sciendo

Scientific Bulletin
Vol. XXIX, No. 1(57), 2024

A RISK ASSESSMENT OF THE HUNGARIAN EID CARD

Norbert NYÁRI
nyari.norbert@uni-obuda.hu

András KERTI
kerti.andras@uni-obuda.hu

ÓBUDA UNIVERSITY, BUDAPEST, HUNGARY

ABSTRACT:

The aim of the present study is to provide an insight to a comprehensive risk assessment of the Hungarian eID card utilizing the ISO/IEC 27005:2022 standard. Unfortunately, the functions of the eID are nowhere near widespread among the Hungarian population. That is why it is time to carry out a risk assessment, which can help to introduce the functions efficiently, and improve the overall security of the eID card. Using the concepts and steps of the international standard ISO/IEC 27005:2022, the external and internal context of the Hungarian eID was determined, and after the asset-based risk identification, the risks that arose were evaluated. A comprehensive risk analysis can greatly help the effective introduction and operation of eGovernment services. The risks identified during the risk assessment, based on the ISO/IEC 27005:2022, performed on the Hungarian eID card can serve as a basis for the planning and development of appropriate IT security best practices and training materials. Previously, no risk analysis of the Hungarian eID was published based on the ISO/IEC 27005:2022. The results can contribute to making existing use cases safer, but it can also be used to create new use cases keeping IT security in mind.

KEYWORDS:

Electronic signature, IT security, information security, electronic identification card, risk assessment

1. Introduction

The eIDAS compliant Hungarian eID card has many use cases. The main areas include electronic identification, public transportation, receiving postal items, travel document within the EU and electronic signature (eSig). It is suitable for storing various data, for example: digital certificate for electronic signature, ICE telephone numbers, residential address data, identification numbers (social security number, personal identification number), fingerprint, etc (Hungarian Ministry of Interior).

The 2014 EU regulation eIDAS (electronic IDentification, Authentication, and trust Services) 'on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC' facilitates the transparent, secure, technology-neutral and trouble-free flow of commerce in the EU, also supporting the Digital Single Market (DSM) for member states (REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, 2014).

DOI: 10.2478/bsaft-2024-0010

© 2024 Norbert Nyári et al. This work is licensed under the Creative Commons Attribution-Non Commercial-No Derivatives 3.0 License.

Being one of the top ten priorities of the European Commission the Digital Single Market Strategy aims to fit the EU's single market for the digital age removing virtual borders, boosting digital connectivity, and making it easier for consumers to access cross-border online content (European Economic and Social Committee, 2020).

eIDAS unifies the use of electronic identification (eID), being effective across borders as well as within individual member states, defining the "electronic trust services" (eTS), ensuring the legal validity of electronic signatures and creating a European internal market for electronic trust services (scrive)(REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, 2014).

The Government decree no. 414/2015. (XII. 23.) on the rules for the issuance of personal identification cards defines a transaction limit, which is the maximum value of the financial transaction that the signer can make with his electronic signature using the eID. The certificates on the eID card are issued by NISZ Zrt., and the transaction limit is 50,000,000 HUF based on the previous legislation (Government decree no. 414/2015 (XII. 23.) on the rules for the issuance of personal identification cards, 2022).

Since January 2023, a new role-based authentication solution is available in Hungary. Using this service, the electronic signatures created using the Hungarian eID card can be supplemented with an attribute certificate that includes the signer's position in an organization at the time of the signature creation. This is however only available for governmental employees for now (Hungarian Ministry of Interior, 2023).

Unfortunately, currently in Hungary electronic trust services and electronic signature services are not considered as a critical infrastructure according to the Act CLXVI of 2012 (Act CLXVI of 2012, 2012). Over time, however, as the use of the document becomes more and more integrated into everyday life citizens will heavily depend on electronic trust services and electronic signature services.

Handling electronic trust service providers and electronic signature services as a critical infrastructure should be reflected in the Hungarian legal environment as well. To adequately protect the infrastructure, it is necessary to develop procedures and best practices, as stated by Somogyi & Nagy (2022) in relation to the financial sector. Since citizens' dependence on eID cards will probably increase over time, it would be recommended to introduce similar solutions as in the case of bank cards (e.g. the possibility of disabling stolen/lost eIDs as soon as possible).

Farkas (2023) states that with the introduction of new technologies, new questions, concerns, and uncertainties (ultimately risks) also appear, the exploration and proper handling of which is at least as important as the development and introduction of the technology itself. When developing new solutions, safety must always be kept in mind in order to reduce risks.

Several previous studies prove the importance of risk management in the field of electronic identification schemes. Related articles are reviewed in the next section.

