjami otrzymanymi we wniosku o wydanie certyfikatu.

Centrum Certyfikacji Signet nie odpowiada za prawdziwość informacji zawartych we wniosku o wydanie certyfikatu. Zakres i sposób weryfikacji danych podanych we wniosku o wydanie certyfikatu jest opisany w rozdziale 3 Polityki.

Centrum Certyfikacji Signet odpowiada za przestrzeganie przyjętych procedur postępowania. W szczególności Centrum Certyfikacji Signet odpowiada za publikowanie aktualnych informacji o unieważnieniach certyfikatów w Repozytorium Centrum Certyfikacji Signet, zgodnie z Polityką.

2.4 Opłaty

Usługi związane z wydawaniem certyfikatów, których dotyczy Polityka, są płatne zgodnie z Umową.

Usługi unieważniania certyfikatów oraz udostępniania informacji o unieważnieniach w postaci list certyfikatów unieważnionych (CRL) są nieodpłatne.

2.5 Publikowanie wydanych certyfikatów i informacji o unieważnieniach

Centrum Certyfikacji Signet publikuje listy certyfikatów unieważnionych w ogólnie dostępnym Repozytorium informacji. Szczegóły organizacji Repozytorium i opis metod dostępu do tych informacji znajdują się pod adresem http://www.signet.pl/repozytorium/.

Certyfikaty wydawane w ramach Polityki nie są publikowane w Repozytorium.

Informacja o unieważnieniu, zawieszeniu i uchyleniu zawieszenia certyfikatu jest publikowana w chwili tworzenia nowej listy certyfikatów unieważnionych. Nowa lista certyfikatów unieważnionych dla certyfikatów wydawanych zgodnie z Polityką jest tworzona w terminie do 1 godziny po każdym unieważnieniu, zawieszeniu i uchyleniu zawieszenia certyfikatu, jednak nie rzadziej, niż co 24 godziny.

2.6 Ochrona informacji

Informacje gromadzone i przetwarzane w ramach realizacji Polityki podlegają ochronie, w zakresie i trybie przewidzianym obowiązującymi na terenie Rzeczypospolitej Polskiej przepisami prawa. Tajemnicą objęte są informacje, których nieuprawnione ujawnienie mogłoby narazić na szkodę odbiorcę usług certyfikacyjnych lub Centrum Certyfikacji Signet.

Centrum Certyfikacji Signet zapewnia, że nie udostępnia stronom trzecim żadnych informacji uzyskanych w ramach realizacji Polityki. Zobowiązanie to nie dotyczy przypadku skierowania żądania o udostępnienie informacji przez władze RP mające odpowiednie umocowanie w obowiązującym prawie.

Centrum Certyfikacji Signet nie udostępnia stronom trzecim certyfikatów, wydawanych w ramach Polityki.

2.7 Prawa własności intelektualnej

Majątkowe prawa autorskie do Polityki są wyłączną własnością TP Internet Sp. z o.o.

3 Weryfikacja tożsamości i uwierzytelnienie

Rozdział ten opisuje sposób weryfikacji tożsamości osoby dokonującej operacji związanych z zarządzaniem certyfikatami oraz przedstawia sposób weryfikacji praw danej osoby do wykonania określonej czynności.

3.1 Rejestracja

Rejestracja, czyli proces przyjęcia i weryfikacji wniosku o wydanie nowego certyfikatu jest przeprowadzana przez odpowiedni urząd rejestracji Centrum Certyfikacji Signet. Po pozytywnym zakończeniu procesu rejestracji następuje wydanie certyfikatu przez urząd certyfikacji.

