

OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia jest dostawa certyfikatów o następujących specyfikacjach technicznych:

- 1) Certyfikat SSL MultiDomain Wildcard (dla wielu domen) klasy OV (Organization Validation) dla stron internetowych z domeny *.ms.gov.pl:
 - okres ważności: 12 miesięcy od daty wygenerowania certyfikatu;
 - liczba domen - wildcard z alternatywną nazwą podmiotu;
 - Subject:
E=postmaster@ms.gov.pl
CN=*.ms.gov.pl S=mazowieckie
L=Warszawa
O=Ministerstwo Sprawiedliwości
C=PL
 - Alternatywna nazwa podmiotu
Nazwa DNS=*.ms.gov.pl
Nazwa DNS=ms.gov.pl
Nazwa DNS=*.apps.ocp.prod.ms.gov.pl
Nazwa DNS=*.apps.ocp.pprod.ms.gov.pl
Nazwa DNS=*.apps.ocp.tst.ms.gov.pl
Nazwa DNS=*.apps.ocp.roz.ms.gov.pl
Nazwa DNS=*.apps.prs-nprod-ocp.ms.gov.pl
Nazwa DNS=*.apps.prs-prod-ocp.ms.gov.pl
Nazwa DNS=*.apps.krs-nprod-ocp.ms.gov.pl
Nazwa DNS=*.apps.krs-prod-ocp.ms.gov.pl
Nazwa DNS=*.apps.ekw-nprod-ocp.ms.gov.pl
Nazwa DNS=*.apps.ekw-prod-ocp.ms.gov.pl
 - certyfikat typu OV (Organization Validation);
 - zgodność ze standardem X.509 v.3 (RFC5280);
 - zabezpieczony funkcją skrótu SHA2;
 - obsługa siły szyfrowania połączeń do 256 bitów;
 - wsparcie dla SGC (Server Gated Cryptography);
 - obsługa kluczy o długości 4096 bitów i więcej
 - minimalna długość kluczy kryptograficznych: RSA lub DSA 2048 bit, EC 571 bit: NIST K-571 oraz NIST B-571;
 - możliwa jest weryfikacja statusu certyfikatu przy pomocy list CRL oraz protokołu OCSP;
 - musi pełnić ochronę przed phishingiem, oszustwami online, fałszowaniem oraz przechwyceniem danych;
 - musi posiadać dane organizacji w certyfikacie;
 - musi być kompatybilny z urządzeniami mobilnymi;

- pomoc techniczna w języku polskim;
 - certyfikat dostarczony w formacie pliku *.pfx;
 - możliwość instalacji na nieograniczonej liczbie serwerów fizycznych.
- 2) Certyfikat SSL klasy OV (Organization Validation) dla strony internetowej afs.gov.pl:
- okres ważności: 12 miesięcy od daty wygenerowania certyfikatu;
 - liczba domen - pojedyncza nazwa domenowa;
 - Subject:
E=postmaster@ms.gov.pl
CN=afs.gov.pl
S=mazowieckie
L=Warszawa
O=Ministerstwo Sprawiedliwości
C=PL
 - Alternatywna nazwa podmiotu
Nazwa DNS=afs.gov.pl
Nazwa DNS=www.afs.gov.pl
 - certyfikat typu OV (Organization Validation);
 - zgodność ze standardem X.509 v.3 (RFC5280);
 - zabezpieczony funkcją skrótu SHA2;
 - obsługa siły szyfrowania połączeń do 256 bitów;
 - wsparcie dla SGC (Server Gated Cryptography);
 - obsługa kluczy o długości 4096 bitów i więcej
 - minimalna długość kluczy kryptograficznych: RSA lub DSA 2048 bit, EC 571 bit: NIST K-571 oraz NIST B-571;
 - możliwa jest weryfikacja statusu certyfikatu przy pomocy list CRL oraz protokołu OCSP;
 - musi pełnić ochronę przed phishingiem, oszustwami online, fałszowaniem oraz przechwyceniem danych;
 - musi posiadać dane organizacji w certyfikacie;
 - musi być kompatybilny z urządzeniami mobilnymi;
 - pomoc techniczna w języku polskim;
 - możliwość instalacji na nieograniczonej liczbie serwerów fizycznych.
- 3) Certyfikat SSL klasy OV (Organization Validation) dla strony internetowej funduszsprawiedliwosci.gov.pl:
- okres ważności: 12 miesięcy od daty wygenerowania certyfikatu;
 - liczba domen - pojedyncza nazwa domenowa;
 - Subject:
E=postmaster@ms.gov.pl
CN= funduszsprawiedliwosci.gov.pl
S=mazowieckie
L=Warszawa
O=Ministerstwo Sprawiedliwości
C=PL
 - Alternatywna nazwa podmiotu
Nazwa DNS= funduszsprawiedliwosci.gov.pl
Nazwa DNS= www.funduszsprawiedliwosci.gov.pl
 - certyfikat typu OV (Organization Validation);
 - zgodność ze standardem X.509 v.3 (RFC5280);
 - zabezpieczony funkcją skrótu SHA2;
 - obsługa siły szyfrowania połączeń do 256 bitów;

