Security Certificates Used in Public Web Sites of Banks in Czech Republic, Slovakia and Hungary

Pavel Petrov [1], Rami Malkawi [2], Andrey Shichkin [3], Georgi Dimitrov [4], Radka Nacheva [5]

[1]*University of Economics - Varna, Varna, Bulgaria*
[2]*Yarmouk University, Irbid, Jordan*
[3]*Ural Federal University, Institute of Industrial Ecology UB RAS, Ekaterinburg, Russia*
[4]*University of Library Studies and Information Technologies, Sofia, Bulgaria*
[5] *University of Economics - Varna, Varna, Bulgaria*

Abstract **– There is a tendency formed during the last years – indicating that the default protocol for accessing web pages is the HTTPS protocol. In order this to be done, a valid SSL/TSL certificate issued by authority body should be used. In the scope of this study during the month of August 2019 we examined the web sites of 22 banks licensed in Czech Republic, 15 banks licensed in Slovakia and 22 banks licensed in Hungary. The survey excludes the foreign bank branches which are not supervised by the respective national central banks. We did this survey trying to outline the "good practices" which are used by domestic system administrators of bank's websites in the respective countries.**

Keywords **– SSL/TSL Certificates; Czech banks; Slovakian banks; Hungarian banks; HTTPS; bank web site.**

1. Introduction

In this comparative study we choose banks which are regulated by the local central banks and they are from the three neighboring landlocked countries located in Central Europe.

DOI: 10.18421/TEM84-17
https://dx.doi.org/10.18421/TEM84-17

Corresponding author: Pavel Petrov,
University of Economics - Varna, Varna, Bulgaria
Email: petrov@ue-varna.bg

Received: 02 October 2019.
Revised: 01 November 2019.
Accepted: 05 November 2019.
Published: 30 November 2019.

These countries share a lot of similarities in demographics and economics characteristics. From monetary policy point of view, there are some differences. The major one is that Slovakia is part of so called "euro zone"/"euro area" and adopted the euro as their currency, while Czech Republic and Hungary are not. From monetary policy point of view, the bank systems of the last mentioned two countries are formally independent from a higher-level supervision from European Central Bank.

Table 1 summarizes some overall data about countries which have general meaning in the context of the current study.

It should be noted that the indicator Gross National Income (GNI), developed by the World Bank and previously known as Gross National Product (GNP), represents the overall foreign and domestic output of economy. It is the overall foreign and domestic output reported by citizens of a country, minus earnings from the country's economy by nonresidents. The indicator GNI per capita is widely used for estimating the overall level of economic development. The Atlas method estimates the size of economies in USA dollars [1]. The Gini coefficient is defined as the relationship of cumulative shares of the population arranged according to the level of equivalized disposable income, to the cumulative share of the equivalized total disposable income received by them [2], [13]. The Human Development Index (HDI) is a summary measure of average achievement in key dimensions of human development: a long and healthy life, being knowledgeable and have a decent standard of living [3].

The governments of all the three countries receive high long-term credit ratings from reputable credit rating organizations such as Moody's, Fitch and Standard&Poor's. The credit rating indicator is an assessment made by the experts from a credit rating organization and estimates the creditworthiness of

the country. It is used to evaluate the probability of expectation about how the government will pay its debts. In this regard, it reflects the international image of the governments [4].

Table 1. Large-scale overall comparison between the Czech Republic, Slovakia and Hungary

Feature	Czech Republic	Slovakia	Hungary
Population [millions] (2018 est.)	10.6	5.5	9.8
Area [km^2]	78 866	49 035	93 030
GDP (nominal) per capita (2019 est)	23 209$	20 155$	17 296$
GNI per capita (by method "Atlas") in 2018	20 260$	18 330$	14 590$
Gini (2018)	24.0	23.2	28.7
HDI (2017)	0.888 (Very High)	0.855 (Very High)	0.838 (Very High)
Currency	CZK	EUR	HUF
S&P Global Ratings (long term)	AA- (2011)	A+ (2015)	BBB (2019)
Moody's Investors Service (long term)	A1 (2018)	A2 (2018)	Baa3 (2018)
Fitch Ratings (long term)	AA- (2019)	A+ (2019)	BBB (2019)

(Sources: Wikipedia, 2019; Eurostat, 2019; World Bank DRG, 2019; UN HDRO, 2019)

From the provided data, we could order the countries regarding overall performance of the economies as follow:

1. The Czech Republic is the most developed from the three countries with the highest GDP per capita, GNI per capita, HDI and credit ratings. Only the Gini indicator put the country on second place.
2. The Slovakia sits in the middle regarding GDP per capita, GNI per capita, HDI and credit ratings. Only the Gini indicator put the country on the last place.
3. The Hungary is the least developed from the three countries with the lowest GDP per capita, GNI per capita, HDI and credit ratings. Only the Gini indicator put the country on the first place.

