signet
Centrum Certyfikacji

Polityka Certyfikacji

Zabezpieczenie poczty elektronicznej dla firm

Klasa 2

Spis treści

1 Wstęp

Niniejsza Polityka Certyfikacji, dalej zwana Polityką, określa szczegółowe rozwiązania (techniczne i organizacyjne) wskazujące sposób, zakres oraz warunki ochrony, tworzenia i stosowania certyfikatów przeznaczonych do zabezpieczenia poczty elektronicznej dla osób fizycznych wskazanych przez firmy (zwane dalej Firmami), które podpisały z Centrum Certyfikacji Signet umowę na świadczenie usług certyfikacyjnych, dalej nazywaną Umową.

Certyfikaty mogą być również wydane dla pracowników firm trzecich lub dla wybranych klientów, wskazanych we wniosku o certyfikat.

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 - Zabezpieczenie poczty elektronicznej dla firm
Zastrzeżenie	Certyfikat wydany zgodnie z dokumentem „Polityka Certyfikacji – Zabezpieczenie poczty elektronicznej dla firm".
Wersja	2.3
Identyfikator polityki OID (ang. Object Identifier)	1.3.6.1.4.1.7999.2.200.10.6.2.3
Urząd realizujący Politykę	CC Signet – CA Klasa 2
Data wydania	23-06-2004
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	04-10-2002	Pierwsza wersja
1.1	08-10-2002	Określenie zasad weryfikacji przez Centrum Certyfikacji Signet tożsamości osoby odpowiedzialnej za weryfikację osób w Firmie. Doprecyzowanie zapisów.
1.2	28-10-2002	Przeniesienie zapisu o granicznej kwocie transakcji do rozszerzenia **certificatePolicies** i usunięcie rozszerzenie i**d-pe-qcStatements**.
2.0	30-06-2003	Usunięcie rozszerzenia listy CRL **issuingDistributionPoint** w związku z aktualizacją oprogramowania. DOTYCZY WSZYSTKICH CERTYFIKATÓW WYDANYCH W RAMACH POLITYKI ! Zmiana wersji Kodeksu Postępowania Certyfikacyjnego. Ujednolicenie stosowanej

Wersja	Data	Opis zmian
		terminologii oraz formy dokumentu w ramach unifikacji dokumentacji Centrum Certyfikacji Signet.
2.1	28-10-2003	Dodanie rozszerzenia dla usługi OCSP. Dodanie opcjonalnej możliwości logowania do systemu z wykorzystaniem certyfikatu. Rozszerzenie zakresu odbiorców certyfikatów na pracowników firm trzecich oraz klientów, wskazanych przez Firmę. Wprowadzenie opcjonalnej możliwości umieszczania nazwy firmy w polu **Subject**.
2.2	13-11-003	Drobne zmiany w opisach procesów rejestracji, wydawania, zawieszania i uchylania zawieszenia certyfikatów
2.2	20-05-2004	DOTYCZY WSZYSTKICH CERTYFIKATÓW WYDAWANYCH W RAMACH POLITYKI: Zmiana definicji wartości atrybutu **nextUpdate** listy certyfikatów unieważnionych, umożliwiająca publikacje list o okresie ważności mniejszym niż 24 godziny.
2.3	23-06-2004	Dodanie możliwości określania wartość atrybutów O i OU w polu subject w Umowie z Firmą; zmiana statusu zapisu o granicznej kwocie transakcji umieszczanego w certyfikacie na opcjonalny.

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 dla osób fizycznych wskazanych przez Firmę, która podpisała z Centrum Certyfikacji Signet Umowę na świadczenie usług certyfikacyjnych. Posiadaczami certyfikatów mogą być pracownicy Firmy lub/oraz wskazani przez Firmę pracownicy firm trzecich i klienci.

W ramach Polityki wydawane są certyfikaty, które mogą być stosowane do:

- uwierzytelniania nadawcy, zapewnienia integralności informacji przesyłanych pocztą elektroniczną, uwierzytelniania przy dostępie do stron WWW, elektronicznego podpisywania dokumentów oraz – opcjonalnie – logowania do domeny systemu Windows;
- zapewnienia poufności poczty elektronicznej.

