

Ha összejön 200.000 Like...

LibreOffice, eSZIG kártya, direct democracy



Szabó Áron
(aron.szabo@egroup.hu)

Budapest
2017-03-25

Ha összejön 200.000 Like...

... akkor ...

ICE BUCKET



CINNAMON

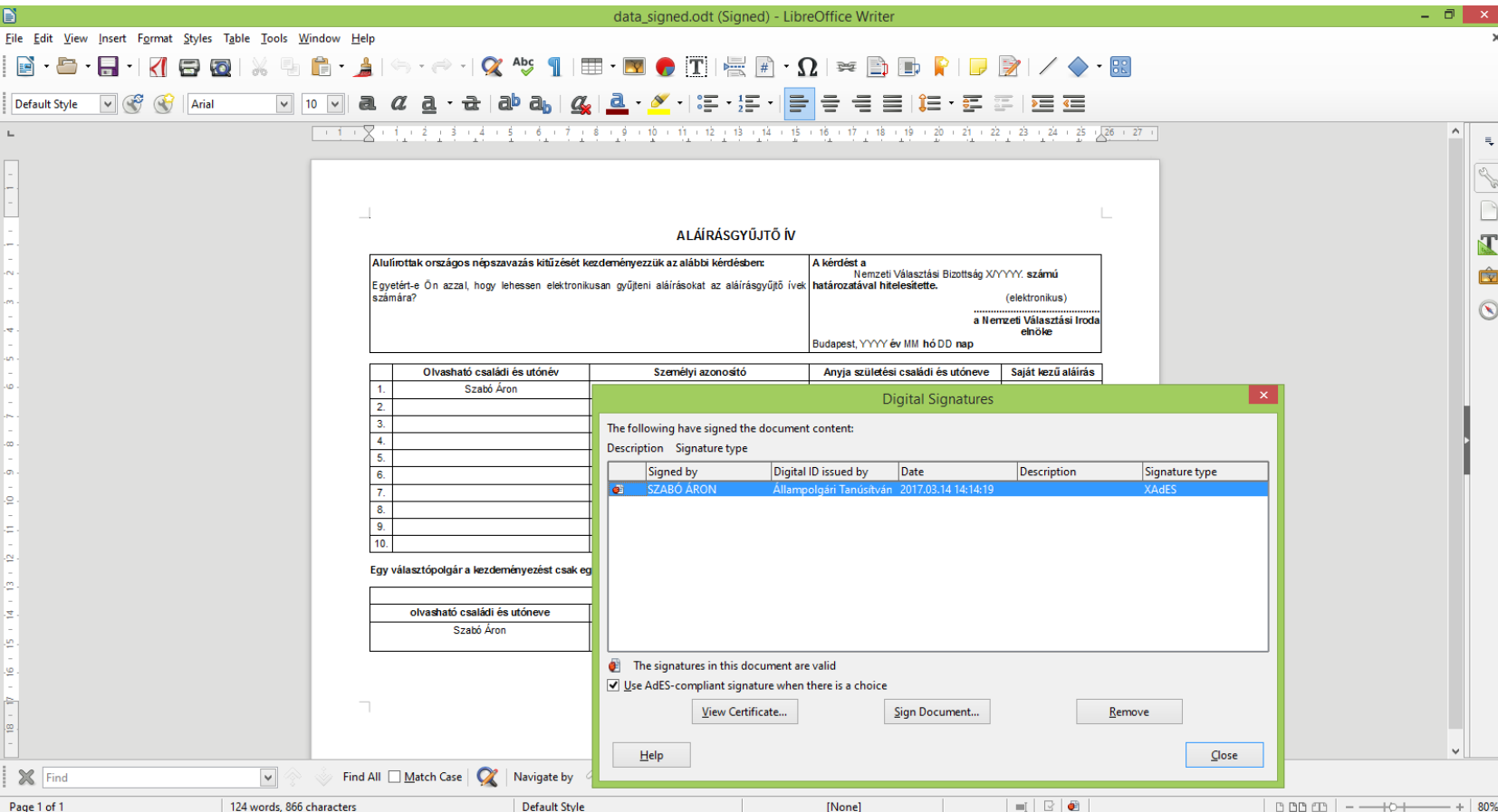


CHALLENGE ACCEPTED!



Ha összejön 200.000 aláírás...

... akkor akár egy országos népszavazást is elrendeltethetek!



The screenshot shows the LibreOffice Writer interface with a document titled "data_signed.odt (Signed)". A "Digital Signatures" dialog box is open, displaying the following information:

ALÁÍRÁSGYŰJTŐ ÍV

A kérészt a Nemzeti Választási Bizottság XY/YYY. számú határozatával hitelesítette. (elektronikus)
a Nemzeti Választási Iroda elnöke
Budapest, YYYY év MM hó DD nap

	Olvasható családi és utónév	Személyi azonosító	Anyja születési családi és utóneve	Saját kezű aláírás
1.	Szabó Áron			
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				

Egy választópolgár a kezdeményezést csak egy alkalommal teheti meg.

olvasható családi és utóneve
Szabó Áron

The "Digital Signatures" dialog box contains the following text and controls:

The following have signed the document content:

Description	Signed by	Digital ID issued by	Date	Description	Signature type
	SZABÓ ÁRON	Állampolgári Tanúsítván	2017.03.14 14:14:19		XAdES

The signatures in this document are valid
 Use AdES-compliant signature when there is a choice

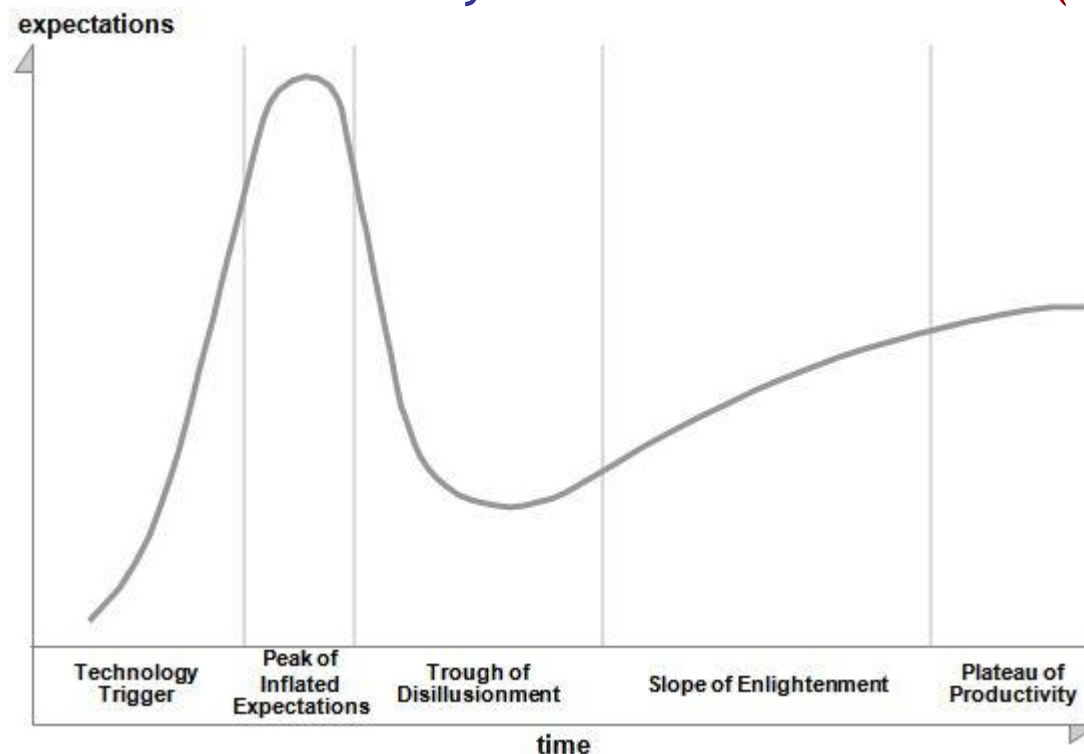
Buttons: View Certificate..., Sign Document..., Remove, Help, Close

Page 1 of 1 | 124 words, 866 characters | Default Style | [None] | 80%

A modell

Most már valóban platóra került az elektronikus aláírás technológia?

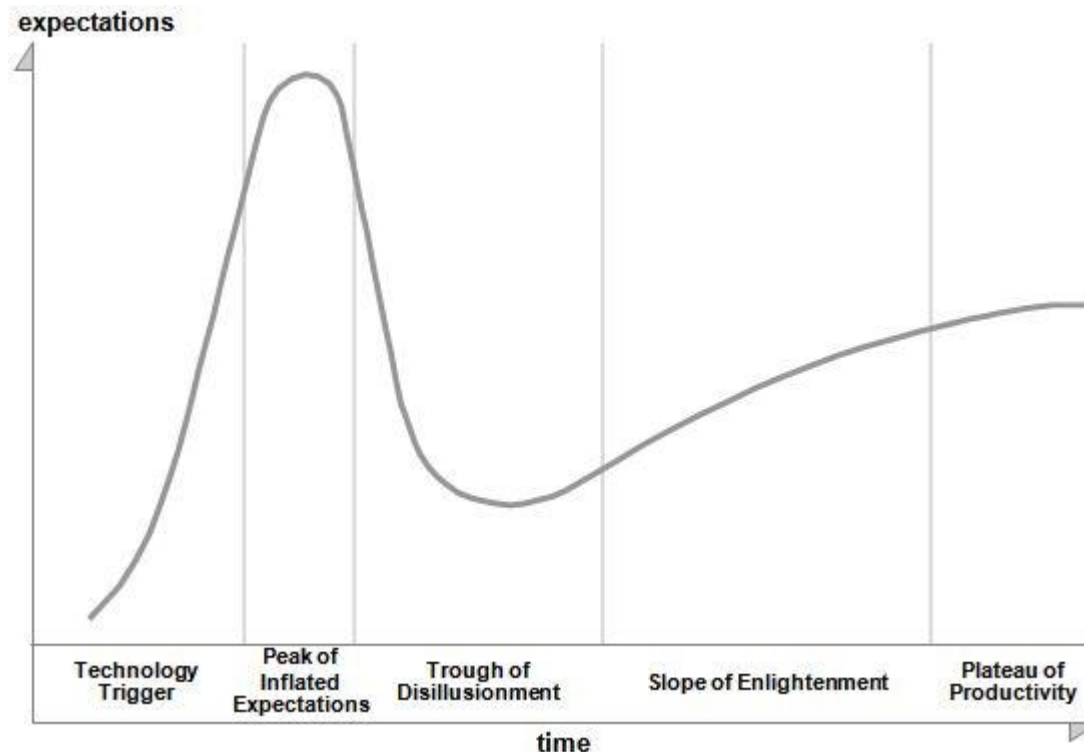
- jogszabályok: eSignatures Directive 1999/93/EC
eIDAS Regulation 910/2014/EU
e-ügyintézés tv. 2015. évi CCXXII. törvény
e-ügyintézés vhr. 451/2016. (XII. 19.) Korm. r.
eSZIG kártya 414/2015. (XII. 23.) Korm. r.



A modell

Most már valóban platóra került az elektronikus aláírás technológia?

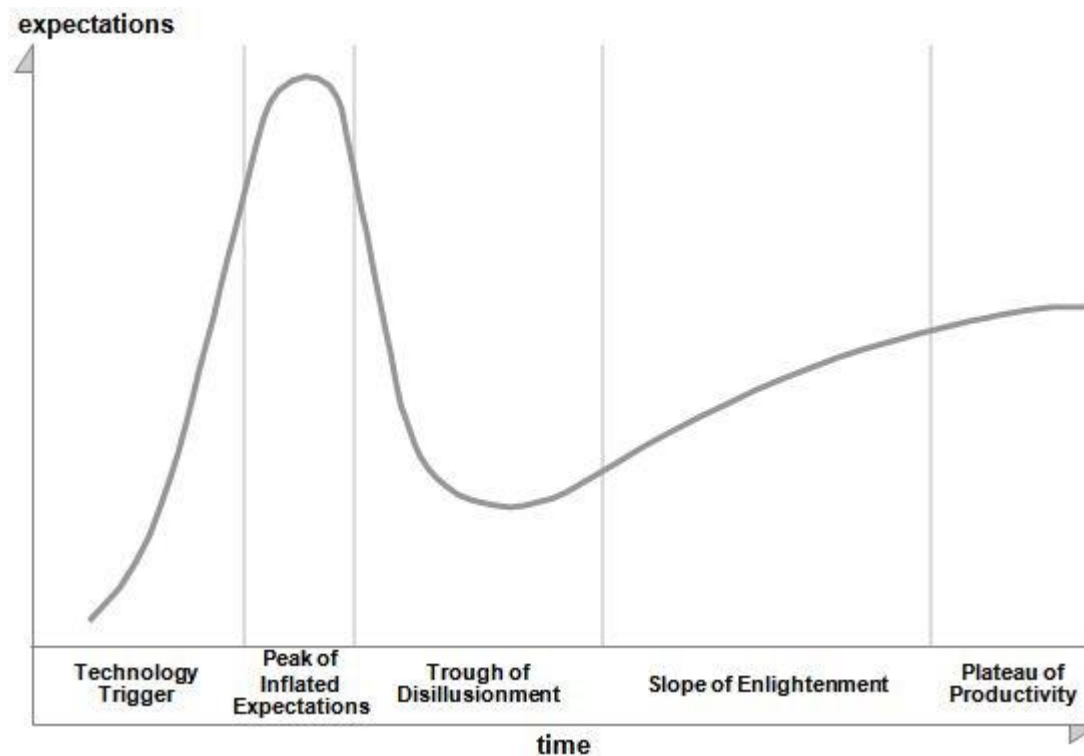
- műszaki szabványok: [ETSI TS 101 903](#) [ETSI TS 102 918](#) [XAdES \(XML Signature\)](#) [ASiC \(XML in ZIP container\)](#)



A modell

Most már valóban platóra került az elektronikus aláírás technológia?

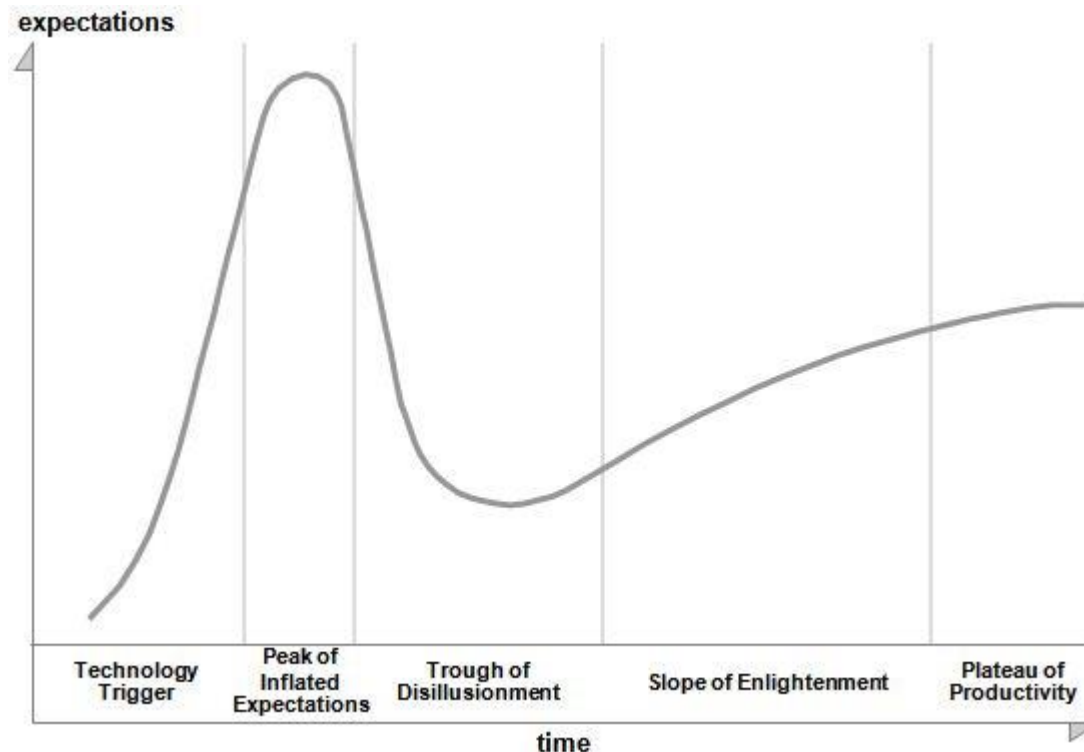
- eszközök: **eSZIG kártya** **eSIGN applet**



A modell

Most már valóban platóra került az elektronikus aláírás technológia?

