Developments of Identification and Trust Services in Public Administration through eIDAS

Otto Izso[1], Dr. Imre Négyesi[2]

1: Doctoral School of Public Administration Sciences; NUPS, Hungary

2: National University of Public Service, Hungary

Abstract

From July 1, 2016, the EU eSignatures Directive (1999/93/EC), was replaced by Regulation (EU) No. 910/2014 on electronic identification and trust services called the eIDAS regulation. eIDAS is the result of the European Union's Digital Agenda aimed to drive digital growth in the Union. As an EU regulation, the eIDAS is directly applicable law in all twenty-eight EU member states and in the European Economic Area. eIDAS wants to ensure that secure electronic identification and authentication is possible for cross-border online services offered by member states and electronic signatures will have the same legal weight as their physical counterparts. The eIDAS regulation was adopted to facilitate seamless digital transactions for individuals, businesses, and public administrations across countries within the European Union in two areas: electronic identification services and trust services. The new regulation expected to foster a climate of trust when it comes to online and digital transactions in the EU.

Keywords: eIDAS, Public Administration, Identification and Trust Services

Introduction

From July 1, 2016, the EU eSignatures Directive (1999/93/EC), was replaced by Regulation (EU) No. 910/2014 on electronic identification and trust services called the eIDAS regulation. eIDAS is the result of the European Union's Digital Agenda[3] aimed to drive digital growth in the Union. As an EU regulation, the eIDAS is directly applicable law in all twenty-eight EU member states and in the European Economic Area. eIDAS wants to ensure that secure electronic identification and authentication is possible for cross-border online services offered by member states and electronic signatures will have the same legal weight as their physical counterparts. The eIDAS regulation was adopted to facilitate seamless digital transactions for individuals, businesses, and public administrations across countries within the European Union in two areas: electronic identification services and trust services. The new regulation expected to foster a climate of trust when it comes to online and digital transactions in the EU.

eIDAS addresses *interoperability* and *transparency* requirements. Compliance with the interoperability common architecture defined by eIDAS[4] enables member states to deliver a framework that will recognize eIDs issued by any of the other member states. With regards to transparency eIDAS requires member states to maintain and publish a list of qualified trust providers and the specific trust services provided by them. A trust service provider must appear on this list to be a qualified. Trust services include digital signatures, time stamping, electronic seal, registered electronic delivery, and website authentication.

According to the eIDAS regulation electronic signatures are classified in the following three categories: simple, advances, and qualified. A *simple electronic signature* is the equivalent of a written signature. Some examples of a simple signatures are a typed name at the bottom of an e-mail, a scanned hand-written signature in a PDF file, or clicking an "I accept" button on a web page. *Advanced electronic signatures* are produced using encryption and can be used across member states. It must have a unique linking capability of identifying the signatory and it must be linked to the signed data in a way that any change in it is detectable. *Qualified electronic signatures* are advanced electronic signatures backed a qualified certificate issued by a trust service provider whose credentials appear in the EU trusted list. Advanced and qualified electronic signatures enable automated processes, digital proof of signatures, non-repudiation.

[3] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS A Digital Agenda for Europe
[4] "eIDAS – Interoperability Architecture" v. 1.00; November 6, 2015;
https://joinup.ec.europa.eu/sites/default/files/document/2015-11/eidas_interoperability_architecture_v1.00.pdf

The Implementing Acts

The European Commission also adopted eight implementing acts related to the eIDAS regulation in 2015 and 2016. Four of them concern electronic identification and the other four relate to electronic trust services:

Implementing acts concerning electronic identification:

- Commission Implementing Decision (EU) 2015/296[5] of 24 February 2015 establishing procedural arrangements for cooperation between Member States on electronic identification pursuant to Article 12(7) of Regulation (EU) No 910/2014
- Commission Implementing Regulation (EU) 2015/1501[6] of 8 September 2015 on the interoperability framework pursuant to Article 12(8) of Regulation (EU) No 910/2014
- Commission Implementing Regulation (EU) 2015/1502[7] of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014
- Commission Implementing Decision (EU) 2015/1984[8] of 3 November 2015 defining the circumstances, formats and procedures of notification pursuant to Article 9(5) of Regulation (EU) No 910/2014

Commission Implementing Decision (EU) 2015/296 of 24 February 2015 establishing procedural arrangements for cooperation between Member States on electronic identification pursuant to Article 12(7) of Regulation (EU) No 910/2014. Member states must work together to ensure interoperable and secure electronic identification systems. The decision also addresses information-sharing and creates a cooperation network supervised by the EC and made up of the member states' representatives and the countries of the EEA.[9]

Commission Implementing Regulation (EU) 2015/1501 of 8 September 2015 on the interoperability framework pursuant to Article 12(8) of Regulation (EU) No 910/2014 This regulation lays the foundation for a technical platform delivering an interoperability interface amongst the different eID systems.[10] Article 11 specifies the minimum set of data for both natural and legal persons to be used in a cross-border context.

