Krajowa Izba Rozliczeniowa S.A.

POLITYKA CERTYFIKACJI KIR
DLA
CERTYFIKATÓW KWALIFIKOWANYCH

Wersja 2.2

Historia dokumentu

Numer wersji	Status	Data wydania
1.0	Dokument zatwierdzony przez Zarząd KIR	14.11.2002 r.
1.1	Dokument zatwierdzony przez Zarząd KIR	27.02.2003 r.
1.2	Dokument zatwierdzony przez Zarząd KIR – wersja poprzednia obowiązująca do 28 lutego 2010 r.	29.01.2004 r.
2.0	Dokument zatwierdzony przez Zarząd KIR – wersja obowiązująca do 9 stycznia 2013 r.	1.03.2010 r.
2.1	Dokument zatwierdzony przez Zarząd KIR – wersja obowiązująca do 1 marca 2015 r.	10.01.2013 r.
2.2	Dokument zatwierdzony przez Zarząd KIR – wersja obowiązująca od 2 marca 2015 r.	26.02.2015 r.

SPIS TREŚCI

1. WSTĘP

„Polityka certyfikacji KIR dla certyfikatów kwalifikowanych", zwana dalej Polityką, określa szczegółowe rozwiązania, w tym techniczne i organizacyjne, wskazujące sposób, zakres oraz warunki tworzenia i stosowania certyfikatów kwalifikowanych, zwanych dalej „certyfikatami". Identyfikator niniejszej Polityki zarejestrowany w Krajowym Rejestrze Identyfikatorów Obiektów ma postać: 1.2.616.1.113571.1.1.

Krajowa Izba Rozliczeniowa S.A. NIP: 526-030-05-17, zarejestrowana w Sądzie Rejonowym dla m.st. Warszawy XIII Wydział Gospodarczy Krajowego Rejestru Sądowego pod nr KRS 0000113064 jest kwalifikowanym podmiotem świadczącym usługi certyfikacyjne w rozumieniu przepisów ustawy z dnia 18 września 2001 r. o podpisie elektronicznym (Dz. U. Nr 130, poz. 1450 z późn. zm.), zwanej dalej „Ustawą o podpisie elektronicznym", wpisanym do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne pod numerem 6, na podstawie decyzji nr 7/014499/03 Ministra Gospodarki, Pracy i Polityki Społecznej.

Usługi certyfikacyjne realizuje KIR, w tym poprzez swoje terenowe jednostki. Lista jednostek KIR wraz z godzinami ich pracy dostępna jest na stronie internetowej KIR www.elektronicznypodpis.pl. Część czynności związanych ze świadczeniem usług certyfikacyjnych, w tym z wydawaniem certyfikatów oraz ich zawieszaniem i unieważnianiem KIR może powierzyć do wykonania podmiotom zewnętrznym, zwanym także „Partnerami".

Wszelką korespondencję związaną ze świadczeniem usług certyfikacyjnych należy kierować na adres siedziby KIR:

Krajowa Izba Rozliczeniowa S.A.
ul. Rtm. W. Pileckiego 65
02-781 Warszawa
z dopiskiem „certyfikaty"

tel. 801 500 207
e-mail: bok@kir.pl

lub na adres terenowych jednostek KIR, jak również drogą elektroniczną na adresy zamieszczone na stronie internetowej KIR.

2. DEFINICJE

Operator – upoważniony przez KIR pracownik zajmujący się rejestracją subskrybentów i przyjmowaniem wniosków o wydanie, zawieszenie i unieważnienie certyfikatów.

Odbiorca usług certyfikacyjnych – osoba fizyczna, prawna lub jednostka organizacyjna nieposiadająca osobowości prawnej, która zawarła z KIR umowę na świadczenie usług certyfikacyjnych.

Subskrybent – osoba fizyczna, której dane osobowe zostały wpisane do certyfikatu.

Klucz prywatny – dane służące do składania podpisu elektronicznego w rozumieniu przepisów Ustawy o podpisie elektronicznym.

Klucz publiczny – dane służące do weryfikacji podpisu elektronicznego w rozumieniu przepisów ustawy o podpisie elektronicznym.

Para kluczy – kluczy prywatny oraz towarzyszący mu klucz publiczny.

3. ZAKRES ZASTOSOWANIA POLITYKI CERTYFIKACJI

Polityka jest stosowana do wydawania i zarządzania kwalifikowanymi certyfikatami kluczy publicznych, wydawanymi przez KIR na podstawie umowy na świadczenie usług certyfikacyjnych zawartej z odbiorcą usług certyfikacyjnych.

4. ŚWIADCZENIE USŁUG CERTYFIKACYJNYCH

4.1. Umowa na świadczenie usług certyfikacyjnych

Podstawą do świadczenia usług certyfikacyjnych jest zawarcie umowy na świadczenie usług certyfikacyjnych, zwanej dalej także „Umową".

Umowa na świadczenie usług certyfikacyjnych może zostać zawarta z osobą fizyczną, osobą prawną lub jednostką organizacyjną nieposiadającą osobowości prawnej. Na podstawie Umowy odbiorca usług certyfikacyjnych wskazuje subskrybentów, dla których zamawia certyfikaty.

4.2. Przeznaczenie certyfikatów

Certyfikaty wydawane zgodnie z niniejszą Polityką będą wykorzystywane do weryfikacji bezpiecznych podpisów elektronicznych i identyfikacji subskrybentów.

Certyfikaty, wydawane zgodnie z zasadami określonymi w niniejszej Polityce, są certyfikatami kwalifikowanymi w myśl Ustawy o podpisie elektronicznym. Bezpieczny podpis elektroniczny weryfikowany przy pomocy kwalifikowanego certyfikatu jest równoważny pod względem skutków prawnych podpisowi własnoręcznemu.

4.3. Zobowiązania KIR

KIR zobowiązuje się w szczególności do:

- wydawania certyfikatów w odpowiedzi na poprawnie złożone w KIR zamówienia certyfikatu;
- rzetelnego weryfikowania tożsamości subskrybentów najpóźniej w chwili przekazywania nośnika klucza prywatnego;
- rzetelnego generowania par kluczy dla subskrybentów na komponentach technicznych stanowiących część bezpiecznego urządzenia do składania podpisów posiadanych lub przeznaczonych dla subskrybentów;
- rzetelnego weryfikowania żądań o wydanie certyfikatów, w przypadku gdy nie są one wytwarzane przez KIR;
- rzetelnego weryfikowania tożsamości osób występujących o unieważnienie lub zawieszenie certyfikatu oraz ich prawa żądania zawieszenia lub unieważnienia certyfikatu;
- unieważniania oraz zawieszania certyfikatów w odpowiedzi na prawidłowo złożone żądanie;
- publikowania na stronie www.elektronicznypodpis.pl listy zwieszonych i unieważnionych certyfikatów;
- ochrony posiadanych danych o subskrybentach;
- ochrony swoich kluczy prywatnych zgodnie z niniejszą Polityką;
- wykonywania innych obowiązków przewidzianych prawem.

