AGENCJA BEZPIECZEŃSTWA WEWNĘTRZNEGO

Warszawa, 2011-08-08

N-15064/2011

Polityka Kryptograficzna
Agencji Bezpieczeństwa Wewnętrznego

Podstawa prawna

- art. 50 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. Nr 182, poz. 1228)
- art. 5 ust. 1 pkt 3 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz.U. z 2010 r. Nr 29, poz. 154, Nr182, poz. 1228, Nr 238, poz. 1578, z 2011 r. Nr 53, poz. 273 oraz Nr 117, poz. 667).

Opracowanie przez Agencję Bezpieczeństwa Wewnętrznego założeń w zakresie polityki kryptograficznej jest związane z koniecznością zapewnienia jak najwyższych standardów dla ochrony informacji niejawnych i środków ochrony kryptograficznej, które powinny być stosowane w urządzeniach i narzędziach kryptograficznych przeznaczonych do ochrony informacji niejawnych, a także w urządzeniach lub narzędziach służących do realizacji zabezpieczenia teleinformatycznego przeznaczonego do ochrony informacji niejawnych. Zgodnie z przepisem art. 50 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. Nr 182, poz. 1228) oraz art. 5 ust. 1 pkt 3 ustawy z dnia 24 maja 2002r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz.U. z 2010 r. Nr 29,

poz. 154, Nr182, poz. 1228, Nr 238, poz. 1578, z 2011 r. Nr 53, poz. 273 oraz Nr 117, poz. 667) Agencja Bezpieczeństwa Wewnętrznego realizuje, w granicach swojej właściwości, zadania związane z ochroną informacji niejawnych oraz wykonuje funkcji krajowej władzy bezpieczeństwa w zakresie ochrony informacji niejawnych w stosunkach międzynarodowych oraz prowadzi badania w procesie certyfikacji urządzeń i narzędzi kryptograficznych przeznaczonych do ochrony informacji niejawnych. W związku z rozwojem nowych technologii Agencja Bezpieczeństwa Wewnętrznego jest odpowiedzialna za kreowanie polityki kryptograficznej poprzez wyznaczenie standardów dla stosowanych środków ochrony kryptograficznej gwarantujących jak najwyższe zabezpieczenie ochrony informacji niejawnych.

Przepisy wewnętrzne obowiązujące w ABW w zakresie prowadzenia procesu certyfikacji

1) Zarządzenie nr 48 Szefa Agencji Bezpieczeństwa Wewnętrznego z dnia 21 lipca 2011r. w sprawie badań i certyfikacji urządzeń i narzędzi kryptograficznych, środków ochrony elektromagnetycznej i urządzeń lub narzędzi realizujących zabezpieczenie teleinformatyczne, wykorzystywanych do ochrony informacji niejawnych prowadzonych przez Departament Bezpieczeństwa Teleinformatycznego.
2) Decyzja nr 150 Szefa Agencji Bezpieczeństwa Wewnętrznego z dnia 18 lipca 2011r. w sprawie upoważnienia do podejmowania decyzji i wykonywania czynności związanych z realizacją przepisów rozdziału 8 ustawy o ochronie informacji niejawnych.

Definicje

Ilekroć w dokumencie jest mowa o następujących terminach należy przez to rozumieć:

Algorytm kryptograficzny – uporządkowany zbiór operacji matematycznych używany do szyfrowania i deszyfrowania informacji.

Algorytm typu A – niejawny algorytm kryptograficzny konstruowany w Agencji Bezpieczeństwa Wewnętrznego lub pod jej nadzorem, oceniony i dopuszczony do stosowania, którego specyfikacja techniczna i implementacja jest niejawna.

Algorytm typu A1 - niejawny algorytm kryptograficzny opracowany w wyniku personalizacji przez ABW algorytmu pierwotnego, oceniony i dopuszczony do stosowania. Specyfikacja techniczna parametrów personalizujących algorytm i implementacja jest niejawna.

Algorytm typu B – algorytm kryptograficzny, oceniony i dopuszczony do stosowania, którego specyfikacja techniczna jest ogólnie dostępna.

Implementacja – fizyczny wynik procesu sprzętowej lub programowej realizacji algorytmu kryptograficznego w komponencie urządzenia lub narzędzia kryptograficznego, tożsamy z opisem matematycznym.