To assist member states with the their own eIDAS compliant implementation, technical specifications are developed by the European Commission with assistance from the eIDAS Expert Group. The technical specifications supporting Commission Implementing Regulation (EU) 2015/1501 are not static as they are subject to further development. To date, there had been two releases (26/11/2016;

[5] https://ec.europa.eu/futurium/en/system/files/ged/celex_32015d0296_en_txt.pdf
[6] https://ec.europa.eu/futurium/en/system/files/ged/celex_32015r1501_en_txt.pdf
[7] https://ec.europa.eu/futurium/en/system/files/ged/celex_32015r1502_en_txt.pdf
[8] https://ec.europa.eu/futurium/en/system/files/ged/celex_32015d1984_en_txt.pdf
[9] www.personalausweisportal.de/EN/Government/eIDAS_Regulation/Regulation_Implementing_Acts/regulation_implementing_actss_node.html
[10] www.personalausweisportal.de/EN/Government/eIDAS_Regulation/Regulation_Implementing_Acts/regulation_implementing_actss_node.html

16/12/2016). The technical specifications cover eIDAS Message Format[11], Interoperability Architecture[12], Crypto Requirements for the eIDAS Interoperability Framework[13], and SAML Attribute Profile[14].

Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014

This implementing regulation establishes minimum technical specifications and procedures for low, substantial and high assurance levels for electronic identification. [15]

Commission Implementing Decision (EU) 2015/1984 of 3 November 2015 defining the circumstances, formats and procedures of notification pursuant to Article 9(5) of Regulation (EU) No 910/2014

This implementing decision sets out the process for notifying the European Commission of an electronic identification system including the description of the technical specifications of the system, definition and justification of the assurance levels. Notification is followed by a peer review of the system by the other member states.[16]

Electronic Trust services:

- Commission Implementing Regulation (EU) 2015/806[17] of 22 May 2015 on the form of the EU Trust Mark for Qualified Trust Services
- Commission Implementing Decision (EU) 2015/1505[18] of 8 September 2015 laying down technical specifications and formats relating to trusted lists
- Commission Implementing Decision (EU) 2015/1506[19] of 8 September 2015 laying down specifications relating to formats of advanced electronic signatures and advanced seals to be recognised by public sector bodies

[11] https://ec.europa.eu/cefdigital/wiki/download/attachments/46992719/eIDAS%20Message%20Format_v1.1-2.pdf?version=1&modificationDate=1497252919575&api=v2

[12] https://ec.europa.eu/cefdigital/wiki/download/attachments/46992719/eidas_interoperability_architecture_v1.00.pdf?version=1&modificationDate=1497252919857&api=v2

[13] https://ec.europa.eu/cefdigital/wiki/download/attachments/46992719/eidas_-_crypto_requirements_for_the_eidas_interoperability_framework_v1.0.pdf?version=1&modificationDate=1497252920224&api=v2

[14] www.personalausweisportal.de/EN/Government/eIDAS_Regulation/Regulation_Implementing_Acts/regulation_implementing_actss_node.html
https://ec.europa.eu/cefdigital/wiki/download/attachments/46992719/eIDAS%20SAML%20Attribute%20Profile%20v1.1_2.pdf?version=1&modificationDate=1497252920100&api=v2

[15] www.personalausweisportal.de/EN/Government/eIDAS_Regulation/Regulation_Implementing_Acts/regulation_implementing_actss_node.html

[16] www.personalausweisportal.de/EN/Government/eIDAS_Regulation/Regulation_Implementing_Acts/regulation_implementing_actss_node.html

[17] https://ec.europa.eu/futurium/en/system/files/ged/celex_32015r0806_en_txt.pdf