- wsparcie dla SGC (Server Gated Cryptography);
 - obsługa kluczy o długości 4096 bitów i więcej
 - minimalna długość kluczy kryptograficznych: RSA lub DSA 2048 bit, EC 571 bit: NIST K-571 oraz NIST B-571;
 - możliwa jest weryfikacja statusu certyfikatu przy pomocy list CRL oraz protokołu OCSP;
 - musi pełnić ochronę przed phishingiem, oszustwami online, fałszowaniem oraz przechwyceniem danych;
 - musi posiadać dane organizacji w certyfikacie;
 - musi być kompatybilny z urządzeniami mobilnymi;
 - pomoc techniczna w języku polskim;
 - możliwość instalacji na nieograniczonej liczbie serwerów fizycznych
- 4) Certyfikat SSL klasy OV (Organization Validation) dla strony internetowej si-dla-sprawiedliwosci.gov.pl:
- okres ważności: 12 miesięcy od daty wygenerowania certyfikatu;
 - liczba domen - pojedyncza nazwa domenowa;
 - Subject:
E=postmaster@ms.gov.pl
CN= si-dla-sprawiedliwosci.gov.pl
S=mazowieckie
L=Warszawa
O=Ministerstwo Sprawiedliwości
C=PL
 - Alternatywna nazwa podmiotu
Nazwa DNS= si-dla-sprawiedliwosci.gov.pl
Nazwa DNS= www. si-dla-sprawiedliwosci.gov.pl
 - certyfikat typu OV (Organization Validation);
 - zgodność ze standardem X.509 v.3 (RFC5280);
 - zabezpieczony funkcją skrótu SHA2;
 - obsługa siły szyfrowania połączeń do 256 bitów;
 - wsparcie dla SGC (Server Gated Cryptography);
 - obsługa kluczy o długości 4096 bitów i więcej
 - minimalna długość kluczy kryptograficznych: RSA lub DSA 2048 bit, EC 571 bit: NIST K-571 oraz NIST B-571;
 - możliwa jest weryfikacja statusu certyfikatu przy pomocy list CRL oraz protokołu OCSP;
 - musi pełnić ochronę przed phishingiem, oszustwami online, fałszowaniem oraz przechwyceniem danych;
 - musi posiadać dane organizacji w certyfikacie;
 - musi być kompatybilny z urządzeniami mobilnymi;
 - pomoc techniczna w języku polskim;
 - możliwość instalacji na nieograniczonej liczbie serwerów fizycznych.
- 5) OPCJA 1 - Certyfikat SSL MultiDomain Wildcard klasy OV (Organization Validation) o specyfikacji technicznej jak dla certyfikatu w pkt 1 powyżej, na okres 12 miesięcy od daty wygenerowania certyfikatu;
- 6) OPCJA 2 - Certyfikat SSL MultiDomain Wildcard klasy OV (Organization Validation) o specyfikacji technicznej jak dla certyfikatu w pkt 1 powyżej, na okres 12 miesięcy od daty wygenerowania certyfikatu;

