Newsletter nr Z/61/2022

Aktualizacja oprogramowania weryfikującego podpisy elektroniczne

W związku z planowaną aktualizacją oprogramowania weryfikującego podpisy elektroniczne zidentyfikowano potencjalny problem dotyczący **stosowania skrótów sha-1**. Zaktualizowana wersja biblioteki kryptograficznej (DSS) wprowadza bardziej rygorystyczne warunki dotyczące stosowania funkcji skrótu, która powinna spełniać minimalne wymagania we wszystkich elementach podpisu. Stosowana dotychczas wersja dopuszczała jako poprawne podpisy, w których części podpisu używają funkcji skrótu o niższych parametrach, zaś tylko główny podpis używa funkcji skrótu o parametrach wymaganych. Przykłady takich sytuacji obrazują poniższe fragmenty:

Nieprawidłowe:

<ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-**sha256**" /><ds:Reference Id="xml_ref_id" URI=""><ds:Transforms><ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" /></ds:Transforms><ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#**sha1**" /><ds:DigestValue>eKjf/jDUomzcSIzfJHklF4qDMvU=</ds:DigestValue></ds:Reference><ds:Reference URI="#signed-props-774bcdcf-ea63-47d8-a76e-6436e2f4d3da" Type="http://uri.etsi.org/01903#SignedProperties"><ds:Transforms><ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" /></ds:Transforms><ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#**sha1**" /><ds:DigestValue>8fEDi4g2UcslKAOBjdaccA9FVfI=</ds:DigestValue>

Prawidłowe:

<ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-**sha256**"/><ds:Reference Id="r-id-715b219e397b4994f643a05c9a4122a5-1" URI=""><ds:Transforms><ds:Transform Algorithm="http://www.w3.org/TR/1999/REC-xpath-19991116"><ds:XPath>not(ancestor-or-self::ds:Signature)</ds:XPath></ds:Transform><ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/></ds:Transforms><ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#**sha256**"/><ds:DigestValue>nw4o3wnGqP7sfhQnhjjBCP/xEwJyw1OxlIFs75hNz6A=</ds:DigestValue></ds:Reference><ds:Reference Type="http://uri.etsi.org/01903#SignedProperties" URI="#ICB_PL-xades-id-715b219e397b4994f643a05c9a4122a5"><ds:Transforms><ds:Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments"/></ds:Transforms><ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#**sha256**"/><ds:DigestValue>KSuQc3JmF7NI2IU94LDqeO1lFfTLOy6U84uIhj0AV90=</ds:DigestValue>

Prosimy o zweryfikowanie, czy Państwa oprogramowanie stosowane do składania podpisów stosuje **funkcję skrótu sha-256 we wszystkich elementach podpisu**. Produkcyjne wdrożenie nowej wersji oprogramowania jest planowane od listopada 2022 roku.

Informujemy jednocześnie, że **w środowisku testowym PUESC** udostępniona została nowa usługa umożliwiająca zweryfikowanie poprawności podpisu, z uwzględnieniem zgodności z nową wersją.

Informacja o publikacji
Data wysyłki: **27.09.2022**
Komórka odpowiedzialna: **Centrum Informatyki Resortu Finansów**