Dodatkowe zobowiązania KIR może określać Umowa.

4.4. Zobowiązania subskrybenta

Subskrybent zobowiązany jest w szczególności do:

- wykorzystywania certyfikatów zgodnie z ich przeznaczeniem wskazanym w danym certyfikacie;
- wykorzystywania certyfikatów do składania bezpiecznych podpisów elektronicznych tylko w okresie ważności certyfikatu w nim wskazanym;
- ochrony swojego klucza prywatnego;
- zgłoszenia żądania unieważniania certyfikatu w przypadkach przewidzianych w Ustawie o podpisie elektronicznym, Umowie, informacji dla subskrybenta lub Polityce.

Umowa może określić bardziej szczegółowy zakres odpowiedzialności subskrybenta, o ile jest ona mu znana. O jej szczególnym zakresie subskrybent może być także poinformowany w pisemnej lub przesłanej elektronicznie do niego informacji.

4.5. Zobowiązania osób ufających

Przez osobę ufającą rozumie się osobę fizyczną, prawną lub jednostkę organizacyjną nieposiadającą osobowości prawnej, która podejmuje działania lub jakąkolwiek decyzję w zaufaniu do podpisanych lub poświadczonych elektronicznie danych z wykorzystaniem klucza publicznego zawartego w certyfikacie wydanym przez KIR lub zaświadczenia certyfikacyjnego KIR.

Osoby ufające są zobowiązane do:

- wykorzystywania certyfikatów zgodnie z ich przeznaczeniem;
- weryfikacji bezpiecznego podpisu elektronicznego lub poświadczenia elektronicznego w chwili dokonywania weryfikacji lub innym wiarygodnym momencie;
- weryfikowania podpisu lub poświadczenia elektronicznego z wykorzystaniem bezpiecznego urządzenia do weryfikacji podpisu elektronicznego i z zachowaniem należytych rygorów bezpieczeństwa, w tym sprawdzenia listy zawieszonych i unieważnionych certyfikatów, list zawieszonych i unieważnionych zaświadczeń certyfikacyjnych i ścieżki certyfikacji.

4.6. Odpowiedzialność KIR

KIR odpowiada za wszelkie szkody spowodowane niewykonaniem lub nienależytym wykonaniem swoich obowiązków w zakresie świadczonych usług, chyba że niewykonanie lub nienależyte wykonanie tych obowiązków jest następstwem okoliczności, za które KIR nie ponosi odpowiedzialności i którym nie mogła zapobiec mimo dołożenia należytej staranności.

KIR nie odpowiada za szkody wynikające z użycia certyfikatów poza zakresem określonym w Polityce certyfikacji, która została wskazana w certyfikacie, w tym w szczególności za szkody wynikające z przekroczenia najwyższej wartości granicznej transakcji, jeżeli wartość ta została ujawniona w certyfikacie.

KIR nie odpowiada za szkody wynikłe z nieprawdziwości danych zawartych w certyfikacie, wpisanych na wniosek osoby składającej podpis elektroniczny lub odbiorcy usług certyfikacyjnych.

KIR nie odpowiada za szkody wynikłe z nieaktualności danych wpisanych do certyfikatu, jeżeli w chwili wydawania certyfikatu były one prawdziwe.

KIR odpowiada za przechowywanie oraz archiwizowanie danych związanych z wydaniem, zawieszaniem i unieważnianiem danego certyfikatu.

KIR odpowiada za bezpieczeństwo kluczy infrastruktury wykorzystywanych w procesie wydawania, zawieszania i unieważniania certyfikatów.

Umowa może określić bardziej szczegółowy zakres odpowiedzialności KIR.

4.7. Odpowiedzialność odbiorcy usług certyfikacyjnych

Odbiorca usług certyfikacyjnych ponosi odpowiedzialność przede wszystkim za prawdziwość i kompletność danych podawanych w zamówieniu o wydanie certyfikatu oraz w żądaniu zawieszenia lub unieważnienia certyfikatu.

Umowa może określić bardziej szczegółowy zakres odpowiedzialności odbiorcy usług certyfikacyjnych.

4.8. Odpowiedzialność finansowa

Łączna odpowiedzialność z tytułu świadczenia przez KIR usług certyfikacyjnych nie może przekroczyć 1 000 000 EUR. Wysokość jednorazowego odszkodowania z tytułu użycia nieprawidłowego certyfikatu wydanego przez KIR nie może przekroczyć 250 000 EUR.

4.9. Opłaty

Opłaty z tytułu świadczenia usług certyfikacyjnych określa cennik usług certyfikacyjnych publikowany na stronie internetowej KIR www.elektronicznypodpis.pl, Umowa, oferta lub inny dokument zawierający propozycje cenowe.

4.10. Kontrola

W zakresie określonym w Ustawie o podpisie elektronicznym KIR podlega kontroli ministra właściwego ds. gospodarki.

4.11. Kompromitacja klucza prywatnego KIR

W przypadku kompromitacji klucza prywatnego KIR S.A,. wykorzystywanego do podpisywania certyfikatów oraz list zawieszonych i unieważnionych certyfikatów, wszystkie wydane dotychczas certyfikaty zostają automatycznie unieważnione.

4.12. Zaprzestanie świadczenia usług certyfikacyjnych w zakresie certyfikatów kwalifikowanych przez KIR

KIR ma prawo do zaprzestania wydawania kwalifikowanych certyfikatów. W takim przypadku wszyscy subskrybenci oraz odbiorcy usług certyfikacyjnych zostaną o tym poinformowani z 90 dniowym wyprzedzeniem. Zgodnie z wymaganiami Ustawy o podpisie elektronicznym wszystkie wydane przez KIR certyfikaty kwalifikowane i związane z tym dokumenty zostaną przekazane do ministra właściwego ds. gospodarki lub podmiotu wskazanego przez ministra. Subskrybenci wykorzystujący certyfikaty oraz potencjalni użytkownicy nie mają z tego powodu prawa dochodzić od KIR żadnych roszczeń.

