

Infrastruktura klucza publicznego IB

Identyfikator dokumentu (OID)	1.3.6.1.4.1.54634.2.1.0
Wersja	005
Data wprowadzenia w życie	2021-11-29
Data wygaśnięcia	do odwołania
Właściciel	Informatyka Bogusławski spółka z ograniczoną odpowiedzialnością sp.k.
Adres publikacji	http://www.ib.pl/pki/

Spis treści

1 Historia zmian.....	1
2 Wstęp.....	1
3 Certyfikaty CA.....	2
3.1 C=PL, O=Informatyka Bogusławski, CN=IB Root CA, serialNumber=20191115.....	2
3.1.1 C=PL, O=Informatyka Bogusławski, CN=IB Root CA OCSP.....	2
3.1.2 C=PL, O=Informatyka Bogusławski, CN=IB Authentication CA, serialNumber=RRRRMMDD.....	3
3.1.2.1 C=PL, O=Informatyka Bogusławski, CN=IB Authentication CA OCSP.....	3
3.1.3 C=PL, O=Informatyka Bogusławski, CN=cybo.pl CA, serialNumber=RRRRMMDD.....	4
3.1.3.1 C=PL, O=Informatyka Bogusławski, CN=cybo.pl CA OCSP.....	4
4 Certyfikaty końcowe.....	5
5 Pozostałe ustalenia.....	6

1 Historia zmian

Wersja	Data	Autor	Opis zmian
001	2019-11-29	Paweł Bogusławski	Utworzenie dokumentu.
002	2019-12-06	Paweł Bogusławski	Aktualizacja przeznaczenia certyfikatów w p. 3.1.3.
003	2020-09-08	Paweł Bogusławski	Aktualizacja przeznaczenia certyfikatów w p. 3.1.2. Dostosowanie informacji dotyczących indywidualnych postanowień umownych w p. 4 i p. 5.
004	2021-01-07	Paweł Bogusławski	Usunięcie serialNumber z certyfikatów OCSP w p. 3.
005	2021-11-29	Paweł Bogusławski	Zmiana podpisu elektronicznego pod CPS z osobistego na kwalifikowany.

2 Wstęp

Niniejszy dokument ustala zasady funkcjonowania infrastruktury klucza publicznego (PKI) spółki Informatyka Bogusławski spółka z ograniczoną odpowiedzialnością spółka komandytowa (zwana dalej „IB”) z siedzibą w Poznaniu, ul. Główna 6 (61-005 Poznań), wpisaną do Rejestru Przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy Poznań - Nowe Miasto i Wilda w Poznaniu, VIII Wydział Gospodarczy Krajowego Rejestru Sądowego pod nr KRS 0000374487, posiadającą NIP 9721223456, nr REGON 301636162.

3 Certyfikaty CA

W skład infrastruktury PKI IB wchodzi następujące certyfikaty CA (w atrybucie serialNumber znajduje się data wygenerowania danego certyfikatu w formacie RRRRMMDD):

3.1 C=PL, O=Informatyka Bogusławski, CN=IB Root CA, serialNumber=20191115

Poziom	1
Numer seryjny	22:11:e3:3e:cf:0c:10:2c:aa:1d:bf:a6:35:2e:e1:67:85:41:5e:7c
Identyfikator klucza	3d:68:cc:b8:e3:7e:c7:2b:3b:e0:59:8a:df:2e:6f:bd:7e:75:f3:4a
Odcisk palca (SHA-1)	e4:f7:cd:61:05:24:bf:4b:47:08:42:5e:7e:26:a1:0b:60:ee:db:a8
Algorytm klucza publicznego	RSA 4096 bit
Opis	<p>Certyfikat służący wyłącznie do podpisywania wymienionych w p. 3:</p> <ul style="list-style-type: none"> • certyfikatów pośrednich CA (subordinate CA), • certyfikatów podpisujących odpowiedzi OCSP dla certyfikatów podpisanych przez ten certyfikat. <p>Klucz prywatny certyfikatu wygenerowany i umieszczony w sprzętowych modułach kryptograficznych (HSM) będących własnością IB przez upoważnionych pracowników IB, bez możliwości skopiowania tego klucza w postaci jawnej poza HSM. Podpisywanie certyfikatów potomnych wykonywane przez upoważnionych pracowników IB, wyłącznie za pomocą upoważnionych systemów (oprogramowanie, komputery) będących własnością IB.</p>
Okres ważności	7305 dni (20 lat)
Adres publikacji certyfikatu	http://www.ib.pl/pki/

