Warszawa, dnia 22 grudnia 2017 r.

RZECZPOSPOLITA POLSKA
MINISTER CYFRYZACJI

Anna Streżyńska

DC-I.5520.14.2017

Wg rozdzielnika

Szanowni Państwo,

W związku ze statuowanym w art. 137 ustawy z dn. 5 września 2016 *o usługach zaufania oraz identyfikacji elektronicznej* (Dz. U. z 2016, poz. 1579) obowiązkiem zaprzestania z dn. 1 lipca 2018 stosowania do składania zaawansowanych podpisów elektronicznych lub zaawansowanych pieczęci elektronicznych funkcji skrótu SHA-1 pragnę uprzejmie przypomnieć o obowiązku dostosowania systemów informatycznych zawierających funkcjonalność składania lub weryfikacji podpisu elektronicznego. W roku 2017 zakończone zostało przygotowanie nadzorowanych przez Ministra Cyfryzacji kwalifikowanych dostawców usług zaufania, którzy uruchomili urzędy certyfikacji przystosowane do świadczenia usług na nowych algorytmach oraz udostępniają testowe certyfikaty, w tym również zgodne z nowymi standardami dla profili certyfikatów kwalifikowanych. W związku z wprowadzaną zmianą technologiczną kwalifikowani dostawcy usług zaufania służą szczegółowymi informacjami odnośnie zmian w parametrach świadczonych usług zaufania.

Proszę o przekazanie Państwa pionom informatycznym lub instytucjom współpracującym i podległym prośby o sprawdzenie oraz dostosowanie aplikacji i systemów na które wpłynie przewidziana w ustawie zmiana oraz upowszechnianie informacji. Dostosowanie aplikacji dostarczanych przez centra certyfikacji nastąpi co do zasady poprzez ich aktualizację. W przypadku podmiotów rozwijających własne oprogramowanie z elementem składania i weryfikacji kwalifikowanych podpisów elektronicznych niezbędny jest uwzględnienie zmiany w projekcie lub skorzystanie z asysty technicznej. W przypadku deweloperów oprogramowania, w tym zwłaszcza systemów EZD lub ESP z wsparciem dla e-podpisu, zachęcam do przygotowania aktualizacji z wykorzystaniem nowszych bibliotek kryptograficznych. W odniesieniu do ważnych dokumentów podpisanych elektronicznie lub

znakowanych czasem na „starych" algorytmach zalecane jest rozważenie znakowania czasem dokumentów z wykorzystaniem znaczników czasu opartych na algorytmach z rodziny SHA2. W wyjątkowych przypadkach, gdy dostosowanie na czas okaże się niemożliwe należy pamiętać o zapewnieniu alternatywnego kanału w którym obsługa podpisu nastąpi z wykorzystaniem np. poprawionych aplikacji udostępnianych przez centra certyfikacji.

W przypadku innych niż wskazanych w ustawie zastosowań algorytmu SHA1 (np. w wewnętrznych infrastrukturach PKI) zalecamy przeprowadzenie oceny ryzyka związanego z dalszym eksploatowaniem narzędzi opartych o stare algorytmu oraz rozważenie zasadności i możliwości zmian. Zachęcamy do sprawdzenia czy w obszarze Państwa działalności istnieją branżowe zalecenia w zakresie zmiany algorytmów kryptograficznych. Przykładowo w zakresie płatności elektronicznych są to: „*Guidelines on cryptographic algorithms usage and key management*" (EPC342-08) wydawane przez European Payment Council.

Korzystając ze sposobności zachęcam do zaktualizowania terminologii stosowanej w systemach informatycznych, dokumentacji tych systemów, regulaminach wewnętrznych, stronach internetowych oraz różnego rodzaju formularzach do nomenklatury zawartej w rozporządzeniu eIDAS. Mimo upływu ponad dwóch lat od wejścia w życie oraz roku od wejścia do stosowania rozporządzenia eIDAS sporadycznie spotyka się nadal stosowanie pojęć takich jak np. „bezpieczny podpis elektroniczny weryfikowany ważnym kwalifikowanym certyfikatem", które powinny być zastąpione pojęciem „kwalifikowany podpis elektroniczny". Terminologia ta nie powinna być już stosowana z uwagi na uchylenie ustawy o podpisie elektronicznym.

Z wyrazami szacunku,

ANNA STREŻYŃSKA
Minister Cyfryzacji
/podpisano kwalifikowanym podpisem elektronicznym/