5. OPIS SPOSOBU TWORZENIA I PRZESYŁANIA DANYCH, KTÓRE ZOSTANĄ OPATRZONE POŚWIADCZENIAMI ELEKTRONICZNYMI

5.1. Bezpieczne urządzenia do składania podpisów

Do generowania certyfikatów, zaświadczeń certyfikacyjnych, list unieważnionych i zawieszonych certyfikatów wykorzystywane są bezpieczne urządzenia do składania podpisów elektronicznych. Urządzenia te są wykorzystywane wyłącznie do świadczenia usług certyfikacyjnych w ramach niniejszej Polityki. Bezpieczne urządzenia do składania podpisów wykorzystywane w KIR posiadają odpowiedni wymagany prawem certyfikat oraz deklaracje dostawców sprzętu i producentów oprogramowania. Bezpieczne urządzenia do składania podpisów wykorzystywane w KIR do generowania certyfikatów oraz list unieważnionych i zawieszonych certyfikatów są zabezpieczone przed nieupoważnionym do-

stępem. Dostęp do urządzeń mają jedynie upoważnione osoby. Każda próba dostępu do danego urządzenia, niezależnie od wyniku oraz czynności związane z wygenerowaniem danych służących do składania podpisu elektronicznego lub poświadczenia elektronicznego są monitorowane i rejestrowane w systemie teleinformatycznym wykorzystywanym do świadczenia usług certyfikacyjnych.

Klucze chroniące dane służące do poświadczania elektronicznego certyfikatów, list unieważnionych certyfikatów oraz zaświadczeń certyfikacyjnych są dzielone na części według schematu progowego (m, n), gdzie wartość „m" wynosi 2, natomiast „n" wynosi 5. Każda z części jest przechowana w osobnych modułach kluczowych będących w posiadaniu osób upoważnionych przez KIR lub w sejfach. Dane do składania poświadczeń elektronicznych pojawiają się w pełnej formie wyłącznie w komponencie technicznym.

5.2. Klucze infrastruktury

Klucze infrastruktury są wykorzystywane do:

- zapewnienia integralności przekazu danych związanych ze świadczeniem usług certyfikacyjnych (żądania o wydanie, zawieszenie lub unieważnienie certyfikatu, informacje o błędach wynikłych w procesie wydawania, zawieszania lub unieważniania certyfikatu);
- zapewnienia integralności rejestrów zdarzeń przechowywanych w KIR;
- zapewnienia integralności danych związanych ze świadczeniem usług certyfikacyjnych, archiwizowanych w KIR;
- zabezpieczania dostępu do oprogramowania oraz urządzeń do składania podpisów wykorzystywanych do świadczenia usług certyfikacyjnych.

5.3. Generowanie certyfikatów, zaświadczeń certyfikacyjnych oraz list unieważnionych i zawieszonych certyfikatów

KIR generuje certyfikaty oraz listy zawieszonych i unieważnionych certyfikatów poświadczając elektronicznie dane w nich zawarte przy pomocy bezpiecznych urządzeń do składania podpisów. Do tworzenia certyfikatów oraz list unieważnionych i zawieszonych certyfikatów KIR wykorzystywane są algorytmy szyfrowe i funkcje skrótu określone w punkcie 14 Polityki. Format i strukturę certyfikatów oraz zaświadczeń certyfikacyjnych określa punkt 9 niniejszej Polityki. Format list unieważnionych i zawieszonych certyfikatów określa punkt 10 niniejszej Polityki.

5.4. Generowanie pary kluczy w imieniu subskrybenta

KIR może generować na komponencie technicznym stanowiącym część bezpiecznego urządzenia do składania podpisów subskrybenta parę kluczy. W takim przypadku generowanie danych odbywa się na bazie generatorów zaimplementowanych w komponencie technicznym. Kluczy prywatny nie jest kopiowany, ani w jakikolwiek inny sposób przechowywany poza komponentem technicznym. Dostęp do danych przechowywanych na komponencie technicznym jest zabezpieczony przed nieuprawnionym wykorzystaniem.

KIR może wydać certyfikat na żądanie certyfikacyjne przygotowane przez podmiot trzeci.

6. OKRES WAŻNOŚCI CERTYFIKATÓW

Maksymalny okres ważności certyfikatu subskrybenta wynosi 2 lata. Początek okresu ważności certyfikatu może być każdorazowo ustalany z odbiorcą usług certyfikacyjnych lub subskrybentem. KIR może na wniosek odbiorcy usług certyfikacyjnych lub subskrybenta wydać certyfikat z dowolnym okresem ważności certyfikatu subskrybenta, jednak okres ten nie może być dłuższy niż 2 lata.

7. ZASADY IDENTYFIKACJI I UWIERZYTELNIANIA

Niniejszy rozdział reguluje procedury identyfikacji subskrybentów występujących do KIR o wydanie certyfikatu oraz procedury identyfikacji osób występujących o unieważnienie, zawieszenie oraz wygenerowanie kolejnego certyfikatu.

7.1. Wydanie pierwszego certyfikatu

Przed wydaniem pierwszego certyfikatu dla danego subskrybenta odbiorca usług certyfikacyjnych podpisuje umowę na świadczenie usług certyfikacyjnych oraz dostarcza do KIR zamówienie zawierające dane niezbędne do przygotowania certyfikatu. Wzór zamówienia udostępniany jest na stronie internetowej KIR www.eletronicznypodpis.pl.

Wydanie subskrybentowi nośnika z parą kluczy, do której KIR wydała certyfikat, wymaga jego osobistego stawiennictwa w placówce KIR lub u Partnera współpracującego z KIR w zakresie wydawania certyfikatów.

Do otrzymania certyfikatu niezbędne jest przedstawienie przez subskrybenta:

- dokumentu tożsamości;
- dokumentu potwierdzającego nadanie numeru NIP, jeżeli został on umieszczony w certyfikacie;
- pliku z żądaniem o wydanie certyfikatu (jeżeli para kluczy jest generowana samodzielnie przez subskrybenta).

KIR może oczekiwać okazania innych dokumentów, w przypadku wnioskowania wpisania do certyfikatu innych danych subskrybenta niż imię i nazwisko oraz numer PESEL lub NIP.

W przypadku gdy subskrybent samodzielnie generuje parę kluczy wówczas do wydania certyfikatu potrzebne jest ponadto przedstawienie pliku z żądaniem o wydanie certyfikatu. Plik ten zawiera klucz publiczny, dla którego ma zostać wygenerowany certyfikat, dane subskrybenta, oraz podpis elektroniczny wygenerowany przy użyciu klucza prywatnego, tworzącego z kluczem publicznym jedną parę.

