

OPIS PRZEDMIOTU ZAMÓWIENIA

Dostawa sprzętowych kluczy bezpieczeństwa

klasy FIDO2 / U2F / NFC / PIV Smart Card

do uwierzytelniania PKI i logowania do domeny – 120 sztuk

Część nr 1 zamówienia – Zadanie nr 8 wniosku o dofinansowanie (Obszar techniczny IT)

1. Informacje ogólne

Niniejszy Opis Przedmiotu Zamówienia (OPZ) określa minimalne wymagania techniczne i funkcjonalne dotyczące dostawy 120 sztuk sprzętowych kluczy bezpieczeństwa przeznaczonych do uwierzytelniania wieloskładnikowego (MFA) oraz uwierzytelniania opartego na certyfikatach X.509 (PKI) w środowisku domenowym Microsoft Active Directory.

Klucze muszą pełnić równocześnie trzy funkcje: sprzętowy token FIDO2/U2F do uwierzytelniania webowego i systemowego, kartę inteligentną (Smart Card) standardu PIV do logowania do domeny Windows z certyfikatem PKI oraz urządzenie z interfejsem NFC do uwierzytelniania mobilnego.

Parametr	Wartość
Przedmiot zamówienia	Sprzętowe klucze bezpieczeństwa FIDO2/U2F/NFC/PIV Smart Card
Liczba sztuk	120 sztuk
Główne zastosowanie	Logowanie do domeny Windows (Active Directory) z certyfikatem X.509 (PKI)
Protokoły uwierzytelniania	FIDO2 (CTAP2), FIDO U2F, PIV Smart Card (NIST SP 800-73), WebAuthn
Interfejsy fizyczne	USB-A (wymagane), NFC (wymagane)
Standard PIV	NIST SP 800-73-4 (lub nowszy)
Certyfikaty X.509	Co najmniej 4 sloty na certyfikaty X.509 (PIV: Authentication, Signature, Key Management, Card Authentication)
Obsługa algorytmów kryptograficznych	RSA 2048 i/lub ECC P-256 (minimum), preferowane RSA 4096, ECC P-384
Kompatybilność z Windows AD	Logowanie do domeny Windows bez dodatkowych sterowników (Smart Card Minidriver lub standard PC/SC)
Stan urządzeń	Fabrycznie nowe, nieużywane, oryginalne
Gwarancja	Minimum 2 lata

2. Kontekst techniczny i cel zamówienia

Zamawiający eksploatuje infrastrukturę domenową opartą na Microsoft Active Directory z własnym Urzędem Certyfikacji (CA) działającym w oparciu o Microsoft Active Directory Certificate Services (AD CS). Dostarczone klucze bezpieczeństwa muszą umożliwiać:

- Zapis certyfikatu użytkownika X.509 wydanego przez CA Zamawiającego do slotu PIV klucza (slot 9a – Authentication).
- Logowanie do domeny Windows (Smart Card Logon) z wykorzystaniem certyfikatu przechowywanego w kluczu – bez konieczności wpisywania hasła domenowego.
- Uwierzytelnianie przez NFC na urządzeniach mobilnych i czytnikach NFC.

- Uwierzytelnianie FIDO2/U2F do aplikacji webowych i systemów obsługujących te standardy.
- Opcjonalne: podpisywanie dokumentów i szyfrowanie poczty elektronicznej z użyciem certyfikatów PKI (sloty 9c i 9d).

Klucze muszą być zgodne ze standardem kart inteligentnych systemu Windows (PC/SC) i obsługiwane przez natywny podsystem kart inteligentnych Windows bez konieczności instalacji zewnętrznych sterowników, lub wymagać instalacji wyłącznie Minidriver/sterownika producenta dostępnego bezpłatnie.