Procedura rejestracji wymaga dostarczenia do Centrum Certyfikacji Signet następujących danych oraz dokumentów:

1. w przypadku certyfikatów dla VPNów i serwerów:
    a. adres serwera, dla którego ma być wydany certyfikat;
    b. nazwa jednostki organizacyjnej, w której jest zainstalowany serwer;
    c. adres (zgodny ze standardem SMTP) konta poczty Administratora odpowiedzialnego za serwer;
    d. klucz publiczny do umieszczenia w certyfikacie.
2. w przypadku certyfikatów dla kontrolerów domen:
    a. wartość DN – do umieszczenia w polu **subject;**
    b. wartość GUID – do umieszczenia w atrybucie **otherName** rozszerzenia **subjectAltName,**
    c. nazwa domenowa kontrolera domeny - do umieszczenia w atrybucie **dNSName** rozszerzenia **subjectAltName.**
    d. adres (zgodny ze standardem SMTP) konta poczty Administratora odpowiedzialnego za kontroler domeny - do umieszczenia w atrybucie **rfc822Name** rozszerzenia **subjectAltName.**

W trakcie rejestracji SĄ WERYFIKOWANE:

- poprawność adresu serwera lub urządzenia:
    - w przypadku certyfikatu na adres domenowy:
        - weryfikacja, czy domena której nazwa jest umieszczona we wniosku o wydanie certyfikatu jest przyznana Firmie – na podstawie

dostarczonego zaświadczenia wystawionego przez organizację zarządzającą daną przestrzenią nazw albo
- weryfikacja, czy podana we wniosku nazwa domenowa nie należy do przestrzeni nazw internetowych (nie kończy się żadnym z zarejestrowanych znaczników dla domen najwyższego poziomu (ang. *top level domain*));

- w przypadku certyfikatu na adres IP:
  - weryfikacja, czy podany adres należy do klasy adresów prywatnych albo
  - weryfikacja, czy podany adres IP należy do klasy przyznanej Firmie – na podstawie informacji uzyskanej w Réseaux IP Européens (www.ripe.net)

- posiadanie klucza prywatnego skojarzonego z kluczem zawartym we wniosku – wniosek musi być zgodny ze standardem pkcs#10 (nie dotyczy certyfikatów kontrolerów domen).

Weryfikacja dostępu do klucza prywatnego skojarzonego z kluczem publicznym umieszczonym we wniosku o wydanie certyfikatu polega na sprawdzeniu poprawności składni dostarczonego wniosku elektronicznego w standardzie PKCS#10.

W trakcie rejestracji NIE JEST WERYFIKOWANY dostęp wnioskodawcy do adresu konta poczty elektronicznej, które ma zostać umieszczone w certyfikacie.

3.2 Wymiana kluczy

Wymiana kluczy jest możliwa tylko poprzez złożenie wniosku o wydanie nowego certyfikatu z nowym kluczem publicznym, zgodnie z procedurami opisanymi w rozdziale 4.1.

3.3 Zawieszanie ważności certyfikatu

Centrum Certyfikacji Signet nie udostępnia usługi zawieszania certyfikatów wydanych w ramach Polityki.

3.4 Uchylanie zawieszenia certyfikatu

Nie dotyczy certyfikatów wydawanych w ramach Polityki.

3.5 Unieważnianie certyfikatu

Unieważnienie certyfikatu wydanego zgodnie z Polityką wymaga złożenia odpowiedniego wniosku o unieważnienie certyfikatu, uwierzytelnienia wnioskodawcy i weryfikacji jego uprawnień do złożenia takiego wniosku.

Uwierzytelnienie wnioskodawcy i weryfikacja uprawnień do złożenia wniosku o unieważnienie certyfikatu przebiega zgodnie z procedurą, ustaloną w Umowie.

3.6 Odnawianie certyfikatu

Certyfikat wydany zgodnie z Polityką może być odnawiany na warunkach, określonych w Umowie. Odnowienie certyfikatu polega na wydaniu nowego

certyfikatu, w którym wszystkie dane za wyjątkiem okresu ważności i klucza publicznego są takie same jak w certyfikacie odnawianym. Centrum Certyfikacji Signet nie wydaje nowego certyfikatu dla klucza publicznego zawartego w certyfikacie, na podstawie którego następuje odnowienie.