7.2. Identyfikator subskrybenta

Na podstawie danych otrzymanych w trakcie rejestracji, tworzony jest, zgodnie z poniższym schematem, identyfikator umożliwiający zidentyfikowanie subskrybenta związanego z kluczem publicznym umieszczonym w certyfikacie.

Identyfikator subskrybenta może zawierać następujące elementy:

Znaczenie	Wartość
nazwa kraju	Dwuliterowy skrót kraju
nazwa powszechna	Nazwa identyfikująca subskrybenta
nazwisko	Nazwisko subskrybenta plus ewentualnie nazwisko rodowe
imiona	Imiona subskrybenta
pseudonim	Nazwa, pod którą znany jest subskrybent lub którą chce się posługiwać
numer seryjny	Numer PESEL i/ lub NIP subskrybenta
organizacja	Nazwa odbiorcy usług certyfikacyjnych, z którą subskrybent jest związany
jednostka organizacyjna	Nazwa jednostki organizacyjnej, z którą subskrybent jest związany
województwo	Nazwa województwa
nazwa miejscowości	Nazwa miejscowości
adres pocztowy	Adres pocztowy

Identyfikator subskrybenta jest tworzony w oparciu o podzbiór powyższych atrybutów, przy czym identyfikator musi być niepusty i unikalny w ramach danej infrastruktury technicznej w KIR.

Certyfikaty mogą być wydawane różnym kategoriom subskrybentów. W ramach każdej kategorii zdefiniowany jest minimalny zestaw atrybutów wchodzących w skład identyfikatora subskrybenta:

- Kategoria I – nazwa kraju, nazwisko, imię (imiona), numer seryjny;
- Kategoria II – nazwa kraju, nazwa własna, numer seryjny;
- Kategoria III – nazwa kraju, pseudonim.

KIR zastrzega, że może odmówić wydania certyfikatu zawierającego identyfikator subskrybenta wg kategorii III.

7.3. Generowanie kolejnego certyfikatu

Jeżeli subskrybent posiada ważny kwalifikowany certyfikat, którego okres ważności zbliża się ku końcowi, odbiorca usług certyfikacyjnych lub subskrybent, o ile posiada stosowne upoważnienie, może wystąpić o wygenerowanie kolejnego kwalifikowanego certyfikatu.
W przypadku gdy subskrybent odbiera osobiście nowy certyfikat w placówce KIR lub u partnera weryfikacja tożsamości subskrybenta oraz jego prawa do otrzymania certyfikatu przebiega tak jak w przypadku pierwszego certyfikatu.
W przypadku gdy subskrybent występuje o wydanie nowego certyfikatu za pośrednictwem sieci Internet wówczas jego tożsamość jest weryfikowana na podstawie aktualnego certyfikatu kwalifikowanego, którym podpisane jest żądanie o odnowienie certyfikatu. Szczegółowy opis procesu odnawiania certyfikatu za pośrednictwem sieci Internet jest dostępny na stronie internetowej KIR www.elektronicznypodpis.pl.

7.4. Generowanie kolejnego certyfikatu po unieważnieniu poprzedniego certyfikatu lub upłynięciu jego terminu ważności

Proces generowania kolejnego certyfikatu po unieważnieniu poprzedniego lub generowania kolejnego certyfikatu w przypadku gdy upłynął okres ważności posiadanego przez subskrybenta certyfikatu, przebiega analogicznie jak proces wystąpienia o pierwszy certyfikat. Weryfikacja tożsamości subskrybenta odbywa się w taki sam sposób, jak w przypadku pierwszej rejestracji. Jeżeli powodem unieważnienia certyfikatu nie była konieczność zmiany identyfikatora subskrybenta, wówczas nowy certyfikat może zawierać nadany wcześniej identyfikator.

7.5. Żądanie unieważnienia lub zawieszenia certyfikatu

O unieważnienie lub zawieszenie certyfikatu występuje subskrybent lub osoba trzecia, o ile jej dane były zawarte w certyfikacie lub inna osoba, o ile wynika to z Ustawy o podpisie elektronicznym, Umowy lub innych zobowiązań KIR.

Certyfikat, który został unieważniony, nie może być następnie uznany za ważny.

KIR unieważnia wydany przez siebie certyfikat, jeżeli:

- certyfikat został wydany na podstawie nieprawdziwych lub nieaktualnych danych;
- stwierdzone zostało naruszenie obowiązków określonych w Ustawie o podpisie elektronicznym;
- subskrybent nie zapewnił należytej ochrony danym służącym do składania podpisu elektronicznego przed nieuprawnionym dostępem do nich;
- zażąda tego subskrybent lub osoba trzecia wskazana w certyfikacie lub inna osoba upoważniona do składania takiego żądania;
- KIR zaprzestaje świadczenia usług w zakresie certyfikatów, a jej praw i obowiązków nie przejmuje żaden inny kwalifikowany podmiot świadczący usługi certyfikacyjne;
- zażąda tego minister właściwy ds. gospodarki;
- subskrybent utracił pełną zdolność do czynności prawnych.

W przypadku powstania uzasadnionego podejrzenia, że istnieją przesłanki do unieważnienia kwalifikowanego certyfikatu, KIR zawiesza certyfikat i podejmuje niezwłocznie działania niezbędne do wyjaśnienia tych wątpliwości.

Upoważnienie do żądania unieważnienia certyfikatu może wynikać z umowy.

Umowa może przewidywać inne niż wymienione powyżej przypadki unieważnienia certyfikatu.

W szczególnym przypadku KIR może unieważnić certyfikat na żądanie odbiorcy usług certyfikacyjnych, nawet gdy ten nie jest do tego odrębnie upoważniony, jeżeli:

- certyfikat został wydany na podstawie Umowy z nim zawartej oraz
- przedstawi i wyda on KIR pisemny dowód powiadomienia subskrybenta o tym, że będzie żądać unieważnienia certyfikatu w KIR.

Wniosek o unieważnienie lub zawieszenie certyfikatu może być złożony:

- osobiście w placówkach KIR, w godzinach pracy KIR;
- telefonicznie na numer infolinii publikowany na stronie internetowej KIR www.elektronicznypodpis.pl w godzinach pracy infolinii;
- całodobowo na stronie internetowej KIR www.elektronicznypodpis.pl.

Wniosek o unieważnienie lub zawieszenie certyfikatu powinien zawierać co najmniej:

- imię i nazwisko osoby zgłaszającej;
- PESEL osoby zgłaszającej lub numer i serię dokumentu tożsamości w przypadku braku PESEL;
- dane dotyczące certyfikatu (np. numer seryjny, identyfikator subskrybenta, okres ważności);
- powód zmiany statusu certyfikatu.