3. Minimalne wymagania techniczne i funkcjonalne

3.1. Interfejsy fizyczne i łączność

Lp.	Wymaganie	Opis wymagania / Parametr minimalny
1	Interfejs USB	Klucz musi posiadać interfejs USB. Akceptowane złącze: USB-A lub USB-C. Zamawiający wymaga podania w ofercie typu złącza USB dla 120 dostarczanych sztuk.
2	Interfejs NFC	Klucz musi posiadać wbudowany interfejs NFC (Near Field Communication) zgodny ze standardem ISO 14443 umożliwiający bezstykową komunikację z czytnikami NFC i urządzeniami mobilnymi.
3	Brak baterii	Klucz musi działać bez baterii – zasilany wyłącznie przez interfejs USB lub indukcyjnie przez NFC.
4	Brak ruchomych części	Klucz nie może posiadać ruchomych części (brak złączy wysuwanych, brak elementów mechanicznych poza ewentualnym przyciskiem dotyku).
5	Przycisk dotyku	Klucz musi posiadać element wymagający fizycznego dotyku użytkownika (touch sensor / przycisk) do potwierdzenia operacji kryptograficznej.
6	Odporność fizyczna	Klucz musi być odporny na: wodę (co najmniej IP67 lub IP68), zgniecenie, wibracje. Obudowa z tworzywa wzmocnionego włóknem szklanym lub materiału o równoważnej wytrzymałości.

3.2. Obsługiwane protokoły i standardy

Lp.	Wymaganie	Opis wymagania / Parametr minimalny
1	FIDO2 / WebAuthn	Klucz musi obsługiwać FIDO2 (CTAP2, CTAP2.1) i WebAuthn (W3C) – uwierzytelnianie passwordless i MFA do aplikacji webowych i systemów operacyjnych.

Lp.	Wymaganie	Opis wymagania / Parametr minimalny
2	FIDO U2F	Klucz musi obsługiwać FIDO U2F (Universal 2nd Factor) – uwierzytelnianie dwuskładnikowe dla aplikacji webowych.
3	PIV Smart Card (NIST SP 800-73)	Klucz musi obsługiwać standard PIV (Personal Identity Verification) zgodny z NIST SP 800-73-4 (lub nowszym) – implementacja karty inteligentnej dla logowania domenowego PKI.
4	OATH-TOTP / OATH-HOTP	Klucz powinien obsługiwać przechowywanie danych uwierzytelniających OATH-TOTP i OATH-HOTP (co najmniej 32 dane uwierzytelniające) – mile widziane.
5	OpenPGP	Klucz powinien obsługiwać OpenPGP (standard ISO/IEC 7816-4) do szyfrowania i podpisywania – mile widziane.
6	PKCS#11	Klucz musi obsługiwać interfejs PKCS#11 umożliwiający współpracę z aplikacjami korzystającymi ze standardowych bibliotek kryptograficznych.
7	PC/SC	Klucz musi być zgodny ze standardem PC/SC (ISO 7816) obsługiwanym natywnie przez system Windows jako urządzenie klasy kart inteligentnych.
8	Certyfikacja FIDO Alliance	Klucz musi posiadać certyfikację FIDO Alliance (FIDO2 Level 1 lub wyższy) – potwierdzoną na liście certyfikowanych urządzeń FIDO Alliance.

3.3. Funkcja PIV Smart Card – wymagania kluczowe

Lp.	Wymaganie	Opis wymagania / Parametr minimalny
1	Sloty PIV na certyfikaty X.509	Klucz musi posiadać co najmniej 4 sloty PIV przeznaczone do przechowywania certyfikatów X.509 i kluczy prywatnych: – Slot 9A: PIV Authentication (logowanie domenowe PKI) – Slot 9B: Management Key – Slot 9C: Digital Signature (podpisywanie cyfrowe) – Slot 9D: Key Management (szyfrowanie) Mile widziane: dodatkowe sloty (np. 9E – Card Authentication, sloty 82–95 dla dodatkowych certyfikatów).
2	Generowanie kluczy na urządzeniu	Klucz musi umożliwiać generowanie par kluczy asymetrycznych bezpośrednio na urządzeniu (on-device key generation) – klucz prywatny nigdy nie opuszcza urządzenia.
3	Import certyfikatu z zewnętrznego CA	Klucz musi umożliwiać zapis certyfikatu X.509 wystawionego przez zewnętrzny Urząd Certyfikacji (CA) do wybranego slotu PIV – w szczególności certyfikatu wydanego przez Microsoft Active Directory Certificate Services (AD CS).