- alkalmazások: LibreOffice ASiC/XAdES
 Adobe Acrobat Reader CMS/PKCS#7
 Microsoft Office ASiC/XAdES

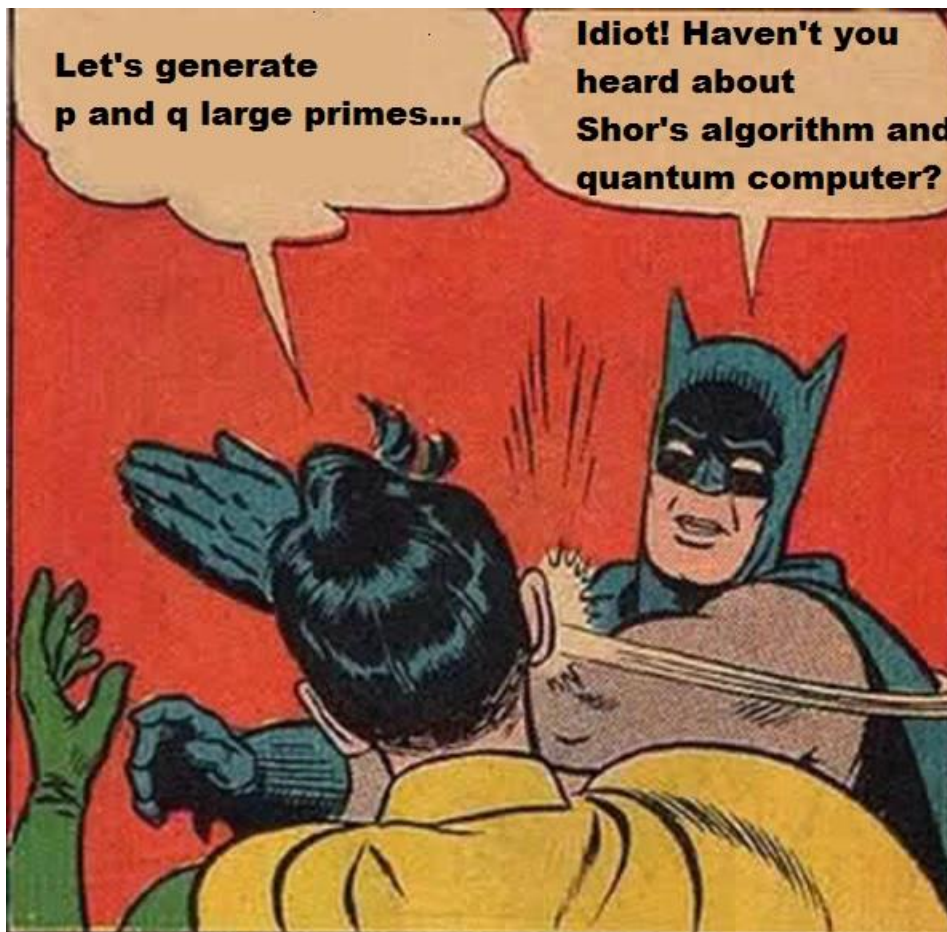


A modell

Most már valóban platóra került az elektronikus aláírás technológia?

- kriptográfia:

classic	RSA, ECDSA, stb.
post-quantum	SPHINCS, HFE stb.



A modell



Miért LibreOffice?

- aláírt **tartalom megjelenítése és aláírás** együttes kezelése

The screenshot shows a LibreOffice Writer window with a document titled 'data_signed.docx - Word'. The document content includes a title 'ALÁÍRÁSGYŰJTŐ IV', a question about electronic signature collection, and a table for signatures. A 'Signatures' sidebar on the right shows a valid signature for 'SZA...' dated '2017.03.14.'. A 'Signature Details' dialog box is open, displaying the following information:

Signature Details

Valid Signature - The signed content has not changed and the signer's certificate is valid.

Signature type: XAdES-EPES

Commitment Type:
Approved this document

Purpose for signing this document:

Signing as: SZABÓ ÁRON
Issued by: Állampolgári Tanúsítványkiadó - Qualified Cit...

Buttons: View..., Close

Links: See the additional signing information that was collected..., See information about the signer...

	Olvasható családi és utónév	Személyi azonosító	Anyja születési családi és utóneve	Saját kezű aláírás
1.	Szabó Áron		Turi-Kováts Filoména	(elektronikus)
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				

Egy választópolgár a kezdemény

olvasható családi és utó				saját kezű aláírása
Szabó Áron		Vonalkód alatti szám: - - - - -		(elektronikus)

Bottom status bar: PAGE 1 OF 1 | 126 WORDS | HUNGARIAN | 100%

A modell

Miért LibreOffice?

- aláírt **tartalom megjelenítése és aláírás** együttes kezelése

The screenshot displays the LibreOffice Writer interface with a document titled "data_signed.odt (Signed) - LibreOffice Writer". The document content includes a form titled "ALÁÍRÁSGYŰJTŐ ÍV" (Signature Collection Form) with sections for "Alufiórtak országos népszavazás kitűzését kezdeményezzük az alábbi kérdésben:" and "A kérdést a Nemzeti Választási Bizottság XY/YYY. számú határozatával hitelesítette." Below this is a table for recording signatures:

	Olvasható családi és utónév	Személyi azonosító	Anyja születési családi és utóneve	Saját kezű aláírás
1.	Szabó Áron			
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				

A "Digital Signatures" dialog box is open, showing a table of signed documents:

Description	Signature type
Signed by: SZABÓ ÁRON Digital ID issued by: Állampolgári Tanúsítván Date: 2017.03.14 14:14:19 Description: (elektronikus) a Nemzeti Választási Iroda elnöke	XAdES

The dialog box also includes a checkbox for "Use AdES-compliant signature when there is a choice" and buttons for "View Certificate...", "Sign Document...", "Remove", and "Close".

On the right side, a "Signatures" panel shows a list of valid signatures:

Valid signatures:
SZA... 2017.03.14.

At the bottom right, a status bar indicates "This document is signed. Any edits made to this document will invalidate the digital signatures. Learn more about signatures in Office documents...".

A modell



Miért LibreOffice?

- nyílt **szabványok** és nyílt **forráskód**

Nemzeti Jogszabálytár x Nemzeti Jogszabálytár x Nemzeti Jogszabálytár x +

njt.hu/cgi_bin/njt_doc.cgi?docid=140923.205329

1479/2011. (XII. 23.) Korm. határozat
Hatályos: 2011.12.24 -

1479/2011. (XII. 23.) Korm. határozat
az egyes közigazgatási szervek által használt elektronikus dokumentumok formátumáról és a nyílt forráskódú irodai szoftverek használatáról

A Kormány egyes közigazgatási szervek nemzetközi szabványon alapuló elektronikus kommunikációjának egységesítése, az együttműködés hatékonyságának javítása, valamint a költséghatékony nyílt forráskódú irodai szoftverek részarányának növelése érdekében az alábbi intézkedések végrehajtásáról döntött.

- A Kormány
 - elrendeli, hogy – a Honvédelmi Minisztérium és az általa irányított szervek kivételével – a Kormány irányítása alatt álló szervek (a továbbiakban: a Kormány irányítása alatt álló szervek) az általuk szövegszerkesztő, táblázatkezelő és prezentációkészítő szoftverekkel (a továbbiakban: irodai szoftverek) előállított, továbbszerkeszthető vagy nem továbbszerkeszthető dokumentumokat egymás közötti elektronikus kommunikációjuk során kizárólag olyan dokumentumformátumban továbbíthatják, amely nyilvánosan hozzáférhető, korlátozás nélkül alkalmazható, nemzetközi szabványügyi szervezet által elfogadott szabványra (a továbbiakban: Szabványok) épül.
 - elrendeli, hogy a Kormány irányítása alatt álló szerveknek bármely külső féllel folytatott kommunikációjuk során képesnek kell lenniük a Szabványoknak megfelelő formátumú dokumentumok fogadására, valamint gondoskodniuk kell az általuk irodai szoftverekkel előállított és nyilvánosan elérhetővé tett dokumentumaik Szabványok szerinti elérhetővé tételéről is.
 - felhívja az a) alpont szerint érintett minisztereket, hogy a felüyleletük alatt álló szervek tekintetében intézkedjenek az a)–b) alpont végrehajtásához szükséges technikai feltételek felméréséről, a feltételek biztosításáról és a technikai végrehajtásról.
Felelős: érintett miniszterek
Határidő: 2012. március 31.
- Az 1. pontban szereplő feladat végrehajtása érdekében a Kormány felhívja a nemzeti fejlesztési minisztert, hogy díjmentesen tegye elérhetővé azokat a szoftver eszközöket, amelyek az olyan szervek számára is lehetővé teszik a szabványoknak megfelelő állományok használatát és előállítását, melyek irodai szoftverei erre alapfunkcióként nem képesek, továbbá folyamatosan gondoskodjon ezen szoftver eszközök elérhetőségéről.
Felelős: nemzeti fejlesztési miniszter
Határidő: 2012. január 31-től folyamatos
- A Kormány irányítása alatt álló szervek között létrejött – a dokumentumformátumokra is kiterjedő – hatályos együttműködési megállapodásokat felül kell vizsgálni a dokumentumformátumok tekintetében, és biztosítani kell az 1. pont a) alpontjában szereplő kötelezettség teljesülését.
Felelős: érintett miniszterek
Határidő: 2012. december 31.
- A Kormány felhívja az 1. pont a) alpontja szerint érintett minisztereket, hogy a felüyleletük alatt álló szervek tekintetében intézkedjenek arról, hogy nem nyílt forráskódú irodai szoftvereket csak műszakilag vagy gazdaságilag indokolt esetben, illetve nemzetközi szerződésekből adódó kötelezettség teljesítése érdekében szerezzenek be, és a megtett intézkedésekről tájékoztassák a nemzeti fejlesztési minisztert.
Felelős: érintett miniszterek
Határidő: 2012. március 31.
- A Kormány felhívja a nemzeti fejlesztési minisztert, hogy a Kormány irányítása alatt álló szervek infokommunikációs tárgyú szerződéseikhez, kötelezettségvállalásaihoz gyakorolt egyetértési joga, valamint ezen szervek közbeszerzési eljárásai indokoltságának megítélésével kapcsolatos feladata keretében a nem nyílt forráskódú irodai szoftverek beszerzéséhez csak műszakilag vagy gazdaságilag indokolt esetben, illetve nemzetközi szerződésekből adódó kötelezettség teljesítése érdekében járuljon hozzá.

Magyar Közlöny Lap- és Könyvkiadó Kft.
A Nemzeti Jogszabálytárban elérhető szövegek tekintetében a Közlönykiadó minden jogot fenntart!

A modell



Miért LibreOffice?

- nyílt szabványok és nyílt forráskód

Nemzeti Jogszabálytár

Nemzeti Jogszabálytár

Nemzeti Jogszabálytár

Nemzeti Jogszabálytár

njt.hu/cgi_bin/njt_doc.cgi?docid=195465.321739

NEMZETI JOGSZABÁLYTÁR

1236/2016. (V. 13.) Korm. határozat

Hatályos: 2016.05.13 -

1236/2016. (V. 13.) Korm. határozat

a nyílt szabványokra épülő, illetve nyílt forráskódú szoftverek közzsférában történő elterjesztéséhez szükséges intézkedésekről

A Kormány

1. a) felhívja a belügyminisztert, hogy a Miniszterelnökséget vezető miniszter, a nemzeti fejlesztési miniszter, valamint a nemzetgazdasági miniszter és a Digitális Jólét Programja összehangolásáért és megvalósításáért felelős miniszterelnöki biztos közreműködésével, a Nemzeti Média és Hírközlési Hatóság bevonásával dolgozzon ki a Kormány számára egy olyan intézkedéscsomagot, amely azt a célt szolgálja, hogy a közigazgatás hatékonyságának megtartása vagy növelése mellett biztosított legyen a közzsférában a nyílt szabványokra épülő, illetve nyílt forráskódú szoftverek további, minél szélesebb körű elterjesztése,

Felelős: belügyminiszter
Miniszterelnökséget vezető miniszter
nemzetgazdasági miniszter
nemzeti fejlesztési miniszter
a Digitális Jólét Programja összehangolásáért és megvalósításáért felelős miniszterelnöki biztos
Határidő: 2016. szeptember 30.

b) felhívja a belügyminisztert, hogy a Miniszterelnökséget vezető miniszter, a nemzeti fejlesztési miniszter, valamint a nemzetgazdasági miniszter, és a Digitális Jólét Programja összehangolásáért és megvalósításáért felelős miniszterelnöki biztos közreműködésével, az a) pontban megjelölt intézkedéscsomagot úgy alakítsa ki, hogy az biztosítsa a közzsféra számára – a versenyfeltételek aránytalan sérelme nélkül – a hazai mikro- és kisvállalkozások szoftveripari szerepének erősödése mellett a gyártói, szállítói vagy ezzel egyenértékű támogatással rendelkező nyílt forráskódra épülő szoftverek elérhetőségét is,

Felelős: belügyminiszter
Miniszterelnökséget vezető miniszter
nemzetgazdasági miniszter
nemzeti fejlesztési miniszter
a Digitális Jólét Programja összehangolásáért és megvalósításáért felelős miniszterelnöki biztos
Határidő: 2016. szeptember 30.

c) felhívja a belügyminisztert, hogy a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. (a továbbiakban: NISZ Zrt.) útján intézkedjen a központi kormányzati informatikai szolgáltató ellátotti körébe tartozó szervek esetében arról, hogy a térítésmentesen elérhető nyílt forráskódú irodai szoftverek – a rendelkezésre álló programok mellett – telepítésre kerüljenek,

Felelős: belügyminiszter
Határidő: azonnal

d) felhívja a belügyminisztert, hogy a c) alpontban jelzett feladathoz kapcsolódóan a NISZ Zrt. útján biztosítsa a felhasználói támogatást, beleértve a felhasználók oktatását is,

Felelős: belügyminiszter
Határidő: azonnal

e) felhívja a Miniszterelnökséget vezető minisztert, hogy a) pontban megjelölt intézkedéscsomagot úgy alakítsa ki, hogy az biztosítsa a közzsféra számára – a versenyfeltételek aránytalan sérelme nélkül – a hazai mikro- és kisvállalkozások szoftveripari szerepének erősödése mellett a gyártói, szállítói vagy ezzel egyenértékű támogatással rendelkező nyílt forráskódra épülő szoftverek elérhetőségét is,

Magyar Közlöny Lap- és Könyvkiadó Kft.
A Nemzeti Jogszabálytárban elérhető szövegek tekintetében a Közlönykiadó minden jogot fenntart!

