Krajowa Izba Rozliczeniowa S.A.

POLITYKA CERTYFIKACJI KIR S.A.
dla
ZAUFANYCH CERTYFIKATÓW NIEKWALIFIKOWANYCH

Wersja 1.4

Historia dokumentu

Numer wersji	Status	Data wydania
1.0	Dokument zatwierdzony przez Zarząd KIR S.A. – wersja obowiązująca do 30 września 2012 r.	19.12.2011 r.
1.1.	Dokument zatwierdzony przez Zarząd KIR S.A. – wersja obowiązująca do 19 grudnia 2013 r.	1.10.2012 r.
1.2.	Dokument zatwierdzony przez Zarząd KIR S.A. – wersja obowiązująca do 24 kwietnia 2014 r.	20.12.2013 r.
1.3.	Dokument zatwierdzony przez Zarząd KIR S.A. – wersja obowiązująca do 19 listopada 2014 r.	18.04.2014 r.
1.4	Dokument zatwierdzony przez Zarząd KIR S.A. – wersja obowiązująca od 20 listopada 2014 r.	13.11.2014 r.

SPIS TREŚCI

1. WSTĘP

„Polityka certyfikacji KIR S.A. dla zaufanych certyfikatów niekwalifikowanych", zwana dalej „Polityką", określa ogólne zasady świadczenia usług certyfikacyjnych, w tym techniczne i organizacyjne rozwiązania, wskazujące sposób, zakres oraz warunki tworzenia i stosowania certyfikatów. Polityka określa proces świadczenia usług certyfikacyjnych oraz jego uczestników. Szczegółowy opis zawiera „Kodeks postępowania certyfikacyjnego KIR S.A. dla zaufanych certyfikatów niekwalifikowanych", zwany dalej „Kodeksem". Definicje pojęć użytych w Polityce są określone w Kodeksie.

Usługi certyfikacyjne w zakresie wydawania zaufanych certyfikatów niekwalifikowanych, zwanych dalej „certyfikatami", realizuje Krajowa Izba Rozliczeniowa S.A., zwana dalej „KIR S.A.", w tym poprzez swoje terenowe jednostki. Lista jednostek KIR S.A. wraz z godzinami ich pracy dostępna jest na stronie internetowej KIR S.A. www.elektronicznypodpis.pl.

2. ZAKRES ZASTOSOWANIA POLITYKI CERTYFIKACJI

Polityka jest stosowana do wydawania i zarządzania certyfikatami wydawanymi przez KIR S.A. Przez certyfikat należy rozumieć elektroniczny plik poświadczony elektronicznie przez KIR S.A., w którym klucz publiczny jest przyporządkowany do subskrybenta i umożliwia jego identyfikację.

Certyfikaty, wydawane zgodnie z Polityką, nie są certyfikatami kwalifikowanymi w myśl ustawy z dnia 18 września 2001 r. o podpisie elektronicznym (Dz. U. Nr 130, poz. 1450 z późn. zm.). Podpis elektroniczny weryfikowany przy pomocy tych certyfikatów nie wywołuje skutków prawnych równorzędnych podpisowi własnoręcznemu.

Certyfikaty opisane w Polityce są generowane przez ośrodek certyfikacji SZAFIR Trusted CA prowadzony przez KIR S.A.

Certyfikaty mogą zawierać dane i służyć do identyfikacji innych podmiotów niż osoby fizyczne.

Odpowiedzialność KIR S.A., w tym finansowa, odpowiedzialność subskrybenta, odbiorcy usług certyfikacyjnych oraz strony ufającej jest określona w Kodeksie.

2.1. Certyfikat standard

Certyfikaty te są przeznaczone do ochrony informacji przesyłanych drogą elektroniczną. Mogą one być wykorzystywane do szyfrowania danych oraz uwierzytelniania i identyfikacji stron komunikacji. Certyfikaty te mogą być wykorzystywane do zabezpieczania poczty elektronicznej oraz do logowania się do systemów lub serwisów, autoryzacji subskrybenta w trakcie zestawiania bezpiecznych połączeń.

W procesie wydawania certyfikatów tego rodzaju operator KIR S.A. weryfikuje tożsamość subskrybenta oraz prawo do uzyskania takiego certyfikatu. Certyfikat przekazywany jest subskrybentowi najczęściej z parą kluczy wygenerowaną na nośniku określonym przez subskrybenta. Dane zawarte w certyfikacie pozwalają na identyfikację subskrybenta posługującego się certyfikatem.