4 Wymagania operacyjne

4.1 Złożenie wniosku o wydanie certyfikatu

Podstawą do wystawienia certyfikatu jest:

- podpisana przez Firmę Umowa zawierająca dane osób dla których mają być wystawione certyfikaty,
- podpisane przez Firmę Zamówienie na usługę, zgodne ze wzorem zawartym w Umowie,

Szczegółowy przebieg procedury rejestracji jest określony w Umowie z Firmą. W trakcie procesu rejestracji ustalane jest hasło do zarządzania certyfikatem.

4.2 Wydanie certyfikatu

Wydanie certyfikatu następuje nie później niż w ciągu 3 dni roboczych po otrzymaniu przez Centrum Certyfikacji Signet podpisanych dokumentów wymienionych w rozdziale 4.1 i przekazaniu poprawnego wniosku o wydanie certyfikatu w postaci elektronicznej, jeśli para kluczy jest generowana przez przyszłego posiadacza certyfikatu.

Po wydaniu certyfikatu jest on przekazywany jego posiadaczowi w sposób uzgodniony przez Strony.

4.3 Akceptacja certyfikatu

Po wydaniu certyfikatu, posiadacz jest zobowiązany do sprawdzenia, czy dane zawarte w certyfikacie są zgodne z danymi podanymi we wniosku o jego wydanie. Jeżeli osoba upoważniona zgłasza się po odbiór certyfikatu osobiście do Centrum Certyfikacji Signet, to potwierdza ona zgodność danych poprzez własnoręczne podpisanie przedłożonego jej oświadczenia.

W przypadku stwierdzenia niezgodności, posiadacz certyfikatu jest zobowiązany niezwłocznie powiadomić o nich Centrum Certyfikacji Signet, złożyć wniosek o unieważnienie wadliwego certyfikatu i nie używać klucza prywatnego, skojarzonego z kluczem publicznym zawartym w tym certyfikacie. Brak zgłoszenia przez posiadacza certyfikatu zastrzeżeń w ciągu 24 godzin uznaje się za potwierdzenie zgodności danych w certyfikacie z danymi we wniosku.

W przypadku, gdy dane zawarte w certyfikacie są niezgodne z danymi podanymi we wniosku, Centrum Certyfikacji Signet wydaje posiadaczowi bezpłatnie nowy certyfikat, zawierający poprawne dane.

Jeśli posiadacz certyfikatu zaakceptował certyfikat zawierający dane niezgodne z danymi podanymi we wniosku, to odpowiada on za szkody spowodowane użyciem tego certyfikatu, jeśli wystąpiły one na skutek tych niezgodności.

4.4 Zawieszanie ważności certyfikatu

Nie dotyczy certyfikatów wydawanych w ramach Polityki.

4.5 Uchylanie zawieszenia ważności certyfikatu

Nie dotyczy certyfikatów wydawanych w ramach Polityki.

4.6 Unieważnianie certyfikatu

Certyfikat wydany w ramach Polityki może zostać unieważniony.

Uwierzytelnienie wnioskodawcy odbywa się zgodnie z postanowieniami rozdziału 3.5. Pozytywna weryfikacja praw do unieważnienia danego certyfikatu prowadzi do nieodwracalnego unieważnienia certyfikatu.

Przebieg procedury unieważniania certyfikatu jest następujący:

- dostarczenie do Centrum Certyfikacji Signet pisemnego wniosku o unieważnienie certyfikatu podpisanego przez osobę odpowiedzialną za usługę do której dostęp jest zabezpieczony unieważnianym certyfikatem;
- telefoniczne potwierdzenie w jednostce organizacyjnej odpowiedzialnej za zarządzanie zasobami ludzkimi firmy, dla której został wydany unieważniany certyfikat, czy osoba która podpisała wniosek o unieważnienie jest w niej zatrudniona i czy jest odpowiedzialna za daną usługę.

Centrum Certyfikacji Signet unieważnia także certyfikat w przypadku:

- otrzymania pisemnego wniosku o unieważnienie uprawnionej strony trzeciej;
- uzyskania informacji o dezaktualizacji informacji zawartych w certyfikacie;
- niedozwolonego lub błędnego wydania certyfikatu na skutek:
  - niespełnienia istotnych warunków wstępnych do wydania certyfikatu,
  - fałszerstwa istotnych danych zawartych w certyfikacie,
  - popełnienia błędów przy wprowadzaniu danych lub innych błędów przetwarzania.

