

## OPIS PRZEDMIOTU ZAMÓWIENIA

1. 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: certyfikat wydawany na maksymalny okres dopuszczony obowiązującymi przepisami oraz wytycznymi CA/Browser Forum. Jednocześnie Wykonawca zapewni ciągłość posiadania ważnego certyfikatu przez 12 miesięcy poprzez wydanie kolejnych certyfikatów (reissue/odnowienie) w ramach wynagrodzenia, przy czym ważność każdego pojedynczego certyfikatu będzie każdorazowo zgodna z limitami obowiązującymi w dacie jego wydania;
- data wygaśnięcia obecnego certyfikatu: 11 czerwca 2026 r.
- liczba domen - wildcard z alternatywną nazwą podmiotu;
  - Subject:  
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 kluczy o długości 4096 bitów i więcej
  - minimalna długość kluczy kryptograficznych: RSA 2048 i wyższe (tj 2048, 3072, 4096) oraz ECDSA NIST P-256, NIST P-384;
  - możliwa jest weryfikacja statusu certyfikatu przy pomocy list CRL oraz protokołu OCSP;
  - 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: certyfikat wydawany na maksymalny okres dopuszczony obowiązującymi przepisami oraz wytycznymi CA/Browser Forum. Jednocześnie Wykonawca zapewni ciągłość posiadania ważnego certyfikatu przez 12 miesięcy poprzez wydanie kolejnych certyfikatów (reissue/odnowienie) w ramach wynagrodzenia, przy czym ważność każdego pojedynczego certyfikatu będzie każdorazowo zgodna z limitami obowiązującymi w dacie jego wydania;
  - data wygaśnięcia obecnego certyfikatu: 29 czerwca 2026 r.
  - liczba domen - pojedyncza nazwa domenowa;
    - Subject:  
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 kluczy o długości 4096 bitów i więcej
  - minimalna długość kluczy kryptograficznych: RSA 2048 i wyższe (tj 2048, 3072, 4096) oraz ECDSA NIST P-256, NIST P-384;
  - możliwa jest weryfikacja statusu certyfikatu przy pomocy list CRL oraz protokołu OCSP;
  - 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: certyfikat wydawany na maksymalny okres dopuszczony obowiązującymi przepisami oraz wytycznymi CA/Browser Forum. Jednocześnie Wykonawca zapewni ciągłość posiadania ważnego certyfikatu przez 12 miesięcy poprzez wydanie kolejnych certyfikatów (reissue/odnowienie) w ramach

wynagrodzenia, przy czym ważność każdego pojedynczego certyfikatu będzie każdorazowo zgodna z limitami obowiązującymi w dacie jego wydania;

- data wygaśnięcia obecnego certyfikatu: 1 lipca 2026 r.
  - liczba domen - pojedyncza nazwa domenowa;
    - Subject:  
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 kluczy o długości 4096 bitów i więcej
  - minimalna długość kluczy kryptograficznych: RSA 2048 i wyższe (tj 2048, 3072, 4096) oraz ECDSA NIST P-256, NIST P-384;
  - możliwa jest weryfikacja statusu certyfikatu przy pomocy list CRL oraz protokołu OCSP;
  - 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: certyfikat wydawany na maksymalny okres dopuszczony obowiązującymi przepisami oraz wytycznymi CA/Browser Forum. Jednocześnie Wykonawca zapewni ciągłość posiadania ważnego certyfikatu przez 12 miesięcy poprzez wydanie kolejnych certyfikatów (reissue/odnowienie) w ramach wynagrodzenia, przy czym ważność każdego pojedynczego certyfikatu będzie każdorazowo zgodna z limitami obowiązującymi w dacie jego wydania
  - data wygaśnięcia obecnego certyfikatu: 2 września 2026 r.
  - liczba domen - pojedyncza nazwa domenowa;
    - Subject:  
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 kluczy o długości 4096 bitów i więcej
  - minimalna długość kluczy kryptograficznych: RSA 2048 i wyższe (tj 2048, 3072, 4096) oraz ECDSA NIST P-256, NIST P-384;
  - możliwa jest weryfikacja statusu certyfikatu przy pomocy list CRL oraz protokołu OCSP;
  - 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) zabezpieczający wiele domen, które Zamawiający wskaże nie później niż w chwili generowania certyfikatu o specyfikacji technicznej:
- okres ważności: certyfikat wydawany na maksymalny okres dopuszczony obowiązującymi przepisami oraz wytycznymi CA/Browser Forum. Jednocześnie Wykonawca zapewni ciągłość posiadania ważnego certyfikatu przez 12 miesięcy poprzez wydanie kolejnych certyfikatów (reissue/odnowienie) w ramach wynagrodzenia, przy czym ważność każdego pojedynczego certyfikatu będzie każdorazowo zgodna z limitami obowiązującymi w dacie jego wydania;
  - liczba domen tożsama jak dla certyfikatu w pkt 1
  - certyfikat typu OV (Organization Validation);
  - zgodność ze standardem X.509 v.3 (RFC5280);
  - zabezpieczony funkcją skrótu SHA2;
  - obsługa kluczy o długości 4096 bitów i więcej
  - minimalna długość kluczy kryptograficznych: RSA 2048 i wyższe (tj 2048, 3072, 4096) oraz ECDSA NIST P-256, NIST P-384;
  - możliwa jest weryfikacja statusu certyfikatu przy pomocy list CRL oraz protokołu OCSP;
  - 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.
- 6) OPCJA 2 - Certyfikat SSL klasy OV (Organization Validation) zgodnie z wymaganiami jak dla certyfikatu w pkt 2 powyżej, dla zabezpieczenia strony internetowej, której adres Zamawiający wskaże nie później niż w chwili generowania certyfikatu. Certyfikat wydawany na maksymalny okres dopuszczony obowiązującymi przepisami oraz wytycznymi CA/Browser Forum. Jednocześnie Wykonawca zapewni ciągłość posiadania ważnego certyfikatu przez 12 miesięcy poprzez wydanie kolejnych certyfikatów (reissue/odnowienie) w ramach wynagrodzenia, przy czym ważność każdego pojedynczego certyfikatu będzie każdorazowo zgodna z limitami obowiązującymi w dacie jego wydania;
- 7) OPCJA 3 - Certyfikat SSL klasy OV (Organization Validation) zgodnie z wymaganiami jak dla certyfikatu w pkt 2 powyżej, dla zabezpieczenia strony internetowej, której adres Zamawiający wskaże nie później niż w chwili generowania certyfikatu. Certyfikat wydawany na maksymalny okres dopuszczony obowiązującymi przepisami oraz wytycznymi CA/Browser Forum. Jednocześnie Wykonawca zapewni ciągłość posiadania ważnego certyfikatu przez 12 miesięcy poprzez wydanie kolejnych certyfikatów (reissue/odnowienie) w ramach wynagrodzenia, przy czym ważność

