

# Security of E-Government Website Encryption in Germany and Hungary

Tamás SZÁDECZKY<sup>1</sup>

*The paper deals with comparative research of the communication security of e-Government services in Germany and Hungary. The focus point of the research is to analyse the cryptographic security algorithms and protocols which encrypt communication in the relations of the citizen and a governmental body. The analysis includes the general e-Government portals, central web services, and specialised services, like taxation and criminal record extracts.*

*The actuality of the topic lies in the fact that the security of the citizens' personal data, used, stored and transferred by the governmental bodies can be in danger. Two examples are the loss of 25 million UK citizens' personal data in 2007 because of a failure of the UK Customs Service and the compromise personally identifiable information of 191 million US citizens, stored in the Voter Database in 2015.*

*The goal of the research is to check the current practice used for governmental communication, based on international standards and current practices.*

*The study compares the e-administration systems of a country of Central Europe which is considered less developed in e-government systems and processes than a Western European country. Based on the evaluation, which can be found at the end of this study, those persons who are responsible for the operation of such systems, can see the actual benchmarks of the communication security. So, this way they can learn about the usage of what communication protocols and cryptographic algorithms are recommended and under what settings.*

**Keywords:** *Hypertext Transfer Protocol Security, information security, transport layer security, web-based governmental services*

## Introduction and Parameters

A channel for the communication between the government and citizen is the data transfer between the e-government website and the citizen's web browser. There is always some personal data exchange, even if the registered client is only viewing the website. The way for securing this communication depends on the responsible government body. Their requirement is applied by the technical operator of the webpage. Even if some rules are set by policies, the practice shall always be evaluated e.g. during an audit, because otherwise, the government body cannot be sure about the level of security. [1] The mode of this evaluation is the technical check of the detailed cryptographic protocols used, including the used algorithms, parameters and key sizes.

---

<sup>1</sup> Ph.D., National University of Public Service, Faculty of Political Sciences and Public Administration, Institute of E-Government; e-mail: [szadeczky.tamas@uni-nke.hu](mailto:szadeczky.tamas@uni-nke.hu)  
The research has been supported by the ÚNKP-17-4-III-NKE-26 New National Excellence Program of the Ministry of Human Capacities.

The Hyper Text Transfer Protocol Secure (HTTPS) communication is a secure way of viewing the web pages, which creates an encrypted connection between the web-server and the client-side browser. However, the protocols, which can be selected, algorithms and parameters are so diversified, that there is a big possibility of faulty or less secure settings. The user hardly ever has control over the security of the communication, and in most of the browsers the technical details are hidden, typically a blue or green bar or padlock is visible. In case of an analysis, we must use specialized tools, and we should check some parameters and settings in detail.

The first step of the security of the HTTPS is the security of the private key of the public key infrastructure (PKI), namely, it identifies the server itself. Here it can be expected the usage of RSA keys, the size of which are at least of the 2048-bit module and the usage of the SHA-256 hash algorithm or better. All this was met in all six analysed web services. The issuer of the certificate must be reliable. Consequently, it must be issued by a recognized certificate authority (CA) or certificate service provider (CSP); however, the issue is more complex than this, and a formal investigation of it faces problems. [2] It would be advantageous if instead of the standard Secure Sockets Layer (SSL) certificates, Extended Validation (EV) certificates would be used for e-government websites, as seen in the case of ELSTER Online. In the case of EV SSL certificates, the control of the identity of the applicant legal person is also carried out, not only the fact is checked, whether the given server is under the influence of the applicant or not. The EV SSL certificate is indicated by the green bar or the name of the certificate holder. The key and the certificate were appropriate in case of every investigated system. The visibility of unencrypted, standard and Extended Validation SSL certificates for the users depends on the browser. In the case of HTTP vs. HTTPS, the difference is hard to see for an inexperienced user. As recent studies have shown, the individual user's awareness is low in Hungary. [3: 65] The EV SSL certificate gives more assurance even for the inexperienced user, therefore increases trust in e-government services. Regardless, a higher level of security culture would also be inevitable from the aspect of cybersecurity. [4: 338]

The next step is the version of the protocol, which carries out the encryption, which can be SSL 2.0, 3.0, Transport Layer Security (TLS) 1.0, 1.1, 1.2. The first two protocols are vulnerable; it is highly inadvisable to use them. The usage of the TLS 1.0 should already be avoided, but unfortunately, in many cases, it must be used because of compatibility reasons. In the case of the TLS 1.1, the bad configurations need to be avoided. However, the TLS 1.2 is appropriate and secure in every setup. It can be mentioned, as a basic problem that only the outdated TLS 1.0 protocol was used in two Hungarian systems and the TLS 1.0 is still accessible in addition to the newer protocol in one-one German and Hungarian case.