Wzór wniosku o unieważnienie/ zawieszenie certyfikatu publikowany jest na stronie internetowej KIR www.elektronicznypodpis.pl.

Podstawą przyjęcia wniosku o unieważnienie lub zawieszenie certyfikatu złożonego osobiście jest pozytywna weryfikacja:

- tożsamości osoby występującej o unieważnienie/ zawieszenie, na podstawie przedstawionego dowodu osobistego lub paszportu i jej prawa do unieważnienia/ zawieszenia certyfikatu;
- danych zawartych we wniosku o unieważnienie/ zawieszenie certyfikatu.

Podstawą przyjęcia wniosku o unieważnienie/ zawieszenie certyfikatu złożonego telefonicznie lub za pośrednictwem Internetu jest pozytywna weryfikacja:

- imienia i nazwiska osoby zgłaszającej;
- PESEL osoby zgłaszającej lub numeru i serii dokumentu tożsamości w przypadku braku PESEL;
- danych dotyczących certyfikatu (np. numer seryjny, identyfikator subskrybenta, okres ważności);

  hasła osoby zgłaszającej.

W przypadku, gdy którakolwiek dana jest nieprawidłowa, wniosek o unieważnienie/ zawieszenie certyfikatu zostaje odrzucony.

W przypadku istnienia uzasadnionego podejrzenia, że istnieją przesłanki do unieważnienia certyfikatu, KIR zawiesi certyfikat i podejmie działania niezbędne do wyjaśnienia ich prawdziwości.

W przypadku wniosku o zawieszenie, gdy wszystkie wymienione informacje są poprawne, KIR zawiesza certyfikat na okres 7 dni.

7.5.1. Hasło do zawieszania i unieważniania certyfikatu

Subskrybent lub inna osoba uprawniona do żądania unieważnienia/ zawieszenia certyfikatu jest obowiązana dostarczyć do KIR hasła do zawieszania i unieważniania certyfikatów. Hasło, zapisane na

kartce, powinno być zapakowane w nieprzezroczystą kopertę. Nieprzekazanie hasła uniemożliwia złożenie żądania unieważnienia lub zawieszenia certyfikatu przez Internet oraz telefonicznie.

Na kopercie wewnętrznej dodatkowo powinny być naniesione następujące dane:

- imię i nazwisko osoby uprawnionej;
- numer PESEL.

W przypadku gdy hasło składa osoba inna niż subskrybent, jest ona zobowiązana do podania podstawy prawnej uprawniającej ją do żądania unieważnienia lub zawieszenia certyfikatu.

Koperty zawierające hasła są przechowywane w KIR, zaś dostęp do nich posiadają jedynie osoby uprawnione w KIR do zawieszania i unieważniania certyfikatów.

Odbiorca usług certyfikacyjnych oraz subskrybent mają prawo do zmiany uprzednio podanych haseł.

8. METODY, TRYB TWORZENIA ORAZ UDOSTĘPNIANIA CERTYFIKATÓW ORAZ LIST UNIEWAŻNIONYCH I ZAWIESZONYCH CERTYFIKATÓW

8.1. Algorytmy szyfrowe

KIR wydaje subskrybentom certyfikaty kwalifikowane dla danych służących do weryfikacji podpisów pochodzących z następujących algorytmów szyfrowych:

- RSA;
- DSA;
- ECDSA;
- ECGDSA.

Identyfikatory oraz szczegółowe minimalne wymagania dla algorytmów szyfrowych określa załącznik nr 6 do niniejszej Polityki.

8.2. Obsługa wniosków o wydanie certyfikatu

Po otrzymaniu zamówienia na certyfikat KIR przystępuje do wydawania certyfikatu na podstawie danych zawartych w zamówieniu. Na komponencie technicznym dedykowanym dla subskrybenta zgłoszonego w zamówieniu KIR generuje parę kluczy oraz nagrywa wygenerowany certyfikat.

Operator, który potwierdził w imieniu KIR tożsamość subskrybenta w momencie przekazania certyfikatu subskrybentowi, poświadcza dokonanie tego potwierdzenia własnoręcznym podpisem oraz podaniem swojego numeru PESEL na potwierdzeniu.

8.3. Wydanie kolejnego certyfikatu

W przypadku, gdy subskrybent przesyła żądanie o wydanie kolejnego certyfikatu telekomunikacyjnie, po otrzymaniu od subskrybenta żądania KIR sprawdza:

- czy subskrybent posiada aktualny certyfikat;
- czy dane w żądaniu są takie same jak dane w aktualnym certyfikacie;
- podpisy elektroniczne dołączone do pliku z żądaniem.

KIR porównuje pola w nowym żądaniu o wydanie certyfikatu z aktualnym certyfikatem. Pola, które są porównywane to:

- identyfikator subskrybenta;
- identyfikator polityki certyfikacji;
- zastosowanie klucza publicznego;

- długość klucza i algorytm.

W przypadku niezgodności żądanie jest odrzucane. O odrzuceniu wniosku subskrybent jest informowany w formie komunikatu o błędzie.

8.4. Wydawanie certyfikatu przez KIR

KIR, wydając certyfikat, poświadcza elektronicznie dane służące do weryfikacji podpisu wraz z danymi o subskrybencie, wykorzystując do tego celu bezpieczne urządzenie do składania podpisów. Poświadczenie elektroniczne składane przez KIR pod certyfikatem jest generowane z wykorzystaniem algorytmu szyfrowego RSA i funkcji skrótu SHA – 1, których identyfikatory i charakterystykę określa punkt 14 Polityki. Dane służące do składania poświadczenia elektronicznego wykorzystywane przez KIR mają długość 2048 bitów.

8.5. Unieważnienie certyfikatu

W przypadku pozytywnej weryfikacji wniosku o unieważnienie/ zawieszenie certyfikatu KIR unieważnia/ zawiesza certyfikat. Unieważnienie/ zawieszenie certyfikatu następuje w momencie wpisania certyfikatu na listę unieważnionych i zawieszonych certyfikatów. Informacja o unieważnieniu/ zawieszeniu certyfikatu jest umieszczana na liście unieważnionych certyfikatów – CRL. KIR zawiadamia subskrybenta i ewentualnie inną osobę o unieważnieniu/ zawieszeniu certyfikatu.

8.6. Zmiana statusu certyfikatu po zawieszeniu

Certyfikat, który został zawieszony, może zostać następnie unieważniony lub uznany za ważny.