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 dwa rodzaje certyfikatów klasy 2:

- certyfikaty klasy 2 do uwierzytelniania nadawcy w wiadomościach poczty elektronicznej, uwierzytelnienia użytkownika przy dostępie do stron WWW, zapewniania integralności informacji przesyłanych pocztą elektroniczną, elektronicznego podpisywania dokumentów oraz – opcjonalnie – logowania do domeny systemu Windows (dalej nazywane certyfikatami do uwierzytelnienia);
- certyfikaty klasy 2 do szyfrowania wiadomości poczty elektronicznej (dalej nazywane certyfikatami do szyfrowania).

Certyfikaty do uwierzytelniania, wydawane w ramach Polityki nie są certyfikatami kwalifikowanymi w rozumieniu ustawy z dnia 18 września 2001 o podpisie elektronicznym (Dz. U. Nr 130, poz. 1450). Podpis elektroniczny weryfikowany przy pomocy tych certyfikatów nie wywołuje skutków prawnych równorzędnych skutkom wywoływanym przez podpis własnoręczny.

Certyfikaty do szyfrowania, 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 fizyczna, której adres e-mail został podany we wniosku o wystawienie certyfikatu i której dane są umieszczone w certyfikacie.

Certyfikaty mogą zawierać nazwę firmy, z którą Centrum Certyfikacji Signet podpisało Umowę, bądź nazwę firmy której udostępniane są certyfikaty.

Certyfikaty te mogą być stosowane w kontaktach służbowych i prywatnych oraz do celów testowych.

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, Regulaminem Usług Certyfikacyjnych oraz Umową. Złożenie wniosku oznacza akceptację warunków świadczenia usługi, w ramach której wydawane są certyfikaty objęte Polityką.

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

Jeżeli klucz prywatny, z którym jest skojarzony klucz publiczny umieszczony w certyfikacie jest osadzony na karcie kryptograficznej, to posiadacz certyfikatu jest zobowiązany do bezpiecznego przechowywania tej karty oraz ochrony kodu PIN karty przed ujawnieniem.

Posiadacz certyfikatu jest zobowiązany do starannego przechowywania hasła do zarządzania certyfikatem oraz jego ochrony przed ujawnieniem.

Posiadacz certyfikatu jest zobowiązany do zaprzestania wykorzystywania klucza prywatnego, który jest skojarzony z kluczem publicznym umieszczonym w certyfikacie do uwierzytelniania, który wygasł lub został unieważniony.

W przypadku utraty kontroli nad kluczem prywatnym, skojarzonym z kluczem publicznym umieszczonym w certyfikacie 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 albo zawieszenie tego certyfikatu.

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

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

2.2.2 Obowiązki osoby weryfikującej tożsamość posiadaczy certyfikatów

Wskazana w Umowie osoba jest odpowiedzialna za zweryfikowanie tożsamości każdej osoby dla której ma być wystawiony certyfikat w ramach Umowy. Weryfikacja tożsamości odbywa się na podstawie ważnego dowodu osobistego albo paszportu.

2.2.3 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.

2.2.4 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.

Centrum Certyfikacji Signet przechowuje każdy klucz prywatny skojarzony z kluczem publicznym umieszczonym w certyfikacie do szyfrowania wydanym w ramach Polityki, przez okres nie krótszy niż 5 lat od momentu jego zarchiwizowania, które następuje niezwłocznie po wygenerowaniu certyfikatu.

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 odpowiada za zweryfikowanie tożsamości osoby, o której mowa w rozdziale 2.2.1, odpowiedzialnej za weryfikację tożsamości pracowników Firmy.

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, uchylaniem zawieszenia i odnawianiem certyfikatów, których dotyczy Polityka, są płatne zgodnie z Umową.

Usługi unieważniania i zawieszania 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 wydane certyfikaty do szyfrowania oraz listy certyfikatów unieważnionych (CRL) 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 do szyfrowania są publikowane w Repozytorium niezwłocznie po ich wydaniu.

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.

Centrum Certyfikacji Signet udostępnia usługę weryfikacji ważności certyfikatu zgodnie z protokołem OCSP dla tych certyfikatów, w których umieszczono rozszerzenie wskazujące na adres serwisu OCSP.