2. Literature review

Pernpruner et al. (2020) presented a new protocol for the usage of eID cards involving multi factor authentication utilizing NFC devices and push notifications. Evaluating the security of their solution they used the OWASP Risk Rating Methodology. The results indicated that doing so eventually reduced overall risk. Furthermore, a formal risk analysis can effectively complement the development of new solutions while enhancing security.

The official OWASP website (OWASP) however states that "there are other more mature, popular, or well-established Risk Rating Methodologies that can be followed". On one hand the list

includes NIST SP 800-30, on the other hand it surprisingly excludes ISO/IEC 27005. According to NIST SP 800-30 (SP 800-30 revision 1, 2012) the two are compatible with each other though.

It is advisable to use the ISO/IEC 27000 family of standards, because an organization can certify the information security management system (ISMS) created based on ISO/IEC 27001 (ISO/IEC 27001:2022, 2022). Furthermore, the Hungarian framework MIBIK (Hungarian IT Security Framework (MIBIK), 2008) (Magyar Informatikai Biztonsági Keretrendszer – Hungarian Information Security Framework) is highly related to the previous standard, because it is based on the ISO/IEC 17799 which is the predecessor of the ISO/IEC 27002.

Leitner & Schaumuller-Bichl (2009) state that the "Austrian Information Security Handbook" contains best practices and recommendations regarding IT security for the Austrian public authorities. Risk analysis is vital for creating an ISMS. Based on the ISO/IEC 27000 family of standards the handbook however does not make any restrictions (nor the ISO/IEC 27001) on the Risk Analysis methodology. They developed the framework ARiMA (Austrian Risk Management Approach) based on the ISO/IEC 27005:2008 and in line with the aforementioned handbook for public authorities combining 'well-established methods and techniques in a new way'.

Schwalm & Alamillo-Domingo (2021) state that the usage of the eIDAS compliant eID cards vary highly in EU members. The utilization of the German eID or the Spanish eID is still low compared to other identification methods. In opposition eIDs in Italy, Denmark and Estonia are widespread. The authors suggest that ISO/IEC 27005:2018 should be used to assess the risks related to the different Levels of Assurance when implementing an eID scheme based on EIDAS.

Nyári (2022) shows that the utilization of the Hungarian eID card is probably even lower due to the serious lack of information of Hungarian citizens related to the eID card and its possibilities. According to Koller (2023), the widespread use of the eID would be greatly facilitated by a mobile application that would make authentication using the ID card easier.

In a case study about the Colombian integrated public transport system (SITP) Mojica Sánchez, Leal Valero & Bareño Gutiérrez (2019) evaluated the risks of the different contactless RFID cards used in the system utilizing the ISO/IEC 27005 standard. According to their conclusion, a methodically performed, customized risk analysis greatly increases the probability of successful implementation of a development.

In their 2019 paper Patiño et al. (2018) state that the National Secretariat of Public Administration of Ecuador applied the ISO/IEC 27005:2011 standard in order to push back cybercrime. Their paper presents a practical guide for governmental entities to manage ICT (Information and Communications Technology) risks alongside with a case study including guidelines contributing to the definition of assessment formats and scales to facilitate the identification of assets, vulnerabilities, threats and controls. It is recommended that experts of the organization from different fields participate in the various stages of the implementation of the methodology, especially when communicating the risk management measures to be implemented.

In the thesis 'A Reference Risk Register for Information Security According to ISO/IEC 27005' Mateus (2016) proposes a reference risk management process through a case study that supports organizations in building their own consolidated, organization-level reference risk registers when performing risk assessments.

When developing eID regulations, legislators must perform rigorous risk analysis and risk management to effectively enforce data protection goals, but, of

course, a risk analysis cannot replace legal regulation and cannot provide immunity from legal accountability, according to Zwingelberg & Hansen (2011).

Lentner & Parycek (2016) examined eID solutions from the point of view of the use of eGovernment services specifically Citizen to Government (C2G) communications (e.g. submissions, motions, requests of documentation). Although the 2016 article is somewhat outdated, there are some important points to consider in their work. The article places emphasis on the risk management applied by legislators in the process of developing and implementing eGovernment services. The main difference of traditional and electronic identification is that in the former case the identification document is linked to the physical appearance of the person, this however cannot be done in the latter case.

Stemming from the latter, in some ways, identity theft is easier in the electronic world, especially if multi-factor authentication is not used. This is confirmed by the research by Paráda & Farkas (2020), according to which there are many different OSINT (Open-Source Intelligence) tools that can be used to collect data on the Internet for the preparation of penetration tests or even attacks. Reconnaissance can be extremely dangerous, since it is usually carried out in an undetectable form on the affected network, so it is mostly unknown to the operators and users of the network.