- każdego pojedynczego certyfikatu będzie każdorazowo zgodna z limitami obowiązującymi w dacie jego wydania;
- 8) OPCJA 4 - Certyfikat SSL klasy OV (Organization Validation) zgodnie z wymaganiami jak dla certyfikatu w pkt 2 powyżej, dla zabezpieczenia strony internetowej, której adres Zamawiający wskaże nie później niż w chwili generowania certyfikatu. Certyfikat wydawany na maksymalny okres dopuszczony obowiązującymi przepisami oraz wytycznymi CA/Browser Forum. Jednocześnie Wykonawca zapewni ciągłość posiadania ważnego certyfikatu przez 12 miesięcy poprzez wydanie kolejnych certyfikatów (reissue/odnowienie) w ramach wynagrodzenia, przy czym ważność każdego pojedynczego certyfikatu będzie każdorazowo zgodna z limitami obowiązującymi w dacie jego wydania;
  - 9) OPCJA 5 - Certyfikat SSL klasy OV (Organization Validation) zgodnie z wymaganiami jak dla certyfikatu w pkt 2 powyżej, dla zabezpieczenia strony internetowej, której adres Zamawiający wskaże nie później niż w chwili generowania certyfikatu. Certyfikat wydawany na maksymalny okres dopuszczony obowiązującymi przepisami oraz wytycznymi CA/Browser Forum. Jednocześnie Wykonawca zapewni ciągłość posiadania ważnego certyfikatu przez 12 miesięcy poprzez wydanie kolejnych certyfikatów (reissue/odnowienie) w ramach wynagrodzenia, przy czym ważność każdego pojedynczego certyfikatu będzie każdorazowo zgodna z limitami obowiązującymi w dacie jego wydania;
  - 10) OPCJA 6 - Certyfikat SSL klasy OV (Organization Validation) zgodnie z wymaganiami jak dla certyfikatu w pkt 2 powyżej, dla zabezpieczenia strony internetowej, której adres Zamawiający wskaże nie później niż w chwili generowania certyfikatu. Certyfikat wydawany na maksymalny okres dopuszczony obowiązującymi przepisami oraz wytycznymi CA/Browser Forum. Jednocześnie Wykonawca zapewni ciągłość posiadania ważnego certyfikatu przez 12 miesięcy poprzez wydanie kolejnych certyfikatów (reissue/odnowienie) w ramach wynagrodzenia, przy czym ważność każdego pojedynczego certyfikatu będzie każdorazowo zgodna z limitami obowiązującymi w dacie jego wydania;
  - 11) OPCJA 7 - Certyfikat SSL klasy OV (Organization Validation) zgodnie z wymaganiami jak dla certyfikatu w pkt 2 powyżej, dla zabezpieczenia strony internetowej, której adres Zamawiający wskaże nie później niż w chwili generowania certyfikatu. Certyfikat wydawany na maksymalny okres dopuszczony obowiązującymi przepisami oraz wytycznymi CA/Browser Forum. Jednocześnie Wykonawca zapewni ciągłość posiadania ważnego certyfikatu przez 12 miesięcy poprzez wydanie kolejnych certyfikatów (reissue/odnowienie) w ramach wynagrodzenia, przy czym ważność każdego pojedynczego certyfikatu będzie każdorazowo zgodna z limitami obowiązującymi w dacie jego wydania;
  - 12) OPCJA 8 - Certyfikat SSL klasy OV (Organization Validation) zgodnie z wymaganiami jak dla certyfikatu w pkt 2 powyżej, dla zabezpieczenia strony internetowej, której adres Zamawiający wskaże nie później niż w chwili generowania certyfikatu. Certyfikat wydawany na maksymalny okres dopuszczony obowiązującymi przepisami oraz wytycznymi CA/Browser Forum. Jednocześnie Wykonawca zapewni ciągłość posiadania ważnego certyfikatu przez 12 miesięcy poprzez wydanie kolejnych certyfikatów (reissue/odnowienie) w ramach wynagrodzenia, przy czym ważność każdego pojedynczego certyfikatu będzie każdorazowo zgodna z limitami obowiązującymi w dacie jego wydania;