From the key exchange procedures, the Diffie-Hellman key exchange (DHE) and Elliptic Curve Diffie-Hellman key exchange (ECDHE) should be supported, namely only these modern procedures make possible the support of the Perfect Forward Secrecy. [5: 581] The Forward Secrecy ensures that it is not possible to decode all earlier communication with the possibly hacked encryption key.

The size of the symmetric keys should be at least 128 bits in the case of Advanced Encryption Standard (AES) algorithm, the weaker, 56 and 112-bit key algorithms cannot be considered secure ones anymore. The Rivest Cipher 4 (RC4) algorithm is vulnerable, it is forbidden to use them, and the Triple Data Encryption Algorithm (3DES) is out-of-date and slow. Consequently, it should be avoided.

From the block cipher modes of operation, the usage of the GCM (Galois CounterMode) is advantageous, and it can be recommended over CBC (Cypher Block Chaining). [6: 549] The diffusion of the used algorithm is also an interesting question but, at the moment, it is not in our scope. [7]

With the usage of the HTTP Strict Transport Security setting, the non-encrypted communication with the server is not allowed, which is the most important parameter to be set. [8]

## A Comparative Analysis: Germany and Hungary

Taking the above-written facts into consideration, the individual, selected general and local administration systems of the Federal Republic of Germany and Hungary have been compared in this paper; they have similar administrative functions. In all cases, the subjects of investigation were the systems, which carry out handling and transforming personal data and enabling customer relationship, at least in one of the countries. During the investigation, the communication protocol compliance assessment of the given system has been carried out. The sampled objects of the investigation are indicated in Table 1.

Table 1. *The analyzed systems.* [Edited by the author.]

Function	Hungary	Germany
General central or local e-government	general e-governmental client gate “Ügyfélkapu” in Hungarian	local administration portal, “Bürgerserviceportal” in German
Taxation services	not applicable: sent with a special application via the general e-governmental client gate	tax administration portal: ELSTER Online
Criminal records	specialized e-government service website “Webes ügysegéd” on “ <a href="http://Nyilvantarto.hu">Nyilvantartó.hu</a> ” in Hungarian	criminal register excerpts on the website of the Federal Office of Justice, “Bundesamt für Justiz, Online-Beantragung von Führungszeugnissen” in German
Separate authentication service	Central Authentication Agent, “Központi Azonosítási Ügynök” in Hungarian	not applicable: authentication service is embedded in the services above, in most of the cases based on the new German personal identity card

As the reader can realize, the 1-to-1 mapping of those services is not possible, due to differences in the approach. At present, our research includes only the highest level of public services; however, as Soukopová, Nemeč, Matějová and Struk shows, there are different aspects also to be considered in local level services. [9]

One sample is a general service, where more e-government services are available. Another example is the web service for the application of the criminal record excerpts. These were similarly available in both countries. Odd examples are the taxation services and a separate

central authentication service, which were available as a separate web-based service in one of the countries.