Lp.	Wymaganie	Opis wymagania / Parametr minimalny
4	Logowanie do domeny Windows (Smart Card Logon)	Klucz musi umożliwiać logowanie do domeny Microsoft Active Directory przy użyciu certyfikatu przechowywanego w slotcie 9A (PIV Authentication), przez podsystem kart inteligentnych Windows (bez konieczności instalacji zewnętrznych sterowników lub wyłącznie z bezpłatnym Minidriver producenta).
5	Ochrona PIN	Dostęp do funkcji PIV musi być chroniony kodem PIN. Wymagania PIN: – Minimalna długość: 6 znaków – Maksymalna długość: co najmniej 8 znaków – Blokada po przekroczeniu konfigurowalnej liczby błędnych prób (domyślnie 3, konfigurowane do max. 255) – Możliwość odblokowania PIN przy użyciu PUK (PIN Unlock Key)
6	Klucz zarządzający (Management Key)	Klucz musi posiadać oddzielny klucz zarządzający (Management Key) do administracji: generowania kluczy, importu certyfikatów, zmiany PIN/PUK. Obsługiwane algorytmy: 3DES lub AES (AES-128/192/256).
7	Potwierdzenie dotykiem (touch policy)	Klucz musi umożliwiać skonfigurowanie polityki wymagającej fizycznego dotyku przycisku przed wykonaniem operacji kryptograficznej PIV (touch policy: always / cached / never).
8	Atestacja klucza (PIV attestation)	Klucz powinien obsługiwać mechanizm atestacji PIV, umożliwiający weryfikację że dany klucz prywatny został wygenerowany na urządzeniu (nie importowany) – przez wystawienie certyfikatu atestacji podpisanego przez CA producenta urządzenia.
9	Pełna funkcjonalność przez NFC	Wszystkie funkcje PIV (zapis certyfikatu, logowanie, podpisywanie) muszą być dostępne zarówno przez USB, jak i przez NFC.
10	Narzędzie do zarządzania	Producent musi dostarczać bezpłatne narzędzie administracyjne (GUI lub CLI) umożliwiające: inicjalizację PIV, generowanie kluczy, zapis certyfikatów, zmianę PIN/PUK, zarządzanie slotami.

3.4. Obsługiwane algorytmy kryptograficzne PIV

Lp.	Wymaganie	Opis wymagania / Parametr minimalny
1	RSA 2048	Wymagane – obsługa kluczy RSA 2048-bit w slotach PIV (9A, 9C, 9D, 9E).
2	ECC P-256 (secp256r1)	Wymagane – obsługa kluczy ECC P-256 w slotach PIV.
3	ECC P-384 (secp384r1)	Wymagane – obsługa kluczy ECC P-384 w slotach PIV.

Lp.	Wymaganie	Opis wymagania / Parametr minimalny
4	RSA 4096	Mile widziane – obsługa kluczy RSA 4096-bit (dostępne w firmware ≥ 5.7).
5	Ed25519	Mile widziane – obsługa kluczy Ed25519 (dostępne w firmware ≥ 5.7).
6	SHA-256 / SHA-384	Klucz musi obsługiwać podpisywanie z użyciem SHA-256 i SHA-384.

3.5. Bezpieczeństwo hardware

Lp.	Wymaganie	Opis wymagania / Parametr minimalny
1	Zabezpieczony kryptoprocesor	Klucz musi posiadać dedykowany sprzętowy kryptoprocesor (secure element / hardware security module) z zabezpieczeniami przed atakami fizycznymi (tamper-resistant hardware).
2	Nieekstrahowalne klucze prywatne	Klucze prywatne przechowywane w urządzeniu nie mogą być w żaden sposób wyeksportowane ani odczytane na zewnątrz urządzenia.
3	Ochrona przed atakami side-channel	Kryptoprocesor powinien posiadać zabezpieczenia przed atakami kanałami bocznymi (side-channel attacks).
4	Brak danych biometrycznych (opcja)	Zamawiający nie wymaga biometrii – klucz może, ale nie musi posiadać czytnika linii papilarnych.
5	Certyfikacja bezpieczeństwa	Klucz powinien posiadać certyfikację bezpieczeństwa sprzętowego: FIPS 140-2 Level 2 (lub wyższy) lub CC EAL5+ (lub wyższy) – mile widziane, nie wymagane bezwzględnie.