A modell



Miért LibreOffice?

- nyílt szabványok és nyílt forráskód

1604/2016. (XI. 8.) Korm. határozat
Hatályos: 2016.11.08 -

1604/2016. (XI. 8.) Korm. határozat
a nyílt forráskódú szoftverek közzsférában történő elterjesztéséről, valamint a nyílt szabványokra épülő, illetve nyílt forráskódú szoftverek közzsférában történő elterjesztéséhez szükséges intézkedésekről szóló 1236/2016. (V. 13.) Korm. határozat végrehajtásából adódó egyes feladatokról

A Kormány
1.
a) felhívja a belügyminisztert, hogy gondoskodjon a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. (a továbbiakban: NISZ Zrt.) által nyújtott, kötelezően biztosítandó központosított informatikai ellátásban részesülő közigazgatási szervek (a továbbiakban: NISZ Zrt. ellátotti körébe tartozó szervek) vonatkozásában arról, hogy a felhasznált zárt forráskódú irodai szoftverlicencként aránya 2017. év végéig legalább 20%-kal, 2018. év végéig legalább 30%-kal, 2019. év végéig legalább 45%-kal, 2020. év végéig legalább 60%-kal csökkenjen a 2016. december 31-i arányokhoz képest;
Felelős: belügyminiszter
Határidő: adott év végéig
b) felhívja az érintett minisztereket, hogy évente tekintsék át – a NISZ Zrt. által biztosított nyílt, valamint az aktuális zárt forráskódú irodai szoftvercsomagokat figyelembe véve – az irányításuk alá tartozó minisztérium és a felügyeletük alatt álló, az a) alponban megjelölt közigazgatási szervek felhasználóinak munkafolyamatai irodai szoftvercsomag igényét, abból a szempontból, hogy mely felhasználók esetében nem lehet áttérni nyílt forráskódú irodai szoftverre és erről indokolással együtt tájékoztassák a belügyminisztert;
Felelős: a honvédelmi miniszter kivételével valamennyi miniszter
Határidő: először 2017. április 30.
2018-tól évente április 30-ig
c) felhívja az érintett minisztereket, hogy a b) alponban meghatározott feladat végrehajtása során vegyék figyelembe az a) alponban foglalt arányokat és tegyék meg a szükséges intézkedéseket annak érdekében, hogy az érintett arányok a minisztériumban teljesüljenek, valamint erről folyamatosan tájékoztassák a Digitális Jólét Programjával kapcsolatos kormányzati feladatok összehangolásáért és megvalósításáért felelős miniszterelnöki biztost;
Felelős: a honvédelmi miniszter kivételével valamennyi miniszter
Határidő: folyamatos
d) felhívja a miniszterelnök kabinetfőnökét, hogy a Digitális Jólét Programjával kapcsolatos kormányzati feladatok összehangolásáért és megvalósításáért felelős miniszterelnöki biztos közreműködésével folyamatosan kísérje figyelemmel a b) alponban foglaltak teljesülését és tegye meg a szükséges intézkedéseket annak érdekében, hogy az egyes érintett minisztériumokban az a) alponban foglalt arányok teljesüljenek;
Felelős: miniszterelnök kabinetfőnöke
Határidő: folyamatos
2. felhívja a belügyminisztert, hogy a Nemzeti Hírközlési és Informatikai Tanács bevonásával a NISZ Zrt. útján az 1. pont b) alpontjában meghatározott feladat végrehajtása érdekében készítsen módszertant az érintett szervezetek számára, amely az egyes munkafolyamatok esetében segít annak megítélésében, hogy szükséges-e zárt forráskódú irodai szoftver az adott feladatok ellátásához;
Felelős: belügyminiszter
Határidő: 2017. január 31.
3. felhívja a belügyminisztert, hogy az informatikai eszközök és szolgáltatók beszerzésének jogszabályban előírt jóváhagyása, valamint az állami szervek informatikai fejlesztéseinek véleményezése kapcsán az elektronikus kormányzati

A modell



Miért LibreOffice?

- fejlesztőbarát megoldás

This PC > Windows8_OS (C:) > ARON > HACK > form > data_Microsoft_Office >

<input type="checkbox"/> Name	Date modified	Type	Size
_rels	2017.03.20. 16:33	File folder	
_xmsignatures	2017.03.20. 16:33	File folder	
docProps	2017.03.20. 16:33	File folder	
word	2017.03.20. 16:33	File folder	
[Content_Types].xml		XML File	2 KB

This PC > Windows8_OS (C:) > ARON > HACK > form > data_LibreOffice

<input type="checkbox"/> Name	Date modified	Type	Size
META-INF	2017.03.20. 16:32	File folder	
content.xml	2017.03.14. 13:00	XML File	31 KB
mimetype	2017.03.14. 13:00	File	1 KB
styles.xml	2017.03.14. 13:00	XML File	13 KB



Miért LibreOffice?

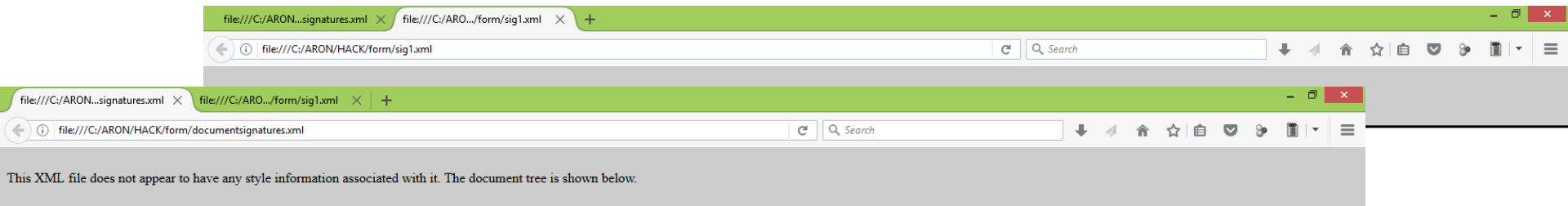
- fejlesztőbarát megoldás

```
file:///C:/ARON...signatures.xml x file:///C:/ARO.../form/sig1.xml x +
file:///C:/ARON/HACK/form/sig1.xml
This XML file does not appear to have any style information associated with it. The document tree is shown below.
- <Signature Id="idPackageSignature">
- <SignedInfo>
  <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
  <SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
  - <Reference Type="http://www.w3.org/2000/09/xmldsig#Object" URI="#idPackageObject">
    <DigestMethod Algorithm="http://www.w3.org/2001/04/xmenc#sha256"/>
    <DigestValue>oGKOEei6qM+PmB/9OT1v1Q1IETL1jcVQas1K/Ks2Vg4=</DigestValue>
    </Reference>
  + <Reference Type="http://www.w3.org/2000/09/xmldsig#Object" URI="#idOfficeObject"></Reference>
  + <Reference Type="http://uri.etsi.org/01903#SignedProperties" URI="#idSignedProperties"></Reference>
  </SignedInfo>
- <SignatureValue>
  b1KKjUpUai6Ppmyz7jWHMiVBmS+o22oYhfgan/QyMJDC+FH5QW5ebP1LnXm5h7ProLh95aNXVeat Po3wz6CjWZmS2cLldy6dAdnkz9MnE59rTti2zaG5P1JHrgF0dphVRpfmKo6sOodaOwSaN/3/B/UZ
  T0AtoBVDH57J1doZjgDa7eGQwYNBQb85aAg5dbkPqntR27qXXoZOVr8kydovjsFnnzMLBouxQjN+ oTFzgbEJsB/X9+7Op5+m8FNQ8YUmadBhnQvdO7HEWDU8sLqIeZbmqS6FzdiOuwKD/GmrLSMWv8g
  LH9gKj1cg+D+Sbdtruedq5Kt879REjk2l2MG/Bw==
  </SignatureValue>
- <KeyInfo>
  - <X509Data>
    + <X509Certificate></X509Certificate>
    </X509Data>
  </KeyInfo>
- <Object Id="idPackageObject">
  + <Manifest></Manifest>
  + <SignatureProperties></SignatureProperties>
  </Object>
- <Object Id="idOfficeObject">
  + <SignatureProperties></SignatureProperties>
  </Object>
- <Object>
  + <xd:QualifyingProperties Target="#idPackageSignature"></xd:QualifyingProperties>
  </Object>
</Signature>
```



Miért LibreOffice?

- fejlesztőbarát megoldás



```
<document-signatures>
- <Signature Id="ID_0043001a007c005900c900fd00400086008d008f001c00b500d70066007f00d8">
  - <SignedInfo>
    <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
    <SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
    - <Reference URI="mimetype">
      <DigestMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#sha256"/>
      <DigestValue>cU2+NwsKcGNmKhfZGyh1Zv6Lq7yFmbYpskR2/4G4NZM=</DigestValue>
    </Reference>
    + <Reference URI="styles.xml"></Reference>
    + <Reference URI="META-INF/manifest.xml"></Reference>
    + <Reference URI="content.xml"></Reference>
    + <Reference URI="#ID_003a000200f20078001b000a004f009b00be00e1000a00c600ba009f00a100f5"></Reference>
    + <Reference URI="#idSignedProperties"></Reference>
  </SignedInfo>
  - <SignatureValue>
    T6CilQpOQuL+v+zWwkDW7RbO7RmXrQ5ZdfYLkzkPgmvtFTT5jtKNlk+YsVu51R EUzHhfgBhSU8Px/Qp1PrkfpsfSKwBTwfy7Kh/HPse7J+Zmlt4n2S0U6LC9CntDi/nY9Ohw3gZp+TFU6/dugo0qP4Hq8so
    /LUZMRVz8Q1GuJfGj7rvQmXm/PN0pGTOhet /9QZp3djUxIIsUtgAsory0s0PQxak/Rw5MP56Y2SOMkK0OwowoJU2zK/EtUK2+z/ 5MkcViRGfVU7tKBqCT6b8+vsTp85/NAtYphqRlfSicFLhMTAVNATS2ddGqyrPnW1
    y6xyGOy2nInKB/UmrBpNwQ==
  </SignatureValue>
  - <KeyInfo>
    - <X509Data>
      + <X509IssuerSerial></X509IssuerSerial>
      + <X509Certificate></X509Certificate>
    </X509Data>
    <KeyInfo>
  - <Object>
    + <SignatureProperties></SignatureProperties>
  </Object>
- <Object>
  + <xd:QualifyingProperties Target="#ID_0043001a007c005900c900fd00400086008d008f001c00b500d70066007f00d8"></xd:QualifyingProperties>
</Object>
</Signature>
</document-signatures>
```

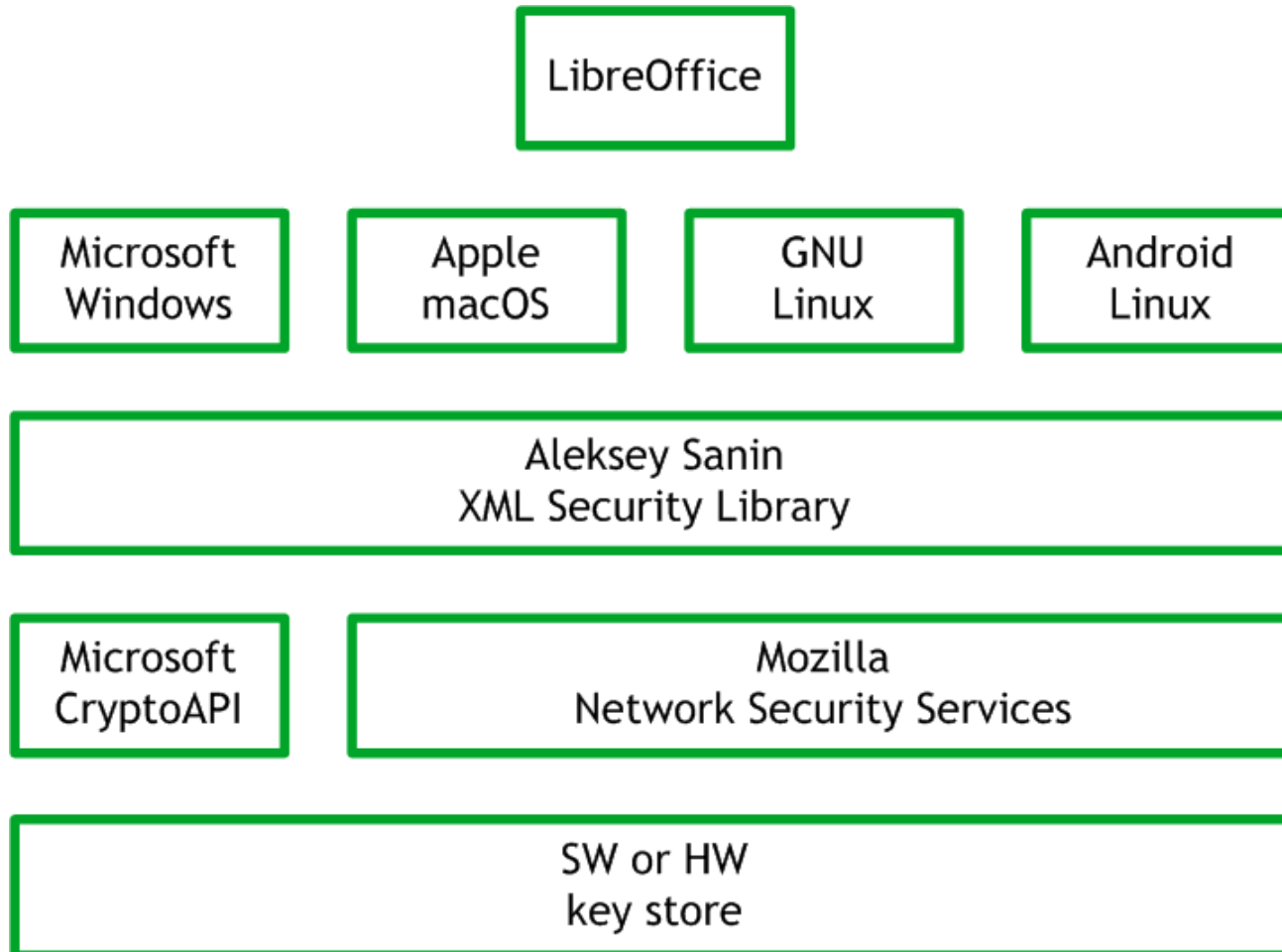
UZ
MWv8g

A modell



Miért LibreOffice?

- kriptográfiai réteg felkészült



A modell



Miért LibreOffice?

- kriptográfiai réteg felkészült

The screenshot shows a web browser window displaying the ETSI website. The address bar shows the URL: www.etsi.org/about/what-we-do/plugtests/calendar-of-events/asic-remote-plugtests-2012. The page features the ETSI logo and a navigation menu with items like Standards, Technologies & Clusters, Membership, News & Events, Committees & Portal, and About us. A search bar and a 'Sign up for ETSI News!' button are also visible. The main content area is titled 'ASiC Remote Plugtests 2012' and contains the following text:

In answer to the European Commission Mandate 460 on Electronic Signatures Standardization, ETSI has initiated several Specialist Task Forces projects (STF).