W przypadku istnienia uzasadnionego podejrzenia, że istnieją przesłanki do unieważnienia certyfikatu, Centrum Certyfikacji Signet zawiesza ważność tego certyfikatu, informuje o tym jego posiadacza i podejmuje działania niezbędne do wyjaśnienia tych wątpliwości.

4.7 Odnawianie certyfikatu

Certyfikat wydany zgodnie z Polityką może być odnawiany. Odnowienie certyfikatu jest możliwe tylko przed upływem terminu ważności odnawianego certyfikatu. Po upływie terminu ważności, posiadacz certyfikatu musi ubiegać się o nowy certyfikat zgodnie z procedurą rejestracji opisaną w rozdziale 3.1.

Szczegółowy przebieg procedury odnowienia certyfikatu jest opisany w Umowie.

5 Techniczne środki zapewnienia bezpieczeństwa

5.1 Generowanie kluczy

Polityka wymaga, żeby para kluczy, z której publiczny jest certyfikowany zgodnie z Polityką, była stowarzyszona z algorytmem RSA i spełniała wymagania opisane w poniższej tabeli.

Rodzaj certyfikatu	Minimalna długość klucza (rozumiana jako moduł p*q)	Sposób generowania klucza	Podmiot generujący klucze
dla serwerów	1024 bity	brak wymagań	posiadacz certyfikatu
dla VPNów	1024 bity	brak wymagań	posiadacz certyfikatu
dla kontrolerów domen	1024 bity	w bezpiecznym środowisku	Centrum Certyfikacji Signet

5.2 Ochrona kluczy posiadacza certyfikatu

Za ochronę klucza prywatnego od chwili jego wygenerowania (w przypadku certyfikatów dla serwerów i VPNów) albo od chwili jego przekazania (dla certyfikatów dla kontrolerów domen) odpowiedzialny jest wyłącznie posiadacz certyfikatu.

5.3 Aktywacja kluczy

Polityka nie przewiduje wymogów w odniesieniu do sposobu aktywacji klucza prywatnego posiadacza certyfikatu.

5.4 Niszczenie kluczy

Polityka nie stawia szczególnych wymogów odnośnie sposobu niszczenia klucza prywatnego, skojarzonego z kluczem publicznym, zawartym w certyfikacie wydanym w ramach Polityki.

Gdy certyfikat wydany zgodnie z Polityką utraci ważność, klucz prywatny skojarzony z kluczem publicznym, umieszczonym w tym certyfikacie powinien zostać usunięty z urządzenia, zgodnie z instrukcją standardowego oprogramowania do zarządzania tym urządzeniem. Jeżeli istnieje taka możliwość, to klucz prywatny powinien zostać zniszczony.

6 Możliwości dostosowania zapisów polityki do wymagań Firmy

Centrum Certyfikacji Signet oraz Firma mogą w Umowie ustalić, że klucze kryptograficzne są generowane przez Centrum Certyfikacji Signet i dostarczane w bezpieczny sposób do Firmy, bądź bezpośrednio do posiadacza certyfikatu; w przypadku generowania kluczy przez Centrum Certyfikacji Signet odpowiedzialność posiadacza certyfikatu związana z ochroną kluczy obowiązuje od momentu przekazania mu nośnika z kluczami (uwaga: Centrum Certyfikacji Signet nie przechowuje żadnej kopii kluczy wygenerowanych w ramach Polityki);

W przypadkach, jeśli specyfika świadczonej usługi tego wymaga, na pisemny wniosek osoby odpowiedzialnej, wskazanej w Umowie możliwe są następujące zamiany profili certyfikatów, wydawanych w ramach Polityki:

- zmiana wartości atrybutu **keyUsage** na podaną we wniosku o certyfikat;
- zmiana wartości rozszerzenia **netscapeCertType** na podaną we wniosku o certyfikat;
- zamiana wartości rozszerzenia **extendedKeyUsage** na podaną we wniosku o certyfikat;

- zmiana wartości rozszerzenia cRLDistributionPoint na podaną we wniosku o certyfikat, lub dodanie nowych atrybutów distributionPoint – jeśli liczba certyfikatów, która ma zostać wydana zgodnie ze zmodyfikowanym profilem przekracza 50 sztuk;
- dodanie rozszerzeń niewymienionych w rozdziale 7.1, a podanych we wniosku o certyfikat.

