KRYPTON POLSKA

# NARODOWA KRYPTOGRAFIA
## Bezpieczeństwo w nowoczesnej technologii


## KRYPTON HSM2

POZIOM BEZPIECZEŃSTWA - **POUFNE**

Bezpieczny moduł sprzętowy chroniąc klucz prywatny Centrum Certyfikacji (ang. Certification Authority – CA) znacząco **podwyższa bezpieczeństwo systemu** KRYPTON K2. Urządzenie umożliwia szybkie podpisywanie żądań certyfikacyjnych i podział sekretu CA na kryptograficzne karty elektroniczne. Urządzenie uzyskało certyfikat do poziomu **POUFNE**.

- Dedykowana platforma sprzętowa
- Sprzętowa realizacja algorytmów kryptograficznych i protokołów
- Bezpieczne przechowywanie kluczy CA
- Podział i odtwarzanie kluczy CA z wykorzystaniem kart elektronicznych

| PARAMETR | WARTOŚĆ /OPIS |
|---|---|
| **Poziom ochrony Informacji Niejawnych** | POUFNE |
| **Kryptografia** | Algorytm symetryczny dla zapewnienia poufności połączenia z CA<br>Algorytm asymetryczny dla zapewnienia silnego uwierzytelniania<br>Fizyczny generator liczb losowych. |
| **Zabezpieczenia fizyczne** | Obudowa zabezpieczona przed penetracją (*tamper-resistant*)<br>i pozostawiająca trwałe ślady przy próbie penetracji (*tamper-proof*) |
| **Ochrona elektromagnetyczna** | Poziom C (opcjonalnie poziom B) według SDIP-27 |
| **Interfejsy komunikacyjne** | 2 interfejsy USB, złącze typu B |
| **Podział interfejsów komunikacyjnych** | 1 interfejs do bezpiecznego połączenia z CA (data)<br>1 interfejs do aktualizacji oprogramowania (upgrade) |
| **Zarządzanie i monitorowanie** | Zdalnie – z poziomu centrum zarządzania<br>Lokalne – za pomocą wbudowanej klawiatury i wyświetlacza |
| **Nośniki kluczy i uwierzytelnianie użytkowników** | Karty kryptograficzne zgodne z normą ISO 7816<br>Personalizowane przez Krypton Polska |
| **Wyświetlacz** | Alfanumeryczny 2 x 16 z podświetleniem |
| **Obudowa** | Rack 19 cali, wysokość modułowa 1 U |
| **Zasilanie** | Zasilacz 230V AC, 30W maks. |
| **Zasilanie podtrzymujące** | Wymienny, dedykowany pakiet akumulatorowy |
| **Inne cechy** | Zdalny i lokalny audyt<br>Rozliczalność działań użytkowników |
| **Certyfikat** | Certyfikat Ochrony Kryptograficznej POUFNE, wydany przez Jednostkę Certyfikującą Departamentu Bezpieczeństwa Teleinformatycznego Agencji Bezpieczeństwa Wewnętrznego. Data ważności: 30.09.2027 r. |

www.krypton-polska.com ul. Komitetu Obrony Robotników 56, 02-146 Warszawa, T: +48 22 823 82 95, F: +48 22 823 82 94, E: krypton@krypton-polska.com

**AGENCJA BEZPIECZEŃSTWA WEWNĘTRZNEGO**

**DEPARTAMENT BEZPIECZEŃSTWA TELEINFORMATYCZNEGO**

# CERTYFIKAT OCHRONY KRYPTOGRAFICZNEJ nr T/4/2021

| | |
|---|---|
| **Przedmiot oceny:** | **Bezpieczny Moduł Sprzętowy KRYPTON HSM2 wersja 1.3** |
| **Producent:** | **Krypton Polska Sp. z o.o.**<br>**02-304 Warszawa, Al. Jerozolimskie 131** |
| **Wnioskodawca:** | **Krypton Polska Sp. z o.o.**<br>**02-304 Warszawa, Al. Jerozolimskie 131** |
| **Kryteria oceny:** | **„Information Technology Security Evaluation Criteria" (ITSEC)** |
| **Dokumentacja badań:** | **Raport z badań nr RZB_IV/2/2021** |
| **Poziom ochrony:** | **Informacje niejawne do klauzuli POUFNE** |
| **Data ważności certyfikatu:** | **do 30.09.2027 r.** |

**SZEF**
**AGENCJI BEZPIECZEŃSTWA WEWNĘTRZNEGO**

*płk Krzysztof WACŁAWEK*

K

0001256

Warszawa, 2021-05-26

# AGENCJA BEZPIECZEŃSTWA WEWNĘTRZNEGO

## DEPARTAMENT BEZPIECZEŃSTWA TELEINFORMATYCZNEGO

# WARUNKI WAŻNOŚCI CERTYFIKATU

### § 1

Informacje niejawne mogą być przetwarzane z wykorzystaniem certyfikowanego urządzenia lub narzędzia kryptograficznego wyłącznie w systemie teleinformatycznym posiadającym akredytację bezpieczeństwa teleinformatycznego wydaną w oparciu o przepisy ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U.2019 poz. 742).

### § 2

Wprowadzenie zmian, z wyłączeniem dozwolonych zmian konfiguracjyjnych w certyfikowanym urządzeniu lub narzędziu kryptograficznym powoduje utratę ważności certyfikatu.

### § 3

1. Agencja Bezpieczeństwa Wewnętrznego sprawuje nadzór nad wypełnieniem przez Użytkownika obowiązków wynikających z posiadania niniejszego certyfikatu.
2. Nadzór sprawowany jest przez funkcjonariuszy ABW i polega na weryfikacji prawidłowości użytkowania certyfikowanego urządzenia lub narzędzia kryptograficznego.
3. Użytkownik zapewni funkcjonariuszom ABW możliwość przeprowadzenia weryfikacji, o której mowa w pkt. 2 oraz udostępni wszelkie informacje niezbędne do stwierdzenia, czy warunki prawidłowego użytkowania certyfikowanego urządzenia lub narzędzia kryptograficznego są przez Użytkownika spełnione.

### § 4

1. Cofnięcie ważności certyfikatu następuje w przypadku utraty przez urządzenie lub narzędzie kryptograficzne zdolności do ochrony informacji niejawnych.
2. Cofnięcie ważności certyfikatu następuje w przypadku utraty przez Producenta zdolności zapewnienia właściwego procesu produkcji certyfikowanego urządzenia lub narzędzia kryptograficznego oraz zasad wynikających z udzielonych uprawnień i licencji.

### § 5

1. Zgodnie z art. 11.4 Enclosure „F" to C-M(2002)49 Przedmiot Oceny może być wykorzystany do ochrony poufności informacji niejawnych o maksymalnej klauzuli NATO CONFIDENTIAL.
2. Zgodnie z art. 10 ust. 6 Decyzji Rady z dnia 23 września 2013 r. w sprawie przepisów bezpieczeństwa dotyczących ochrony informacji niejawnych UE, Przedmiot Oceny może być wykorzystany do ochrony poufności informacji niejawnych Unii Europejskiej o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL w obrębie krajowych systemów teleinformatycznych.



DEPARTAMENT BEZPIECZEŃSTWA TELEINFORMATYCZNEGO ABW, 00-993 WARSZAWA UL. RAKOWIECKA 2A
TEL: 585-75-67, 585-87-46 FAX: 585-79-31