## ***Methodology***

During testing, we were carrying out two experiments. On the one hand, there were analysed the detailed characteristic features and parameters of the HTTPS communication of all the six systems in the system of the Qualys SSL Labs. [16] Qualys is one of the market leading manufacturers of vulnerability-analyzer systems. The Qualys SSL Labs service carries out detailed technical analysis regarding the algorithmic parameters and the HTTPS protocol of the web page, which provides the encrypted connection. The most important results of the several pages long, detailed analysis are summarized in Table 2. In case of every described website, the SSL Labs shows an overall result which is indicated in a separate figure. (Figures 1–6.) The overall rating provides a classification based on the most important security characteristic features which range from F (the worst) to A+ (the best). Here the goal is to achieve the best possible result, but the good result itself does not mean an assurance for meeting certain requirements yet. For example, the PCI DSS forbids the usage of the TLS 1.0, but the SSL Labs does not impair the assessment of the website when the TLS 1.2 is also accessible in addition to the TLS 1.0. During the testing, a control investigation was carried out to prove the most important findings of the Qualys SSL Labs. In the control tests, we were using a Firefox 51.0.3 browser, which ran under a Windows 7 SP 1 (Build 7601). In those tests, the encryption package, which was used during communication, had to be the same as the highest-level security of HTTPS communication setting recognized by the SSL Labs, which was primarily preferred on the server side. In addition to all this, we carried out a control-inspection regarding the issuer of the certificate, the modulus-size of the private key, and the other characteristic features of the certificate (the reliability of the issuer, the hash algorithm and the type of the validation).

## ***General E-Governmental Client Gate (<https://gate.gov.hu>)***

This website is the centralized identification system of the e-public administration. The clear majority of the e-government services, which are accessible in Hungary, carry out authentication through this system. One-factor exclusively, the knowledge-based identification is used here. The maximum period of validity of the password is two years.

The SSL certificate of the server has been issued by the Microsec e-Szigno SSL CA 2014, which is a qualified certificate authority in Hungary. The encryption package, which was used during the control inspection is TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA, 128-bit key, TLS 1.0. The detailed results of the tests are in Table 2, and the summary is in Figure 1.

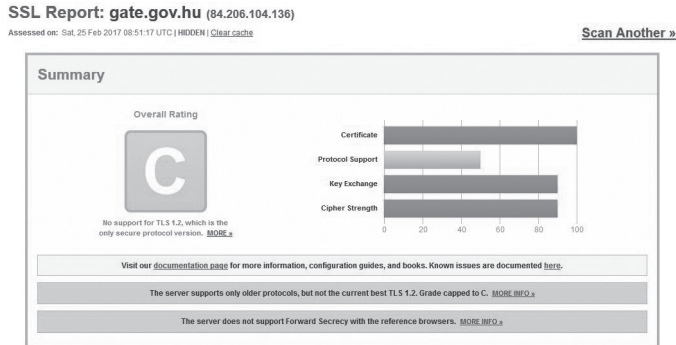


Figure 1. SSL report of [gate.gov.hu](https://gate.gov.hu). [17]

### *The Specialized E-Government Services of Hungary ([www.nyilvantarto.hu](http://www.nyilvantarto.hu))*

The web-based administrative assistant (in Hungarian: Webes ügysegéd) hosted on [www.nyilvantarto.hu](http://www.nyilvantarto.hu) is suitable for administration of criminal records, vehicle management and extracts from the register of births and marriages. Its identification is different from the identification system of the client gate. It uses the best TLS 1.2 for communication, but the earlier versions are also accessible. The identification happens by providing the username and the password combination, which are used in the client gate.

The SSL certificate of the server has been issued by the Microsec e-Szigno SSL CA 2014, which is a qualified certificate authority in Hungary. The encryption package, which was used during the control inspection is TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA, 256-bit key, TLS 1.2. The detailed results of the tests are in Table 2, and the summary is in Figure 2.

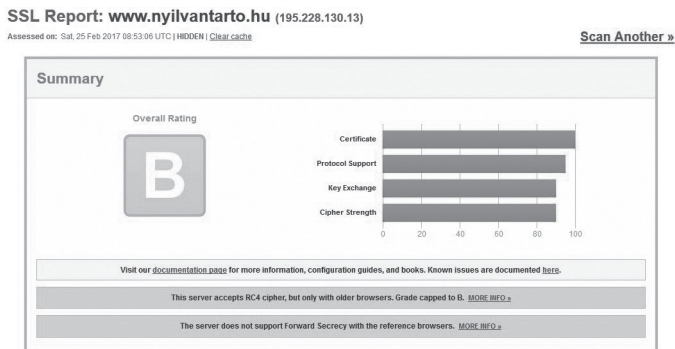


Figure 2. SSL report of [www.nyilvantarto.hu](http://www.nyilvantarto.hu). [18]

### *The Central Authentication Agent of Hungary (<https://kau.gov.hu>)*

The Central Authentication Agent is an integrated identification interface of the regulated public management services, which is a legally defined service in Hungary. The identification

can be carried out by the client gate username-password combination and by the identification certificate which is stored in the new type Personal Identification Card. Unfortunately, for the time being, this latter function does not work. Despite the fact that it is the integrated identification platform of the future, it, unfortunately, uses the same outdated protocols and settings for securing data traffic, as the client gate does.