Certyfikacja – proces badawczo-analityczny potwierdzający poprawność i skuteczność zastosowanych w urządzeniu i/lub narzędziu rozwiązań, w tym kryptograficznych, oraz poprawność i skuteczność współdziałania tych rozwiązań do ochrony informacji niejawnych, których ochrona wynika z ustawy.

Założenia polityki kryptograficznej

Polityka kryptograficzna opracowana w DBTI ABW jest polityką Agencji Bezpieczeństwa Wewnętrznego w zakresie stosowania, dopuszczania, przeprowadzania certyfikacji i badań urządzeń i narzędzi kryptograficznych służących do ochrony informacji niejawnych.

Polityka kryptograficzna ABW określa generalne zasady w tym zakresie dotyczące producentów urządzeń i narzędzi kryptograficznych służących do ochrony informacji niejawnych.

Podstawowymi wymaganiami kryptograficznymi obowiązującymi dla urządzeń i narzędzi wchodzących w skład polityki kryptograficznej ABW jest dokument „Minimalne Wymagania Kryptograficzne Departamentu Bezpieczeństwa Teleinformatycznego ABW dla urządzeń kryptograficznych służących do ochrony informacji niejawnych”*. Dokument określa fundamentalne wymagania stawiane urządzeniom kryptograficznym projektowanym i produkowanym do zapewnienia poufności informacjom niejawnym.

Główne zasady polityki kryptograficznej

1) Do ochrony poufności informacji o klauzuli TAJNE lub wyższej stosuje się algorytmy typu A.
2) Algorytm kryptograficzny typu A w postaci opisu matematycznego nie jest przekazywany producentom urządzeń przeznaczonych do kryptograficznej ochrony informacji niejawnych.
3) Do ochrony poufności informacji o klauzuli POUFNE stosuje się algorytmy typu A1. Algorytm A1 może być zastosowany do ochrony informacji niejawnych o klauzuli tajne

* Ze względu na charakter i zawartość dokument jest niejawny, udostępniany podmiotom po spełnieniu wymagań ustawowych.

wyłącznie w sytuacjach nadzwyczajnych, określonych przez ABW, w których m.in. mogłoby nastąpić skompromitowanie algorytmu typu A

4) Wytworzone przez ABW przed 2008 r. algorytmy typu A1 w związku z postępem technologicznym i rozwojem nauk matematycznych oraz nowoczesnymi metodami obliczeniowymi, z dniem 16 sierpnia 2011 r. nie mogą być wykorzystywane przez producentów nowych urządzeń i narzędzi kryptograficznych służących do ochrony informacji niejawnych. Środki ochrony kryptograficznej zawierające implementację wyżej wymienionego algorytmu A1 zgłoszone do certyfikacji w ABW po 16 sierpnia 2011r. nie będą poddawane procesom certyfikacji i nie uzyskają certyfikatu ABW dopuszczającego do ochrony informacji niejawnych. Certyfikaty ochrony kryptograficznej wydane przez ABW dla urządzeń kryptograficznych zawierających implementacje algorytmu A1 zachowują ważność tylko do końca okresu, na jaki zostały wydane.
5) W przypadku wniosków o przeprowadzenie certyfikacji urządzeń i narzędzi kryptograficznych służących do ochrony informacji niejawnych, które zostały złożone przed dniem 16 sierpnia 2011 roku, dla których nie zostały zawarte porozumienia o przeprowadzenie certyfikacji - podmiot wnioskujący o przeprowadzenie certyfikacji zostanie zobowiązany do wykonania zmian w urządzeniu lub narzędziu kryptograficznym, celem zastosowania nowych rozwiązań kryptograficznych w zakresie zastosowania algorytmów opracowanych przez ABW. Podmioty wnioskujące o przeprowadzenie certyfikacji zostaną zobowiązane w porozumieniu o przeprowadzenie certyfikacji do wprowadzenia zmian w urządzeniu lub narzędziu kryptograficznym pozwalających na wykorzystanie nowego algorytmu w terminie 60 dni od dnia udostępnienia przez ABW jego implementacji (dotyczy algorytmu A i A1) lub przekazania opisu (dotyczy wyłącznie algorytmu A1).
6) Implementacji algorytmów w urządzeniach i narzędziach kryptograficznych służących do ochrony informacji niejawnych dla algorytmów typu A i A1 dokonuje wyłącznie ABW. Producent urządzeń lub narzędzi kryptograficznych zobowiązany jest do zapewnienia środowiska i mechanizmów umożliwiających implementację algorytmów.
7) Implementacje algorytmów typu A i A1 są wgrywane do urządzeń i narzędzi kryptograficznych bezpośrednio w ABW na stanowiskach personalizacyjnych przygotowanych dla danego urządzenia lub narzędzia.
8) Algorytmy publiczne – algorytmy typu B są implementowane bezpośrednio przez producenta urządzeń lub narzędzi kryptograficznych.

