LIETUVOS VYRIAUSIASIS ARCHYVARAS

ĮSAKYMAS
DĖL LIETUVOS VYRIAUSIOJO ARCHYVARO 2009 M. RUGSĖJO 7 D. ĮSAKYMO NR. V-60 „DĖL ELEKTRONINIU PARAŠU PASIRAŠYTO ELEKTRONINIO DOKUMENTO SPECIFIKACIJOS ADOC-V1.0 PATVIRTINIMO“ PAKEITIMO

2018 m. balandžio 5 d. Nr. VE-20
Vilnius

1. P a k e i č i u Elektroniniu parašu pasirašyto elektroninio dokumento specifikacijos ADOC-V1.0, patvirtintos Lietuvos vyriausiojo archyvaro 2009 m. rugsėjo 7 d. įsakymu Nr. V-60 „Dėl Elektroniniu parašu pasirašyto elektroninio dokumento specifikacijos ADOC-V1.0 patvirtinimo“ (su visais pakeitimais), 14 priedą ir jį išdėstau nauja redakcija (pridedama).

2. N u s t a t a u, kad šis įsakymas įsigalioja 2018 m. balandžio 30 d.

Lietuvos vyriausiasis archyvaras Ramojus Kraujelis

Elektroniniu parašu pasirašyto elektroninio dokumento specifikacijos ADOC-V1.0
14 priedas

ELEKTRONINIAMS PARAŠAMS FORMUOTI NAUDOJAMI ALGORITMAI

Elektroniniams parašams formuoti gali būti naudojami tik šie algoritmai:

Algoritmas	Identifikatorius
Santraukos sudarymas (angl. „Digest“)	
SHA1	http://www.w3.org/2000/09/xmldsig#sha1
SHA256	http://www.w3.org/2001/04/xmlenc#sha256
Kodavimas (angl. „Encoding“)	
Base64	http://www.w3.org/2000/09/xmldsig#base64
Pasirašymas (angl. „Signature“)	
DSAwithSHA1 (DSS)	http://www.w3.org/2000/09/xmldsig#dsa-sha1
RSAwithSHA1	http://www.w3.org/2000/09/xmldsig#rsa-sha1
RSAwithSHA256	http://www.w3.org/2001/04/xmldsig-more#rsa-sha256
ecdsa-sha256	https://www.w3.org/2001/04/xmldsig-more#ecdsa-sha256
Kanonizavimas (angl. „Canonicalization“)	
Canonical XML 1.0 (omits comments)	http://www.w3.org/TR/2001/REC-xml-c14n-20010315
Canonical XML 1.0 with Comments	http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments
Canonical XML 1.1 (omits comments)	http://www.w3.org/2006/12/xml-c14n11
Canonical XML 1.1 with Comments	http://www.w3.org/2006/12/xml-c14n11#WithComments
Transformavimas (angl. „Transform“)	
XPath	http://www.w3.org/TR/1999/REC-xpath-19991116
Base64	http://www.w3.org/2000/09/xmldsig#base64

_____