Edu et al. (Jide Edu, 2023) provide a review of different National electronic Identification Systems (NeID) and their challenges, pointing out the best practices of risk mitigation including recurring risk assessment and implementing effective security measures. The study shows the different categories of risks (eg. 'Security and privacy concerns', 'Legal and regulatory issues') and through multiple case studies it presents successful and secure implementations like the Estonian eID system which is said to be the most advanced eID system in the world. In addition, the authors state that the associated risks must be explored and well communicated to all stakeholders to create safe, user-friendly services.

According to Megyeri & Farkas (2017) the risk management of IT systems is an extremely important task; IT systems can be made safer by analysing attack methods and managing the risks they cause. They point out that the regulations in the Hungarian public sector require state organizations to implement risk management built into their processes and reviewed on an annual basis. They also emphasize the importance of risk assessment related to critical infrastructure elements.

There are however many standards related to risk analysis e.g. ISO 31000 - Risk analysis, NIST SP 800-30 Rev. 1 - Guide for Conducting Risk Assessments and ISO/SAE 21434 - Road vehicles Cybersecurity engineering. ISO 31000 is not for information security, neither ISO/SAE 21434, so these two are out of the scope of this study. There are also subjective reasons why we chose ISO/IEC 27005:2022. No new version of the NIST standard has been published since 2012. Moreover, ISO/IEC 27005:2022 seems to be underrated in Hungary, since it cannot be purchased on the official website of the Hungarian Standards Board (mszt.hu), nor is it translated into Hungarian. We would like to show that the application of the standard in question has many practical benefits (ISO)(SP 800-30 revision 1, 2012).

This section gives a good impression of the importance and usefulness of risk management in the field of eID documents. The proper risk analysis of the Hungarian electronic identity card and the electronic signature functionality would be vital for the development of adequate infrastructure protection. Considering this, a comprehensive risk analysis of the Hungarian eID based on the ISO/IEC 27005:2022 standard should be conducted. We will no longer write the year of the

standard ':2022', and where we refer to the standard as 'ISO/IEC 27005', we mean the 2022 edition. In the next sections, we present a possible application of the mentioned standard.

3. Methodology

The ISO/IEC 27000 family consists of quite a lot of standards. The most popular is ISO/IEC 27001, because organizations can certify their ISMS-s based on the standard. The ISO/IEC 27002 is closely related to the former one since it provides guidance on implementing ISO/IEC 27001. The ISO/IEC 27005 is about risk management, this is the one we used while writing this paper (ISO).

There are sector specific standards in the family worth mentioning: ISO/IEC 27033 provides guidance on identifying and managing network security risks. Furthermore, ISO/IEC 27034 presents guidelines on application security, it can be applied on both third-party and in-house developed applications (ISO).

Such standards should definitely be used in hardware/software development projects of this scale, like eID schemes.

Conducting the risk assessment of the Hungarian eID card we have followed the guidance of the ISO/IEC 27005:2022 standard. The steps are shown in Figure no. 1 below (ISO/IEC 27005:2022, 2022).

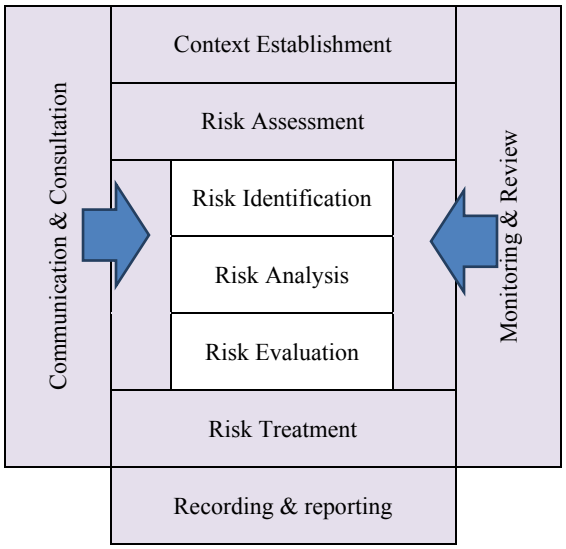


Figure no. 1: *Information Security Risk Management Process*
(Source: Author's contribution, based on ISO/IEC 27005)

In the Context Establishment phase the internal and external environment of the eID should be described in detail, including the legal environment (national and international regulations), relevant standards. The Information Security Risk Criteria are to be established as well, like the Risk Acceptance Criteria (RAC) and criteria for conducting the risk assessment. After that the methodology (qualitative or quantitative) should be selected keeping in mind, that the repeated risk assessments should be consistent and comparable (ISO/IEC 27005:2022, 2022).