The STF428 addressed the needs of Testing activities which should be performed rapidly leading to a quick and easy improvement of the functionality of the existing e-Signature standardization deliverables and bringing them up to date with current practices.

One of the purposes of the STF 428 was to prepare a first interoperability test event on ASiC (Associated Signature Container ETSI TS 102 918) signatures. This preparation includes:

- The production of the whole test suite
- The production of all the material documenting how to conduct the interoperability event
- The deployment in the ETSI portal of the suitable PKI and tools required for supporting the interoperability test event conduction

Following the STF 428, ETSI Centre for Testing and Interoperability (CTI) organized the first remote Plugtests Interop event for ASiC Signatures from 19 November to 21 December 2012. The event was initially planned to end on 7th December but it has been extended to 21st December following several requests from the participants. The reason was that the amount of testing activities was extremely high within the initial scheduled period, due to high participation in the event as well as the high number of test descriptions agreed.

This Remote event aimed at conducting interoperability test cases on ASiC signatures (Associated Signature Container ETSI TS 102 918). This testing provided full test coverage of this specification.

Several updates to the ETSI specifications have been transformed into Change Request documents which have been presented to the ETSI ESI meeting in March 2013.

A modell



Miért LibreOffice?

- kriptográfiai réteg felkészült

ETSII - ASiC Remote Plugte... x 76142 - EU-conform digit... x 105983 - Supporting ECDS... x +

www.etsi.org/about/what-we-do/plugtests/calendar-of-events/asic-remote-plugtests-2012

ETSII - ASiC Remote Plugte... x 76142 - EU-conform digit... x 105983 - Supporting ECDS... x +

https://bugs.documentfoundation.org/show_bug.cgi?id=76142

Bugzilla - Bug 76142 EU-conform digital signatures (XAdES, ASiC container) in Libre Office Last modified: 2016-11-12 13:43:38 UTC

Home | New | Browse | Search | Search [?] | Reports | Help | New Account | Log In | Forgot Password

Bug 76142 - EU-conform digital signatures (XAdES, ASiC container) in Libre Office

Status: RESOLVED FIXED **Reported:** 2014-03-13 21:50 UTC by Aron Szabo
Alias: None **Modified:** 2016-11-12 13:43 UTC ([History](#))
Product: LibreOffice **CC List:** 6 users ([show](#))
Component: LibreOffice ([show other bugs](#)) **See Also:**
Version: unspecified [Crash report or crash signature:](#)
(earliest affected)
Hardware: Other All
Importance: medium normal
Assignee: Miklos Vajna
QA Contact:
URL:
Whiteboard: target:5.2.0
Keywords:
Depends on:
Blocks:

Attachments

Libre Office document with XAdES-signature (SHA-1 based) (14.24 KB, application/vnd.oasis.opendocument.text) Details
<small>2014-03-16 13:26 UTC, Aron Szabo</small>
Libre Office document with XAdES-signature (SHA-256 based) (16.96 KB, application/vnd.oasis.opendocument.text) Details
<small>2014-03-16 13:27 UTC, Aron Szabo</small>
Add an attachment (proposed patch, testcase, etc.) View All

Note
You need to [log in](#) before you can comment on or make changes to this bug.

A modell



Miért LibreOffice?

- kriptográfiai réteg felkészült

ETS - ASIC Remote Plugte... x 76142 - EU-conform digit... x 105983 - Supporting ECDS... x +

www.etsi.org/about/what-we-do/plugtests/calendar-of-events/asic-remote-plugtests-2012

ETS - ASIC Remote Plugte... x 76142 - EU-conform digit... x 105983 - Supporting ECDS... x +

ETS - ASIC Remote Plugte... x 76142 - EU-conform digit... x 105983 - Supporting ECDS... x +

https://bugs.documentfoundation.org/show_bug.cgi?id=105983

Bugzilla - Bug 105983 Supporting ECDSA (NIST P-256 curve) signatures created by Hungarian citizen eID card (Linux/macOS) Last modified: 2017-03-08 10:12:13 UTC

Home | New | Browse | Search | Search [?] | Reports | Help | New Account | Log In | Forgot Password

Bug 105983 - Supporting ECDSA (NIST P-256 curve) signatures created by Hungarian citizen eID card (Linux/macOS)

Status: RESOLVED FIXED

Reported: 2017-02-13 14:42 UTC by Aron Szabo

Modified: 2017-03-08 10:12 UTC ([History](#))

CC List: 1 user ([show](#))

Alias: None

Product: LibreOffice

Component: LibreOffice ([show other bugs](#))

Version: 5.3.0.3 release ([earliest affected](#))

Hardware: All Linux (All)

Importance: medium normal

Assignee: Miklos Vajna

QA Contact:

URL:

Whiteboard: target:5.4.0

Keywords:

Depends on:

Blocks: [Digital-Signatures](#)

Show dependency [tree](#) / [graph](#)

See Also:

Crash report or crash signature:

Attachments

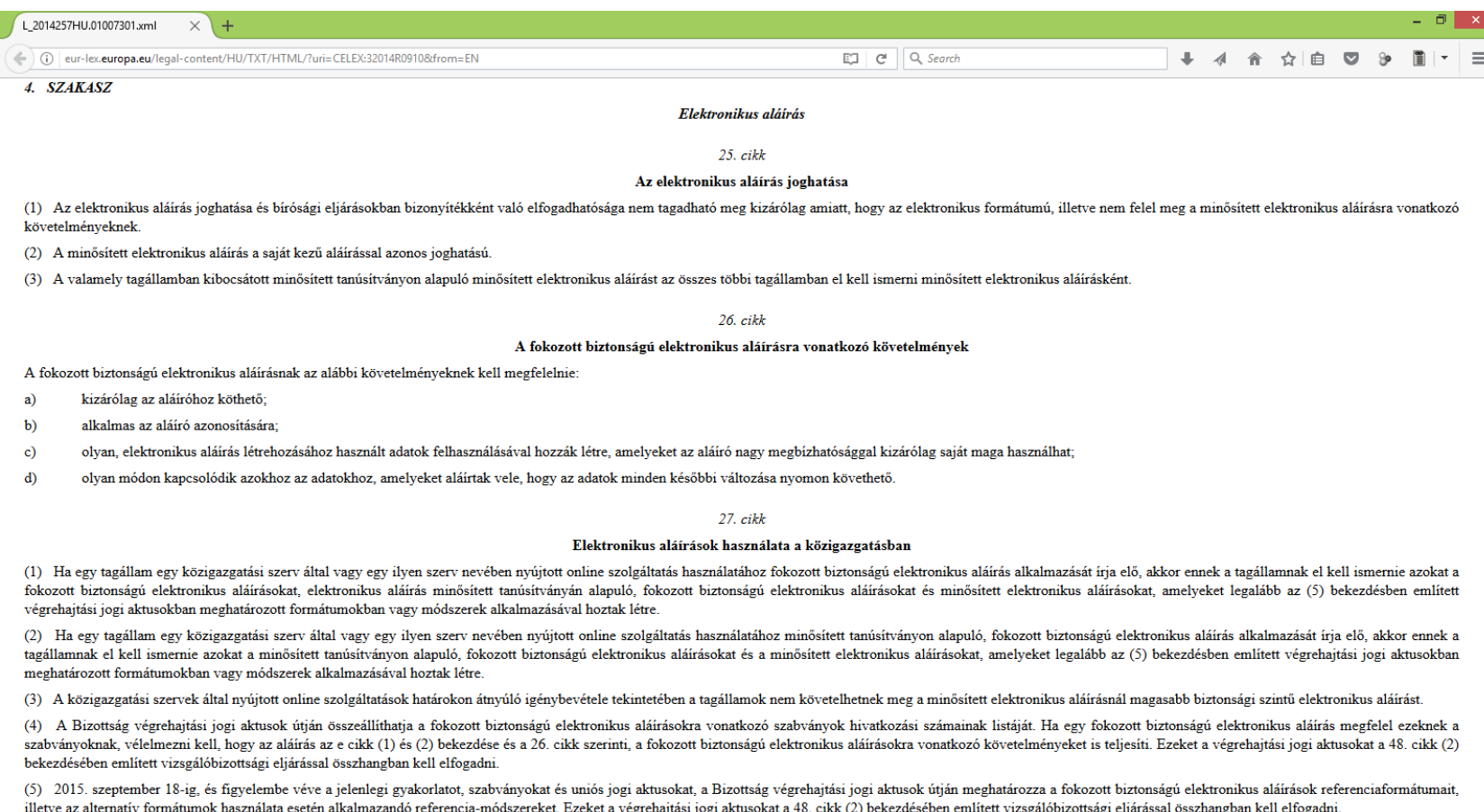
LibreOffice document with ECDSA signature (8.07 KB, application/vnd.oasis.opendocument.text) 2017-02-13 14:42 UTC, Aron Szabo	Details
canonicalized SignedInfo (2.06 KB, text/plain) 2017-02-13 14:43 UTC, Aron Szabo	Details
binary SignatureValue (72 bytes, text/plain) 2017-02-13 14:44 UTC, Aron Szabo	Details
base64-encoded public key from X.509 certificate (178 bytes, text/plain) 2017-02-13 14:45 UTC, Aron Szabo	Details

A modell

Miért eSZIG kártya?

- *Az eSzemélyre [...] 2016. május 27-től igényelt tanúsítványokkal minősített aláírás hozható létre.*

https://eszemelyi.hu/gyik/gyik_elektronikus_alairas



The screenshot shows a browser window displaying a legal document from eur-lex.europa.eu. The document is titled "4. SZAKASZ" and contains sections on "Elektronikus aláírás" (Electronic signature) and "A fokozott biztonságú elektronikus aláírásra vonatkozó követelmények" (Requirements for qualified electronic signatures). The text is in Hungarian and discusses the legal status and requirements for electronic signatures, including the use of qualified certificates and the security of the signing process.

4. SZAKASZ

Elektronikus aláírás

25. cikk

Az elektronikus aláírás joghatása

(1) Az elektronikus aláírás joghatása és bírósági eljárásokban bizonyítékként való elfogadhatósága nem tagadható meg kizárólag amiatt, hogy az elektronikus formátumú, illetve nem felel meg a minősített elektronikus aláírásra vonatkozó követelményeknek.

(2) A minősített elektronikus aláírás a saját kezű aláírással azonos joghatású.

(3) A valamely tagállamban kibocsátott minősített tanúsítványon alapuló minősített elektronikus aláírást az összes többi tagállamban el kell ismerni minősített elektronikus aláírásként.

26. cikk

A fokozott biztonságú elektronikus aláírásra vonatkozó követelmények

A fokozott biztonságú elektronikus aláírásnak az alábbi követelményeknek kell megfelelnie:

a) kizárólag az aláíróhoz köthető;

b) alkalmas az aláíró azonosítására;

c) olyan, elektronikus aláírás létrehozásához használt adatok felhasználásával hozták létre, amelyeket az aláíró nagy megbízhatósággal kizárólag saját maga használhat;

d) olyan módon kapcsolódik azokhoz az adatokhoz, amelyeket aláírtak vele, hogy az adatok minden későbbi változása nyomon követhető.

27. cikk

Elektronikus aláírások használata a közigazgatásban

(1) Ha egy tagállam egy közigazgatási szerv által vagy egy ilyen szerv nevében nyújtott online szolgáltatás használatához fokozott biztonságú elektronikus aláírás alkalmazását írja elő, akkor ennek a tagállamnak el kell ismernie azokat a fokozott biztonságú elektronikus aláírásokat, elektronikus aláírás minősített tanúsítványon alapuló, fokozott biztonságú elektronikus aláírásokat és minősített elektronikus aláírásokat, amelyeket legalább az (5) bekezdésben említett végrehajtási jogi aktusokban meghatározott formátumokban vagy módszerek alkalmazásával hoztak létre.

(2) Ha egy tagállam egy közigazgatási szerv által vagy egy ilyen szerv nevében nyújtott online szolgáltatás használatához minősített tanúsítványon alapuló, fokozott biztonságú elektronikus aláírás alkalmazását írja elő, akkor ennek a tagállamnak el kell ismernie azokat a minősített tanúsítványon alapuló, fokozott biztonságú elektronikus aláírásokat és a minősített elektronikus aláírásokat, amelyeket legalább az (5) bekezdésben említett végrehajtási jogi aktusokban meghatározott formátumokban vagy módszerek alkalmazásával hoztak létre.

(3) A közigazgatási szervek által nyújtott online szolgáltatások határon átnyúló igénybevétele tekintetében a tagállamok nem követelhetnek meg a minősített elektronikus aláírásnál magasabb biztonsági szintű elektronikus aláírást.

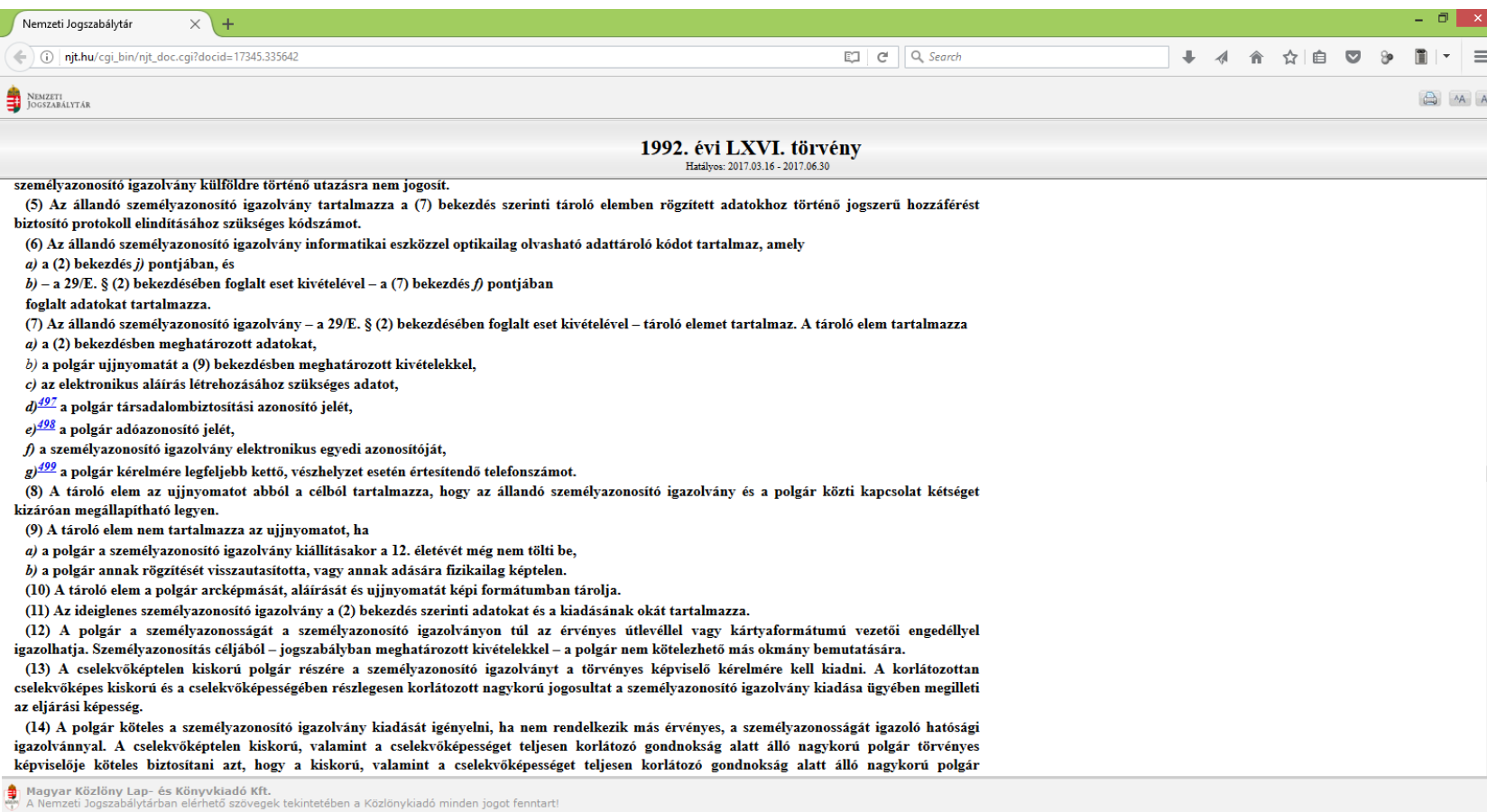
(4) A Bizottság végrehajtási jogi aktusok útján összeállíthatja a fokozott biztonságú elektronikus aláírásokra vonatkozó szabványok hivatkozási számainak listáját. Ha egy fokozott biztonságú elektronikus aláírás megfelel ezeknek a szabványoknak, vélelmezni kell, hogy az aláírás az e cikk (1) és (2) bekezdése és a 26. cikk szerinti, a fokozott biztonságú elektronikus aláírásokra vonatkozó követelményeket is teljesíti. Ezeket a végrehajtási jogi aktusokat a 48. cikk (2) bekezdésében említett vizsgálóbizottsági eljárással összhangban kell elfogadni.