Zmiana statusu certyfikatu na ważny może nastąpić wyłącznie na wniosek złożony osobiście w KIR. Wzór wniosku o zmianę statusu jest dostępny na stronie internetowej KIR www.elektronicznypodpis.pl. Zmiana statusu na nieważny odbywa się w sposób określony w punkcie 7.5 niniejszej Polityki.

Jeżeli w ciągu 7 dni od daty zawieszenia certyfikatu nie został złożony wniosek o zmianę jego statusu, wówczas certyfikat zostaje unieważniony.

Jeżeli unieważnienie certyfikatu następuje po jego uprzednim zawieszeniu, wówczas data unieważnienia certyfikatu jest identyczna z datą zawieszenia certyfikatu.

Weryfikacja tożsamości osoby składającej wniosek o zmianę statusu zawieszonego certyfikatu oraz samego wniosku odbywa się w taki sam sposób, jak w przypadku składania żądania unieważnienia/zawieszenia certyfikatu.

8.7. Listy zawieszonych i unieważnionych certyfikatów

Po zawieszeniu lub unieważnieniu certyfikatu, KIR generuje listę zawieszonych i unieważnionych certyfikatów. Lista ta zawiera:

- wskazanie czasu jej powstania;
- wskazanie czasu publikacji następnej listy zawieszonych i unieważnionych certyfikatów;
- numer seryjny zawieszonego/ unieważnionego certyfikatu;
- wskazanie czasu zawieszenia/ unieważnienia certyfikatu;
- przyczynę zawieszenia/ unieważnienia certyfikatu.

Po cofnięciu uprzedniego zawieszenia certyfikatu, informacja o takim certyfikacie jest usuwana z listy zawieszonych i unieważnionych certyfikatów.

Z listy zawieszonych i unieważnionych certyfikatów mogą nie zostać usunięte informacje o certyfikatach unieważnionych, których okres ważności nadany przez KIR upłynął.

Szczegółowy opis konstrukcji listy zawieszonych i unieważnionych certyfikatów określa punkt 10 niniejszej Polityki.

8.8. Publikacje i repozytorium

Informacje dotyczące usług certyfikacyjnych świadczonych przez KIR, w informacje nt. sposobu zawierania Umów, obsługi zamówień i odnowień certyfikatów są udostępniane wszystkim zainteresowanym na stronie internetowej KIR www.elektronicznypodpis.pl lub w placówkach KIR.

Listy zawieszonych i unieważnionych certyfikatów są generowane przez KIR nie rzadziej niż co 12 godzin lub po zawieszeniu albo unieważnieniu certyfikatu. Aktualizacja list odbywa się nie później niż w ciągu 1 godziny od zawieszenia lub unieważnienia certyfikatu.

Aktualne listy CRL generowane przez KIR są bezpłatnie udostępniane wszystkim zainteresowanym na stronie internetowej KIR www.elektronicznypodpis.pl.

Wszystkie wydane przez KIR certyfikaty przechowywane są w KIR co najmniej przez okres wymagany przez Ustawę o podpisie elektronicznym.

9. OPIS ELEKTRONICZNYCH STRUKTUR DANYCH ZAWARTYCH W CERTYFIKATACH

Zawartość certyfikatów oraz zaświadczeń certyfikacyjnych generowanych przez KIR została opisana w notacji ASN.1 określonej w normie ISO/IEC 8824 – Information technology – Open Systems Interconnection – Specification of Abstract Syntax Notation One (ASN.1), wydanej przez International Organization for Standardization.

Certyfikaty oraz zaświadczenia certyfikacyjne, wydawane przez KIR, składają się z trzech części:

- treści certyfikatu (*tbsCertificate*);
- identyfikatora algorytmu podpisu elektronicznego (*signatureAlgorithm*);
- podpisu elektronicznego (*signature*).

Pierwsza część certyfikatu (*tbsCertificate)* składa się z następujących podstawowych pól:

Nazwa pola	Znaczenie pola	Treść
version	oznaczenie wersji certyfikatu	2
serialNumber	numer seryjny certyfikatu	unikalny w ramach systemu do wydawania certyfikatów kwalifikowanych numer certyfikatu
signature	identyfikator oraz parametry podpisu stosowane przez KIR do poświadczenia elektronicznego danego certyfikatu	{iso(1) member-body(2) US(840) rsadsi(113549) pkcs(1) 1 5 }
issuer	identyfikator wyróżniający podmiot świadczący usługi certyfikacyjne, który wydał certyfikat	C=PL; O=Krajowa Izba Rozliczeniowa S.A. CN= oznaczenie ośrodka odpowiedzialnego za generowanie certyfikatów; numer wpisu w rejestrze
validity	oznaczenie początku i końca ważności certyfikatu wydanego przez KIR	czas wygenerowania certyfikatu i końca okresu ważności certyfikatu z dokładnością co do sekundy
subject	identyfikator podmiotu związanego z kluczem publicznym umieszczonym w certyfikacie	wartość o której mowa w punkcie 7.2 Polityki
subjectPublicKeyInfo	wartość klucza publicznego wraz z identyfikatorem algorytmu, z którym stowarzyszony jest klucz	klucz publiczny przedstawiony przez subskrybenta
extensions	rozszerzenia standardowe i niestan-	zgodnie z tabelą poniżej

	dardowe	

Dopuszczalne rozszerzenia certyfikatu przedstawia poniższa tabela:

Rozszerzenie standardowe/ niestandardowe	Nazwa rozszerzenia	Krytyczne/ Niekrytyczne	Znaczenie rozszerzenia	Treść
Rozszerzenia standardowe	*authorityKeyIdentifier*	niekrytyczne	identyfikator klucza publicznego służącego do weryfikacji wydanego certyfikatu	identyfikator
	subjectKeyIdentifier	niekrytyczne	identyfikator certyfikatu zawierający określony klucz publiczny subskrybenta	identyfikator
	keyUsage	krytyczne	określa sposób wykorzystania klucza publicznego	nonRepudiation
	certificatePolicies	krytyczne	określa politykę certyfikacji, zgodnie z którą wydany jest dany certyfikat	- identyfikator (1.2.616.113571.1.1) i opis polityki; - oświadczenie, że certyfikat jest certyfikatem kwalifikowanym wydanym przez kwalifikowany podmiot świadczący usługi certyfikacyjne
	subjectAltName	krytyczne/ niekrytyczne	inna, uzupełniająca nazwa właściciela certyfikatu, np. adres poczty elektronicznej	Zgodnie ze wskazaniem subskrybenta lub podmiotu podpisującego umowę na świadczenie usług certyfikacyjnych
	basicConstraints	krytyczne	umożliwia sprawdzenie czy właściciel certyfikatu jest użytkownikiem końcowym, czy też podmiotem wydającym certyfikaty	pusta sekwencja
	cRLDistributionPoints	niekrytyczne	określa adresy, pod którymi jest publikowana aktualna lista CRL	http://www.kir.com.pl/certyfikacja_kluczy/CRL_OZKx.crl lub http://www.elektronicznypodpis.pl/crl/crl_ozkx.crl; gdzie x stanowi oznaczenie ośrodka/systemu informatycznego KIR odpowiedzialnego za wydawanie certyfikatów
	subjectDirectoryAttributes	niekrytyczne	dodatkowe atrybuty powiązane z właścicielem certyfikatu	w polu tym mogą wystąpić: - stanowisko; - adres poczty elektronicznej.

