POLITYKA CERTYFIKACJI KIR
dla
ZAUFANYCH CERTYFIKATÓW NIEKWALIFIKOWANYCH

Wersja 1.13

Historia dokumentu

Numer wersji	Status	Data wydania
1.0	Dokument zatwierdzony przez Zarząd KIR – wersja obowiązująca do 30 września 2012 r.	19.12.2011 r.
1.1.	Dokument zatwierdzony przez Zarząd KIR – wersja obowiązująca do 19 grudnia 2013 r.	1.10.2012 r.
1.2.	Dokument zatwierdzony przez Zarząd KIR – wersja obowiązująca do 24 kwietnia 2014 r.	20.12.2013 r.
1.3.	Dokument zatwierdzony przez Zarząd KIR – wersja obowiązująca do 19 listopada 2014 r.	18.04.2014 r.
1.4	Dokument zatwierdzony przez Zarząd KIR – wersja obowiązująca do 1 marca 2015 r.	13.11.2014 r.
1.5	Dokument zatwierdzony przez Zarząd KIR – wersja obowiązująca do 10 lipca 2016 r.	26.02.2015 r.
1.6	Dokument zatwierdzony przez Zarząd KIR – wersja obowiązująca do 6 maja 2018 r.	30.06.2016 r.
1.7	Dokument zatwierdzony przez Zarząd KIR – wersja obowiązująca od 7 maja 2018 r.	12.04.2018 r.
1.7	Przegląd dokumentu. Dokument aktualny	26.03.2020 r.
1.8	Dokument zatwierdzony przez Zarząd KIR – wersja obowiązująca od 1 września 2020 r. do 17 września 2020 r.	26.08.2020 r.
1.9	Dokument zatwierdzony przez Zarząd KIR – wersja obowiązująca od 18 września 2020 r. do 30 czerwca 2021 r.	17.09.2020 r.
1.10	Dokument zatwierdzony przez Zarząd KIR – wersja obowiązująca od 1 lipca 2021 r. do 11 października 2022 r.	23.06.2021 r.
1.11	Dokument zatwierdzony przez Zarząd KIR – wersja obowiązująca od 12 października 2022 r. do 19 października 2023 r.	12.10.2022 r.
1.12	Dokument zatwierdzony przez Zarząd KIR – wersja obowiązująca od 20 października 2023 r. do 2 kwietnia 2024 r.	20.10.2023 r.
1.13	Dokument zatwierdzony przez Zarząd KIR – wersja obowiązująca od 3 kwietnia 2024 r.	2.04.2024 r.

SPIS TREŚCI

1. WSTĘP

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

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

2. ZAKRES ZASTOSOWANIA POLITYKI CERTYFIKACJI

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

Certyfikaty, wydawane zgodnie z Kodeksem, nie są kwalifikowanymi certyfikatami. 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.

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

Odpowiedzialność KIR, w tym finansowa, odpowiedzialność subskrybenta, zamawiającego 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 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 TLS

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

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

Identyfikator polityki dla certyfikatów TLS wydanych do 31 sierpnia 2020 r. wyglądają następująco:

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

Identyfikatory polityk dla certyfikatów TLS wydanych po 1 września 2020 r. wyglądają następująco:

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

oraz dodatkowo jeden z poniższych identyfikatorów zgodności z Baseline Requirements Certificate Policy for the Issuance and Management of Publicly - Trusted Certificates:

- dla certyfikatów TLS DV:

  joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) domain-validated(1)

- dla certyfikatów TLS OV:

  joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) organization-validated(2)

2.3. Certyfikat testowy

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

W procesie wydawania certyfikatów testowych operator KIR 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 zamawiającego.

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)
```

2.4. Certyfikat Elixir

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

W procesie wydawania certyfikatów tego rodzaju operator KIR 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)
```

2.5. 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 weryfikuje tożsamość subskrybenta oraz jego prawo do uzyskania certyfikatu. Proces obejmuje również weryfikację, czy serwer lub domena pozostają w dyspozycji zamawiającego.

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).
```

2.6. Certyfikat S/MIME

Certyfikat S/MIME służy do zabezpieczenia poczty elektronicznej.

W procesie wydawania certyfikatów operator KIR weryfikuje tożsamość subskrybenta oraz jego prawo do uzyskania certyfikatu. Proces obejmuje również weryfikację, czy adres e-mail pozostaje w dyspozycji zamawiającego.

Identyfikatory polityk dla certyfikatów S/MIME wyglądają następująco:

iso(1) member-body(2) pl (616) organization(1) id-kir(113571) id-szafir(1) id-nkw(2) id-szafir-SMIME(10)

oraz dodatkowo jeden z poniższych idetyfikatorów zgodności z S/MIME Baseline Requirements - Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates

- dla certyfikatów S/MIME MV:

  joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) smime-baseline(5) mailbox-validated (1) multipurpose (2)

- dla certyfikatów S/MIME OV:

  joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) smime-baseline(5) organization-validated (2) multipurpose (2)

- dla certyfikatów S/MIME SV:

  joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) smime-baseline(5) sponsor-validated (3) multipurpose (2)

- dla certyfikatów S/MIME IV:

  joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) smime-baseline(5) individual-validated (4) multipurpose (2)

3. ŚWIADCZENIE USŁUG ZAUFANIA

Podstawą świadczenia usług zaufania jest zawarcie umowy na świadczenie usług zaufania 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 zamawiający 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, zamawiającego, innej upoważnionej osoby lub samodzielnie przez KIR. Szczegóły dotyczące zmiany statusu certyfikatu określa Kodeks.

4. SUBSKRYBENT

Subskrybent jest zobowiązany przede wszystkim do ochrony posiadanego klucza prywatnego związanego z kluczem publicznym zawartym w wydanym mu przez KIR certyfikacie. W przypadku stwierdzenia lub podejrzenia naruszenia bezpieczeństwa klucza prywatnego subskrybent i zamawiający zobowiązani są zgłosić do KIR 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 pieczęci elektronicznych w chwili dokonywania weryfikacji lub innym wiarygodnym momencie z wykorzystaniem listy zawieszonych i unieważnionych certyfikatów dla certyfikatów oraz pieczęci elektronicznych 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 przeprowadza co 12 miesięcy okresowy przegląd Polityki. Okresowy przegląd obejmuje weryfikację Polityki na zgodność z obowiązującymi wymaganiami CA/Browser Forum: Baseline Requirements, S/MIME Baseline Requirements oraz Mozilla Root Security Policy i Kodeksem.

Ponadto, zmiany w Polityce mogą być wprowadzane w zależności od potrzeb, w szczególności na skutek wykrycia błędów. Zmiany mogą również wynikać z sugestii zgłaszanych przez osoby zainteresowane.

Zmiany wprowadzane w Polityce nie mogą prowadzić do niezgodności lub sprzeczności z Kodeksem.

Po zatwierdzeniu przez KIR zmian zaktualizowana Polityka będzie publikowana na www.elektronicznypodpis.pl.

Informacje dotyczące usług zaufania świadczonych przez KIR, w tym informacje na temat sposobu zawierania Umów, obsługi zamówień i odnowień certyfikatów są udostępniane wszystkim zainteresowanym na stronie internetowej KIR lub w placówkach KIR.

Listy zawieszonych i unieważnionych certyfikatów są generowane przez KIR 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 zaufania określa cennik usług zaufania publikowany na stronie internetowej www.elektronicznypodpis.pl, Umowa, oferta lub inny dokument zawierający propozycje cenowe.