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 udostępnia stronom trzecim wyłącznie informacje zawarte w certyfikatach opublikowanych w Repozytorium. Zobowiązanie to nie dotyczy przypadku skierowania żądania o udostępnienie informacji przez władze RP mające odpowiednie umocowanie w obowiązującym prawie.

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.

W trakcie rejestracji, wnioskodawca, którym jest osoba upoważniona wskazana w Umowie dostarcza do Centrum Certyfikacji Signet następujące dane oraz dokumenty:

1. imię i nazwisko przyszłego posiadacza certyfikatu;
2. adres konta poczty elektronicznej, który będzie wykorzystywany w procesie rejestracji i zostanie umieszczony w certyfikacie;
3. klucz publiczny do umieszczenia w certyfikacie do uwierzytelniania, jeśli para kluczy jest generowana przez przyszłego posiadacza;
4. nazwę pod którą firma w której jest zatrudniony posiadacz certyfikatu jest zarejestrowana w odpowiednim dla niej rejestrze i która będzie umieszczona w wystawionym certyfikacie, jeśli Umowa to przewiduje;
5. opcjonalnie – nazwę domenową posiadacza certyfikatu.

W trakcie rejestracji SĄ WERYFIKOWANE:

- uprawnienia wnioskodawcy do składania wniosku o wydanie certyfikatu w ramach Polityki – na podstawie Umowy;

- nazwa Firmy – na podstawie dostarczonego zaświadczenia o zatrudnieniu podpisanego przez upoważnioną osobę w firmie (jeśli nazwa firmy ma być umieszczona w certyfikacie);
- posiadanie przez przyszłego posiadacza klucza prywatnego skojarzonego z kluczem publicznym przeznaczonym do umieszczenia w certyfikacie do uwierzytelniania – klucz publiczny jest dostarczany we wniosku, podpisanym skojarzonym z nim kluczem prywatnym przyszłego posiadacza – w przypadku generowania pary kluczy przez przyszłego posiadacza certyfikatu;
- posiadanie przez przyszłego posiadacza dostępu do konta pocztowego, którego adres zostanie umieszczony w certyfikacie – Centrum Certyfikacji Signet wysyła na to konto informacje niezbędne do prawidłowego zakończenia procesu rejestracji i/lub instalacji certyfikatu.

W trakcie rejestracji NIE JEST WERYFIKOWANA tożsamość przyszłego posiadacza certyfikatu. Za weryfikację tożsamości jest odpowiedzialna osoba, o której mowa w rozdz. 2.2.2.

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 certyfikatu

W trakcie procedury zawieszenia certyfikatu następuje uwierzytelnienie wnioskodawcy i sprawdzenie uprawnień do składania wniosku o wykonanie takiej operacji. Uwierzytelnienie wnioskodawcy i weryfikacja uprawnień do składania wniosku o zawieszenie certyfikatu polega na sprawdzeniu zgodności hasła podanego w trakcie procedury zawieszania z hasłem do zarządzania certyfikatem ustalonym podczas procesu rejestracji.

3.4 Uchylanie zawieszenia certyfikatu

Uchylenie zawieszenia certyfikatu jest możliwe tylko po osobistym stawieniu się posiadacza certyfikatu w punkcie rejestracji Centrum Certyfikacji Signet i po wykazaniu przez niego, że przypuszczenia na podstawie, których zawieszono certyfikat okazały się fałszywe.

Przed uchyleniem zawieszenia certyfikatu weryfikowana jest tożsamość posiadacza, na podstawie okazanego dowodu osobistego lub paszportu.

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 unieważnienia certyfikatu polega na sprawdzeniu zgodności hasła podanego w trakcie procedury unieważniania z hasłem do zarządzania certyfikatem ustalonym podczas procesu rejestracji.

3.6 Odnawianie certyfikatu

Certyfikat wydany zgodnie z Polityką może być odnawiany. 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.

Odnowienie certyfikatu jest możliwe tylko przed upływem terminu ważności odnawianego certyfikatu i jedynie w przypadku, jeśli dane na podstawie których wydano certyfikat nie uległy zmianie. Po upływie terminu ważności lub w przypadku zmiany danych, posiadacz certyfikatu musi ubiegać się o nowy certyfikat zgodnie z procedurą rejestracji opisaną w rozdziale 3.1.