- 7) OPCJA 3 - Certyfikat SSL MultiDomain Wildcard klasy OV (Organization Validation) o specyfikacji technicznej jak dla certyfikatu w pkt 1 powyżej, na okres 12 miesięcy od daty wygenerowania certyfikatu;
- 8) OPCJA 4 - Certyfikat SSL klasy OV (Organization Validation) o specyfikacji technicznej jak dla certyfikatu w pkt 2 powyżej, dla zabezpieczenia strony internetowej, której adres Zamawiający wskaże nie później niż w chwili generowania certyfikatu, na okres 12 miesięcy od daty wygenerowania certyfikatu;
- 9) OPCJA 5 - Certyfikat SSL klasy OV (Organization Validation) o specyfikacji technicznej jak dla certyfikatu w pkt 2 powyżej, dla zabezpieczenia strony internetowej, której adres Zamawiający wskaże nie później niż w chwili generowania certyfikatu, na okres 12 miesięcy od daty wygenerowania certyfikatu;
- 10) OPCJA 6 - Certyfikat SSL klasy OV (Organization Validation) o specyfikacji technicznej jak dla certyfikatu w pkt 2 powyżej, dla zabezpieczenia strony internetowej, której adres Zamawiający wskaże nie później niż w chwili generowania certyfikatu, na okres 12 miesięcy od daty wygenerowania certyfikatu;
- 11) OPCJA 7 - Certyfikat SSL klasy OV (Organization Validation) o specyfikacji technicznej jak dla certyfikatu w pkt 2 powyżej, dla zabezpieczenia strony internetowej, której adres Zamawiający wskaże nie później niż w chwili generowania certyfikatu, na okres 12 miesięcy od daty wygenerowania certyfikatu;
- 12) OPCJA 8 - Certyfikat SSL klasy OV (Organization Validation) o specyfikacji technicznej jak dla certyfikatu w pkt 2 powyżej, dla zabezpieczenia strony internetowej, której adres Zamawiający wskaże nie później niż w chwili generowania certyfikatu, na okres 12 miesięcy od daty wygenerowania certyfikatu;
- 13) OPCJA 9 - Certyfikat SSL klasy OV (Organization Validation) o specyfikacji technicznej jak dla certyfikatu w pkt 2 powyżej, dla zabezpieczenia strony internetowej, której adres Zamawiający wskaże nie później niż w chwili generowania certyfikatu, na okres 12 miesięcy od daty wygenerowania certyfikatu;
- 14) OPCJA 10 - Certyfikat SSL klasy OV (Organization Validation) o specyfikacji technicznej jak dla certyfikatu w pkt 2 powyżej, dla zabezpieczenia strony internetowej, której adres Zamawiający wskaże nie później niż w chwili generowania certyfikatu, na okres 12 miesięcy od daty wygenerowania certyfikatu;
- 15) OPCJA 11 - Certyfikat SSL klasy OV (Organization Validation) o specyfikacji technicznej jak dla certyfikatu w pkt 2 powyżej, dla zabezpieczenia strony internetowej, której adres Zamawiający wskaże nie później niż w chwili generowania certyfikatu, na okres 12 miesięcy od daty wygenerowania certyfikatu;
- 16) OPCJA 12 - Certyfikat SSL klasy OV (Organization Validation) o specyfikacji technicznej jak dla certyfikatu w pkt 2 powyżej, dla zabezpieczenia strony internetowej, której adres Zamawiający wskaże nie później niż w chwili generowania certyfikatu, na okres 12 miesięcy od daty wygenerowania certyfikatu;
- 17) OPCJA 13 - Certyfikat SSL klasy OV (Organization Validation) o specyfikacji technicznej jak dla certyfikatu w pkt 2 powyżej, dla zabezpieczenia strony internetowej, której adres Zamawiający wskaże nie później niż w chwili generowania certyfikatu, na okres 12 miesięcy od daty wygenerowania certyfikatu;
- 18) OPCJA 14 - Certyfikat SSL klasy OV (Organization Validation) o specyfikacji technicznej jak dla certyfikatu w pkt 2 powyżej, dla zabezpieczenia strony internetowej, której adres Zamawiający wskaże nie później niż w chwili generowania certyfikatu, na okres 12 miesięcy od daty wygenerowania certyfikatu;
- 19) OPCJA 15 - Certyfikat SSL klasy OV (Organization Validation) o specyfikacji technicznej jak dla certyfikatu w pkt 2 powyżej, dla zabezpieczenia strony internetowej, której adres Zamawiający wskaże nie później niż w chwili generowania certyfikatu, na okres 12 miesięcy od daty wygenerowania certyfikatu;

- [illegible]