Then, in the Risk Assessment phase, the Risk Identification sub-step follows. Firstly, either the asset-based or the new event-based approach introduced in the 2022 version of the standard should be selected. Defining the risk owners for each identified risk is very important, since they have the authority, responsibility, and competence to manage the risks identified (ISO/IEC 27005:2022, 2022).

After that comes the Risk Analysis where the previously established different criteria are applied in order to determine the

levels of risk. Risk owners should be involved and consulted with during this sub-step since they are the experts of their field, being able to give the most accurate estimations. This is a highly subjective process with many uncertainties though like personal, methodological, or systemic. To reduce subjectiveness an assessment team should be utilized instead of only one person (ISO/IEC 27005:2022, 2022).

The Evaluation of Information Security Risks follows. This step is less subjective because the calculated levels of identified risks should be compared to the Risk Acceptance Criteria established in the first step. The agreement of the risk owners should be obtained when deciding on acceptance. Practically, accepted risks do not require mitigation, only monitoring. This step can be performed in a more sophisticated way as well when different classes of risks (e.g. non-compliance risks) are established with different acceptance criteria (ISO/IEC 27005:2022, 2022).

Risks above the acceptable level need treatment, which is done in the following phase 'Risk Treatment'. According to the ISO/IEC 27005 standard (ISO/IEC 27005:2022, 2022), there are four, combinable, ways to treat risks:

- Avoidance: stop the actions or operations which are at the mercy of the risk in question in order to lower the likelihood to zero.
- Modification: reduce the likelihood or the consequences (or both).
- Sharing: get third parties involved (e.g. subcontractor, insurance company).
- Retention: well informed decision to retain risk usually by the top management, practically carrying the risky actions or operations on.

Controls may be necessary to be enforced to implement the risk treatment options. The suggested 93 controls are listed in the ISO/IEC 27001, divided into four themes: organizational, people, physical and technology. Controls can be further divided into preventive, detective, and corrective classes. As an ISO/IEC 27001 (ISO/IEC 27001:2022, 2022) requirement, the document Statement of Applicability should be created including the list of the necessary controls and the excluded controls with justification. Custom controls can be applied as well in a documented manner (ISO/IEC 27005:2022, 2022).

The Risk Treatment Plan is also required by the ISO/IEC 27001 standard (ISO/IEC 27001:2022, 2022). This document as well needs the approval of the risk owners. It should state how the organization intends to modify the risk that needs treatment. There is almost always Residual Risk though, which is the risk that remains after the treatment with, of course, the approval of the risk owners. The risk treatment is however not part of this study due to space limitations.

A risk assessment should be a repeatable process in planned intervals, the results of the assessments conducted in different times should be consistent and comparable. It should also be an integral part of the business operations. The risk assessment should be continuously improved over time, revising the methodology, refining the different risk criteria etc. (ISO/IEC 27005:2022, 2022).

The following section will show how the above concepts, methodology and criteria can be applied to the Hungarian eID card.

4. Results and discussion

In this case, an entire country, Hungary, should be understood instead of an organization, because most of the citizens could be involved in using the eID somehow. But in order to stay consistent with the standard, we will use the term 'organization' hereafter. In the following, we present an insight of the proposed course of risk management regarding the Hungarian eID.

4.1. Context establishment

Speaking of an EU member state, the external context of the organization regarding the Hungarian eID is the

European Union and the Digital Single Market. The internal context, Hungary itself, includes the Ministry of Interior, Citizens' Administrative Bureaus, third party subcontractors (like NISZ Zrt. as the developer and operator of many Hungarian eGovernment services including the eSignature feature of the eID(NISZ Zrt.); and IdomsoftZrt. as the developer and operator of the Hungarian eID infrastructure (Idomsoft Zrt.)), the various eGovernment services, and finally the Hungarian citizens eligible to eIDs.

Relevant national and international regulations, standards, and other policies, including but not limited to, are shown in the Table no. 1 below.

Table no. 1

Relevant regulations, standards

Name	Type
REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL (known as eIDAS)	International regulation
Directive (EU) 2022/2555 (known as NIS2)	International regulation
Government decree no. 414/2015. (XII. 23.) on the rules for the issuance of personal identification cards	National regulation
Act CCXXII of 2015 on the general rules of electronic administration and trust services	National regulation
Informative about services related to e-signatures that can be requested for identity cards by NISZ Zrt.	Organizational Policy
Act L of 2013 on the electronic information security of state and local government bodies	National regulation
Ministry of Interior Edict 41/2015. (VII. 15.) of 2015 on technological security and the requirements for secure information devices and products, as well as classification into security class and security level, as defined in Act L. of 2013 on the electronic information security of state and local government bodies	National regulation
Government Edict 187/2015. (VII. 13.) of 2015 on the duties and powers of the authorities responsible for the security supervision of electronic information systems, as well as the information security supervisor, as well as on the definition of closed-purpose electronic information systems	National regulation
ISO/IEC 27033 – network security	International standard
ISO/IEC 27034 – application security	International standard

(Source: Author's contribution)

The Risk Appetite of the organization should be low since the privacy and the identity of the citizens are at stake. Furthermore, financial transactions and contracts can be authorized using the electronic signature feature of the Hungarian eID. There is no room for unjustified risk-taking when it comes to people's money or privacy.