W trakcie odnawiania certyfikatu JEST WERYFIKOWANY dostęp posiadacza odnawianego certyfikatu do klucza prywatnego, skojarzonego z kluczem publicznym umieszczonym w tym certyfikacie. W przypadku odnawiania certyfikatu do uwierzytelniania, weryfikowany jest także dostęp do klucza prywatnego skojarzonego z kluczem publicznym umieszczonym we wniosku o odnowienie certyfikatu.

W trakcie odnawiania certyfikatu NIE JEST WERYFIKOWANA tożsamość posiadacza odnawianego certyfikatu.

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, w którym dane zostały potwierdzone przez osobę, o której mowa w rozdziale 2.2.2,
- podpisane przez przyszłego posiadacza oświadczenie, potwierdzające zapoznanie się z Polityką i Regulaminem Usług Certyfikacyjnych.

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 następnym dniu roboczym 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 Centrum Certyfikacji Signet wysyła na podany we wniosku o wydanie certyfikatu adres poczty elektronicznej informacje niezbędne do poprawnego zakończenia procesu instalacji certyfikatu.

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.

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 certyfikatu

Certyfikat wydany w ramach Polityki może zostać zawieszony. Uwierzytelnienie wnioskodawcy odbywa się zgodnie z postanowieniami rozdziału 3.3. Pozytywna weryfikacja praw do żądania zawieszenia certyfikatu prowadzi do zawieszenia certyfikatu.

Jeżeli w ciągu 168 godzin zawieszenie nie zostanie uchylone, to certyfikat zostanie automatycznie unieważniony.

Procedura składania wniosku o zawieszenie certyfikatu jest określona w Umowie.

4.5 Uchylanie zawieszenia certyfikatu

Uchylenie zawieszenia certyfikatu jest możliwe tylko po osobistym stawieniu się jego posiadacza w punkcie rejestracji Centrum Certyfikacji Signet.

Uwierzytelnienie wnioskodawcy odbywa się zgodnie z postanowieniami rozdziału 3.4.

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 złożenia wniosku o unieważnienie danego certyfikatu prowadzi do nieodwracalnego unieważnienia certyfikatu. Przebieg procedury unieważniania certyfikatu jest określony w Umowie.

Centrum Certyfikacji Signet unieważnia także certyfikat w przypadku:

- otrzymania pisemnego wniosku o unieważnienie od posiadacza lub 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 ten certyfikat, 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 4.1.

Procedura odnowienia certyfikatu jest inicjowana przez Centrum Certyfikacji Signet. Na 28 dni przed upływem terminu ważności certyfikatu, na adres poczty elektronicznej zawarty w certyfikacie przesłana zostanie informacja o możliwości odnowienia certyfikatu.

W procesie odnawiania certyfikatu do uwierzytelniania, nowa para kluczy jest generowana przez posiadacza odnawianego certyfikatu. Przekazany do Centrum Certyfikacji Signet klucz publiczny jest umieszczany w odnowionym certyfikacie.

W procesie odnawiania certyfikatu do szyfrowania, nowa para kluczy jest generowana przez Centrum Certyfikacji Signet. Klucz publiczny jest umieszczany w odnowionym certyfikacie, a skojarzony z nim klucz prywatny podlega archiwizacji.

Warunkiem odnowienia certyfikatu jest przekazanie przez Firmę do Centrum Certyfikacji Signet zlecenia odnowienia certyfikatu zawierającego informacje pozwalające zidentyfikować certyfikat, który ma być odnowiony nie później niż 7 dni przed upływem terminu ważności tego certyfikatu. Opłata za odnowienie certyfikatu musi wpłynąć na konto Centrum Certyfikacji Signet zgodnie z warunkami Umowy.

4.8 Odzyskiwanie klucza prywatnego

Na wniosek posiadacza certyfikatu do szyfrowania albo uprawnionego przedstawiciela Firmy, Centrum Certyfikacji Signet może udostępnić wnioskodawcy kopię klucza prywatnego, skojarzonego z kluczem publicznym umieszczonym w certyfikacie. W trakcie procedury odzyskiwania klucza Centrum Certyfikacji Signet sprawdza tożsamość wnioskodawcy w oparciu o jego dokument tożsamości.