(5) 2015. szeptember 18-ig, és figyelembe véve a jelenlegi gyakorlatot, szabványokat és uniós jogi aktusokat, a Bizottság végrehajtási jogi aktusok útján meghatározza a fokozott biztonságú elektronikus aláírások referenciaformátumait, illetve az alternatív formátumok használata esetén alkalmazandó referencia-módszereket. Ezeket a végrehajtási jogi aktusokat a 48. cikk (2) bekezdésében említett vizsgálóbizottsági eljárással összhangban kell elfogadni.

A modell

Miért eSZIG kártya?

- eSIGN applet mellett eID, ePASS, eNEK (MIFARE) applet is található rajta, amelyekben egyéb adatok is tárolódnak



Nemzeti Jogszabálytár

njt.hu/cgi_bin/njt_doc.cgi?docid=17345.335642

1992. évi LXVI. törvény
Hatályos: 2017.03.16 - 2017.06.30

személyazonosító igazolvány külföldre történő utazásra nem jogosít.

(5) Az állandó személyazonosító igazolvány tartalmazza a (7) bekezdés szerinti tároló elemben rögzített adatokhoz történő jogszerű hozzáférést biztosító protokoll elindításához szükséges kódszámot.

(6) Az állandó személyazonosító igazolvány informatikai eszközzel optikailag olvasható adattároló kódot tartalmaz, amely

a) a (2) bekezdés j) pontjában, és

b) – a 29/E. § (2) bekezdésében foglalt eset kivételével – a (7) bekezdés f) pontjában foglalt adatokat tartalmazza.

(7) Az állandó személyazonosító igazolvány – a 29/E. § (2) bekezdésében foglalt eset kivételével – tároló elemet tartalmaz. A tároló elem tartalmazza

a) a (2) bekezdésben meghatározott adatokat,

b) a polgár ujjnyomatát a (9) bekezdésben meghatározott kivételekkel,

c) az elektronikus aláírás létrehozásához szükséges adatot,

d)⁴⁹⁷ a polgár társadalombiztosítási azonosító jelét,

e)⁴⁹⁸ a polgár adóazonosító jelét,

f) a személyazonosító igazolvány elektronikus egyedi azonosítóját,

g)⁴⁹⁹ a polgár kérelmére legfeljebb kettő, vészhelyzet esetén értesítendő telefonszámot.

(8) A tároló elem az ujjnyomatot abból a célból tartalmazza, hogy az állandó személyazonosító igazolvány és a polgár közti kapcsolat kétséget kizáróan megállapítható legyen.

(9) A tároló elem nem tartalmazza az ujjnyomatot, ha

a) a polgár a személyazonosító igazolvány kiállításakor a 12. életévét még nem tölti be,

b) a polgár annak rögzítését visszautasította, vagy annak adására fizikailag képtelen.

(10) A tároló elem a polgár arcképmását, aláírását és ujjnyomatát képi formátumban tárolja.

(11) Az ideiglenes személyazonosító igazolvány a (2) bekezdés szerinti adatokat és a kiadásának okát tartalmazza.

(12) A polgár a személyazonosságát a személyazonosító igazolványon túl az érvényes útlevelemmel vagy kártyaformátumú vezetői engedéllyel igazolhatja. Személyazonosságát céljából – jogszabályban meghatározott kivételekkel – a polgár nem kötelezhető más okmány bemutatására.

(13) A cselekvőképtelen kiskorú polgár részére a személyazonosító igazolványt a törvényes képviselő kérelmére kell kiadni. A korlátozottan cselekvőképes kiskorú és a cselekvőképességében részlegesen korlátozott nagykorú jogosult a személyazonosító igazolvány kiadása ügyében megilleti az eljárési képesség.

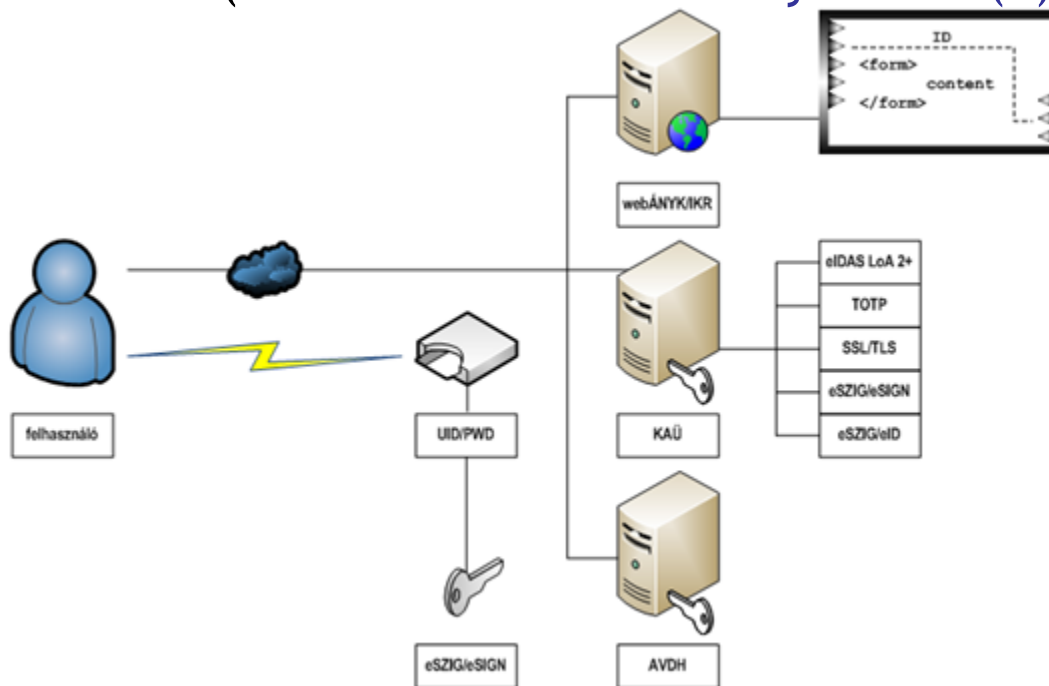
(14) A polgár köteles a személyazonosító igazolvány kiadását igényelni, ha nem rendelkezik más érvényes, a személyazonosságát igazoló hatósági igazolvánnyal. A cselekvőképtelen kiskorú, valamint a cselekvőképességet teljesen korlátozó gondnokság alatt álló nagykorú polgár törvényes képviselője köteles biztosítani azt, hogy a kiskorú, valamint a cselekvőképességet teljesen korlátozó gondnokság alatt álló nagykorú polgár

Magyar Közlöny Lap- és Könyvkiadó Kft.
A Nemzeti Jogszabálytárban elérhető szövegek tekintetében a Közlönykiadó minden jogot fenntart!

A modell

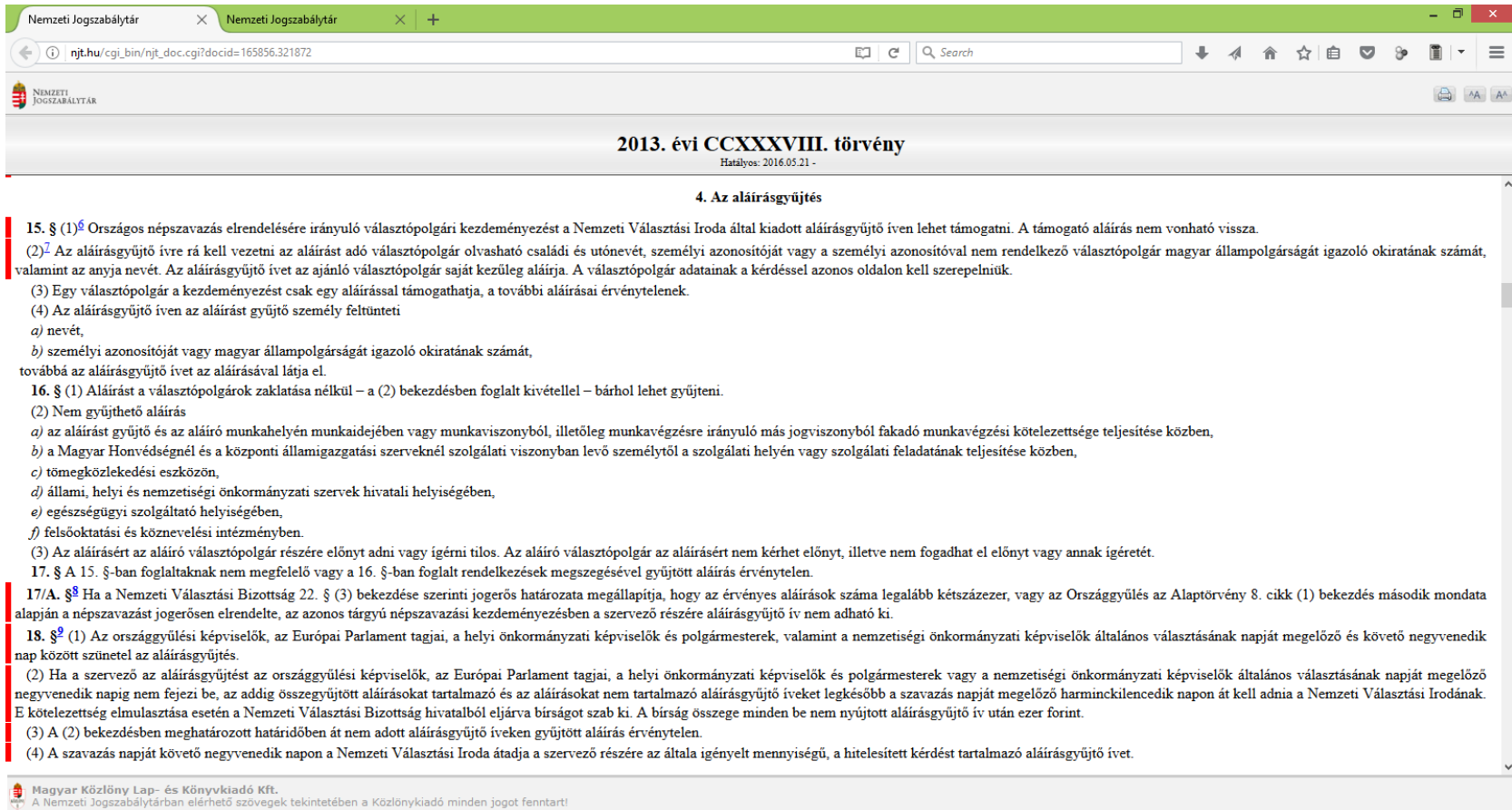
Miért eSZIG kártya?

- **eSIGN** applet mellett **AVDH** aláírás-szolgáltatás is használható lehet - **KAÜ** felhasználó-hitelesítés után - **teljes bizonyító erejű magánokirat** esetén (2016. évi CXXX. törvény 325. § (1) g))
- **közokirat** esetén figyelni kell az azonos joghatásra, hiteles elektronikus másolatkészítésre is (2016. évi CXXX. törvény 324. § (1))



Miért népszavazási aláírásgyűjtés?

- közokirat, saját kezű aláírás, tömeges, költséghatékony



Nemzeti Jogszabálytár

njt.hu/cgi_bin/njt_doc.cgi?docid=165856.321872

NEMZETI JOGSZABÁLYTÁR

2013. évi CCXXXVIII. törvény

Hatályos: 2016.05.21 -

4. Az aláírásgyűjtés

15. § (1)⁸ Országos népszavazás elrendelésére irányuló választópolgári kezdeményezést a Nemzeti Választási Iroda által kiadott aláírásgyűjtő íven lehet támogatni. A támogató aláírás nem vonható vissza.

(2)⁷ Az aláírásgyűjtő ívre rá kell vezetni az aláírást adó választópolgár olvasható családi és utónévét, személyi azonosítóját vagy a személyi azonosítóval nem rendelkező választópolgár magyar állampolgárságát igazoló okiratának számát, valamint az anyja nevét. Az aláírásgyűjtő ívet az ajánló választópolgár saját kezűleg aláírja. A választópolgár adatainak a kérdéssel azonos oldalon kell szerepelniük.

(3) Egy választópolgár a kezdeményezést csak egy aláírással támogathatja, a további aláírásai érvénytelenek.

(4) Az aláírásgyűjtő íven az aláírást gyűjtő személy feltüntetni

- a) nevét,
- b) személyi azonosítóját vagy magyar állampolgárságát igazoló okiratának számát,

továbbá az aláírásgyűjtő ívet az aláírásával látja el.

16. § (1) Aláírást a választópolgárok zaklatása nélkül – a (2) bekezdésben foglalt kivétellel – bárhol lehet gyűjteni.

(2) Nem gyűjthető aláírás

- a) az aláírást gyűjtő és az aláíró munkahelyén munkaidejében vagy munkaviszonyból, illetőleg munkavégzésre irányuló más jogviszonyból fakadó munkavégzési kötelezettsége teljesítése közben,
- b) a Magyar Honvédségnél és a központi államigazgatási szerveknél szolgálati viszonyban levő személytől a szolgálati helyén vagy szolgálati feladatának teljesítése közben,
- c) tömegközlekedési eszközön,
- d) állami, helyi és nemzetiségi önkormányzati szervek hivatali helyiségében,
- e) egészségügyi szolgáltató helyiségében,
- f) felsőoktatási és köznevelési intézményben.

(3) Az aláírást az aláíró választópolgár részére előnyt adni vagy ígérni tilos. Az aláíró választópolgár az aláírást nem kérhet előnyt, illetve nem fogadhat el előnyt vagy annak ígérését.