As external observers however, we do not have access to the various contracts concluded between the Hungarian state and the subcontractors, neither to the controls contained in them, nor to the results of previous risk managements, if there were any.

The suggested risk acceptance criteria are established on a consequence-possibility basis as follows: any risk with a level above low needs to be mitigated. The colour codes in the risk matrix are shown in Table no. 2.

We decided to follow a combined quantitative-qualitative approach based on the tables of Annex A of the ISO/IEC 27005 standard (ISO/IEC 27005:2022, 2022) when determining likelihood, consequences, and levels of risk.

Table no. 2

Colour codes in the risk matrix Source

Classes	Risk evaluation	Levels of risk
Low (green)	'Acceptable as is'	Very low, Low
Moderate (amber)	'Tolerable under control'	Medium
High (red)	'Unacceptable'	High, Very high

(Source: Author's contribution based on ISO/IEC 27005:2022, 2022)

Based on the published statistics (KSH, 2023) by the Hungarian Central Statistical Office (KSH), in October 2023, the net average earnings of those employed full-time was 389 300 HUF per month, which means 4 671 600 HUF per year. As previously stated, one can use the Hungarian eID card for contracts with a maximum value of 50 000 000 HUF. This limit is more than ten times the Hungarian average annual salary.

Table no. 3

Scale of consequences Source

Consequences	Description	A loss of
Catastrophic	'Sector or regulatory consequences beyond the organization.'	50,000,000 HUF and above
Critical	'Disastrous consequences for the organization'	4,000,000 HUF – 49,999,999 HUF
Serious	'Substantial consequences for the organization'	300,000 HUF – 3,999,999 HUF
Significant	'Significant but limited consequences for the organization'	20,000 HUF – 299,999 HUF
Minor	'Negligible consequences for the organization'	< 20,000 HUF

(Source: Author's contribution based on ISO/IEC 27005:2022, 2022)

Considering the above facts, Table no. 3 shows a scale for the classification of consequences.

Table no. 4 below contains the applied scale of likelihood based on the ISO/IEC 27005 standard.

Table no. 4

Scale of likelihood

Likelihood	Description
Almost certain	'The likelihood of the risk scenario is very high'
Very likely	'The likelihood of the risk scenario is high'
Likely	'The likelihood of the risk scenario is significant'
Rather unlikely	'The likelihood of the risk scenario is low
Unlikely	'The likelihood of the risk scenario is very low''

(Source: ISO/IEC 27005:2022, 2022)

The risk levels with the colour codes used are shown in Table no. 5 below. The different classes are visually separated in the table in order to help the decision on whether a risk should be managed or accepted.

Table no. 5

Levels of risk

Likelihood	Consequences				
	Catastrophic	Critical	Serious	Significant	Minor
Almost certain	Very high	Very high	High	High	Medium
Very likely	Very high	High	High	Medium	Low
Likely	High	High	Medium	Low	Low
Rather unlikely	Medium	Medium	Low	Low	Very low
Unlikely	Low	Low	Low	Very low	Very low

(Source: ISO/IEC 27005:2022, 2022)

4.2. Risk assessment

In this section we present the actual risk assessment with an asset-based approach of risk identification as a first step.

4.2.1. Risk identification

When using the asset-based approach, the very first step should be the identification of the assets. In table no. 6 below the list of discovered assets are shown without claiming to be exhaustive. The stakeholders are in the last column. The first column contains the assigned unique identifier for each of the assets.

Table no. 6

Register of assets

ID	Asset	Stakeholder
A1	eID card	Citizen
A2	PIN number for electronic authentication	Citizen
A3	PUK number for electronic authentication	Citizen
A4	PIN number for electronic signature	Citizen
A5	PUK number for electronic signature	Citizen
A6	PUK number plastic card for electronic authentication	Citizen
A7	PUK number plastic card for electronic signature	Citizen
A8	Personal data stored on eID chip	Citizen
A9	Hardware card reader for eID	Citizen
A10	'eSzemélyiM' mobile application	Citizen
A11	Mobile device for running 'eSzemélyiM' mobile application	Citizen
A12	The PC used for electronic authentication or electronic signature	Citizen
A13	The software used for electronic signature	Citizen
A14	The Hungarian eID infrastructure	Hungarian government
A15	The PKI infrastructure for electronic signature	Hungarian government
A16	eGovernment services	Hungarian government
A17	Electronic signature certificate stored on eID card	Citizens

(Source: Author's contribution)

The following step is to identify the risks in an asset-based approach. Practically speaking a risk is the possibility that a threat can exploit a vulnerability of an asset so all the assets in the above asset registry must be examined one by one to see what vulnerabilities they may be exposed to and what threats may exploit them (ISO/IEC 27005:2022, 2022).

