AGENCJA BEZPIECZEŃSTWA WEWNĘTRZNEGO

DEPARTAMENT BEZPIECZEŃSTWA TELEINFORMATYCZNEGO

CERTYFIKAT OCHRONY KRYPTOGRAFICZNEJ nr T/4/2016

Przedmiot oceny:	**Urządzenie CompCrypt Delta-1R/2048 z oprogramowaniem systemowym w wersji 1.14**
Producent:	**ENIGMA Systemy Ochrony Informacji Sp. z o.o. 02-230 Warszawa, ul. Jutrzenki 116**
Wnioskodawca:	**ENIGMA Systemy Ochrony Informacji Sp. z o.o. 02-230 Warszawa, ul. Jutrzenki 116**
Kryteria oceny:	**„Information Technology Security Evaluation Criteria" (ITSEC)**
Data wykonania badań:	**05.12.2016 r. – 20.12.2016 r.**
Dokumentacja badań:	**SPRAWOZDANIE Z BADAŃ nr S_LOK/05/2016, N-Pf-36309/2016**
Poziom ochrony:	**Informacje niejawne o klauzuli, co najwyżej „POUFNE", wyłącznie w zakresie generacji kluczy i certyfikatów.**

Certyfikat urządzenia nie obejmuje usług poufności informacji niejawnych przekazywanych w formie transmisji poza strefy ochronne.

Data ważności certyfikatu: **do 31.12.2022 r.**

SZEF
AGENCJI BEZPIECZEŃSTWA WEWNĘTRZNEGO

prof. dr hab. Piotr POGONOWSKI

Warszawa, dnia 29.12.2016 r.

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.2010.182.1228).

§ 2

1. Wprowadzenie zmian, z wyłączeniem dozwolonych zmian konfiguracjyjnych w certyfikowanym urządzeniu lub narzędziu kryptograficznym powoduje utratę ważności certyfikatu.
2. Zerwanie bądź uszkodzenie naklejek holograficznych zawierających nr certyfikatu zgodności lub naklejek zabezpieczających 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 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.