The SSL certificate of the server has been issued by the NetLock Expressz (Class C) Certificate Service Provider, which is a qualified certificate authority in Hungary. The encryption package, which was used during the control inspection is TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA, 128-bit key, TLS 1.0. The detailed results of the tests are in Table 2, and the summary is in Figure 3.

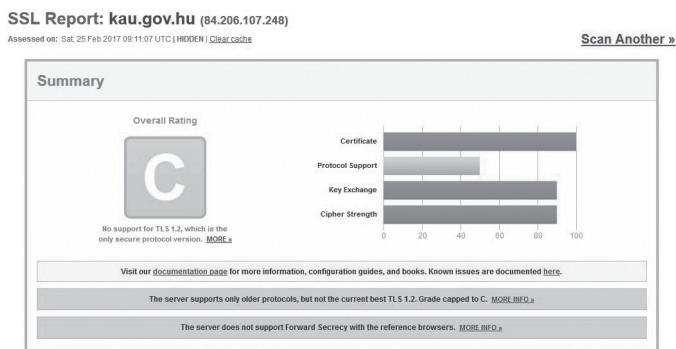


Figure 3. SSL report of *kau.gov.hu*. [18]

### ***The Local Administration Portal of Germany ([www.buergerserviceportal.de](http://www.buergerserviceportal.de))***

There is no such integrated, general e-public administrative portal in Germany which would totally comply with the Hungarian client gate described above. What we inspect here is the web page which assures access to the separate provincial administrative functions. Such type of services of the federal states can be accessed through this portal, but the system separates all these from each other. The communication operates with TLS 1.2 protocol and with appropriate, modern encryption algorithms. The applied certificate assures the highest accessible security. The only possible way to carry out the identification is using the authentication certificate, which can be found in the new type Personal Identification Card, (“der neue Personalausweis”, nPA in German) and in the electronic residence permit, (“elektronisches Aufenthaltstitel”, eAT in German). So that the citizen can use a two-factor identification. The certificate, which is stored in the chip on the ID card, can be accessed with the PIN of the holder. The use of ID cards causes a problem because services are not accessible in such an extensive way, as it would in case of the client gate, due to the fact that it is necessary for the citizens to have new types of Identification Cards activated with the new functions, and they also must own appropriate card readers. This identification method practically excludes from the service those foreigners, who live in Germany.

The SSL certificate of the server has been issued by the T-Systems International GmbH, which is a qualified certificate authority in Germany. The encryption package, which was used

during the control inspection is TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256, 128-bit key, TLS 1.2. The detailed results of the tests are in Table 2, and the summary is in Figure 4.

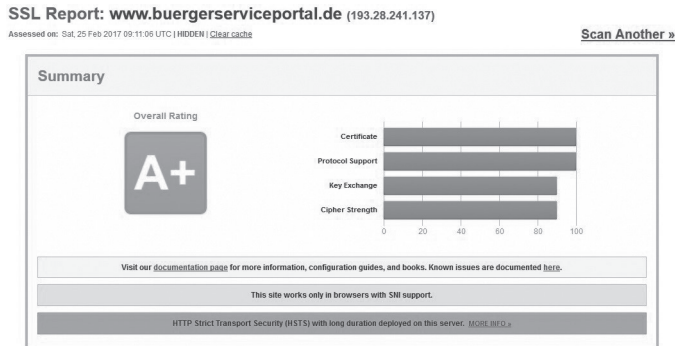


Figure 4. SSL report of [www.buergerserviceportal.de](http://www.buergerserviceportal.de). [19]

### The Tax Administration Portal of Germany ([www.elsteronline.de](http://www.elsteronline.de))

An integrated system of tax administration procedures is used at federal level in Germany. The personal income tax returns and other tax requests can be submitted through this portal called ELSTER Online. The encryption is even at a higher level than it is in case of the previous service, namely, here is used a 256-bit AES key. As it can also be seen in the tests, the setting of the web page is free from more significant configuration problems. The identification is carried out by default with the personal ID cards and the electronic residence permit, as it has been described earlier, but a soft certificate or a username-password pair are also usable.