- 13) OPCJA 9 - Certyfikat SSL klasy OV (Organization Validation) zgodnie z wymaganiami jak dla certyfikatu w pkt 2 powyżej, dla zabezpieczenia strony internetowej, której adres Zamawiający wskaże nie później niż w chwili generowania certyfikatu. Certyfikat wydawany na maksymalny okres dopuszczony obowiązującymi przepisami oraz wytycznymi CA/Browser Forum. Jednocześnie Wykonawca zapewni ciągłość posiadania ważnego certyfikatu przez 12 miesięcy poprzez wydanie kolejnych certyfikatów (reissue/odnowienie) w ramach wynagrodzenia, przy czym ważność każdego pojedynczego certyfikatu będzie każdorazowo zgodna z limitami obowiązującymi w dacie jego wydania;
- 14) OPCJA 10 – Certyfikat SSL MultiDomain Wildcard klasy OV (Organization Validation) zabezpieczający dwie domeny wildcardowe, które Zamawiający wskaże nie później niż w chwili generowania certyfikatu o specyfikacji technicznej:
- okres ważności: certyfikat wydawany na maksymalny okres dopuszczony obowiązującymi przepisami oraz wytycznymi CA/Browser Forum. Jednocześnie Wykonawca zapewni ciągłość posiadania ważnego certyfikatu przez 12 miesięcy poprzez wydanie kolejnych certyfikatów (reissue/odnowienie) w ramach wynagrodzenia, przy czym ważność każdego pojedynczego certyfikatu będzie każdorazowo zgodna z limitami obowiązującymi w dacie jego wydania;
  - certyfikat typu OV (Organization Validation);
  - zgodność ze standardem X.509 v.3 (RFC5280);
  - zabezpieczony funkcją skrótu SHA2;
  - obsługa kluczy o długości 4096 bitów i więcej
  - minimalna długość kluczy kryptograficznych: RSA 2048 i wyższe (tj 2048, 3072, 4096) oraz ECDSA NIST P-256, NIST P-384;
  - możliwa jest weryfikacja statusu certyfikatu przy pomocy list CRL oraz protokołu OCSP;
  - 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
- 15) OPCJA 11 – 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:
- okres ważności: certyfikat wydawany na maksymalny okres dopuszczony obowiązującymi przepisami oraz wytycznymi CA/Browser Forum. Jednocześnie Wykonawca zapewni ciągłość posiadania ważnego certyfikatu przez 12 miesięcy poprzez wydanie kolejnych certyfikatów (reissue/odnowienie) w ramach wynagrodzenia, przy czym ważność każdego pojedynczego certyfikatu będzie każdorazowo zgodna z limitami obowiązującymi w dacie jego wydania;
  - certyfikat typu OV (Organization Validation);
  - zgodność ze standardem X.509 v.3 (RFC5280)
  - zabezpieczony funkcją skrótu SHA2
  - obsługa kluczy o długości RSA 2048 bitów
  - minimalna długość kluczy kryptograficznych: RSA 2048 i wyższe (tj 2048, 3072, 4096) oraz ECDSA NIST P-256, NIST P-384;

- możliwa jest weryfikacja statusu certyfikatu przy pomocy list CRL oraz protokołu OCSP
- Obsługa 11 domen wildcard w polu SAN

2. Certyfikaty muszą pełnić ochronę przed oszustwami online, fałszowaniem oraz przechwyceniem danych.