Rozszerzenia niestandardowe	*qcStatement*	niekrytyczne	deklaracja wydawcy certyfikatu kwalifikowanego	- limit transakcji, którą jednorazowo można potwierdzić za pomocą certyfikatu; - wskazania, w czyim imieniu działa właściciel certyfikatu (dopuszczalne wartości: a) we własnym imieniu; b) jako przedstawiciel innej osoby fizycznej, osoby prawnej albo jednostki organizacyjnej nie posiadającej osobowości prawnej; c) w charakterze członka organu albo organu osoby prawnej albo jednostki organizacyjnej nie posiadającej osobowości prawnej d) jako organ władzy publicznej Przedstawione deklaracje nie są obligatoryjne.

10. SPIS ELEKTRONICZNYCH STRUKTUR DANYCH ZAWARTYCH W LISTACH ZAWIESZONYCH I UNIEWAŻNIONYCH CERTYFIKATÓW

Zawartość listy zawieszonych i unieważnionych certyfikatów generowanej przez KIR została opisana w notacji ASN.1 określonej w normie ISO/IEC 8824 – Information technology – Open Systems Interconnection – Specification of Abstract Syntax Notation One (ASN.1), wydanej przez International Organization for Standardization.

Lista zawieszonych i unieważnionych certyfikatów składa się z trzech części:

- treści certyfikatu (*tbsCertList*);
- identyfikatora algorytmu podpisu elektronicznego (*signatureAlgorithm*);
- podpisu elektronicznego (*signature*).

Pierwsza część listy CRL (*tbsCertList)* składa się z następujących podstawowych pól:

Nazwa pola	Znaczenie pola	Treść
version	oznaczenie wersji listy zawieszonych i unieważnionych certyfikatów	1
signature	identyfikator oraz parametry podpisu stosowane przez KIR do poświadczenia elektronicznego danego certyfikatu	{iso(1) member-body(2) US(840) rsadsi(113549) pkcs(1) 1 5 }
issuer	identyfikator wyróżniający podmiot świadczący usługi certyfikacyjne, który wydał certyfikat	C=PL; O=Krajowa Izba Rozliczeniowa S.A. CN= oznaczenie ośrodka odpowiedzialnego za generowanie certyfikatów; numer wpisu w rejestrze
thisUpdate	data wydania listy zawieszonych i unieważnionych certyfikatów	czas wygenerowania listy CRL z dokładnością do sekundy

nextUpdate	planowany czas wydania kolejnej listy	planowany czas wygenerowania kolejnej listy CRL z dokładnością do sekundy
revokedCertificates	lista zawieszonych i unieważnionych certyfikatów	– numer seryjny certyfikatu – data i czas unieważniania/ zawieszenia certyfikatu – kod unieważniania/ zawieszania certyfikatu
crlExtension	rozszerzenia listy zawieszonych i unieważnionych certyfikatów (status: niekrytyczne)	– identyfikator klucza podmiotu do weryfikacji podpisu pod listą zawieszonych i unieważnionych certyfikatów – numer listy zawieszonych i unieważnionych certyfikatów

Dopuszczalne kody unieważniania/ zawieszenia certyfikatu to:

- *unspecified* – przyczyna unieważnienia certyfikatu nie jest znana;
- *keyCompromise* – certyfikat został unieważniony z powodu kompromitacji lub podejrzenia kompromitacji danych służących do składania podpisu elektronicznego;
- *affiliationChanged* – certyfikat został unieważniony z powodu zmiany danych zawartych w certyfikacie;
- *susperseded* – certyfikat został unieważniony z powodu zastąpienia danych służących do składania podpisu elektronicznego;
- *cessationOfOpertion* – certyfikat został unieważniony z powodu zaprzestania używania go do celu, dla którego został wydany;
- *privilige Withdrawn* – certyfikat został unieważniony z powodu zmiany danych zawartych w certyfikacie, określających rolę właściciela certyfikatu;
- *certificateHold* – certyfikat został zawieszony.

W przypadku wystąpienia kodu *certificateHold* lista zawieszonych i unieważnionych certyfikatów może zawierać dodatkowe rozszerzenie niekrytyczne określające możliwe instrukcje postępowania z zawieszonym certyfikatem:

- wskazanie konieczności skontaktowania się z wydawcą certyfikatu w celu wyjaśnienia przyczyny zawieszenia certyfikatu;
- wskazanie obligatoryjnego odrzucenia rozpatrywanego certyfikatu.

11. SPOSÓB ZARZĄDZANIA DOKUMENTAMI ZWIĄZANYMI ZE ŚWIADCZENIEM USŁUG CERTYFIKACYJNYCH

KIR przechowuje i archiwizuje dokumenty oraz dane w postaci elektronicznej, bezpośrednio związane z wykonywanymi kwalifikowanymi usługami certyfikacyjnymi, w sposób zapewniający bezpieczeństwo przechowywanych dokumentów i danych. Dostęp do dokumentów i danych związanych ze świadczeniem usług certyfikacyjnych mogą mieć wyłącznie osoby upoważnione przez KIR , posiadające przeszkolenie w zakresie ochrony danych osobowych i dopuszczone do ich przetwarzania.

Dokumenty i dane w postaci elektronicznej są przechowywane w bazie danych osobowych systemu SZAFIR, zgłoszonej do rejestru prowadzonego przez Głównego Inspektora Ochrony Danych Osobowych. Przechowywanie odbywa się z wykorzystaniem technik zapewniających integralność danych zgodnie z wymaganiami ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedno-

lity Dz.U. z 2002 r., Nr. 101, poz. 926 z późn.zm.), zwanej dalej „Ustawą o ochronie danych osobowych”.