The SSL certificate of the server has been issued by the Symantec Class 3 EV SSL CA-G3, which is a qualified certificate authority in Germany. The encryption package, which was used during the control inspection is TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384, 256-bit key, TLS 1.2. The detailed results of the tests are in Table 2, and the summary is in Figure 5.

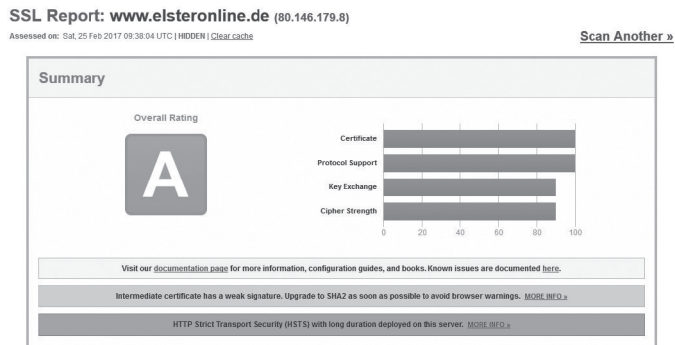


Figure 6. SSL report of [www.elsteronline.de](http://www.elsteronline.de) [20]

## **The Criminal Register in Germany** ([www.fuehrungszeugnis.bund.de](http://www.fuehrungszeugnis.bund.de))

The request concerning issuing a criminal record is carried out electronically at federal level in an integrated system on the web page of the Federal Office of Justice. This web page uses the protocol and algorithm, which has already been described at the tax administration web page, here the security settings of the web page are also appropriate. The identification here is also carried out with using the nPA and eAT.

The SSL certificate of the server has been issued by the “Zentrum fuer Informationsverarbeitung und Informationstechnik ZIVIT CA-G01”, which is a federal state operated certificate authority in Germany. The encryption package, which was used during the control inspection is TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384, 256-bit key, TLS 1.2. The detailed results of the tests are in Table 2 and the summary is in Figure 6.

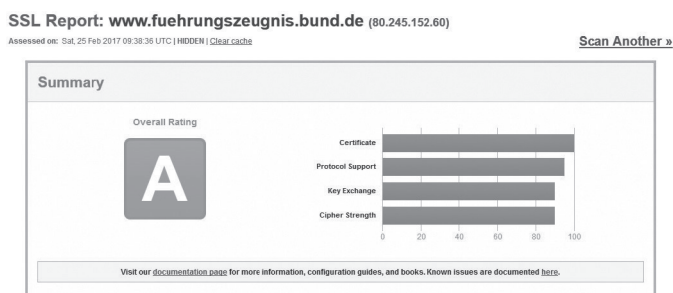


Figure 6. SSL report of [fuehrungszeugnis.bund.de](http://fuehrungszeugnis.bund.de). [21]

## **Evaluation, Conclusions**

The major problem we found during our analysis, is the fact that the user has lack of control and low level of awareness. Human-related errors are typical attack vectors. Therefore, these are also a focus topic in regulation. [10] However, the browsers are not supporting enough the users. The visibility of unencrypted, standard and Extended Validation SSL certificates for the users are shown in Figures 1 to 6. The EV SSL certificate gives more assurance even for the inexperienced user, therefore increases trust in e-government services. Although the IT security is a focus topic after the public administration reform in Hungary, the security awareness level will increase slowly, so public servants are also not likely to realize a problem from the service provision side. [11]



Figure 7. Browser search bar when opening a site without encryption in Firefox. [22]



Figure 8. Browser search bar when opening a site with standard SSL certificate in Firefox. [23]





Figure 9. Browser search bar when opening a site with an Extended Validation SSL certificate in Firefox. [24]