[18] https://ec.europa.eu/futurium/en/system/files/ged/celex_32015d1505_en_txt.pdf

[19] https://ec.europa.eu/futurium/en/system/files/ged/celex_32015d1506_en_txt.pdf

- Commission Implementing Decision (EU)2016/650[20] of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices

The Standards

European Telecommunications Standards Institute (ETSI)[21] supports eIDAS through the establishment of necessary standards in six functional areas:

1. Signature creation and validation
2. Signature creation and other related devices
3. Cryptographic suites
4. Trust service providers supporting digital signatures and related services
5. Trust application service providers
6. Trust service status lists providers

ETSI issues the following document types required for standardization:

- Guidance
- Policy & security requirements
- Technical specifications
- Conformity assessment
- Testing conformance & interoperability

Electronic Identification Card (EIC)[22]

Each period of the European EIC evolution can be characterized by a concept, functional user group, European interoperability idea and security solutions.

Following the adoption of the EU eSignatures Directive (1999/93/EC), the period of key cards can be placed between 2002 and 2007. The electronic identification cards function as a key to access and manage server based personal data. Primary example of key card is the Estonian national identity card (see more detail about this later). The Estonian national identity card functions as an analog personal identification document, but is also required for accessing electronic public services. The built-in chip allows digital identification of a person and the use of electronic signatures.

After the launch of the European Citizen Card concept and standards in 2008/2009 support for electronic signature on contact chip cards strengthened. Data for personal identification appeared in

[20] https://ec.europa.eu/futurium/en/system/files/ged/celex_32016d0650_en_txt.pdf
[21] Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures: overview (TR 119 100 v1.1.1); http://www.etsi.org/deliver/etsi_tr/119100_119199/119100/01.01.01_60/tr_119100v010101p.pdf
[22] "Az új, tároló elemet tartalmazó személyazonosító igazolvány bevezetésével összefüggő változások", SZAKMAI OKTATÓANYAG, 2015. p. 5-6

the memory of the chip and security features and data protection had undergone substantial advances. Belgium and Portugal (based on the Belgian card) cards are considered the initiators of this area.

The German personal identification card (nPA) opened a new area in 2010. The document was the first to include a contactless chip and serve as a travel document, electronic identification and electronic signature.

eID Schemes

Country	Name of the eID scheme	Type	Status
Austria	National Citizen ID	Multimean	In use
Belgium	National ID	Smartcard	In use
Bulgaria	National ID	Smartcard	In development
Croatia	e-Citizen	Multimean	In use
Cyprus	ARIADNI	Login	In use
	National ID	TBC	In development
Czech Republic	National ID	Smartcard	In development
	mojeID	Login	In use
Denmark	NemID	Login	In use
Estonia	National ID	Multimean	In use
Finland	FINeID	Certificates	In use
	TUPAS	Mobile	In use
France	FranceConnect	Login	In development
Germany	National ID	Smartcard	In use
Greece	ERMIS portal	Login	In use
	National ID	Smartcard	In development
Hungary	eSzemelyi	Smartcard	In use
Ireland	MyGovID	Login	In use
Italy	SPID	Multimean	In use
	National ID	Smartcard	In development
Latvia	eParaksts	Smartcard	In use
Lithuania	National ID	Smartcard	In use
Luxembourg	National ID	Smartcard	In use
	LuxTrust	Multimean	In use
Malta	National eID	Smartcard	In use
Netherlands	DigID	Login	In use
	eHerkenning	Login	In use
	Federation: Idensys, iDIN, DigID	Multimean	In development
Poland	National ID	Smartcard	In development
Portugal	Cartão do Cidadão	Smartcard	In use
	Chave Móvel Digital	Mobile	In use
Romania	National ID	Smartcard	In development
Slovakia	National ID	Smartcard	In use
Slovenia	eUprava	Certificates	In use
Spain	National ID	Smartcard	In use
	Various*	Certificates	In use
	Cl@ve	Login	In use
Sweden	Bank ID	Multimean	In use
	e-Legitimation (Telia)	Multimean	In use
United Kingdom	GOV.UK VERIFY	Multimean	In use

Table 1. Status of eIDs in Europe – Source: CEF Digital/Country overview; https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Country+Overview+-+eID

STATUS OF eIDs

The electronic identification schemes already in use or under development in Europe (see Table1.) illustrate that eIDAS allows member states flexibility to implement their choice of electronic identification if it complies with specifications set out by eIDAS. Smart card/chip enabled electronic identification cards are the preferred choice with sixteen of the member states opting for this option. Ten of these countries already use the smart card enabled ID card and another six are under development. eIDAS also does not require member states to introduce electronic identification as a mandatory/national identification document.