Wydanie certyfikatu o niestandardowym profilu następuje po uprzedniej akceptacji profilu przez Kierownika Centrum Certyfikacji Signet.

7 Profile certyfikatów i listy certyfikatów unieważnionych (CRL)

Poniżej przedstawione zostały profile certyfikatów i listy certyfikatów unieważnionych (listy CRL) wydawanych zgodnie z Polityką.

Dla podstawowych pól certyfikatu i listy CRL, w kolumnie 'Atrybut' podano nazwy poszczególnych pól i atrybutów zgodne ze standardem X.509 w wersji 3.

Wartości atrybutów w polach **Issuer** i **Subject** podawane są w kolejności od korzenia drzewa katalogu, zgodnie ze standardem X.500.

Dla rozszerzeń certyfikatu i listy CRL, w kolumnie „Rozszerzenie" podano nazwy poszczególnych rozszerzeń i atrybutów wraz z ich identyfikatorem obiektu, a w kolumnie 'Rozszerzenie krytyczne' określono, czy dane rozszerzenie jest krytyczne, czy nie.

W kolumnie 'Wartość' zawarte są wartości poszczególnych pól i atrybutów lub rozpoczynające się znakiem # opisy sposobu określenia wartości pola i komentarze.

7.1 Profile certyfikatów

Certyfikaty wydawane zgodnie z Polityką mają następującą strukturę:

7.1.1 Profil certyfikatu dla serwerów

Certyfikat dla serwerów ma następującą budowę:

Atrybut	Wartość
version	2 # certyfikat zgodny z wersją 3 standardu X.509
serialNumber	# jednoznaczny w ramach urzędu CC Signet - CA Klasa 2 numer, nadawany przez ten urząd
signature	1.2.840.113549.1.1.5 #SHA1 z szyfrowaniem RSA - identyfikator algorytmu stosowanego do elektronicznego poświadczenia certyfikatu
issuer	C = PL, O = TP Internet Sp. z o.o., OU = Centrum Certyfikacji Signet, CN = CC Signet - CA Klasa 2 # Nazwa wyróżniona Urzędu CA wydającego certyfikaty w ramach Polityki
validity	# Okres ważności certyfikatu
not before	# data i godzina wydania certyfikatu (GMT w formacie UTCTime)
not after	# data i godzina wydania certyfikatu + 365 dni (GMT w formacie UTCTime)

subject	C = PL
	O = # nazwa organizacji podana we wniosku,
	OU = #nazwa jednostki organizacyjnej podana we wniosku
	CN = # adres serwera podany we wniosku

subjectPublicKeyInfo	
algorithm	rsaEncryption # identyfikator algorytmu, z którym stowarzyszony jest klucz publiczny posiadacza certyfikatu
subjectPublicKey	# klucz publiczny posiadacza certyfikatu

W certyfikacie umieszczone są następujące rozszerzenia zgodne ze standardem X.509:

Rozszerzenie	Rozszerzenie Krytyczne	Wartość
keyUsage **2.5.29.15**	TAK	B0h
(0) digitalSignature	**-**	**1 # klucz do realizacji podpisu elektronicznego**
(1) nonRepudiation	-	0
(2) keyEncipherment	**-**	**1 # klucz do wymiany klucza**
(3) dataEncipherment	**-**	**1 # klucz do szyfrowania danych**
(4) keyAgreement	-	0
(5) keyCertSign	-	0
(6) crlSign	-	0
(7) encipherOnly	-	0
(8) decipherOnly	-	0
extendedKeyUsage **2.5.29.37**	NIE	1.3.6.1.5.5.7.3.1 #id-kp-serverAuth
authorityKeyIdentifier **2.5.29.35**	NIE	-
keyIdentifier	-	# identyfikator klucza urzędu do weryfikacji podpisu pod certyfikatem
subjectKeyIdentifier **2.5.29.14**	NIE	# identyfikator klucza posiadacza certyfikatu, umieszczonego w polu subjectPublicKeyInfo
basicConstraints **2.5.29.19**	NIE	-
cA	-	FAŁSZ
netscapeCertType **2.16.840.1.113730.1.1**	NIE	sslServer #40h
subjectAltName **2.5.29.17**	NIE	# alternatywna nazwa posiadacza certyfikatu
iPAddress		# adres ip urządzenia (pole opcjonalne)
dNSName		# nazwa domenowa urządzenia (pole opcjonalne)
rfc822Name	-	# adres e-mail posiadacza certyfikatu
cRLDistributionPoint **2.5.29.31**	NIE	-
distributionPoint	-	http://www.signet.pl/repozytorium/crl/klasa2.crl
certificatePolicies **2.5.29.32**	NIE	-
policyIdentifier	-	1.3.6.1.4.1.7999.2.200.10.13.1.0

Rozszerzenie	Rozszerzenie Krytyczne	Wartość
policyQualifierID 1.3.6.1.5.5.7.2.1	-	http://www.signet.pl/repozytorium/dokumenty/klasa2/pc_csiu2_1_0.pdf
qualifier 1.3.6.1.5.5.7.2.2	-	Certyfikat wystawiony zgodnie z dokumentem "Polityka Certyfikacji – Certyfikaty dla serwerow i urzadzen". Nie jest certyfikatem do weryfikacji podpisu elektronicznego.

7.1.2 Profil certyfikatu dla VPNów

Certyfikat dla VPNów ma następującą budowę:

Atrybut	Wartość
version	2 # certyfikat zgodny z wersją 3 standardu X.509
serialNumber	# jednoznaczny w ramach urzędu CC Signet - CA Klasa 2 numer, nadawany przez ten urząd
signature	1.2.840.113549.1.1.5 #SHA1 z szyfrowaniem RSA - identyfikator algorytmu stosowanego do elektronicznego poświadczenia certyfikatu
issuer	C = PL, O = TP Internet Sp. z o.o., OU = Centrum Certyfikacji Signet, CN = CC Signet - CA Klasa 2 # Nazwa wyróżniona Urzędu CA wydającego certyfikaty w ramach Polityki
validity	# Okres ważności certyfikatu
not before	# data i godzina wydania certyfikatu (GMT w formacie UTCTime)
not after	# data i godzina wydania certyfikatu + 365 dni (GMT w formacie UTCTime)

subject	C = PL
	O = # nazwa organizacji podana we wniosku,
	OU = #nazwa jednostki organizacyjnej podana we wniosku
	CN = # adres IP albo nazwa domenowa urządzenia

subjectPublicKeyInfo	
algorithm	rsaEncryption # identyfikator algorytmu, z którym stowarzyszony jest klucz publiczny posiadacza certyfikatu
subjectPublicKey	# klucz publiczny posiadacza certyfikatu

W certyfikacie umieszczone są następujące rozszerzenia zgodne ze standardem X.509:

Rozszerzenie	Rozszerzenie Krytyczne	Wartość
keyUsage 2.5.29.15	TAK	B0h
(0) digitalSignature	**-**	**1 # klucz do realizacji podpisu elektronicznego**
(1) nonRepudiation	-	0
(2) keyEncipherment	**-**	**1 # klucz do wymiany klucza**
(3) dataEncipherment	**-**	**1 # klucz do szyfrowania danych**
(4) keyAgreement	-	0
(5) keyCertSign	-	0
(6) crlSign	-	0
(7) encipherOnly	-	0
(8) decipherOnly	-	0