Annex A of the ISO/IEC 27005 standard contains a comprehensive list of both threats and vulnerabilities, based on which lists the following table of risks can be created for each of the assets (ISO/IEC 27005:2022, 2022). As in the previous table we assigned a unique identifier for each of the risks ('Risk ID' column) regarding an asset. Table no. 7 shows the risks of asset number A1, the eID card. The 'Vulnerability' column contains the possible vulnerabilities (based on the standard) of the asset in question, the 'threat' column lists the threats (based on the standard) that may exploit the vulnerability.

Table no. 7

Risks of Asset A1 – eID card

Risks of asset	**A1 – eID card**		
Vulnerabilty	**Risk ID**	**Theat**	**Risk owner**
'VH03 Susceptibility to humidity, dust, soiling'	A1R1	'TP01 Fire'	Citizen
	A1R2	'TP02 Water'	Citizen
	A1R3	'TP06 Dust, corrosion, freezing'	Citizen
	A1R4	'TN04 Meteorological phenomenon'	Citizen
	A1R5	'TN05 Flood'	Citizen
	A1R6	'TH19 Incorrect use of devices'	Citizen
'VH04 Sensitivity to electromagnetic radiation'	A1R7	'TI06 Electromagnetic radiation'	Citizen
	A1R8	'TI08 Electromagnetic pulses'	Citizen
	A1R9	'TH19 Incorrect use of devices'	Citizen
'VH06 Susceptibility to voltage variations'	A1R10	'TI06 Electromagnetic radiation'	Citizen
	A1R11	'TI08 Electromagnetic pulses'	Citizen
	A1R12	'TH19 Incorrect use of devices'	Citizen
'VH07 Susceptibility to temperature variations'	A1R13	'TI07 Thermal radiation'	Citizen
	A1R14	'TH19 Incorrect use of devices'	Citizen
'VH08 Unprotected storage'	A1R15	'TH08 Theft of digital identity or credentials'	Developer of eID cards
'VH10 Uncontrolled copying'	A1R16	'TH08 Theft of digital identity or credentials'	Developer of eID cards
'VP03 Insufficient security training'	A1R17	'TH19 Incorrect use of devices'	Citizen
	A1R18	'TC01 Error in use'	Citizen
'VP04 Incorrect use of software and hardware'	A1R19	'TH19 Incorrect use of devices'	Citizen
	A1R20	'TH12 Tampering with hardware'	Citizen
	A1R21	'TC01 Error in use'	Citizen
'VP05 Poor security awareness'	A1R22	'TH04 Remote spying'	Citizen
	A1R23	'TH05 Eavesdropping'	Citizen
	A1R24	'TH06 Theft of media or documents'	Citizen
	A1R25	'TH12 Tampering with hardware'	Citizen

(Source: Author's contribution based on ISO/IEC 27005:2022, 2022)

The table above is an example of how risks should be identified for each of the assets. The first column is Vulnerability, the values came from the ISO/IEC 27005 standard. Most of the vulnerabilities can be exploited by multiple threats, so the vulnerabilities may be in merged cells. The second column is the unique identifier of the risk which has the number of the relevant asset combined into. The third column contains the threats (from ISO/IEC 27005) that can exploit the vulnerabilities in the first column. The last column is the Risk owner. Unfortunately, we are in no position to get the approval of risk owners, but if the relevant bodies were to prepare a risk analysis of the Hungarian eID based on our proposed methodology, they should definitely do so.

As a next step each risk should be analysed in terms of likelihood and consequences to determine whether the risk must be mitigated or can be accepted based on the risk acceptance criteria.

4.2.2. Risk analysis

For each of the identified risks in the previous section the likelihood and consequence values should be estimated. The following tables show a few examples of combined quantitative-qualitative risk analysis. Firstly, let us examine the A1R2 risk (Table no. 8), which is the possible damage of the eID card due to exposure to water.

In normal, everyday life situations, the probability of the above occurring is unlikely, but the consequences need to be thought through a little more. The organization in this scenario is Hungary. From the country's point of view a damaged eID card is so irrelevant, that it should not even considered a risk, but for the holder of the eID card this means loss of

time and money. So, speaking of consequences we looked at risks at the point of view of the risk owners.