Przechowywaniu i archiwizacji przez okres 20 lat, od momentu utworzenia danego dokumentu i danych, podlegają:

- kwalifikowane certyfikaty i zaświadczenia certyfikacyjne wydane przez KIR ;
- listy zawieszonych i unieważnionych kwalifikowanych certyfikatów wydanych przez KIR ;
- listy unieważnionych zaświadczeń certyfikacyjnych wydanych przez KIR;
- umowy na świadczenie usług certyfikacyjnych;
- inne dokumenty zgodnie z wymaganiami prawnymi.

W przypadku zaprzestania wydawania certyfikatów przez KIR, wszystkie wymienione powyżej dokumenty będą przekazane do ministra właściwego ds. gospodarki lub wskazanego przez niego podmiotu. Subskrybenci i odbiorcy usług certyfikacyjnych nie będą ponosili z tego tytułu żadnych kosztów.

12. POUFNOŚĆ INFORMACJI I OCHRONA DANYCH OSOBOWYCH

KIR zapewnia, że wszelkie informacje związane ze świadczeniem usług certyfikacyjnych, które nie zostały jednoznacznie zakwalifikowane jako jawne, podlegają ochronie przed ich ujawnieniem na zasadach określonych w obowiązujących przepisach prawa.

Ochronie podlegają informacje znajdujące się w posiadaniu KIR:

- wewnętrzne procedury dotyczące świadczenia usług certyfikacyjnych;
- klucze prywatne infrastruktury KIR wykorzystywanej do świadczenia usług certyfikacyjnych;
- hasła do zawieszania i unieważniania certyfikatów;
- archiwum, zapisy logów funkcjonowania systemu teleinformatycznego wykorzystywanego do świadczenia usług certyfikacyjnych;
- dane subskrybentów związane z wydawaniem, unieważnianiem i zawieszaniem certyfikatów subskrybentów.

Wszystkie wydawane przez KIR certyfikaty podlegają ochronie zgodnie z wymaganiami przepisów o ochronie danych osobowych.

Przetwarzanie danych osobowych w KIR odbywa się na zasadach określonych w Ustawie o ochronie danych osobowych i wydanych do niej przepisów wykonawczych. Każdej osobie, której został wydany certyfikat, przysługują uprawnienia wynikające z tej Ustawy.

13. ZABEZPIECZENIA TECHNICZNE I ORGANIZACYJNE

13.1. Ochrona fizyczna

Pomieszczenia, w których odbywa się przetwarzanie danych związanych z wydawaniem, zawieszaniem lub unieważnianiem certyfikatów, oraz w których odbywa się generowanie, zawieszanie i unieważnianie certyfikatów, podlegają ochronie fizycznej zgodnie z wymaganiami Ustawy o podpisie elektronicznym i Ustawy o ochronie danych osobowych. Zastosowane środki ochrony zabezpieczają przed:

- dostępem osób nieuprawnionych do pomieszczeń;
- skutkami naturalnych katastrof i zdarzeń losowych;

- pożarami;
- awarią infrastruktury;
- zalaniem wodą, kradzieżą, włamaniem i napadem.

Zastosowane środki ochrony fizycznej pomieszczeń obejmują między innymi:

- system kontroli dostępu do pomieszczeń;
- system ochrony przeciwpożarowej;
- system alarmowy klasy SA3.

13.2. Zabezpieczenia techniczne

13.2.1. Zabezpieczenia sieci teleinformatycznej

Dostęp do systemu teleinformatycznego, w ramach którego świadczone są usługi certyfikacyjne, jest zabezpieczony zgodnie z wymaganiami określonymi w Ustawie o podpisie elektronicznym i przepisach wykonawczych do tej Ustawy.

13.2.2. Komponenty techniczne

W przypadku generowania danych do składania podpisów dla subskrybentów przez KIR, czynność ta jest wykonywana w dedykowanych do tego celu komponentach technicznych. Wszystkie dane, pozwalające na odtworzenie wygenerowanego klucza prywatnego, są automatycznie niszczone bezpośrednio po zakończeniu procesu generacji danych do składania podpisów elektronicznych.

13.3. Ośrodek zapasowy

Na wypadek awarii podstawowego ośrodka, którym zlokalizowana jest infrastruktura wykorzystywana do świadczenia usług certyfikacyjnych, uniemożliwiającej świadczenie usług certyfikacyjnych, prace systemu przejmuje zapasowy system zlokalizowany w siedzibie zapasowej. W przypadku awarii, zapasowy system na bieżąco przejmuje pracę związaną z unieważnianiem, zawieszaniem certyfikatów i publikacją list zawieszonych i unieważnionych certyfikatów.

13.4. Zabezpieczenia kadrowe

Kadra zajmująca się świadczeniem usług certyfikacyjnych posiada kwalifikacje wymagane w Ustawie o podpisie elektronicznym, a w szczególności wiedzę z zakresu infrastruktury klucza publicznego oraz przetwarzania danych osobowych.

14. IDENTYFIKATORY I WYMAGANIA DLA ALGORYTMÓW SZYFROWYCH I FUNKCJI SKRÓTU

Lp	Algorytm	Identyfikator algorytmu	Wymagania
1.	RSA	{join-iso-ccitt(2) ds.(5) module (1) algorithm(8) encryptionAlgorithm(1) 1}	- minimalna długość klucza, rozumianego jako moduł p*q, wynosi 1020 bitów; - długości liczb pierwszych p i q, składających się na moduł, nie mogą się różnić więcej niż o 30 bitów.
2.	DSA	{iso(1) member-body(2) us(840) x9-57(10040)x9cm(4) 1}	- minimalna długość klucza, rozumianego jako moduł p, wynosi 1024 bity; - minimalna długość parametru q, będącego dzielnikiem liczby (p-1), wynosi 160 bitów.
3.	ECDSA	{iso(1) member-body(2) us(840) ansi-X9-62(10045) ecdsa-with-SHA1(1)}	- minimalna długość parametru g wynosi 160 bitów;

			- minimalny współczynnik r0 wynosi 10^4; - minimalna klasa wynosi 200.
4.	ECGDSA		- minimalna długość parametru g wynosi 160 bitów; - minimalny współczynnik r0 wynosi 10^4; - minimalna klasa wynosi 200.
5.	SHA – 1	{iso(1) identifiedOrganization(3) oIW(14) oIWSecSig(3) oIWAlgo-rithm(2) 26}	
6.	RIPEMD – 160	{iso(1) identifiedOrganization(3) tele-trust(36) algorithm(3) hashAlgo-rithm(2) 1}	