Germany was the first country to notify in July 2017. The notification process refers to the selection, peer review and official addition of national eID schemes to the eIDAS Network. The German electronic identification card (Der Personalausweis) enables citizens to access a variety of services from municipal, state and federal public administration system, to registering for university courses, and logging onto various insurance, financial and other services' websites. The card can also function as a travel card on Deutche Bahn. The biometric identifiers are restricted for use by the police and in border control, and are not available for online purposes.[23]

One of the most digitally developed countries in the world, ***Estonia*** has extensive experience with electronic identification. Estonia introduced electronic national identity cards in 2002 and currently has nearly 1.3 million national eIDs in force. In addition to serve as a traditional personal identification document, the eID comes with several functionalities, including:

- online access (login) to governmental institutions, public services, e-business services, banks and various other e-services in Estonia
- sign document electronically
- encrypt/decrypt documents
- i-voting
- e-prescriptions
- customer/loyalty card

Digi-ID is a stripped-down version of the above described national ID without the analog personal identification features, but with very similar electronic functionalities.

It is also possible to obtain a mobile-id with many of the same digital functionalities as the national ID, but without the need for a card reader.

Estonia also offers e-Residency to non-Estonians with the primary purpose of running location independent EU businesses online. [24]

[23] www.personalausweisportal.de/EN/Home/home_node.html
[24] www.id.ee/?lang=en

Emerging Security Risk[25]

Chip based electronic identification cards are considered very secure. However, Estonia had to block the certificates some 760 000 cards early November 2017 as a pre-emptive step based on a threat assessment by the authorities. As international cybercrime networks had become aware of a security flaw, the Estonian government decided to block the impacted certificates to prevent the possibility of e-identity theft.

The Estonian government understood that the e-state cannot function without unquestionable trust and delay would have increased the risk of actual identity theft which in turn would have raised serious questions in citizens concerning their trust in the e-state.

CER Estonia also posted a warning about the possibility that cybercriminals may attempt to exploit this situation and asked the public not to respond to any messages offering assistance with the ID card update, but instead forward them to CERT EE.[26]

While the security flaw identified (ROCA vulnerability) impacted only certain cards issued between specific dates, it still highlights the issue that digital identifications are not immune to flaws and when corrupted it may lead to a large-scale problem e.g. certificates on over 50% of the active Estonian national ID cards had to be blocked.

Hungary passed a number of legislations, including the Act CCXXII of 2015 regarding the electronic administration and general rules for trust services[27], 24/2016. (VI. 30.) of the Minister of Interior, providers of trust services and detailed requirements[28], 26/2016. (VI. 30.) of the Minister of Interior, trust, and records kept by the content of the notifications relating to the provision of trust services[29] and by the 414/2015. (XII. 23.) Government Decree on the Issuance of an Identity Card and the Single Facsimile and Signature Records Rules[30] to ensure regulatory alignment with eIDAS.

Hungary issues electronic personal identification cards since January 1, 2016. The cardholder's name, place of birth, date of birth, citizenship, mother's maiden name, sex, photo, signature, expiration date of the ID card, document identification number, date of issuance, and issuing authority are printed on

[25] Press Release: "Estonia will block the certificates of 760 000 ID cards as of the evening of 3 November"; November 2, 2017; https://www.id.ee/?id=30610&read=38341
[26] https://twitter.com/CERT_EE/status/926475950883328000
[27] 2015. évi CCXXII. törvény Törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól, MK 2015/202. (XII. 23.) p. 26809-26859
[28] 24/2016. (VI. 30.) BM rendelet Rendelet a bizalmi szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről; MK 2016/95. (VI. 30.) p. 7675- 7687
[29] 26/2016. (VI. 30.) BM rendelet Rendelet a bizalmi felügyelet által vezetett nyilvántartások tartalmáról és a bizalmi szolgáltatás nyújtásával kapcsolatos bejelentésekről; MK 2016/95. (VI. 30.) p. 7689 - 7694
[30] 414/2015. (XII. 23.) Korm. rendelet a személyazonosító igazolvány kiadása és az egységes arcképmás- és aláírás-felvételezés szabályairól, MK 2015/202. (XII. 23.) p. 26992- 27013

the card. The card also has an ICAO standard machine-readable zone (MRZ) which includes the key data elements required for personal identification.[31]

