SZYFRATOR NARODOWY

Szyfrator Narodowy jest urządzeniem skonstruowanym przez zespół kryptologów Instytutu Matematyki i Kryptologii Wydziału Cybernetyki Wojskowej Akademii Technicznej oraz inżynierów firmy WASKO S.A. w ramach konsorcjum Nauki i Przemysłu Wojskowej Akademii Technicznej, czyli uczelni narodowej oraz firmy z kapitałem narodowym. Narodowy Szyfrator powstał jako rezultat projektu rozwojowego Nr O R00 0031 06 „Implementacja systemu kryptograficznego w oparciu o innowacyjne technologie półprzewodnikowe" (8.12.2008 - 7.12.2010). Projekt był finansowany ze środków Ministerstwa Nauki i Szkolnictwa Wyższego w ramach VI konkursu Departamentu Badań na Rzecz Bezpieczeństwa i Obronności Państwa wspieranego przez Ministerstwo Obrony Narodowej.

Narodowy Szyfrator został skonstruowany tak, aby był odporny na znane ataki kryptoanalizy, badania pola elektromagnetycznego i ulotu oraz ataki fizyczne. Jest to urządzenie na obecny stan wiedzy nie do złamania. W przeciwieństwie do sprzętu zagranicznego można sprawdzić, że nie ma w nim „bocznych furtek". System kryptograficzny jest nowatorski i został oparty na krzywych eliptycznych. Wyposażony jest we własną implementację AES 256 pozbawioną wad. W konstrukcji zastosowano najnowsze struktury układów programowalnych. Posiada unikalne zabezpieczenie systemowe. Szyfrator Narodowy może znaleźć zastosowanie zarówno w sektorze cywilnym (banki, przemysł, logistyka, biznes), jak również w agendach administracji rządowej i służbach mundurowych. Może być stosowany wszędzie tam, gdzie konieczna jest ochrona informacji wrażliwych, np. dotyczących ochrony zdrowia, informacji z miejsc klęsk żywiołowych oraz do ochrony własnych informacji finansowych. Istnieje zainteresowanie szyfratorem narodowym ze strony firm. Prowadzone są rozmowy. Warto podkreślić, że każde państwo posiada własne narodowe szyfratory do przesyłania informacji niejawnych. W tym sensie narodowy szyfrator może znaleźć zastosowanie w polskim systemie narodowym.

Obecne rozwiązanie będzie wprowadzane dla ochrony danych przesyłanych pomiędzy użytkownikami.

Planuje się modernizację, uzyskanie mniejszych rozmiarów, zmniejszenie liczby interfejsów, zwiększenie szybkości pracy procesu szyfrowania/deszyfrowania w zależności od wymagań użytkownika. Premiera narodowego szyfratora odbyła się na XVIII Międzynarodowym Salonie Przemysłu Obronnego (2010).

Narodowy Szyfrator został wyróżniony:
Główną nagrodę GRAND PRIX, dyplomem i złotym medalem na IV International Warsaw Invention Show - IWIS 2010, Warszawa 20-22.2010.
Nagrodą Ministra Nauki i Szkolnictwa Wyższego za międzynarodowe osiągnięcia wynalazcze na 18. Giełdzie Wynalazków, Warszawa 7.03.2011.
Złotym medalem i dyplomem na Międzynarodowych Targach Innowacji Gospodarczych i Naukowych INTARG, Katowice 15-17.04.2011.
Złotym medalem na 110. Międzynarodowych Targach Wynalazczości CONCOURS-LEPINE, 27.04. – 8.05. 2011, Paryż.
Złotym medalem z wyróżnieniem oraz nagrodą specjalną: Special Award Energy and Environment INNOVA 2011 na 60.
Targach Wynalazczości, Badań Naukowych i Nowych Technik Brussels INNOVA 2011, Bruksela 17-19.11.2011.
Nagrodą Rektora WAT (2011).
Dyplomem Ministra Nauki i Szkolnictwa Wyższego na XVIII Giełdzie Wynalazków, Warszawa 6-11.03.2012.

Kierownik projektu: prof. dr hab. n. mat. inż. Jerzy August Gawinecki, Dyrektor Instytutu Matematyki i Kryptologii, Wydział Cybernetyki WAT.

Wydział Cybernetyki
Instytut Matematyki i Kryptologii
Piotr Kacprzyk
tel. +48 22 683 95 56
e-mail: pkacprzyk@wat.edu.pl