Identyfikator polityki dla certyfikatów standard wygląda następująco:

```
iso(1) member-body(2) pl (616) organization(1) id-kir(113571) id-szafir(1)
id-nkw(2) id-szafir-standard(3)
```

2.2. Certyfikat do podpisywania kodów

Certyfikaty do podpisywania kodów są przeznaczone do potwierdzania autentyczności i pochodzenia kodów binarnych. Na podstawie danych zawartych w certyfikacie można określić autora bądź podmiot udostępniający kod programu lub aplikacji.

W procesie wydawania certyfikatów tego rodzaju operator KIR S.A. weryfikuje tożsamość subskrybenta oraz prawo do uzyskania takiego certyfikatu oraz potwierdza wiarygodność danych wpisanych do certyfikatu.

Dane zawarte w certyfikacie pozwalają na identyfikację podmiotu posługującego się certyfikatem.

Identyfikator polityki dla certyfikatów do podpisywania kodów wygląda następująco:

```
iso(1) member-body(2) pl (616) organization(1) id-kir(113571) id-szafir(1)
id-nkw(2) id-szafir-kod(4)
```

2.3. Certyfikat VPN

Certyfikat VPN pozwala na identyfikację routerów w sieciach zarówno lokalnych, jak i internetowych. Pozwala tworzyć wirtualne sieci prywatne poprzez zestawianie szyfrowanych połączeń.

W procesie wydawania certyfikatów operator KIR S.A. weryfikuje tożsamość subskrybenta oraz jego prawo do uzyskania certyfikatu. Proces może obejmować również weryfikację, czy urządzenie sieciowe pozostaje w dyspozycji odbiorcy usług certyfikacyjnych.

Identyfikator polityki dla certyfikatów VPN wygląda następująco:

```
iso(1) member-body(2) pl (616) organization(1) id-kir(113571) id-szafir(1)
id-nkw(2) id-szafir-VPN(5)
```

2.4. Certyfikat SSL

Certyfikat SSL pozwala na potwierdzanie autentyczności serwerów www oraz zestawianie bezpiecznych połączeń w oparciu o protokoły SSL i TSL. Certyfikat może zawierać dane pojedynczego serwera www lub też serwerów stowarzyszonych w ramach jednej domeny.

W procesie wydawania certyfikatów operator KIR S.A. weryfikuje tożsamość subskrybenta oraz jego prawo do uzyskania certyfikatu. Proces obejmuje również weryfikację, czy serwer www lub domena pozostają w dyspozycji odbiorcy usług certyfikacyjnych.

Identyfikator polityki dla certyfikatów SSL wygląda następująco:

```
iso(1) member-body(2) pl (616) organization(1) id-kir(113571) id-szafir(1)
id-nkw(2) id-szafir-SSL(6)
```

2.5. Certyfikat testowy

Certyfikaty te są przeznaczone do sprawdzenia współpracy z systemem bądź rozwiązaniem informatycznym subskrybenta.

W procesie wydawania certyfikatów testowych operator KIR S.A. weryfikuje prawo subskrybenta do uzyskania takiego certyfikatu. W przypadku, gdy certyfikat testowy ma służyć do sprawdzenia możliwości zestawiania bezpiecznych połączeń, proces obejmuje również weryfikację, czy serwer www lub domena pozostają w dyspozycji odbiorcy usług certyfikacyjnych.

Identyfikator polityki dla certyfikatów testowych wygląda następująco:

```
iso(1) member-body(2) pl (616) organization(1) id-kir(113571) id-szafir(1)
id-nkw(2) id-szafir-test(7)
```

2.6. Certyfikat ELIXIR

Certyfikaty te są przeznaczone do ochrony informacji przesyłanych w ramach systemów ELIXIR i EuroELIXIR prowadzonych przez KIR S.A. Mogą one być wykorzystywane do szyfrowania danych oraz uwierzytelniania i identyfikacji stron komunikacji. Tego rodzaju certyfikaty są wydawane wyłącznie uczestnikom systemów ELIXIR i EuroELIXIR.

W procesie wydawania certyfikatów tego rodzaju Operator KIR S.A. weryfikuje tożsamość subskrybenta oraz prawo do uzyskania takiego certyfikatu. Dane zawarte w certyfikacie pozwalają na identyfikację subskrybenta posługującego się certyfikatem.