Centrum Certyfikacji Signet informuje Firmę o każdym wniosku o odzyskanie klucza prywatnego oraz o wyniku jego rozpatrzenia.

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 następujące wymagania:

- długość klucza (rozumiana jako moduł p*q) – co najmniej 1024 bity;
- sposób generowania klucza:
  - w przypadku certyfikatów do uwierzytelniania – ustalony w Umowie;
  - w przypadku certyfikatów do szyfrowania - bezpieczne środowisko Centrum Certyfikacji Signet.

5.2 Ochrona kluczy posiadacza certyfikatu

Za ochronę klucza prywatnego od momentu jego przekazania posiadaczowi certyfikatu odpowiedzialny jest wyłącznie posiadacz certyfikatu.

Centrum Certyfikacji Signet jest odpowiedzialne za ochronę przechowywanych kopii kluczy prywatnych, skojarzonych z kluczami publicznymi zawartymi w certyfikatach do szyfrowania, aż do momentu ich zniszczenia.

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 do uwierzytelniania, wydany zgodnie z Polityką utraci ważność, klucz prywatny skojarzony z kluczem publicznym, umieszczonym w tym certyfikacie powinien zostać usunięty z nośnika, na którym się znajduje lub dostęp do niego powinien zostać zablokowany w sposób nieodwracalny.

Gdy certyfikat do szyfrowania, wydany zgodnie z Polityką utraci ważność, klucz prywatny skojarzony z kluczem publicznym, umieszczonym w tym certyfikacie może być wykorzystywany do odszyfrowywania danych, powinien jednak być nadal przechowywany w bezpieczny sposób. Jeżeli posiadacz certyfikatu nie będzie już wykorzystywał klucza prywatnego, to może go usunąć lub zniszczyć w wybrany przez siebie sposób.

Centrum Certyfikacji Signet niszczy kopię klucza prywatnego przechowywaną w bezpiecznym archiwum nie wcześniej niż po 5 latach od jego zarchiwizowania.

6 Możliwości dostosowania zapisów polityki do wymagań użytkownika

Nie przewiduje się możliwości dostosowywania Polityki do wymagań posiadacza certyfikatu. W Umowie mogą zostać ustalone jedynie te procedury, które zostały wymienione w treści Polityki.

7 Profil certyfikatu 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 Profil certyfikatu

Certyfikaty wydawane zgodnie z Polityką mają następującą strukturę:

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 = # zgodnie z opisem pod tabelą
	OU = # nazwa jednostki organizacyjnej Firmy (pole opcjonalne)
	CN = # imię i nazwisko posiadacza certyfikatu
	E = #adres e-mail posiadacza certyfikatu

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 zależności od zapisów Umowy, atrybut **O** pola **Subject** może zawierać nazwę firmy, w której jest zatrudniony posiadacz certyfikatu, lub opis "Zabezpieczenie poczty elektronicznej dla firm". W certyfikatach do szczególnych zastosowań, strony mogą określić w Umowie inną zawartość atrybutów **O** i **OU.**