17. § A 15. §-ban foglaltaknak nem megfelelő vagy a 16. §-ban foglalt rendelkezések megszegésével gyűjtött aláírás érvénytelen.

17/A. §⁸ Ha a Nemzeti Választási Bizottság 22. § (3) bekezdése szerinti jogerős határozata megállapítja, hogy az érvényes aláírások száma legalább kétszázezer, vagy az Országgyűlés az Alaptörvény 8. cikk (1) bekezdés második mondata alapján a népszavazást jogerősen elrendelte, az azonos tárgyú népszavazási kezdeményezésben a szervező részére aláírásgyűjtő ív nem adható ki.

18. §⁹ (1) Az országgyűlési képviselők, az Európai Parlament tagjai, a helyi önkormányzati képviselők és polgármesterek, valamint a nemzetiségi önkormányzati képviselők általános választásának napját megelőző és követő negyvenedik nap között szünetel az aláírásgyűjtés.

(2) Ha a szervező az aláírásgyűjtést az országgyűlési képviselők, az Európai Parlament tagjai, a helyi önkormányzati képviselők és polgármesterek vagy a nemzetiségi önkormányzati képviselők általános választásának napját megelőző negyvenedik napig nem fejezi be, az addig összegyűjtött aláírásokat tartalmazó és az aláírásokat nem tartalmazó aláírásgyűjtő íveket legkésőbb a szavazás napját megelőző harminckilencedik napon át kell adnia a Nemzeti Választási Irodának. E kötelezettség elmulasztása esetén a Nemzeti Választási Bizottság hivatalból eljárva bírságot szab ki. A bírság összege minden be nem nyújtott aláírásgyűjtő ív után ezer forint.

(3) A (2) bekezdésben meghatározott határidőben át nem adott aláírásgyűjtő íveken gyűjtött aláírás érvénytelen.

(4) A szavazás napját követő negyvenedik napon a Nemzeti Választási Iroda átadja a szervező részére az általa igényelt mennyiségű, a hitelesített kérdést tartalmazó aláírásgyűjtő ívet.

Magyar Közlöny Lap- és Könyvkiadó Kft.
A Nemzeti Jogszabálytárban elérhető szövegek tekintetében a Közlönykiadó minden jogot fenntart!

A modell

Miért népszavazási aláírásgyűjtés?

- közokirat, saját kezű aláírás, tömeges, költséghatékony

The screenshot shows the Hungarian National Election Portal (Nemzeti Jogszabálytár) displaying the text of Article 8 of the Hungarian Basic Law (Alaptörvény) regarding national referendums. The page is titled "Magyarország Alaptörvénye" and "Országos népszavazás".

8. cikk

(1) Legalább kétszáz ezer választópolgár kezdeményezésére az Országgyűlés országos népszavazást rendel el. A köztársasági elnök, a Kormány vagy százezer választópolgár kezdeményezésére az Országgyűlés országos népszavazást rendelhet el. Az érvényes és eredményes népszavazáson hozott döntés az Országgyűlésre kötelező.

(2) Országos népszavazás tárgya az Országgyűlés feladat- és hatáskörébe tartozó kérdés lehet.

(3) Nem lehet országos népszavazást tartani

a) az Alaptörvény módosítására irányuló kérdésről;

b) a központi költségvetésről, a központi költségvetés végrehajtásáról, központi adónméről, illetékről, járulékról, vámról, valamint a helyi adók központi feltételeiről szóló törvény tartalmáról;

c) az országgyűlési képviselők, a helyi önkormányzati képviselők és polgármesterek, valamint az európai parlamenti képviselők választásáról szóló törvények tartalmáról;

d) nemzetközi szerződésből eredő kötelezettségről;

e) az Országgyűlés hatáskörébe tartozó személyi és szervezetalkotási kérdésről;

f) az Országgyűlés feloszlásáról;

g) képviselő-testület feloszlásáról;

h) hadiállapot kinyilvánításáról, rendkívüli állapot és szükségállapot kihirdetéséről, valamint megelőző védelmi helyzet kihirdetéséről és meghosszabbításáról;

i) katonai műveletekben való részvétellel kapcsolatos kérdésről;

j) közkegyelem gyakorlásáról.

(4) Az országos népszavazás érvényes, ha az összes választópolgár több mint fele érvényesen szavazott, és eredményes, ha az érvényesen szavazó választópolgárok több mint fele a megfogalmazott kérdésre azonos választ adott.

A köztársasági elnök

9. cikk

(1) Magyarország államfője a köztársasági elnök, aki kifejezi a nemzet egységét, és öröködik az államszervezet demokratikus működése felett.

(2) A köztársasági elnök a Magyar Honvédség főparancsnoka.

(3) A köztársasági elnök

a) képviseli Magyarországot;

b) részt vehet és felszólalhat az Országgyűlés ülésein;

c) törvényt kezdeményezhet;

d) országos népszavazást kezdeményezhet;

e) kitűzi az országgyűlési képviselők, a helyi önkormányzati képviselők és polgármesterek általános választását, valamint az európai parlamenti választás és az országos népszavazás időpontját;

f) különleges jogrendet érintő döntéseket hoz;

g) kezdeményez az Országgyűlés elnöki feladatát.

Magyar Közlöny Lap- és Könyvkiadó Kft.
A Nemzeti Jogszabálytárban elérhető szövegek tekintetében a Közlönykiadó minden jogot fenntart!

A modell

Miért népszavazási aláírásgyűjtés?

- „Az aláírásgyűjtés” előtt:
„A népszavazásra javasolt kérdés benyújtása” és „A kérdés hitelesítése”

Nemzeti Jogszabálytár

njt.hu/cgi_bin/njt_doc.cgi?docid=165856.321872

NEMZETI JOGSZABÁLYTÁR

2013. évi CCXXXVIII. törvény
Hatályos: 2016.05.21 -

ORSZÁGOS NÉPSZAVAZÁS KEZDEMÉNYEZÉSE

1. A választópolgári kezdeményezés szervezője

2. § (1) Országos népszavazás kitűzésére irányuló választópolgári kezdeményezést

- olyan magánszemély, aki az országgyűlési képviselők választásán választó lehet,
- párt,
- a nem párt jogállású egyesület (a továbbiakban: egyéb egyesület) a létesítő okiratában meghatározott céllal összefüggő kérdésben szervezhet.

(2) Egy kezdeményezésnek több szervezője is lehet. Ebben az esetben a szervezők egy személyt jelölnek ki a választási szervekkel való kapcsolattartásra.

2. A népszavazásra javasolt kérdés benyújtása

3. § (1)² A szervezőnek a népszavazásra javasolt kérdést, az aláírásgyűjtés megkezdése előtt – a kérdés hitelesítése céljából – be kell nyújtania a Nemzeti Választási Bizottsághoz.

- Egy aláírásgyűjtő íven egy kérdés szerepelhet.
- Az a magánszemély szervező a kérdés benyújtásakor a nevét, lakcímét és személyi azonosítóját, ennek hiányában a magyar állampolgárságát igazoló okirata számát közli a Nemzeti Választási Bizottsággal.
- Az egyéb egyesület a létesítő okiratát is csatolja a kérdés benyújtásakor.
- A Nemzeti Választási Iroda a párt és az egyéb egyesület létezését és adatainak hitelességét a civil szervezetek bírósági nyilvántartásában ellenőrzi.

4. § (1) A kérdést legalább húsz, de legfeljebb harminc választópolgár támogató aláírásával ellátva kell benyújtani.

- A támogató aláírások gyűjtését megelőzően a szervezőnek az adatkezelést az adatvédelmi nyilvántartásba be kell jelentenie.
- A támogató választópolgár aláírására a 15. § (2) és (3) bekezdését kell alkalmazni.
- A Nemzeti Választási Iroda a központi névjegyzékben ellenőrzi a szervező és a támogató választópolgárok választójogát.
- A támogató választópolgárok számának megállapításakor a magánszemély szervezőt is figyelembe kell venni.

5. § A köztársasági elnök és a Kormány az általa kezdeményezett népszavazásra javasolt kérdést – hitelesítés céljából – benyújtja a Nemzeti Választási Bizottsághoz.

6. § (1) A kérdést személyesen vagy postai úton lehet benyújtani.

- A benyújtás időpontjának a kérdés Nemzeti Választási Irodánál történő érkeztetése számít.

7. § A kérdés benyújtását követő munkanapon a Nemzeti Választási Iroda nyilvánosságra hozza a benyújtott kérdést, a benyújtás időpontját, valamint a szervező nevét.

8. §³ (1) Nem nyújtható be azonos tárgyú kérdés azt követően, ha

- a Nemzeti Választási Bizottság 22. § (3) bekezdése szerinti jogerős határozata megállapítja, hogy az érvényes aláírások száma legalább kétszázezer, aa) a népszavazás elrendelésének elutasításáról szóló határozat jogerőre emelkedéséig, ab) a népszavazás megtartásáig, vagy

A modell

Miért népszavazási aláírásgyűjtés?

- „Az aláírásgyűjtés” után:
„A népszavazás elrendelése” és „A szavazás módja”

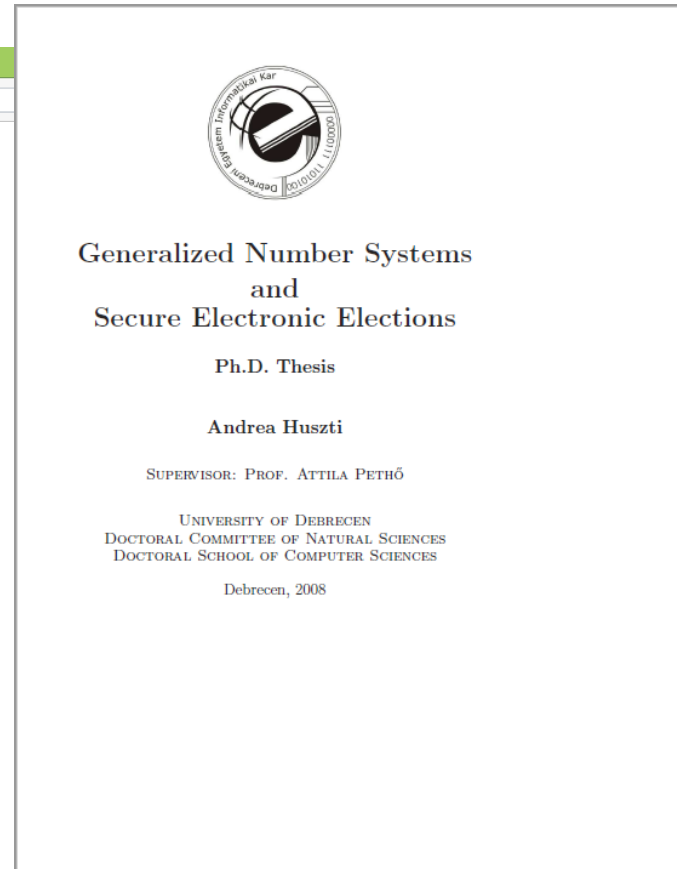


Inside D21

Democracy 2.1 : Our Mission

Democracy 2.1 (D21) is a global project launched in 2014 to transform the way communities make decisions.

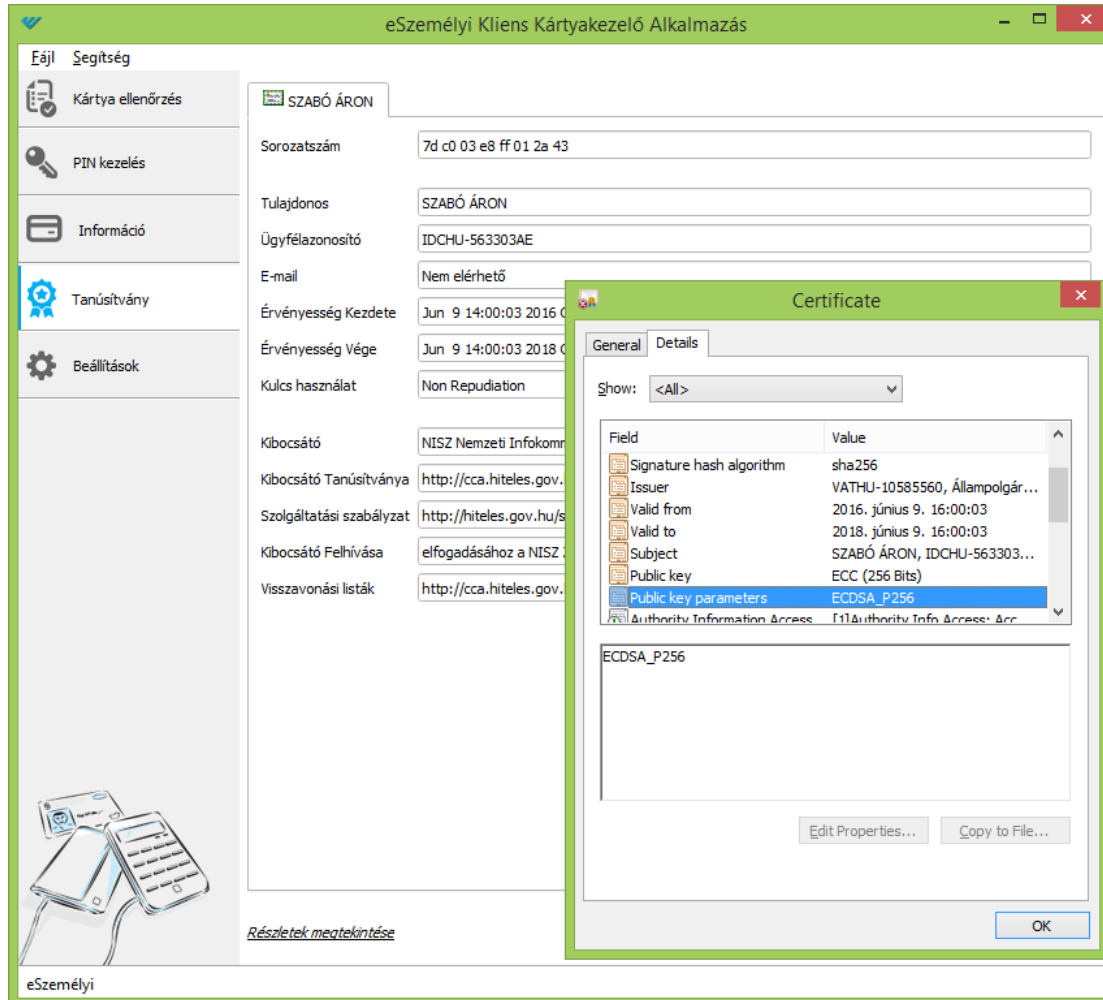
The project combines an innovative voting system developed by Czech mathematician and anti-corruption activist Karel Janeček, and a digital platform which allows anyone to build



Az aláírásgyűjtés

Az aláírás létrehozása felhasználói (GUI) vagy gépi (WS) felületen keresztül:

- eSZIG kártya előkészítése



The screenshot displays the 'eSzemélyi Kliens Kártyakezelő Alkalmazás' (ePersonal Client Card Management Application) interface. The main window shows the profile of 'SZABÓ ÁRON' with various fields for identification and contact information. A 'Certificate' dialog box is open, showing the details of a certificate issued by 'VATHU-10585560, Állampolgár...'. The certificate is valid from 2016. június 9. 16:00:03 to 2018. június 9. 16:00:03. The public key parameters are 'ECDSA_P256'. The dialog box also includes buttons for 'Edit Properties...', 'Copy to File...', and 'OK'.

