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

2019 m. sausio 28 d. Nr. VE-6

Vilnius

1. P a k e i č i u Elektroniniu parašu pasirašyto elektroninio dokumento specifikaciją ADOC-V1.0, patvirtintą 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):

1.1 Pakeičiu 14 priedą ir jį išdėstau nauja redakcija (pridedama).

1.2. Pakeičiu 16 priedą ir jį išdėstau nauja redakcija (pridedama).

2. N u s t a t a u, kad šis įsakymas įsigalioja 2019 m. liepos 1 d.

Dokumentų ir archyvų valdymo ir naudojimo skyriaus vedėja, laikinai atliekanti Lietuvos vyriausiojo archyvaro funkcijas — Daiva Lukšaitė

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“)	
SHA256	http://www.w3.org/2001/04/xmlenc#sha256
Kodavimas (angl. „Encoding“)	
Base64	http://www.w3.org/2000/09/xmldsig#base64
Pasirašymas (angl. „Signature“)	
RSAwithSHA256	http://www.w3.org/2001/04/xmldsig-more#rsa-sha256
ecdsa-sha256	http://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

_____

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

ATSKIRŲ METADUOMENŲ ELEMENTŲ PASIRAŠYMO PAVYZDYS

Elektroninio parašo rinkmenoje esančios nuorodos (elemento <*ds:Reference*>), nurodančios į pasirašomą XML elementą (su atributo *ID* reikšme „*viza_1*“), esančio pasirašomųjų metaduomenų rinkmenoje *metadata/signableMetadata.xml*, pavyzdys:

```
<Reference URI="metadata/signableMetadata.xml">
  <Transforms>
    <Transform Algorithm="http://www.w3.org/TR/1999/REC-xpath-19991116">
      <XPath>ancestor-or-self::*[@ID='viza_1']</XPath>
    </Transform>
    <Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
  </Transforms>
  <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
  <DigestValue>
laLx7bCKdhILgs7HyTykd2GGOfBL6sfSrrotwDnUNxU=</DigestValue>
</Reference>
```

_____