9) W szczególnie uzasadnionych przypadkach algorytmy kryptograficzne A1 mogą być przekazane producentowi urządzeń przeznaczonych do ochrony kryptograficznej informacji niejawnych na warunkach i w oparciu o zasady określone przez ABW. ABW zastrzega możliwość, na warunkach przez siebie określonych, wgrywania implementacji algorytmu typu A1 w środowisku producenta pod własnym nadzorem. Przypadek ten jest przypadkiem szczególnym, wynikającym z oceny przez ABW możliwości technologicznych i proceduralno-organizacyjnych producenta oraz spełnienia przez producenta wymagań bezpieczeństwa.
10) Na korzystanie z algorytmów typu A i A1, które zostaną przekazane producentowi urządzeń w formie implementacji udzielona, zostanie przez ABW nieodpłatna licencja na wykorzystanie algorytmu na okres ważności certyfikatu. Umowa licencyjna zostanie zawarta z producentem, którego urządzenia albo narzędzia kryptograficzne uzyskają pozytywny wynik badań w procesie certyfikacji pozwalający na wydanie przez ABW certyfikatu dla urządzeń albo narzędzi kryptograficznych przeznaczonych do ochrony informacji niejawnych. Producent urządzeń zostanie zobowiązany do poniesienia kosztów związanych z personalizacją, rozumianą jako osadzenie w posiadającym certyfikat wyrobie algorytmu kryptograficznego oraz skojarzonych z nim danych na zasadach określonych w odrębnym porozumieniu.
11) Projektowanie, wytwarzanie lub modernizacja urządzeń narzędzi kryptograficznych służących do ochrony informacji niejawnych, dla zapewnienia prawidłowego wykorzystania implementacji algorytmu kryptograficznego musi być od początku realizowane we współpracy oraz pod nadzorem i na zasadach określonych przez ABW.
12) Opracowanie przez ABW koncepcji rozwiązań kryptograficznych i ich implementacji służących do zapewnienia ochrony przetwarzanych informacji niejawnych, na wniosek podmiotu wnioskującego o opracowanie takich rozwiązań i ich implementacji, wymagają zawarcia umowy w przedmiotowym zakresie. Majątkowe prawa autorskie do rozwiązań opracowanych przez ABW na mocy zawartej umowy będą przysługiwać wyłącznie Skarbowi Państwa reprezentowanemu przez Szefa ABW. Z podmiotem wnioskującym o wykonanie rozwiązań kryptograficznych i ich implementacji służących do zapewnienia ochrony przetwarzanych informacji niejawnych zostanie zawarta odpowiednia umowa licencyjna.
13) Akredytacje na systemy teleinformatyczne udzielone przed dniem wejścia w życie ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych, w których wykorzystywane są środki ochrony kryptograficznej zawierające algorytmy opracowane przez ABW przed

2008 r. zachowają ważność do czasu, na jaki została udzielona akredytacja, nie dłużej jednak niż przez okres 5 lat od dnia wejścia w życie cytowanej ustawy.

14) ABW nie będzie udzielało akredytacji dla systemu teleinformatycznego w przypadku stwierdzenia wykorzystania w tych systemach środków ochrony kryptograficznej, które zostały wprowadzone do obrotu bez wymaganych przepisami prawa zgód i pozwoleń lub bez zgody ABW w przypadku obrotu certyfikowanym wyrobem poza terytorium RP bez wprowadzenia zmian konstrukcyjnych.

/-/ gen. bryg. Krzysztof Bondaryk