Field	Value
Signature hash algorithm	sha256
Issuer	VATHU-10585560, Állampolgár...
Valid from	2016. június 9. 16:00:03
Valid to	2018. június 9. 16:00:03
Subject	SZABÓ ÁRON, IDCHU-563303...
Public key	ECC (256 Bits)
Public key parameters	ECDSA_P256
Authority Information Access	[1]Authority Info Access: Acc...

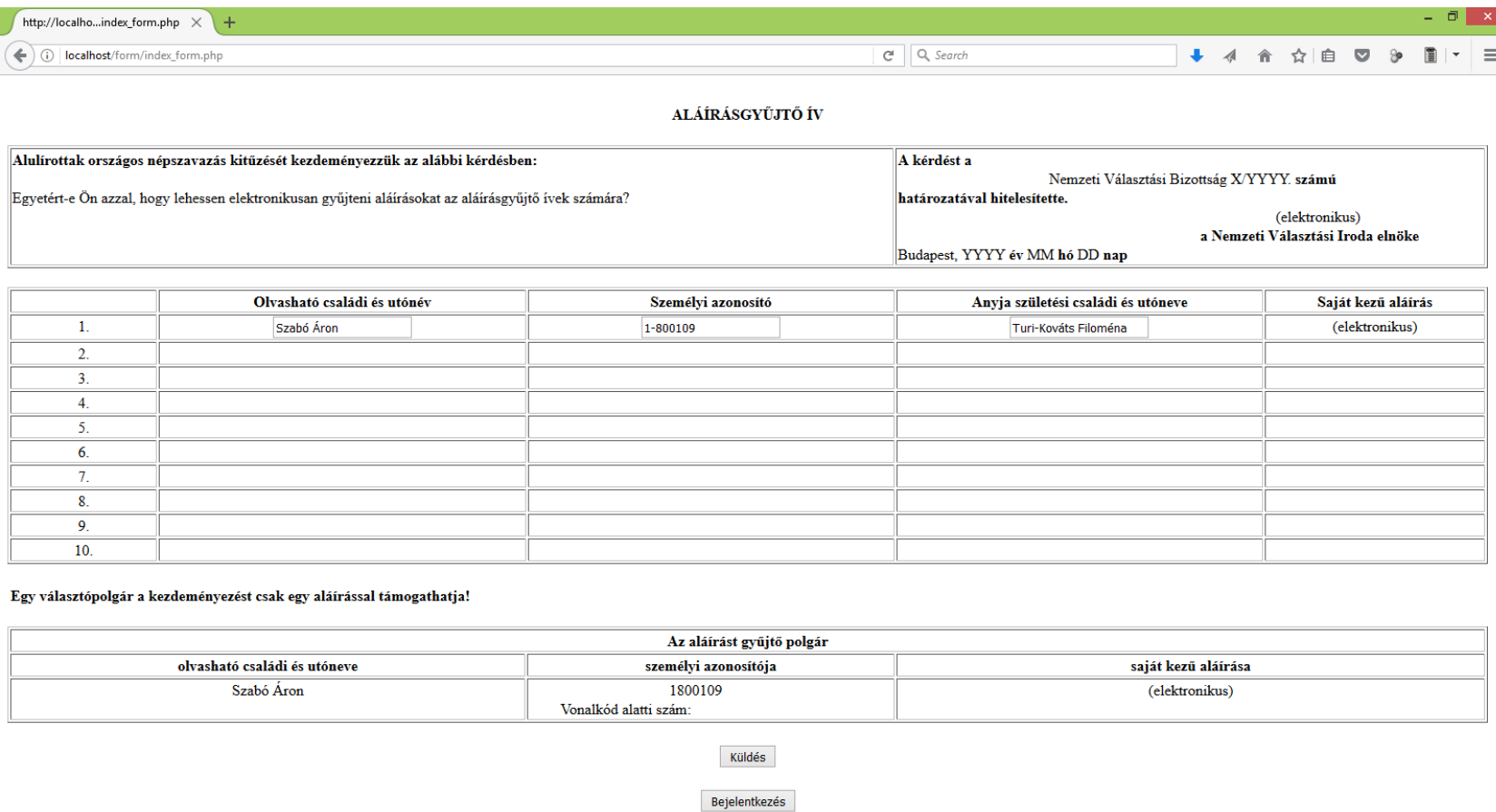
ECDSA_P256

[Részletek meatekintése](#)

Az aláírásgyűjtés

Az aláírás létrehozása felhasználói (GUI) vagy gépi (WS) felületen keresztül:

- webes űrlapos felület megnyitása a böngészőben



The screenshot shows a web browser window with the URL `http://localhost/form/index_form.php`. The page title is "ALÁÍRÁSGYŰJTŐ ÍV".

Alulírottak országos népszavazás kitzüzését kezdeményezzük az alábbi kérdésben:
Egyetért-e Ön azzal, hogy lehessen elektronikusan gyűjteni aláírásokat az aláírásgyűjtő ívek számára?

A kérdést a Nemzeti Választási Bizottság X/YYYY. számú **határozatával hitelesítette.**
(elektronikus)
a Nemzeti Választási Iroda elnöke
Budapest, YYYY év MM hó DD nap

	Olvasható családi és utónév	Személyi azonosító	Anyja születési családi és utóneve	Saját kezű aláírás
1.	<input type="text" value="Szabó Áron"/>	<input type="text" value="1-800109"/>	<input type="text" value="Turi-Kováts Filoména"/>	(elektronikus)
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				

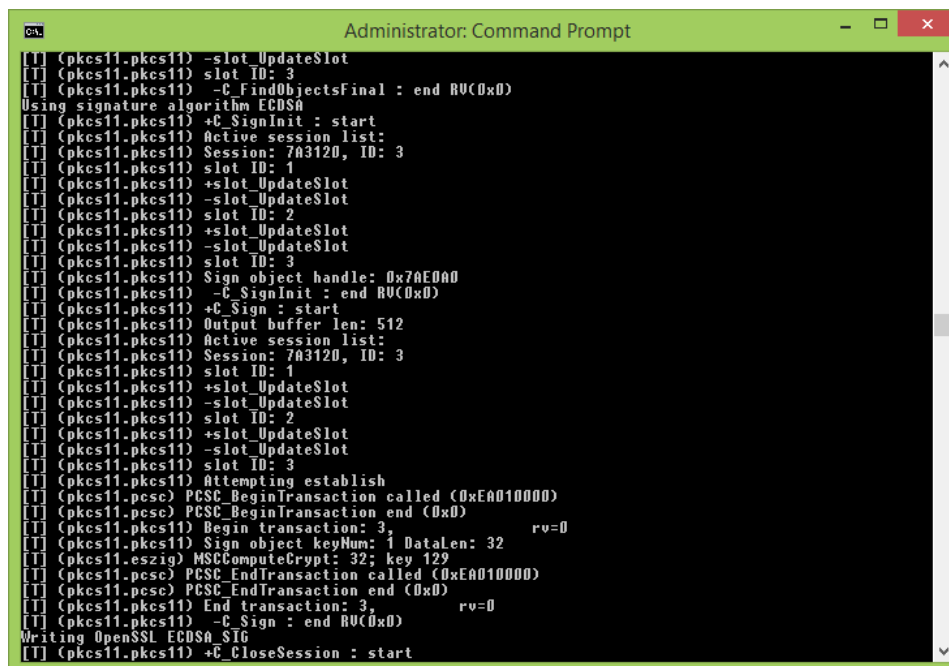
Egy választópolgár a kezdeményezést csak egy aláírással támogathatja!

Az aláírást gyűjtő polgár		
olvasható családi és utóneve	személyi azonosítója	saját kezű aláírása
Szabó Áron	1800109	(elektronikus)
Vonalkód alatti szám:		

Az aláírásgyűjtés

Az aláírás létrehozása felhasználói (GUI) vagy gépi (WS) felületen keresztül:

- a lenyomat kódolása eSZIG kártyával OpenSC (PKCS#11) révén
pkcs11-tool.exe --module C:/Windows/SysWOW64/eszig-pkcs11.dll
--login --pin 1234567 --sign --id 1 --input SignedInfo_binary_hash.txt
--output SignatureValue_binary.txt --mechanism ECDSA
- a kódolt lenyomat visszaküldése és az aláírt dokumentum tárolása

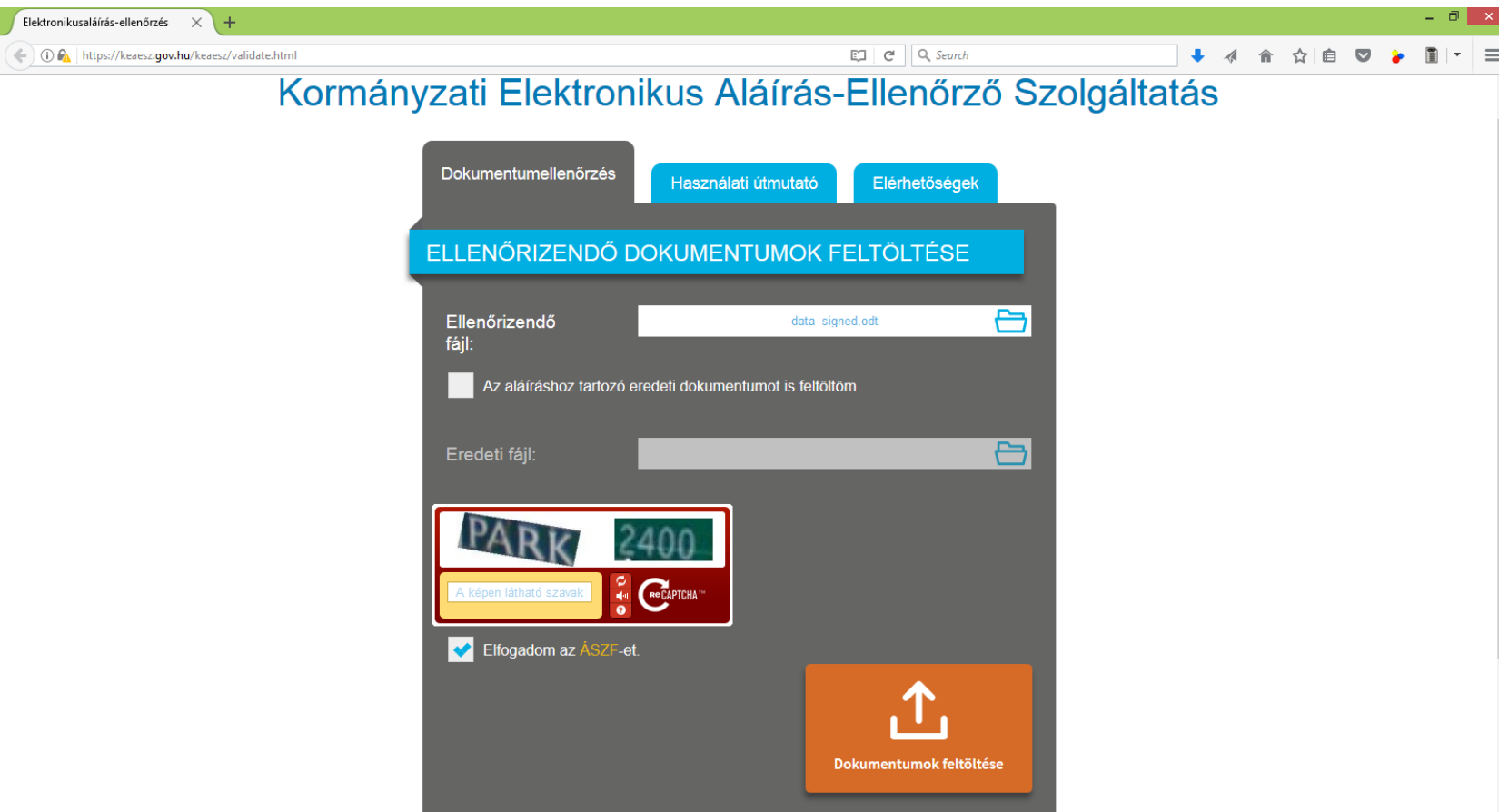


```
Administrator: Command Prompt
[!] (pkcs11.pkcs11) -slot_UpdateSlot
[!] (pkcs11.pkcs11) slot ID: 3
[!] (pkcs11.pkcs11) -C_FindObjectsFinal : end RV(0xD)
Using signature algorithm ECDSA
[!] (pkcs11.pkcs11) +C_SignInit : start
[!] (pkcs11.pkcs11) Active session list:
[!] (pkcs11.pkcs11) Session: 7A3120, ID: 3
[!] (pkcs11.pkcs11) slot ID: 1
[!] (pkcs11.pkcs11) +slot_UpdateSlot
[!] (pkcs11.pkcs11) -slot_UpdateSlot
[!] (pkcs11.pkcs11) slot ID: 2
[!] (pkcs11.pkcs11) +slot_UpdateSlot
[!] (pkcs11.pkcs11) -slot_UpdateSlot
[!] (pkcs11.pkcs11) slot ID: 3
[!] (pkcs11.pkcs11) Sign object handle: 0x7AE0A0
[!] (pkcs11.pkcs11) -C_SignInit : end RV(0xD)
[!] (pkcs11.pkcs11) +C_Sign : start
[!] (pkcs11.pkcs11) Output buffer len: 512
[!] (pkcs11.pkcs11) Active session list:
[!] (pkcs11.pkcs11) Session: 7A3120, ID: 3
[!] (pkcs11.pkcs11) slot ID: 1
[!] (pkcs11.pkcs11) +slot_UpdateSlot
[!] (pkcs11.pkcs11) -slot_UpdateSlot
[!] (pkcs11.pkcs11) slot ID: 2
[!] (pkcs11.pkcs11) +slot_UpdateSlot
[!] (pkcs11.pkcs11) -slot_UpdateSlot
[!] (pkcs11.pkcs11) slot ID: 3
[!] (pkcs11.pkcs11) Attempting establish
[!] (pkcs11.pcsc) PCSC BeginTransaction called (0xEA010000)
[!] (pkcs11.pcsc) PCSC BeginTransaction end (0xD)
[!] (pkcs11.pkcs11) Begin transaction: 3, rv=0
[!] (pkcs11.pkcs11) Sign object keyNum: 1 DataLen: 32
[!] (pkcs11.eszig) MSCComputeCrypt: 32; key 129
[!] (pkcs11.pcsc) PCSC EndTransaction called (0xEA010000)
[!] (pkcs11.pcsc) PCSC EndTransaction end (0xD)
[!] (pkcs11.pkcs11) End transaction: 3, rv=0
[!] (pkcs11.pkcs11) -C_Sign : end RV(0xD)
Writing OpenSSL ECDSA Sig
[!] (pkcs11.pkcs11) +C_CloseSession : start
```

Az aláírásgyűjtés

Az aláírás ellenőrzése felhasználói (GUI) vagy gépi (WS) felületen keresztül:

- az aláírt dokumentum elküldése ellenőrzésre



Elektronikus aláírás-ellenőrzés

https://keasz.gov.hu/keasz/validate.html

Kormányzati Elektronikus Aláírás-Ellenőrző Szolgáltatás

Dokumentumellenőrzés Használati útmutató Elérhetőségek

ELLENŐRIZENDŐ DOKUMENTUMOK FELTÖLTÉSE

Ellenőrizendő fájl: data_signed.odt

Az aláíráshoz tartozó eredeti dokumentumot is feltöltöm

Eredeti fájl:

A képen látható szavak reCAPTCHA

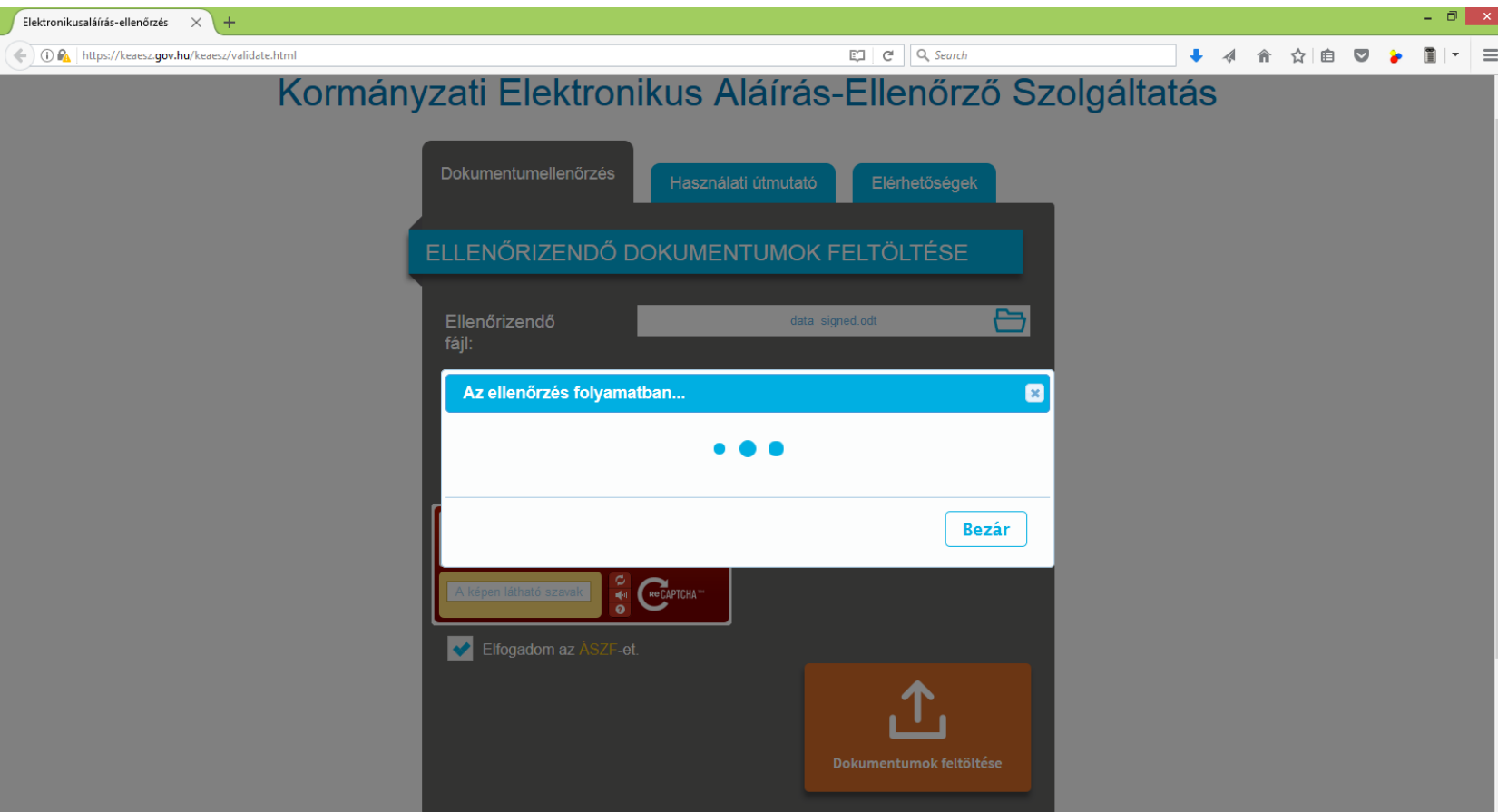
Elfogadom az ÁSZF-et.

Dokumentumok feltöltése

Az aláírásgyűjtés

Az aláírás ellenőrzése felhasználói (GUI) vagy gépi (WS) felületen keresztül:

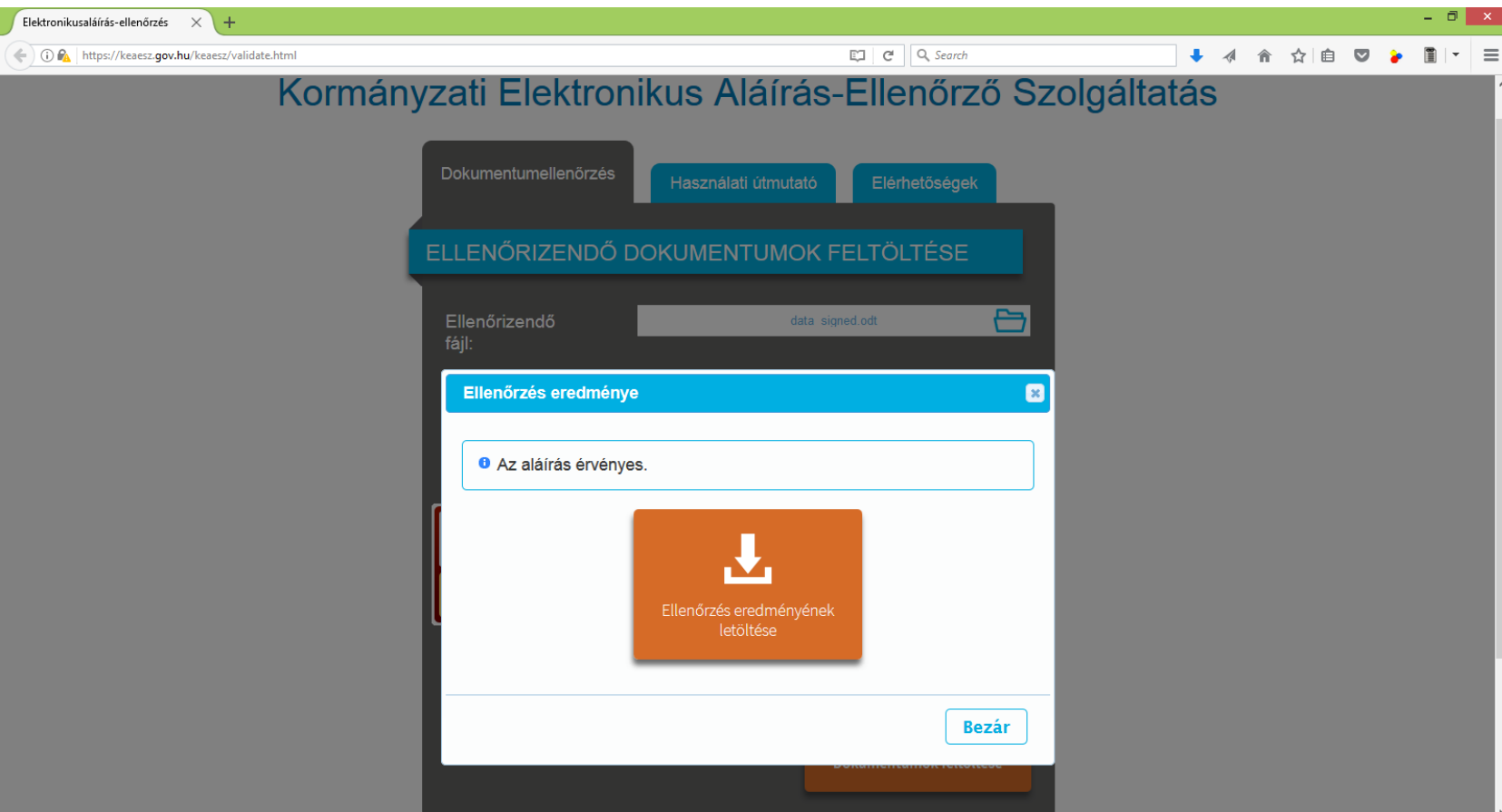
- az aláírt dokumentum ellenőrzése



Az aláírásgyűjtés

Az aláírás ellenőrzése felhasználói (GUI) vagy gépi (WS) felületen keresztül:

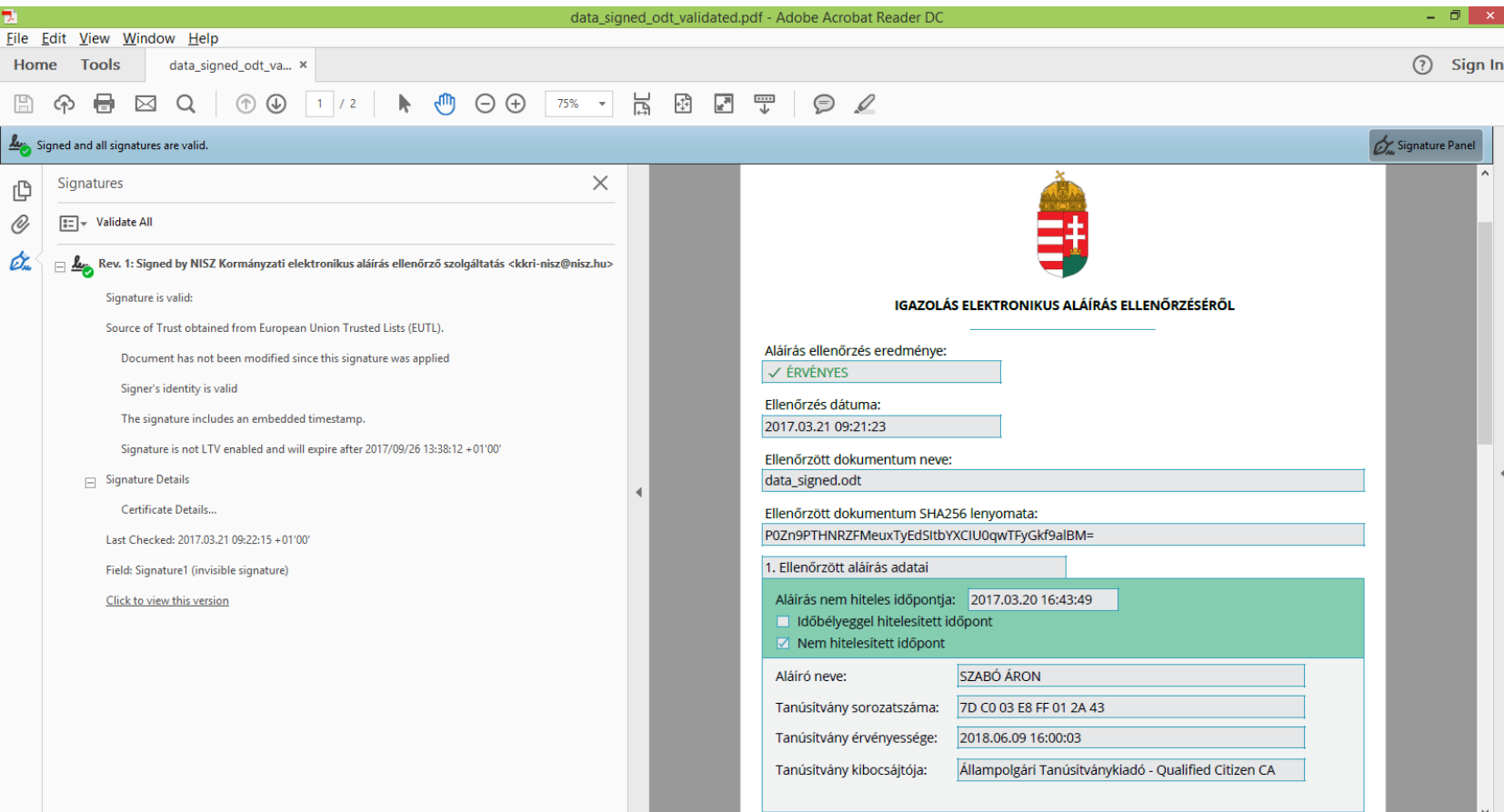
- az aláírt dokumentum ellenőrzési eredményének letöltése



Az aláírásgyűjtés

Az aláírás ellenőrzése felhasználói (GUI) vagy gépi (WS) felületen keresztül:

- az aláírt dokumentum ellenőrzési eredményének megjelenítése



data_signed_odt_validated.pdf - Adobe Acrobat Reader DC

File Edit View Window Help

Home Tools data_signed_odt_va... x Sign In

Signed and all signatures are valid. Signature Panel

Signatures

Validate All

Rev. 1: Signed by NISZ Kormányzati elektronikus aláírás ellenőrző szolgáltatás <kkri-nisz@niz.hu>

Signature is valid:

Source of Trust obtained from European Union Trusted Lists (EUTL).

Document has not been modified since this signature was applied

Signer's identity is valid

The signature includes an embedded timestamp.

Signature is not LTV enabled and will expire after 2017/09/26 13:38:12 +01'00'

Signature Details

Certificate Details...

Last Checked: 2017.03.21 09:22:15 +01'00'

Field: Signature1 (invisible signature)

[Click to view this version](#)

IGAZOLÁS ELEKTRONIKUS ALÁÍRÁS ELLENŐRZÉSÉRŐL

Aláírás ellenőrzés eredménye:
✓ ÉRVÉNYES

Ellenőrzés dátuma:
2017.03.21 09:21:23

Ellenőrzött dokumentum neve:
data_signed.odt

Ellenőrzött dokumentum SHA256 lenyomata:
POZn9PTHNRZFMeuxTyEdSibYXCIU0qWTFyGkF9alBM=

1. Ellenőrzött aláírás adatai

Aláírás nem hiteles időpontja: 2017.03.20 16:43:49

Időbélyeggel hitelesített időpont

Nem hitelesített időpont

Aláíró neve: SZABÓ ÁRON

Tanúsítvány sorozatszama: 7D C0 03 E8 FF 01 2A 43

Tanúsítvány érvényessége: 2018.06.09 16:00:03

Tanúsítvány kibocsájtója: Állampolgári Tanúsítványkiadó - Qualified Citizen CA

Az aláírásgyűjtés

Az aláírás ellenőrzése felhasználói (GUI) vagy gépi (WS) felületen keresztül:

- az aláírt dokumentum megjelenítése

The screenshot shows the LibreOffice Writer interface with a document titled "data_signed.odt (Signed)". A dialog box titled "Digital Signatures" is open, displaying the following information:

The following have signed the document content:

Description	Signature type
Signed by: SZABÓ ÁRON Digital ID issued by: Állampolgári Tanúsítván Date: 2017.03.14 14:14:19 Description: Signature type: XAdES	XAdES

Below the table, there are checkboxes and buttons:

- The signatures in this document are valid
- Use AdES-compliant signature when there is a choice
- Buttons: View Certificate..., Sign Document..., Remove, Help, Close

The background document is a form titled "ALÁÍRÁSGYŰJTŐ ÍV" (Signature Collection Form) with fields for personal identification and a table for recording signatures.

Köszönöm a figyelmet!



Már csak **199.999** aláírásra van szükség!



Szabó Áron
(aron.szabo@egroup.hu)