The chip imbedded card has four key electronic functions. The electronic travel document function (ePASS) allows citizens to use electronic gate entry system and other automatic electronic passenger entry systems where available - primarily at airports/ports in the Schengen-zone. The ePASS function also supports certain law enforcement task by making identification of a person easier and more secure. The electronic identification function (eID) allows citizens access to eGovernment and on-line public administration systems more effectively and at a higher security level than previous access methods (e.g. username/password). Full eIDAS compatibility of the Hungarian eID will also enable Hungarian citizens to access these systems in other EU countries as the cross-border capabilities rolled out in the member states. Access to and use of the social security number (TAJ) and tax identification number stored in the chip are also part of the eID function. The electronic signature function (eSIGN) is capable providing qualified electronic signatures with the same legal weight as their physical counterparts in accordance with Act. XXXV. 2001. Although the Hungarian electronic national ID is not issued in the National Unified Card System (NEK), the other electronic services function (eNEK) allows the card holder to access on-line NEK services. Other functions also include the ability to use electronic public transportation services (e.g. eTicket) given that these future systems are compatible with the NEK system. The range of additional electronic/on-line services accessible with the electronic national ID is expected to grow substantially in the future.

	2016 H1	Proportion of applicants as a ratio to total eligible	2017 H1	Proportion of applicants as a ratio to total eligible
Cards w/o chip	58,545	74.3%	63,949	86.3%
Fingerprint	324,649	56.7%	265,564	49.0%
e-Signature	46,701	8.5%	30,550	5.9%
Emergency Contact Number			187,956	28.1%

Table 2. Number of applications and the ratio of applications among total eligible for selected key functions and services of the Hungarian eID. Author's own creation. Source: Elektronikus közszolgáltatásokat és ügyfélszolgálati tevékenységet összefoglaló monitoring jelentés - 2017. I. félév

[31] "Az új, tároló elemet tartalmazó személyazonosító igazolvány bevezetésével összefüggő változások", SZAKMAI OKTATÓANYAG, 2015. p. 8

Analysis of the take up of the new electronic functions provided by the Hungarian eID card reveals, that most citizens over the age of sixty-five elect to receive the identification document without chip imbedded. Primary reason appears to be the fact that citizens over the age of sixty-five are allowed by law to receive a no chip card with no expiration date. However, it should be noted that while the ratio of no-chip cards appears to be very high among the eligible age group, overall these cards make up a lesser, but still sizable 9.6% of total new applications.

Recording of cardholder's fingerprint on the chip has declined versus 2016 and is slightly below fifty percent. The likely primary reason for this citizens' concern for privacy and lack of understanding how fingerprint data effect utility of the card either way. The very low take-up (5.9% vs 8.5% in H1 2017 vs. H1 2016) appears to be a strong indicator that applicants do not understand and see the benefit of having e-signing capability in their hands which also reflects the fact that the use of e-signatures is not wide spread in Hungary.

As one of the objectives of the introduction of eIDs and eSignatures is providing citizens with convenient time-saving on-line remote access to public services, it is important to consider the country's starting point in terms of eGovernment and digital readiness. According to the most resent (2017) Digital Economy and Society Index (DESI), Hungary ranks 21th out of the EU 28 and belongs to the Low Performing Cluster of countries together with Romania, Bulgaria, Greece, Italy, Croatia, Poland, Cyprus, and Slovakia.