Figure 10. Browser search bar when opening a site without encryption in Internet Explorer. [25]

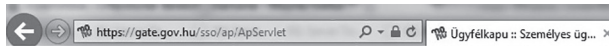


Figure 11. Browser search bar when opening a site with standard SSL certificate in Internet Explorer. [26]



Figure 12. Browser search bar when opening a site with an Extended Validation SSL certificate in Internet Explorer. [27]







It is hard for the user to see if the connection is HTTP or HTTPS. The difference is only a padlock logo somewhere. The details of the connection protocol are not visible for the user in Chrome. In the Internet Explorer, only the certificate details are visible. Firefox shows the most details. Therefore, this was used for the control measurement.

The overall rating of SSL Labs provides a classification based on the most important security characteristic features, which extends from F (the worst) to A+ (the best).

The comparison of the results of the tests is in Table 2. The analysis does not include vulnerability analysis, because it needs previous authorization to avoid legal impacts. With the usage of OWASP TOP 10 threat analysis, the risks from attacks, e.g. cross-site request forgery (CSRF), cross-site scripting (XSS) or SQL injection might be significantly lowered. [12]

Table 2. Results of the analysis. [Edited by the author.]

Country	Hungary			Germany		
	3.2	3.3	3.4	3.5	3.6	3.7
<b>Properties/Section</b>	3.2	3.3	3.4	3.5	3.6	3.7
<b>Certificate RSA key [bit]</b>	2048	2048	2048	4096	2048	2048
<b>Certificate hash-algorithm</b>	SHA-256	SHA-256	SHA-256	SHA-256	SHA-256	SHA-256
<b>Trustworthy CA</b>	yes	yes	yes	yes	yes	yes
<b>Extended validation</b>	no	no	no	no	yes	no
<b>TLS version</b>	1.0	1.0; 1.1; 1.2	1.0	1.2	1.2	1.0; 1.1; 1.2

Country	Hungary			Germany		
<b>Key exchange</b>	RSA	ECDHE, RSA	RSA	ECDHE, DHE	ECDHE	ECDHE, DHE, RSA
<b>Symmetric key [bit]</b>	112, 128, 256	112, 128, 256	112, 128, 256	128, 256	128, 256	128, 256
<b>Block cypher mode</b>	CBC	CBC	CBC	CBC, GCM	CBC, GCM	CBC, GCM
<b>RC4 support</b>	no	yes	no	no	no	no
<b>3DES support</b>	yes	yes	yes	no	no	yes
<b>Forward Secrecy</b>	no	partly	no	yes	yes	partly
<b>HTTP Strict Transport Security</b>	no	no	no	yes	yes	no
<b>Overall Rating (A+ is the best, F is the worst)</b>						

The application of inappropriate protocols, algorithms, and parameters makes possible the attack against web pages or the communication channel; for example, the vulnerability of the TLS, which can be exploited, came to light in the last few years. Regarding the fact that the application of the out-of-date encryption poses a direct danger, concerning the data of the citizens, it is inevitable to change these into up-to-date solutions. All the investigated German e-government services almost totally comply with the security requirements of our era. The application of them do not pose any danger, at least from a technological point of view regarding the data of the citizens; still, here, too it is recommended to disable the TLS 1.0 and 1.1. The application of the ownership and knowledge-based multi-factor identification is to be especially highlighted instead of the exclusively knowledge-based identification. All this provides extremely high security, but unfortunately, it significantly limits the wide access to the e-government functions. A solution can be found to all this by the introduction of the digital identity card, which has been applied in Estonia; it is also accessible for foreigners and ensures full access to all e-public services. [13: 24] In contrast to Hungary, where there is no governmental requirement, guidance or best practice, in Germany it exists. Similarly to ETSI communication security guidelines, the Federal IT Security Agency of Germany (BSI) has specified the requirements. Both the minimum standards for SSL/TLS [14] and the BSI TR-03116-4 [15] requires the usage of TLS 1.2 with Perfect Forward Secrecy from 2015. However, the tested services did not fully comply (see Table 2). However, it is always recommended to use in the e-government services the standards and recommendations, which meet the international best practice, for example, the usage of the NIST and ETSI standards.