3.1.1 C=PL, O=Informatyka Bogusławski, CN=IB Root CA OCSP

Poziom	2
Algorytm klucza publicznego	RSA 2048 bit
Opis	<p>Certyfikaty podpisane przez certyfikat CA z CN=IB Root CA opisany w p. 3.1, służące wyłącznie do podpisywania odpowiedzi OCSP dla certyfikatów podpisanych przez ten certyfikat CA.</p> <p>Klucze prywatne certyfikatów generowane i umieszczane w systemach będących własnością IB przez upoważnionych pracowników IB. Podpisywanie odpowiedzi OCSP wyłącznie za pomocą upoważnionych systemów (oprogramowanie, komputery) będących własnością IB.</p>
Okres ważności	397 dni

3.1.2 C=PL, O=Informatyka Bogusławski, CN=IB Authentication CA, serialNumber=RRRRMMDD

Poziom	2
Algorytm klucza publicznego	RSA 2048 bit
Opis	<p>Certyfikaty pośrednie podpisane przez certyfikat CA z CN=IB Root CA opisany w p. 3.1, służące wyłącznie do podpisywania certyfikatów końcowych służących do:</p> <ul style="list-style-type: none">• uwierzytelniania pracowników IB,• uwierzytelniania systemów i usług IB,• uwierzytelniania systemów i usług wspieranych przez IB. <p>Klucze prywatne certyfikatów generowane i umieszczane w sprzętowych modułach kryptograficznych (HSM) będących własnością IB przez upoważnionych pracowników IB, bez możliwości skopiowania tych kluczy w postaci jawnej poza HSM. Podpisywanie certyfikatów potomnych wykonywane przez upoważnionych pracowników IB, wyłącznie za pomocą upoważnionych systemów (oprogramowanie, komputery) będących własnością IB.</p>
Okres ważności	3653 dni (10 lat)
Adres publikacji certyfikatu	http://www.ib.pl/pki/

3.1.2.1 C=PL, O=Informatyka Bogusławski, CN=IB Authentication CA OCSP

Poziom	3
Algorytm klucza publicznego	RSA 2048 bit
Opis	<p>Certyfikaty podpisane przez dany certyfikat CA opisany w p. 3.1.2, służące wyłącznie do podpisywania odpowiedzi OCSP dla certyfikatów podpisanych przez ten certyfikat CA.</p> <p>Klucze prywatne certyfikatów generowane i umieszczane w systemach będących własnością IB przez upoważnionych pracowników IB. Podpisywanie odpowiedzi OCSP wyłącznie za pomocą upoważnionych systemów (oprogramowanie, komputery) będących własnością IB.</p>
Okres ważności	397 dni

3.1.3 C=PL, O=Informatyka Bogusławski, CN=cybo.pl CA, serialNumber=RRRRMMDD

Poziom	2
Algorytm klucza publicznego	RSA 2048 bit
Opis	<p>Certyfikaty pośrednie podpisane przez certyfikat CA z CN=IB Root CA opisany w p. 3.1, służące wyłącznie do podpisywania certyfikatów końcowych służących do:</p> <ul style="list-style-type: none">• uwierzytelniania użytkowników w serwisach udostępnianych przez IB w ramach usługi cybo.pl,• uwierzytelniania autorów informacji przekazywanych do IB w ramach usługi cybo.pl. <p>Klucze prywatne certyfikatów generowane i umieszczane w sprzętowych modułach kryptograficznych (HSM) będących własnością IB przez upoważnionych pracowników IB, bez możliwości skopiowania tych kluczy w postaci jawnej poza HSM. Podpisywanie certyfikatów potomnych nadzorowane przez upoważnionych pracowników IB, wyłącznie za pomocą upoważnionych systemów (oprogramowanie, komputery) będących własnością IB.</p>
Okres ważności	3653 dni (10 lat)
Adres publikacji certyfikatu	http://www.ib.pl/pki/

3.1.3.1 C=PL, O=Informatyka Bogusławski, CN=cybo.pl CA OCSP

Poziom	3
Algorytm klucza publicznego	RSA 2048 bit
Opis	<p>Certyfikaty podpisane przez dany certyfikat CA opisany w p. 3.1.3, służące wyłącznie do podpisywania odpowiedzi OCSP dla certyfikatów podpisanych przez ten certyfikat CA.</p> <p>Klucze prywatne certyfikatów generowane i umieszczane w systemach będących własnością IB przez upoważnionych pracowników IB. Podpisywanie odpowiedzi OCSP, wyłącznie za pomocą upoważnionych systemów (oprogramowanie, komputery) będących własnością IB.</p>
Okres ważności	397 dni

4 Certyfikaty końcowe

Zasady opisane w tym punkcie dotyczą certyfikatów końcowych, które są podpisywane przez te z CA wymienionych w p. 3, które podpisują certyfikaty końcowe.