The damaged document must be replaced, which on the one hand has a cost, and on the other hand, administration means a day off from work, and then the new document must be presented to various service providers and banks, which means another day of administration. Two days off and the additional costs together amount to approx. 50 000 HUF with average earnings, which means that the consequences of losing the document are 'Significant'. The colour codes are applied right away.

Table no. 8

Risk analysis of risk A1R2

Risk analysis of risk	**A1R2**	
Likelihood	**Consequences**	**Level of risk**
Unlikely	Significant	Very low

The next example, A1R22 (Table no. 9) is about a poorly trained user who is not security-aware being remotely spied on while using the eID card. This case in itself does not necessarily cause financial damage, but leakage of the PIN code(s) (by even a keylogger software) used for identification and/or electronic signature may even lead to the theft of the user's identity. Without physical possession of the card, it is not possible to cause financial damage with the PIN codes themselves, but if the attacker obtains the card in a next step, it is a completely different situation. The user may also use the same PIN code for other devices.

Table no. 9

Risk analysis of risk A1R22

Risk analysis of risk	**A1R22**	
Likelihood	**Consequences**	**Level of risk**
Rather unlikely	Catastrophic	Medium

We deemed the overall level of this risk as Medium because however the likelihood is rather low, the consequences can be Catastrophic, since in case of occurrence the owner of the card may even suffer serious financial disadvantages.

Each identified risk should be analysed in detail. However, due to content limitations, we do not describe more cases in this study.

4.2.3. Risk evaluation

For each analysed risks, it must be determined whether it needs to be managed or not based on the risk acceptance criteria (RAC). The level of risk of the former example, A1R2 is below the acceptance criteria, so it can be accepted as is. The latter example, A1R22, however falls in the other category requiring mitigation.

After determining the list of risks to be managed, it is advisable to establish a priority order. Based on this, one can start creating the risk treatment plan. Of course, there may be residual risks that fall into the category to be managed, but the organization still decides to tolerate them.

5. Conclusions

The takeaway of the literature review is that many countries over the world use ISO/IEC 27005 based risk assessments in developing and operating eGovernment services. Carrying out risk assessments when implementing new developments greatly contributes to the development of adequate security and user experience, and to successful implementation.

Carrying out a comprehensive risk analysis of the Hungarian eID card would be advisable based on the method described in this study in order to ensure the safest

and most reliable service possible. As a further research direction, we aimed to develop a detailed list of possible attackers and their motivations to prepare a risk analysis that takes into account as many aspects as possible.

As our results show, the ISO/IEC 27005:2022 standard can be applied to the Hungarian eID card in order to explore various risks. The method presented in this study naturally needs further, detailed development. As mentioned earlier, it is not enough to carry out a risk analysis once though. New functions may appear over time for the Hungarian eID, that may hide additional risks. The other reason why the risk analysis of the eID must be carried out again later is the increase in prevalence. Currently, it is not widespread, not part of the daily routine. As dependence on the document may increase over time with the increasing number of use-cases, new risks may arise, or the likelihood of existing risks may increase.

REFERENCES

Act CLXVI of 2012 on the identification, designation and protection of essential systems and facilities. (2012). Hungary Legislation.

European Economic and Social Committee. (2020). *The digital single market - trends and opportunities for SMEs (own-initiative opinion)*. Available at: https://www.eesc.europa.eu/en/our-work/opinions-information-reports/opinions/digital-single-market-trends-and-opportunities-smes-own-initiative-opinion, accessed on December 12, 2023.

Farkas, T. (2023). A kommunikációs és információs rendszerek értelmezése napjainkban: Követelmények és kihívások. In *Tóth, András (Ed) Új típusú kihívások az infokommunikációban* (pp. 11-30). Budapest, Magyarország: Ludovika Egyetemi Kiadó.

Government decree no. 414/2015. (XII. 23.) on the rules for the issuance of personal identification cards (01 01, 2022). Available at: https://njt.hu/jogszabaly/2015-414-20-22, accessed on December 12, 2023.

Hungarian IT Security Framework (MIBIK). In Hungarian (2008).

Hungarian Ministry of Interior. (2023, 01 01). *Role-Based Certification Central Platform Service. In Hungarian*. Available at: https://szeusz.gov.hu/szeusz/SZTSZ, accessed on December 11, 2023.

Hungarian Ministry of Interior. (n.d.). *eSzemélyi - Services.* Available at: https://eszemelyi.hu/en/services/, accessed on December 14, 2023.

Hungarian Ministry of Interior. (n.d.). *eSzemélyi - WHY IS AN eID CARD USEFUL?* Available at: https://eszemelyi.hu/en/the-eid-card/#why-is-an-eid-card-useful, accessed on December 12, 2023.