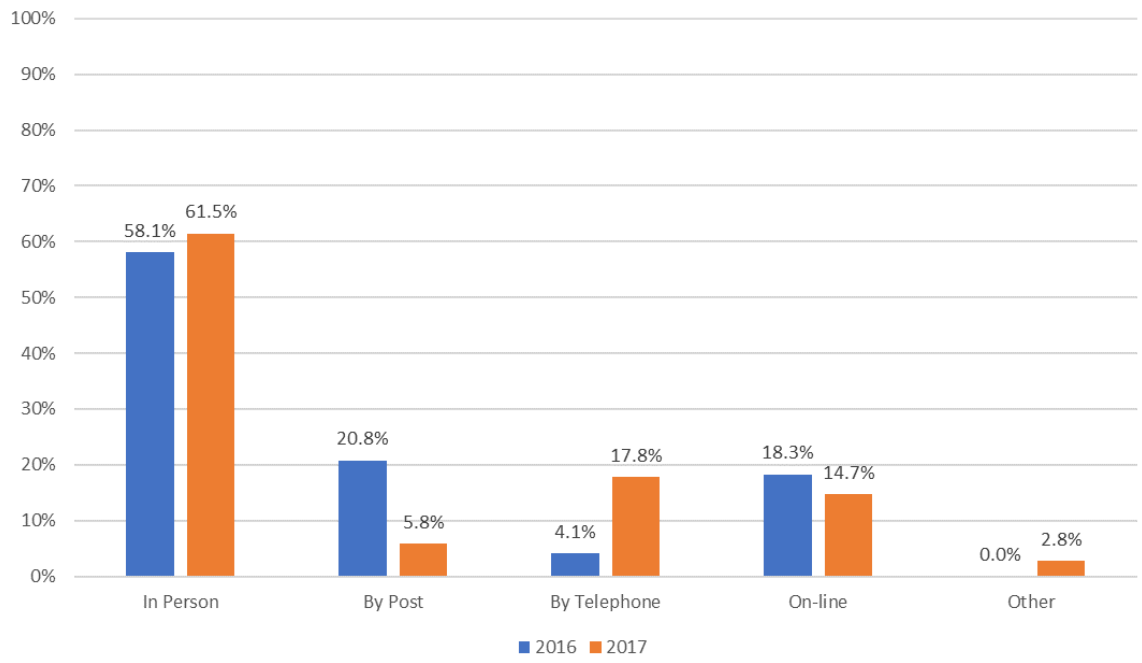

Chart 1. Utilization of public administration channels available. Author's own creation, Source: Jó Állam Jelentés 2017

The 2017 Good State and Governance Report examined through which channels the Hungarian public access public administration services (see chart 1). The survey had found that despite the progress made increasing online accessibility of public services, the clear majority of public administration services are still conducted off-line/in person (61.5%, 2017), usage of postal services has dropped considerably compared to the prior year (5.8%, 2017 vs 20.8%, 2016), and it appears that this drop indicated a shift in client preference conducting public administration services by telephone. Surprisingly, share of online/digital public services have also declined from just above 18% in 2016 to below 15% in 2017. The report identifies many factors contributing to this trend. The primary reason cited by the report is that most cases cannot be fully completed online. In addition, limited digital accessibility and lack competence; lack of trust in online customer service; impersonal nature of the online world and preference of face-to-face interaction, lack of clarity what, where and how can be done, time consuming to figure out what should be done, and too complicated instructions are some of the other key reasons identified by the report.

The report provides the following recommendations which should be consider in order to increase the share of higher value added online public services in client interactions.

- Development of comprehensive strategy to move clients to online channels and stop parallel development of all off-line channels
- Mandatory, strong motivation to move clients to online channels, instead of the voluntary migration based on perceived benefits
- Education and service marketing to combat competency and trust gaps

Conlcusion

The European Union eGovernment Action Plan 2016-2020 sets out an ambitious vision to deliver ". . . open, efficient and inclusive, providing borderless, personalised, user-friendly, end-to-end digital public services to all citizens and businesses in the EU" by 2020. It also sets the principles to be observed by the initiatives designed to accelerate the digital transformation of European governments. Public administrations should be digital by default, should ask for the same information only once, should be inclusive and accessible to all regardless of age or disability. In addition, openness and transparency, cross-borders access and interoperability of digital public services together with trustworthiness and security are the key principles to ensure trust and take up of electronic public services. eIDAS enabled electronic identification and trust services are important components of delivering this strategy.

Education of the public concerning new developments in eGovernment/electronic public administration is also a key factor of success. Informing citizens of the possible current and expected future use of eID functionalities should gradually improve the take-up of the new electronic functionalities such as e-signature. Completing the digital transformation of public administration services and engaging the private sector in developing new ways of utilising the electronic functions (e.g. financial services, public/private transport, etc.) of the eID should also drive up interest. While

electronic identification card and e-signatures functionalities imbedded in them are here to stay, mobile and smart device technology are also key areas of focus given the wide use of these devices in Europe. Many of the member states already have electronic identification and signature functionalities on mobile/smart devices (see Table 1.)