Rozszerzenie	Rozszerzenie Krytyczne	Wartość
authorityKeyIdentifier 2.5.29.35	NIE	-
keyIdentifier	-	# identyfikator klucza urzędu do weryfikacji podpisu pod certyfikatem
subjectKeyIdentifier 2.5.29.14	NIE	# identyfikator klucza posiadacza certyfikatu, umieszczonego w polu subjectPublicKeyInfo
basicConstraints 2.5.29.19	NIE	-
cA	-	FAŁSZ
subjectAltName 2.5.29.17	NIE	# alternatywna nazwa posiadacza certyfikatu
iPAddress		# adres ip urządzenia (pole opcjonalne)
dNSName		# nazwa domenowa urządzenia (pole opcjonalne)
rfc822Name	-	# adres e-mail posiadacza certyfikatu (pole opcjonalne)
cRLDistributionPoint 2.5.29.31	NIE	-
distributionPoint	-	http://www.signet.pl/repozytorium/crl/klasa2.crl
certificatePolicies 2.5.29.32	NIE	-
policyIdentifier	-	1.3.6.1.4.1.7999.2.200.10.13.1.0
policyQualifierID 1.3.6.1.5.5.7.2.1	-	http://www.signet.pl/repozytorium/dokumenty/klasa2/pc_csiu2_1_0.pdf
qualifier 1.3.6.1.5.5.7.2.2	-	Certyfikat wystawiony zgodnie z dokumentem "Polityka Certyfikacji - Certyfikaty dla serwerow i urzadzen". Nie jest certyfikatem do weryfikacji podpisu elektronicznego.

7.1.3 Profil certyfikatu dla kontrolerów domen

Certyfikat kontrolerów domen, ma następującą budowę:

Atrybut	Wartość
version	2 # certyfikat zgodny z wersją 3 standardu X.509
serialNumber	# jednoznaczny w ramach urzędu CC Signet - CA Klasa 2 numer, nadawany przez ten urząd
signature	1.2.840.113549.1.1.5 #SHA1 z szyfrowaniem RSA - opis algorytmu stosowanego do podpisywania certyfikatu
issuer	C = PL, O = TP Internet Sp. z o.o., OU = Centrum Certyfikacji Signet, CN = CC Signet - CA Klasa 2 # Nazwa wyróżniona Urzędu CA wydającego certyfikaty w ramach Polityki
validity	# Okres ważności certyfikatu
not before	# data i godzina wydania certyfikatu (GMT w formacie UTCTime)
not after	# data i godzina wydania certyfikatu + 365 dni

subject	CN = # nazwa domenowa kontrolera domeny
	OU = # nazwa jednostki organizacyjnej lub grupy urządzeń (pole opcjonalne)
	DC = # poszczególne fragmenty nazwy domeny, podane we wniosku (może

	występować wielokrotnie)
subjectPublicKeyInfo	
algorithm	1.2.840.113549.1.1.1 #rsaEncryption - identyfikator algorytmu, z którym jest stowarzyszony klucz publiczny posiadacza certyfikatu
subjectPublicKey	# klucz publiczny posiadacza certyfikatu

W certyfikacie kontrolera domeny umieszczone są następujące rozszerzenia zgodne ze standardem X.509:

Rozszerzenie	Rozszerzenie Krytyczne?	Wartość
keyUsage **(2.5.29.15)**	TAK	A0h # wartość podana w zapisie szesnastkowym
(0) digitalSignature		**1 # klucz do realizacji podpisu elektronicznego**
(1) nonRepudiation		0
(2) keyEncipherment		**1 # klucz do wymiany klucza**
(3) dataEncipherment		0
(4) keyAgreement		0
(5) keyCertSign		0
(6) crlSign		0
(7) encipherOnly		0
(8) decipherOnly		0
extendedKeyUsage **2.5.29.37**	NIE	1.3.6.1.5.5.7.3.2 #id-kp-clientAuth 1.3.6.1.5.5.7.3..1 # id-kp-serverAuth
certificateTemplateName **1.3.6.1.4.1.311.20.2**	NIE	DomainController
authorityKeyIdentifier **2.5.29.35**	NIE	-
keyIdentifier	-	# identyfikator klucza urzędu do weryfikacji podpisu pod certyfikatem
subjectKeyIdentifier **2.5.29.14**	NIE	# identyfikator klucza posiadacza certyfikatu umieszczonego w polu **subjectPublicKeyInfo**
basicConstraints	NIE	-
cA	-	FAŁSZ
subjectAltName **2.5.29.17**	NIE	# alternatywna nazwa posiadacza certyfikatu
otherName		1.3.6.1.4.1.311.25.1 = # wartość GUID podana we wniosku (uwaga!!! dopuszcza się stosowanie wyłącznie wielkich liter)
dNSName		# nazwa domenowa serwera, podana we wniosku
rfc822Name	-	# adres e-mail Administratora (posiadacza certyfikatu)
cRLDistributionPoint **2.5.29.31**	NIE	-
distributionPoint	-	http://www.signet.pl/repozytorium/crl/klasa2.crl
certificatePolicies **2.5.29.32**	NIE	-
policyIdentifier	-	1.3.6.1.4.1.7999.2.200.10.13.1.0
policyQualifierID	-	http://www.signet.pl/repozytorium/dokumenty/klasa2/pc_csiu2_1_0.

1.3.6.1.5.5.7.2.1		pdf
qualifier 1.3.6.1.5.5.7.2.2	-	Certyfikat wystawiony zgodnie z dokumentem "Polityka Certyfikacji - Certyfikaty dla serwerow i urzadzen". Nie jest certyfikatem do weryfikacji podpisu elektronicznego.

7.2 Profil listy certyfikatów unieważnionych (CRL)

Lista certyfikatów unieważnionych ma następującą budowę:

Atrybut	Wartość
version	1 # lista zgodna z wersją 2 standardu X.509
signature	1.2.840.113549.1.1.5 #SHA1 z szyfrowaniem RSA - identyfikator algorytmu stosowanego do elektronicznego poświadczenia listy CRL
issuer	C = PL O = TP Internet Sp. z o.o., OU = Centrum Certyfikacji Signet, CN = CC Signet - CA Klasa 2, # Nazwa wyróżniona Urzędu CA wydającego certyfikaty w ramach Polityki
thisUpdate	# data i godzina publikacji listy (GMT w formacie UTCTime)
nextUpdate	# data i godzina publikacji listy + nie więcej niż 24 godziny. (GMT w formacie UTCTime)
revokedCertificates	# lista unieważnionych i zawieszonych certyfikatów o następującej składni:
serialNumber	# numer seryjny unieważnionego certyfikatu
revocationDate	# data i godzina unieważnienia certyfikatu (GMT w formacie UTCTime)
reasonCode 2.5.29.21	# jeden z kodów przyczyny unieważnienia certyfikatu, zgodnie z opisem pod tabelą

Pole **reasonCode** jest niekrytycznym rozszerzeniem pola listy CRL revokedCertificates, które umożliwia określenie przyczyny unieważnienia certyfikatu lub wskazania, że jest on zawieszony. Kod ten może przyjmować jedną z następujących wartości:

- unspecified (0) - nieokreślona ;
- keyCompromise (1) - kompromitacja klucza;
- cACompromise (2) - kompromitacja klucza CC;
- affiliationChanged (3) - zmiana danych posiadacza certyfikatu;
- superseded (4) - zastąpienie (odnowienie) klucza;
- cessationOfOperation (5) - zaprzestanie używania certyfikatu do celu, w jakim został wydany;
- certificateHold (6) - certyfikat został zawieszony;

W liście certyfikatów unieważnionych umieszczone są następujące rozszerzenia:

Rozszerzenie	Rozszerzenie Krytyczne	Wartość
cRLNumber 2.5.29.20	NIE	# numer listy CRL nadawany przez urząd CC Signet - CA Klasa 2
authorityKeyIdentifier 2.5.29.35	NIE	
keyIdentifier	-	# identyfikator klucza urzędu do weryfikacji elektronicznego poświadczenia listy CRL