Identyfikator polityki dla certyfikatów ELIXIR wygląda następująco:

```
iso(1) member-body(2) pl (616) organization(1) id-kir(113571) id-szafir(1)
id-nkw(2) id-szafir-ELIXIR(8)
```

2.7. Certyfikat Standard Server

Certyfikat Standard Server pozwala na potwierdzanie autentyczności serwerów, w tym serwerów działających w sieci wewnętrznej organizacji. Certyfikat może zawierać dane pojedynczego serwera lub też serwerów stowarzyszonych w ramach jednej domeny.

W procesie wydawania certyfikatów operator KIR S.A. weryfikuje tożsamość subskrybenta oraz jego prawo do uzyskania certyfikatu. Proces obejmuje również weryfikację, czy serwer lub domena pozostają w dyspozycji odbiorcy usług certyfikacyjnych.

Identyfikator polityki dla certyfikatów Standard Server wygląda następująco:

`iso(1) member-body(2) pl (616) organization(1) id-kir(113571) id-szafir(1) id-nkw(2) id-szafir-Server(9).`

3. ŚWIADCZENIE USŁUG CERTYFIKACYJNYCH

Podstawą świadczenia usług certyfikacyjnych jest zawarcie umowy na świadczenie usług certyfikacyjnych polegających na wydawaniu certyfikatów, zwanej dalej „Umową”.

Umowa 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 lub którzy będą odpowiedzialni za odbiór certyfikatów.

Podstawą wydania pierwszego oraz kolejnego certyfikatu, w tym odnowienia certyfikatu jest złożenie zamówienia oraz weryfikacja tożsamości subskrybenta i prawa do uzyskania certyfikatu. Sposób weryfikacji tożsamości oraz prawa do uzyskania certyfikatu zależy od rodzaju certyfikatu oraz od tego czy jest to pierwszy, czy też kolejny certyfikat dla danego subskrybenta. Szczegóły dotyczące wydania certyfikatu określa Kodeks.

Unieważnienie, zawieszenie lub odwieszenie certyfikatu może nastąpić tylko w odniesieniu do certyfikatu, którego okres ważności nie upłynął i może być zrealizowane na wniosek subskrybenta, podmiotu, którego dane są zawarte w certyfikacie, odbiorcy usług certyfikacyjnych, innej upoważnionej osoby lub samodzielnie przez KIR S.A. Szczegóły dotyczące zmiany statusu certyfikatu określa Kodeks.

4. SUBSKRYBENT

Subskrybent jest zobowiązany do przede wszystkim do ochrony posiadanego klucza prywatnego związanego z kluczem publicznym zawartym w wydanym mu przez KIR S.A. certyfikacie. W przypadku stwierdzenia lub podejrzenia naruszenia bezpieczeństwa klucza prywatnego subskrybent i odbiorca usług certyfikacyjnych zobowiązani są zgłosić do KIR S.A. wniosek o zawieszenie lub unieważnienie certyfikatu.

5. STRONA UFAJĄCA

Strona ufająca jest zobowiązana do wykorzystywania certyfikatów zgodnie z ich przeznaczeniem oraz do weryfikowania podpisu elektronicznego lub cyfrowego i poświadczenia elektronicznego w chwili dokonywania weryfikacji lub innym wiarygodnym momencie z wykorzystaniem listy zawieszonych i unieważnionych certyfikatów dla certyfikatów i zaświadczeń certyfikacyjnych wchodzących w skład właściwej ścieżki certyfikacji. Przed podjęciem jakichkolwiek czynności w zaufaniu do certyfikatu strona ufająca powinna zapoznać się z postanowieniami Kodeksu.

6. ZMIANY POLITYK, PUBLIKACJE

KIR S.A. ma prawo do okresowych aktualizacji Polityki. Po zatwierdzeniu przez KIR S.A. zmian zaktualizowana Polityka będzie publikowana na www.elektronicznypodpis.pl. Informacje dotyczące usług certyfikacyjnych świadczonych przez KIR S.A., w tym informacje na temat sposobu zawierania Umów, obsługi zamówień i odnowień certyfikatów są udostępniane wszystkim zainteresowanym na stronie internetowej KIR S.A. lub w placówkach KIR S.A.

Listy zawieszonych i unieważnionych certyfikatów są generowane przez KIR S.A. nie rzadziej niż co 24 godziny lub po zawieszeniu albo unieważnieniu certyfikatu. Aktualizacja list odbywa się nie później niż w ciągu 1 godziny od zawieszenia lub unieważnienia certyfikatu.

7. OPŁATY

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