Infrastruktura PKI IB zapewnia zgodność z następującymi parametrami kluczy i certyfikatów końcowych (inne parametry mogą ale nie muszą być obsługiwane):

- klucze RSA o długościach 2048 lub 3072 lub 4096 bitów,
- funkcje skrótu SHA-256 lub SHA-512.

Maksymalny okres ważności certyfikatów końcowych wynosi 397 dni.

Ważność danego certyfikatu końcowego może być sprawdzona za pomocą usługi OCSP (ang. *Online Certificate Status Protocol*, zwanej dalej „OCSP”) udostępnionej przez IB pod adresem URL, który znajduje się w treści tego certyfikatu.

IB może unieważnić certyfikat końcowy w OCSP w następujących przypadkach:

- otrzymanie przez IB od właściciela certyfikatu końcowego żądania unieważnienia tego certyfikatu końcowego, zawierającego powód unieważnienia,
- ujawnienie osobom nieupoważnionym klucza prywatnego, do którego wystawiony został certyfikat końcowy,
- wystawienie certyfikatu końcowego wadliwie lub z naruszeniem prawa lub z naruszeniem umów zawartych z IB,
- naruszenie bezpieczeństwa systemów lub danych IB, które skutkuje brakiem zaufania do wystawionego certyfikatu końcowego.

IB unieważnia certyfikat końcowy w OCSP w terminie do 3 dni od momentu otrzymania przez IB informacji o zdarzeniu uzasadniającym unieważnienie zgodnie z postanowieniami niniejszego punktu.

W przypadku unieważnienia certyfikatu końcowego w OCSP z winy IB, IB zapewni właścicielowi nowy, ważny certyfikat podpisany zgodnie z postanowieniami niniejszego dokumentu, posiadający parametry funkcjonalne (np. pozostały okres ważności, dane) odpowiadające certyfikatowi unieważnionemu w OCSP.

W przypadku umieszczenia w certyfikacie końcowym danych osobowych, będą one przetwarzane przez IB w celu obsługi certyfikatu przez cały okres ważności certyfikatu oraz przez następne 10 lat, zgodnie z [Polityką prywatności IB](#).

IB nie ponosi odpowiedzialności za użycie certyfikatów końcowych w celach innych niż opisane w niniejszym dokumencie.

IB zastrzega sobie prawo do ustalenia treści wszystkich informacji umieszczonych w certyfikacie końcowym, za wyjątkiem danych klucza tego certyfikatu końcowego.

Właściciel certyfikatu zobowiązany jest do sprawdzenia poprawności otrzymanego od IB certyfikatu końcowego przed rozpoczęciem korzystania z niego a w przypadku stwierdzenia problemu – powstrzymanie się od korzystania z niego i zgłoszenie problemu do IB.

IB nie oferuje usług zarządzania kluczami certyfikatów końcowych (np. generowanie, instalowanie, wybór oprogramowania/sprzętu).

Wyłącznie odpowiedzialność za bezpieczeństwo kluczy prywatnych do certyfikatów końcowych (w tym proces generowania klucza prywatnego certyfikatu końcowego, jego długość, algorytm, przechowywanie, poufność, ograniczenia dostępu) ponosi właściciel tych kluczy prywatnych.

5 Pozostałe ustalenia

Termin „dzień” używany w niniejszym dokumencie oznacza dzień kalendarzowy (24 godziny).

Okres ważności certyfikatów liczony jest od momentu podpisania certyfikatu przez CA.

IB nie instaluje certyfikatów CA opisanych w p. 3 jako zaufanych w powszechnie dostępnych systemach ani nie wnioskuję o takie instalowanie.

Podmioty, które instalują certyfikaty opisane w p. 3 jako zaufane robią to w oparciu o własną ocenę ich bezpieczeństwa i na własne ryzyko.

IB nie oferuje żadnych zabezpieczeń ani ubezpieczeń w związku z korzystaniem z certyfikatów opisanych w p. 3 lub certyfikatów przez nie podpisanych.

Postanowienia z p. 4 oraz z p. 5 mogą zostać zmienione w przypadku certyfikatów końcowych podpisywanych dla określonego podmiotu, w indywidualnej umowie zawartej między IB a tym podmiotem.

Niniejszy dokument został sporządzony w postaci elektronicznej i został opatrzony [kwalifikowanym podpisem elektronicznym](#) przez osobę lub osoby upoważnione do reprezentowania IB zgodnie z wpisem do KRS nr 0000374487.