Idomsoft Zrt. (n.d.). *Electronic Identification Document (eszemélyi). In Hungarian.* Available at: https://idomsoft.hu/rolunk/termekeink/eszemelyi/, accessed on December 12, 2023.

ISO. (n.d.). *iso.org.* Available at: www.iso.org, accessed on January 02, 2023.

ISO/IEC 27001:2022 (2022).

ISO/IEC 27005:2022 (2022).

Jide Edu, M.H. (2023). Exploring the Risks and Challenges of National Electronic Identity (NeID) System. *International Conference on AI and the Digital Economy (CADE 2023)*, 118-123.

Koller, M. (2023). Smart Devices as Security Aspects of Personal Authentication Interface Technology. In Hungarian. *Hadmérnök, Vol. 18, Issue 1*, 109-124.

KSH. (2023, 12 21). *The average gross salary was HUF 564,400 in October 2023, 14.0% higher than a year earlier.* In Hungarian. Available at: https://www.ksh.hu/gyorstajekoztatok/ker/ker2310.html, accessed on January 02, 2024.

Leitner, A., & Schaumüller-Bichl, I. (2009). ARiMA - a new approach to implement ISO/IEC 27005. *2nd International Symposium on Logistics and Industrial Informatics*, 1-6.

Lentner, G., & Parycek, P. (2016). Electronic identity (eID) and electronic signature (eSig) for eGovernment services – a comparative legal study. *Transforming Government People Process and Policy*.

Mateus, G.B. (2016, 11). *A Reference Risk Register for Information Security According to ISO/IEC 27005.* Available at: https://fenix.tecnico.ulisboa.pt/downloadFile/1689244997256215/68217-Thesis.pdf, accesses on December 11, 2023.

Megyeri, L., & Farkas, T. (2017). Risk management, science or swindle? In Hungarian. *Hadmérnök, Vol. 12. Issue 3*, 198-209.

Mojica Sánchez, I.F., Leal Valero, S.A., & Bareño Gutiérrez, R. (2019). Risks Found in Electronic Payment Cards on Integrated Public Transport System Applying the ISO 27005 Standard. Case Study Sitp D.C Colombia. *Congreso Internacional de Innovación y Tendencias en Ingenieria (CONIITI)*, 1-6.

NISZ Zrt. (n.d.). *Services.* In Hungarian. Available at: https://nisz.hu/szolgaltatasaink, accessed on December 12, 2023.

Nyári, N. (2022). The Current State and Possibilities of eSzemélyi and Electronic Signature Technology in Hungary. In Hungarian. *Biztonságtudományi Szemle, Vol. 4, Issue 2*, 61-73.

OWASP. (n.d.). *OWASP Risk Rating Methodology.* Available at: https://owasp.org/www-community/OWASP_Risk_Rating_Methodology, accessed on December 11, 2023.

Paráda, I., & Farkas, T. (2020). Reconnaissance and Analysis in the Penetration Test 1 Information Gathering Techniques. *Hadmérnök, Vol. 15, Issue 1*, 159-182.

Patiño, S., Solís, F., Yoo, S.G., & Arroyo, R. (2018). ICT Risk Management Methodology Proposal for Governmental Entities Based on ISO/IEC 27005. *International Conference on eDemocracy & eGovernment (ICEDEG)*, 75-82.

Pernpruner, M., Carbone, R., Silvio, R., & Sciarretta, G. (2020). The Good, the Bad and the (Not So) Ugly of Out-Of-Band Authentication with eID Cards and Push Notifications: Design, Formal and Risk Analysis. *Proceedings of the Tenth ACM Conference on Data and Application Security and Privacy (CODASPY '20)*. doi:https://doi.org/10.1145/3374664.3375727.

REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL (07 23, 2014).

Schwalm, S., & Alamillo-Domingo, I. (2021). Self-Sovereign-Identity & eIDAS: a Contradiction? Challenges and Chances of eIDAS 2.0. *European Review of Digital Administration & Law - Erdal, Vol. 2, Issue 2,* 89-108.

scrive. (n.d.). *eIDAS and the Digital Single Market.* Available at: https://www.scrive.com/trust-center/eidas-summary/, accessed on January 02, 2024.

Somogyi, T., & Nagy, R. (2022). Cyber Threats and Security Challenges in the Hungarian Financial Sector. *Contemporary Military Challenges, Vol. 24, Issue 3*, 15-29. Available at: https://doi.org/10.33179/BSV.99.SVI.11.CMC.24.3.1.

SP 800-30 revision 1 (2012).

Zwingelberg, H., & Hansen, M. (2011). Privacy Protection Goals and Their Implications for eID Systems. *7th PrimeLife International Summer School (PRIMELIFE)*, 245-260.