Algorytm funkcji skrótu SHA-1 nierekomendowany, co nie znaczy wycofany

Kategoria: Aktualności
Opublikowano: poniedziałek, 18, luty 2019 08:12
Artur Duda
Odsłony: 1179

Podpisy kwalifikowane, które złożono z użyciem ważnych certyfikatów i przy wykorzystaniu algorytmu SHA-1 pozostają ważne. Oznacza to, że dokumenty podpisane z użyciem SHA-1 są podpisane prawidłowo i nie ma podstaw do ich odrzucenia. Aplikacje weryfikujące oraz usługi walidacji nadal wspierają podpisy złożone z wykorzystaniem tego algorytmu i można polegać na wynikach, które zgłaszają.

Do czasu formalnego wycofania przez Europejski Instytut Standardów Technicznych (ETSI) algorytm SHA-1 spełnia wymogi dla walidacji kwalifikowanych podpisów elektronicznych z art. 32 eIDAS. Należy odróżnić sytuacje awaryjnego wycofania skompromitowanych algorytmów kryptograficznych wobec których udowodniono, że nie zapewniają one wymaganego poziomu bezpieczeństwa od procesów stopniowej migracji na algorytmy zapewniające większy poziom bezpieczeństwa.

W przypadku SHA-1 mamy do czynienia z drugim przypadkiem, to znaczy rekomendacji przejścia ze stosowania tego algorytmu na rzecz kolejnych generacji algorytmu funkcji skrótu (np. SHA-2, SHA-3). Umożliwi to ewolucyjne przejście aplikacji oraz urządzeń do składania i weryfikacji podpisów elektronicznych na wyższy poziom zabezpieczeń.

Źródło: www.gov.pl/web/cyfryzacja