## References

- [1] SZÁDECZKY T.: The role of technology. Auditing and certification in the field of data security. In. GERGELY L. Sz. (ed.): *Privacy in the Workplace. Data Protection Law and Self-regulation in Germany and Hungary*. Budapest: HVG-ORAC, 2012. 311–337.
- [2] HAWANNA, V., KULKARNI, V. Y., RANE, R. A., MESTRI, P., PANCHAL, S.: [Risk Rating System of X.509 Certificates](#). *Procedia Computer Science*, 89 (2016), 152–161.
- [3] SASVÁRI P., NEMESLAKI A., RAUCH, W.: Old Monarchy in the New Cyberspace: Empirical Examination of Information Security Awareness among Austrian and Hungarian Enterprises. *Academic and Applied Research in Military and Public Management Science (AARMS)*, 14 1 (2015), 63–78.
- [4] SHERIFI, S. G., NAGY K.: Small Countries and Cyber Defence. *Academic and Applied Research in Public Management Science (AARMS)*, 12 2 (2013), 329–342.
- [5] GASTERMANN, B., STOPPER, M., KOSSIK, A., KATALINIC, B.: Secure Implementation of an On-Premises Cloud Storage Service for Small and Medium-Sized Enterprises. *Annals of DAAAM & Proceedings*, 25 1 (2014), 574–583.
- [6] GUERON, S., KOUNAVIS, M.: Efficient implementation of the Galois CounterMode using a carry-less multiplier and a fast reduction algorithm. *Information Processing Letters*, 110 14–15 (2010), 549–553. <https://doi.org/10.1016/j.ipl.2010.04.011>
- [7] CHUNGATH, S., LAKSHMY, K. V., SETHUMADHAVAN, M.: Measuring Diffusion in Stream Ciphers using Statistical Testing Methods. *Defence Science Journal*, 62 1 (2012), 6–10. <https://doi.org/10.14429/DSJ.62.1435>
- [8] KISA, K. E., TATLI, E. I.: Analysis of HTTP Security Headers in Turkey. *International Journal of Information Security Science*, 5 4 (2016). [www.researchgate.net/profile/Emin\\_Tatli/publication/307931790\\_Analysis\\_of\\_HTTP\\_Security-Headers\\_in\\_Turkey/links/57d2653e08ae601b39a27faf/Analysis-of-HTTP-Security-Headers-in-Turkey.pdf](http://www.researchgate.net/profile/Emin_Tatli/publication/307931790_Analysis_of_HTTP_Security-Headers_in_Turkey/links/57d2653e08ae601b39a27faf/Analysis-of-HTTP-Security-Headers-in-Turkey.pdf) (Downloaded: 25.02.2017)
- [9] SOUKOPOVÁ, J., NEMEC, J., MATĚJOVÁ, L., STRUK, M.: Municipality Size and Local Public Services: Do Economies of Scale Exist? *The NISPAcee Journal of Public Administration and Policy*, 7 2 (2014), 151–171. <https://doi.org/10.2478/nispa-2014-0007>
- [10] SZÁDECZKY T.: Information Security Law and Strategy in Hungary, *Academic and Applied Research in Military and Public Management Science (AARMS)*, 14 4 (2015) 281–289.
- [11] GELLÉN M.: Public Administration Education in a Legalistic Setting: New Tendencies in Hungarian Public Administration and Training. *The NISPAcee Journal of Public Administration and Policy*, 6 2 (2013), 53–67. <https://doi.org/10.2478/nispa-2013-0006>
- [12] GOSWAMI, S., KRISHNAN, N. R., VERMA, M., SWARNKAR, S., MAHAJAN, P.: [Reducing Attack Surface of a Web Application by Open Web Application Security Project Compliance](#). *Defence Science Journal*, 62 5 (2012), 324–330.
- [13] SÄRAV, S., KERIKMÄE, T., KASPER, Á.: The means of virtual migration – e-residency in e-Estonia. *Információs Társadalom*, 16 2 (2016), 8–31. <http://dx.doi.org/10.22503/infvars.XVI.2016.2.1>
- [14] *Mindeststandard des BSI für den Einsatz des SSL/TLS-Protokolls durch Bundesbehörden*. [Minimum standard of BSI for usage of SSL/TLS protocols by government authorities.] [www.bsi.bund.de/SharedDocs/Downloads/DE/](http://www.bsi.bund.de/SharedDocs/Downloads/DE/)