References

Dumortier, Jos. "Regulation (EU) No 910/2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market (eIDAS Regulation)." SSRN Scholarly Paper. Rochester, NY: Social Science Research Network, July 1, 2016.

European Union: Regulation EU No 910/2014 of the European Parliament and of the Council, 23 July 2014. http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A32014R0910&from=EN

European Union: "eIDAS – Interoperability Architecture" v. 1.00; November 6, 2015; https://joinup.ec.europa.eu/sites/default/files/document/2015-11/eidas_interoperability_architecture_v1.00.pdf

European Union: Commission Implementing Decision (EU) 2015/296 of 24 February 2015 establishing procedural arrangements for cooperation between Member States on electronic identification pursuant to Article 12(7) of Regulation (EU) No 910/2014; https://ec.europa.eu/futurium/en/system/files/ged/celex_32015d0296_en_txt.pdf

European Union: Commission Implementing Regulation (EU) 2015/1501 of 8 September 2015 on the interoperability framework pursuant to Article 12(8) of Regulation (EU) No 910/2014; https://ec.europa.eu/futurium/en/system/files/ged/celex_32015r1501_en_txt.pdf

European Union: Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014; https://ec.europa.eu/futurium/en/system/files/ged/celex_32015r1502_en_txt.pdf

European Union: Commission Implementing Decision (EU) 2015/1984 of 3 November 2015 defining the circumstances, formats and procedures of notification pursuant to Article 9(5) of Regulation (EU) No 910/2014; https://ec.europa.eu/futurium/en/system/files/ged/celex_32015d1984_en_txt.pdf

European Union: Commission Implementing Regulation (EU) 2015/806 of 22 May 2015 on the form of the EU Trust Mark for Qualified Trust Services; https://ec.europa.eu/futurium/en/system/files/ged/celex_32015r0806_en_txt.pdf

European Union: Commission Implementing Decision (EU) 2015/1505 of 8 September 2015 laying down technical specifications and formats relating to trusted lists; https://ec.europa.eu/futurium/en/system/files/ged/celex_32015d1505_en_txt.pdf

European Union: Commission Implementing Decision (EU) 2015/1506 of 8 September 2015 laying down specifications relating to formats of advanced electronic signatures and advanced seals to be recognised by public sector bodies; https://ec.europa.eu/futurium/en/system/files/ged/celex_32015d1506_en_txt.pdf

European Union: Commission Implementing Decision (EU)2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices; https://ec.europa.eu/futurium/en/system/files/ged/celex_32016d0650_en_txt.pdf

Elektronikus közszolgáltatásokat és ügyfélszolgálati tevékenységet összefoglaló monitoring jelentés - 2017. I. félév, Belügyminisztérium - Informatikai Helyettes Államtitkárság,

Négyesi Imre: Az elektronikus aláírás lehetőségei a Magyar Honvédségben I. (Nemzetvédelmi Egyetemi Közlemények, 11. évfolyam/3. szám (2007), 110-121. oldal, ISSN 1417-7323);

Négyesi Imre: Az elektronikus aláírás lehetőségei a Magyar Honvédségben II. (Nemzetvédelmi Egyetemi Közlemények, 11. évfolyam/3. szám (2007), 122-137. oldal, ISSN 1417-7323);

Kaiser et. al, Jó Állam Jelentés 2017, Dialóg Campus Kiadó, 2017

Leitold, Herbert. “Challenges of eID Interoperability: The STORK Project.” In Privacy and Identity Management for Life, 144–50. IFIP Advances in Information and Communication Technology. Springer, Berlin, Heidelberg, 2010.

Török, Rikk: New methods to protect our network systems; AMERICAN JOURNAL OF RESEARCH EDUCATION AND DEVELOPMENT 2017:(1) pp. 4-16. (2017) ISSN 2471-9986

Press Release: “Estonia will block the certificates of 760 000 ID cards as of the evening of 3 November”; November 2, 2017; https://www.id.ee/?id=30610&read=38341

Tsakalakis, Niko, Kieron O’Hara, and Sophie Stalla-Bourdillon. “Identity Assurance in the UK: Technical Implementation and Legal Implications Under the eIDAS Regulation.” In Proceedings of the 8th ACM Conference on Web Science, 55–65. WebSci ’16. New York, NY, USA: ACM, 2016.