- której adres Zamawiający wskaże nie później niż w chwili generowania certyfikatu, na okres 12 miesięcy od daty wygenerowania certyfikatu
- 33) OPCJA 29 - Certyfikat SSL klasy OV (Organization Validation) o specyfikacji technicznej jak dla certyfikatu w pkt 2 powyżej, dla zabezpieczenia strony internetowej, której adres Zamawiający wskaże nie później niż w chwili generowania certyfikatu, na okres 12 miesięcy od daty wygenerowania certyfikatu
- 34) OPCJA 30 - Certyfikat SSL klasy OV (Organization Validation) o specyfikacji technicznej jak dla certyfikatu w pkt 2 powyżej, dla zabezpieczenia strony internetowej, której adres Zamawiający wskaże nie później niż w chwili generowania certyfikatu, na okres 12 miesięcy od daty wygenerowania certyfikatu
- 35) OPCJA 31 - Certyfikat SSL klasy OV (Organization Validation) o specyfikacji technicznej jak dla certyfikatu w pkt 2 powyżej, dla zabezpieczenia strony internetowej, której adres Zamawiający wskaże nie później niż w chwili generowania certyfikatu, na okres 12 miesięcy od daty wygenerowania certyfikatu
- 36) OPCJA 32 - Certyfikat SSL klasy OV (Organization Validation) o specyfikacji technicznej jak dla certyfikatu w pkt 2 powyżej, dla zabezpieczenia strony internetowej, której adres Zamawiający wskaże nie później niż w chwili generowania certyfikatu, na okres 12 miesięcy od daty wygenerowania certyfikatu
- 37) OPCJA 33 - Certyfikat SSL klasy OV (Organization Validation) o specyfikacji technicznej jak dla certyfikatu w pkt 2 powyżej, dla zabezpieczenia strony internetowej, której adres Zamawiający wskaże nie później niż w chwili generowania certyfikatu, na okres 12 miesięcy od daty wygenerowania certyfikatu
- 38) OPCJA 34 – Certyfikat SSL MultiDomain Wildcard klasy OV (Organization Validation) zabezpieczający jedną domeną wildcardową, którą Zamawiający wskaże nie później niż w chwili generowania certyfikatu, na okres 12 miesięcy od daty wygenerowania certyfikatu o specyfikacji technicznej:
- certyfikat typu OV (Organization Validation);
 - zgodność ze standardem X.509 v.3 (RFC5280);
 - zabezpieczony funkcją skrótu SHA2;
 - obsługa siły szyfrowania połączeń do 256 bitów;
 - wsparcie dla SGC (Server Gated Cryptography);
 - obsługa kluczy o długości 4096 bitów i więcej
 - minimalna długość kluczy kryptograficznych: RSA lub DSA 2048 bit, EC 571 bit: NIST K-571 oraz NIST B-571;
 - możliwa jest weryfikacja statusu certyfikatu przy pomocy list CRL oraz protokołu OCSP;
 - musi pełnić ochronę przed phishingiem, oszustwami online, fałszowaniem oraz przechwyceniem danych;
 - musi posiadać dane organizacji w certyfikacie;
 - musi być kompatybilny z urządzeniami mobilnymi;
 - pomoc techniczna w języku polskim;
 - certyfikat dostarczony w formacie pliku *.pfx;
 - możliwość instalacji na nieograniczonej liczbie serwerów fizycznych
- 39) OPCJA 35 - Certyfikat SSL MultiDomain Wildcard klasy OV (Organization Validation) zabezpieczający jedną domeną wildcardową, którą Zamawiający wskaże nie później niż w chwili generowania certyfikatu o specyfikacji technicznej, którą wskazano w Opcji nr 34 powyżej na okres 12 miesięcy od daty wygenerowania certyfikatu
- 40) OPCJA 36 - Certyfikat SSL MultiDomain Wildcard klasy OV (Organization Validation) zabezpieczający jedną domeną wildcardową, którą Zamawiający wskaże nie później

niż w chwili generowania certyfikatu o specyfikacji technicznej, którą wskazano w Opcji nr 34 powyżej na okres 12 miesięcy od daty wygenerowania certyfikatu,

41) Opcja 37 - Certyfikat SSL MultiDomain Wildcard klasy OV (Organization Validation) zabezpieczający jedną domeną wildcardową, którą Zamawiający wskaże nie później niż w chwili generowania certyfikatu, o specyfikacji technicznej, którą wskazano w Opcji nr 34 powyżej na okres 12 miesięcy od daty wygenerowania certyfikatu,

42) Opcja 38 – Certyfikat SSL MultiDomain Wildcard klasy OV (Organization Validation) zabezpieczający jedenaście domen wildcardowych, które Zamawiający wskaże nie później niż w chwili generowania certyfikatu, na okres 12 miesięcy od daty wygenerowania certyfikatu o specyfikacji technicznej:

- zgodność ze standardem X.509 v.3 (RFC5280)
- zabezpieczony funkcją skrótu SHA2
- obsługa siły szyfrowania połączeń do 256 bitów
- wsparcie dla SGC (Server Gated Cryptography)
- obsługa kluczy o długości RSA 2048 bitów
- minimalna długość kluczy kryptograficznych: RSA lub DSA 2048 bit, EC 571 bit: NIST K-571 oraz NIST B-571
- możliwa jest weryfikacja statusu certyfikatu przy pomocy list CRL oraz protokołu OCSP
- Obsługa 11 domen wildcard w polu SAN

43) Opcja 39 - Certyfikat SSL MultiDomain Wildcard klasy OV (Organization Validation) zabezpieczający jedenaście domen wildcardowych, które Zamawiający wskaże nie później niż w chwili generowania certyfikatu, o specyfikacji technicznej, którą wskazano w Opcji nr 38 powyżej na okres 12 miesięcy od daty wygenerowania certyfikatu,

44) Opcja 40 - Certyfikat SSL MultiDomain Wildcard klasy OV (Organization Validation) zabezpieczający jedenaście domen wildcardowych, które Zamawiający wskaże nie później niż w chwili generowania certyfikatu, o specyfikacji technicznej, którą wskazano w Opcji nr 38 powyżej na okres 12 miesięcy od daty wygenerowania certyfikatu.