- [BSI/Mindeststandards/Mindeststandard\\_BSI\\_TLS\\_1\\_2\\_Version\\_1\\_0.pdf?\\_\\_blob=publicationFile&v=4](#) (Downloaded: 05.04.2018)
- [15] *Technische Richtlinie BSI TR-03116 Kryptographische Vorgaben für Projekte der Bundesregierung. Teil 4: Kommunikationsverfahren in Anwendungen.* (Technical guideline BSI TR-03116 Cryptographic requirements for federal government projects. Part 4: Communication requirements in applications. 24.03.2017) [www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03116/BSI-TR-03116-4.pdf?\\_\\_blob=publicationFile&v=3](http://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03116/BSI-TR-03116-4.pdf?__blob=publicationFile&v=3) (Downloaded: 05.04.2018)
- [16] *Qualys SSL Labs.* [www.ssllabs.com/ssltest/index.html](http://www.ssllabs.com/ssltest/index.html) (Downloaded: 19.03.2017)
- [17] *Qualys SSL Labs.* [www.ssllabs.com/ssltest/analyze.html?d=gate.gov.hu&hideResults=on](http://www.ssllabs.com/ssltest/analyze.html?d=gate.gov.hu&hideResults=on) (Downloaded: 25.05.2017)
- [18] *Qualys SSL Labs.* [www.ssllabs.com/ssltest/analyze.html?d=kau.gov.hu&hideResults=on](http://www.ssllabs.com/ssltest/analyze.html?d=kau.gov.hu&hideResults=on) (Downloaded: 25.02.2017)
- [19] *Qualys SSL Labs.* [www.ssllabs.com/ssltest/analyze.html?d=www.buergerserviceportal.de&hideResults=on](http://www.ssllabs.com/ssltest/analyze.html?d=www.buergerserviceportal.de&hideResults=on) (Downloaded: 25.02.2017)
- [20] *Qualys SSL Labs.* [www.ssllabs.com/ssltest/analyze.html?d=www.elsteronline.de&hideResults=on](http://www.ssllabs.com/ssltest/analyze.html?d=www.elsteronline.de&hideResults=on) (Downloaded: 25.02.2017)
- [21] *Qualys SSL Labs.* [www.ssllabs.com/ssltest/analyze.html?d=www.fuehrungszeugnis.bund.de&hideResults=on](http://www.ssllabs.com/ssltest/analyze.html?d=www.fuehrungszeugnis.bund.de&hideResults=on) (Downloaded: 25.02.2017)
- [22] [www.bund.de](http://www.bund.de) shown in Firefox 52.0.2. [www.bund.de/Content/DE/Home/homepage\\_node.html](http://www.bund.de/Content/DE/Home/homepage_node.html) (Downloaded: 06.04.2017)
- [23] [gate.gov.hu](http://gate.gov.hu) shown in Firefox 52.0.2. <https://gate.gov.hu/sso/ap/ApServlet> (Downloaded: 06.04.2017)
- [24] *ELSTER Online* shown in Firefox 52.0.2. [www.elsteronline.de/eportal/Oeffentlich.tax](http://www.elsteronline.de/eportal/Oeffentlich.tax) (Downloaded: 06.04.2017)
- [25] [www.bund.de](http://www.bund.de) shown in Internet Explorer 11.0.9600.18617 [www.bund.de/Content/DE/Home/homepage\\_node.html](http://www.bund.de/Content/DE/Home/homepage_node.html) (Downloaded: 06.04.2017)
- [26] [gate.gov.hu](http://gate.gov.hu) shown in Internet Explorer 11.0.9600.18617 <https://gate.gov.hu/sso/ap/ApServlet> (Downloaded: 06.04.2017)
- [27] *ELSTER Online* shown in Internet Explorer 11.0.9600.18617 [www.elsteronline.de/eportal/Oeffentlich.tax](http://www.elsteronline.de/eportal/Oeffentlich.tax) (Downloaded: 06.04.2017)