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

Rozszerzenie	Rozszerzenie Krytyczne	Wartość
keyUsage 2.5.29.15	TAK	80h # wartość podana w zapisie szesnastkowym
(0) digitalSignature	-	**1 # klucz do realizacji podpisu elektronicznego**
(1) nonRepudiation	-	0
(2) keyEncipherment	-	0
(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 1.3.6.1.5.5.7.3.4 #id-kp-emailProtection 1.3.6.1.4.1.311.20.2.2 #smartCardLogon (opcjonalnie)
authorityKeyIdentifier 2.5.29.35	NIE	-
keyIdentifier	-	# identyfikator klucza urzędu do weryfikacji elektronicznego poświadczenia certyfikatu
subjectKeyIdentifier 2.5.29.14	NIE	# identyfikator klucza posiadacza certyfikatu, umieszczonego w polu **subjectPublicKeyInfo**
basicConstraints 2.5.29.19	NIE	-
cA	-	FAŁSZ
subjectDirectoryAttributes 2.5.29.9	NIE	# opcjonalne
X520Title	-	# nazwa stanowiska posiadacza certyfikatu
subjectAltName 2.5.29.17	NIE	# alternatywna nazwa posiadacza certyfikatu
rfc822Name	-	# adres e-mail posiadacza certyfikatu
otherName	-	1.3.6.1.4.1.311.20.2.3=#domenowa_nazwa_użytkownika@nazwa_domeny (UPN – atrybut opcjonalny)
authorityInformationAccess 1.3.6.1.5.5.7.1.1	NIE	# opcjonalne (jeśli podawana jest lokalizacja usługi OCSP)
accessMethod	-	1.3.6.1.5.5.7.48.1 # ocsp – identyfikator obiektu usługi OCSP
accessLocation	-	# adres URL dostępu do usługi OCSP
cRLDistributionPoint 2.5.29.31	NIE	-
distributionPoint	-	http://www.signet.pl/repozytorium/crl/klasa2.crl
certificatePolicies 2.5.29.32	NIE	-
policyIdentifier	-	1.3.6.1.4.1.7999.2.200.10.6.2.3
policyQualifierID 1.3.6.1.5.5.7.2.1	-	http://www.signet.pl/repozytorium/dokumenty/klasa2/pc_zpef2_2_3.pdf

Rozszerzenie	Rozszerzenie Krytyczne	Wartość
qualifier 1.3.6.1.5.5.7.2.2	-	Certyfikat niekwalifikowany, wydany zgodnie z dokumentem „Polityka Certyfikacji – Zabezpieczenie poczty elektronicznej dla firm". Graniczna kwota transakcji <wartość_z_umowy> PLN. # gdzie <wartość_z_umowy> jest zastąpiona kwotą określoną w Umowie

W przypadku gdy Umowa nie określa granicznej kwoty transakcji lub odbiorca usług certyfikacyjnych nie wyraża zgody na umieszczenie tej wartości atrybut qualifier (1.3.6.1.5.5.7.2.2) zawiera tylko tekst: Certyfikat niekwalifikowany, wydany zgodnie z dokumentem „Polityka Certyfikacji – Zabezpieczenie poczty elektronicznej dla firm".

Natomiast w certyfikacie do szyfrowania umieszczone są następujące rozszerzenia zgodne ze standardem X.509:

Rozszerzenie	Rozszerzenie Krytyczne	Wartość
keyUsage 2.5.29.15	TAK	30h # wartość podana w zapisie szesnastkowym
(0) digitalSignature	-	0
(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	1.3.6.1.5.5.7.3.4 #id-kp-emailProtection
authorityKeyIdentifier 2.5.29.35	NIE	-
keyIdentifier	-	# identyfikator klucza urzędu do weryfikacji elektronicznego poświadczenia certyfikatu
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
rfc822Name	-	# adres e-mail posiadacza certyfikatu
authorityInformationAccess 1.3.6.1.5.5.7.1.1	NIE	# opcjonalne (jeśli podawana jest lokalizacja usługi OCSP)
accessMethod	**-**	1.3.6.1.5.5.7.48.1 # ocsp – identyfikator obiektu usługi OCSP
accessLocation	**-**	# adres URL dostępu do usługi OCSP
cRLDistributionPoint 2.5.29.31	NIE	-
distributionPoint	-	http://www.signet.pl/repozytorium/crl/klasa2.crl

Rozszerzenie	Rozszerzenie Krytyczne	Wartość
certificatePolicies **2.5.29.32**	NIE	-
policyIdentifier	-	1.3.6.1.4.1.7999.2.200.10.6.2.3
policyQualifierID **1.3.6.1.5.5.7.2.1**	-	http://www.signet.pl/repozytorium/dokumenty/klasa2/pc_zpef2_2_3.pdf
qualifier **1.3.6.1.5.5.7.2.2**	-	Certyfikat wydany zgodnie z dokumentem „Polityka Certyfikacji – Zabezpieczenie poczty elektronicznej dla firm". Nie jest certyfikatem w rozumieniu ustawy z dn. 18.09.01 o podpisie elektronicznym.

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 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	

Rozszerzenie	Rozszerzenie Krytyczne	Wartość
keyIdentifier	-	# identyfikator klucza urzędu do weryfikacji elektronicznego poświadczenia listy CRL