3.6. Kompatybilność systemowa i integracja

Lp.	Wymaganie	Opis wymagania / Parametr minimalny
1	Windows (Smart Card Logon / AD)	Klucz musi obsługiwać logowanie do domeny Active Directory (Smart Card Logon) na systemach: Windows 10, Windows 11, Windows Server 2016/2019/2022.
2	Windows Smart Card Minidriver	Klucz musi być obsługiwany przez system Windows jako urządzenie klasy Smart Card. Sterownik (Minidriver) producenta – jeśli wymagany – musi być bezpłatny i dostępny do pobrania ze strony producenta.
3	Microsoft Active Directory Certificate Services (AD CS)	Certyfikat X.509 wystawiony przez AD CS Zamawiającego musi być możliwy do importu do slotu PIV 9A klucza i użycia do Smart Card Logon do domeny.

Lp.	Wymaganie	Opis wymagania / Parametr minimalny
4	macOS	Klucz powinien obsługiwać logowanie i uwierzytelnianie na systemach macOS (co najmniej macOS 12 Monterey lub nowszy) – mile widziane.
5	Linux	Klucz powinien obsługiwać uwierzytelnianie na systemach Linux (przez OpenSC/PKCS#11) – mile widziane.
6	iOS / Android (NFC)	Klucz musi umożliwiać uwierzytelnianie FIDO2/U2F przez NFC z urządzeniami mobilnymi iOS (co najmniej iOS 16) i Android (co najmniej Android 8).
7	Przeglądarka	Klucz musi być kompatybilny z głównymi przeglądarkami internetowymi obsługującymi WebAuthn: Google Chrome, Mozilla Firefox, Microsoft Edge.
8	Azure AD / Entra ID	Klucz powinien być kompatybilny z Microsoft Azure AD / Entra ID do uwierzytelniania FIDO2 i/lub PIV (CBA – Certificate-Based Authentication) – mile widziane.

4. Zestawienie asortymentowe

Lp.	Oznaczenie	Opis pozycji	Ilość
1	Sprzętowy klucz bezpieczeństwa FIDO2/U2F/NFC/PIV	Sprzętowy klucz bezpieczeństwa z interfejsem USB (USB-A lub USB-C) i NFC, obsługujący: FIDO2 (CTAP2), FIDO U2F, PIV Smart Card (NIST SP 800-73), RSA 2048 / ECC P-256/P-384, co najmniej 4 sloty X.509 PIV, logowanie do domeny Windows AD, odporność IP67/IP68, certyfikat FIDO Alliance.	120 szt.

5. Warunki gwarancji

- Gwarancja producenta na urządzenia: minimum 2 lata od daty dostawy.
- Gwarancja musi być możliwa do weryfikacji i rejestracji w systemie producenta na podstawie numeru seryjnego urządzenia.
- Dostęp do aktualizacji firmware urządzenia przez cały okres gwarancji za pośrednictwem portalu producenta (jeśli producent udostępnia aktualizacje firmware).
- W przypadku awarii urządzenia w okresie gwarancji – wymiana na nowe urządzenie tego samego modelu.

6. Warunki dostawy

- Klucze muszą być dostarczone fabrycznie nowe, nieużywane, w oryginalnych opakowaniach producenta.
- Klucze muszą być dostarczone w fabrycznym stanie niezainicjalizowanym – bez wgranych certyfikatów, ustawionych kodów PIN/PUK ani skonfigurowanych poświadczeń, chyba że Zamawiający uzgodni inaczej.
- Wykonawca zobowiązany jest dostarczyć dokumentację techniczną (karta katalogowa, instrukcja inicjalizacji PIV, link do narzędzia administracyjnego).
- Wykonawca zobowiązany jest wskazać dostępność bezpłatnego narzędzia do inicjalizacji PIV i zarządzania certyfikatami (GUI lub CLI) producenta urządzenia.
- Dostawa do miejsca wskazanego przez Zamawiającego w terminie określonym w umowie.