We raise the hypothesis that information technologies used in the domestic banks will reflect the described ranging of countries regarding overall performance of the economies. More specifically, we expect that the domestic banks in Czech Republic will comply more closely to good practices in web security than the domestic banks in Slovakia and Hungary. Also, we expect that domestic banks in Hungary will deviate from the good practices in web security more often compared to Czech Republic and Slovakia.

We are confident that the web technologies are a major element of the IT infrastructure on every bank and in generally in these institutions there are no lacks of funding and the chance to use any software, including expensive and one with high quality. The web technologies become an essential part of every part of the bank's online business, so performance and most important – security, cannot be sacrificed for any reason whatsoever.

As it is known, when using HTTP/0.9/1.0/1.1 text protocols, the so called "man in the middle" could intercept all network traffic and read the exchanged queries and responses between the web client and the web server. Unfortunately, even without the use of complex technical means, the content of the network packets which are used by text protocols can easily be read [17]. Very often a confidential data is exchanged, e.g. bank card numbers used for payment, user passwords, sensitive information, etc. In this case the best option is to use the protocol HTTPS which is specially intended for these cases [18]. It is also known as "Secure HTTP", "HTTP Secure", "HTTP over SSL", "HTTP over TLS", "HTTP over SSL/TLS" etc. The use of a crypted connection increases the processing load on the server and client side for each network connection, resulting in busier CPU time and more amount of RAM [14], [15]. In the last years, this is not considered as a significant reason, because of the great benefits which communication security provides to the users and banks.

2. Methodology and Computational Details

In our study home pages of 22 Czech, 15 Slovakian and 22 Hungarian banks were inspected in August 2019. The methodology of the study is based partially on methodology used in previous studies on web technologies used in banks [5], [6], [7], [16].

The lists of banks authorized to operate in Czech Republic, Slovakia and Hungary were taken from the websites of Czech National Bank [8] (Table 2), Bank of Slovenia [9] (Table 3) and Magyar Nemzeti Bank [10] (Table 4).

Table 2. Presence of the HTTPS protocol in public bank's web sites from Czech Republic

№	Bank's Name	Bank's Domain	HTTPS Support
1	Air Bank a.s.	airbank.cz	yes
2	Banka CREDITAS a.s.	creditas.cz	yes
3	Česká exportní banka, a.s.	ceb.cz	yes
4	Česká spořitelna, a.s.	csas.cz	yes
5	Českomoravská stavební spořitelna, a.s.	cmss.cz	yes
6	Českomoravská záruční a rozvojová banka, a.s.	cmzrb.cz	yes
7	Československá obchodní banka, a. s.	csob.cz	yes
8	Equa bank a.s.	equabank.cz	yes
9	Expobank CZ a.s.	expobank.cz	yes
10	Fio banka, a.s.	fio.cz	yes
11	Hypoteční banka, a.s.	hypotecnibanka.cz	yes
12	Industrial and Commercial Bank of China, odštěpný závod	icbc-cz.com	**NO**
13	J & T BANKA, a.s.	jtbank.cz	yes
14	Komerční banka, a.s.	kb.cz	yes
15	Modrá pyramida stavební spořitelna, a.s.	modrapyramida.cz	yes
16	MONETA Money Bank, a.s.	moneta.cz	yes
17	PPF banka a.s.	ppfbanka.cz	yes
18	Raiffeisen stavební spořitelna a.s.	rsts.cz	yes
19	Raiffeisenbank a.s.	rb.cz	yes
20	Sberbank CZ, a.s.	sberbankcz.cz	yes
21	UniCredit Bank, a.s.	unicreditbank.cz	yes
22	Wüstenrot hypoteční banka a.s./Wüstenrot - stavební spořitelna a.s.	wuestenrot.cz	yes

In the survey the main used method consists of analyzing the responses returned by the public accessible bank web servers. The web browser Chrome version 73 and a typical desktop PC with Windows 10 Professional Edition x64, was used. The browser module "Web Developer Tools" was activated.

Table 3. Presence of the HTTPS protocol in public bank's web sites from Slovakia (Slovak Republic)

№	Bank's Name	Bank's Domain	HTTPS Support
1	Abanka d.d.	abanka.si	yes
2	Addiko Bank d.d.	addiko.si	yes
3	Banka Intesa Sanpaolo d.d.	intesasanpaolobank.si	yes
4	Banka Sparkasse d.d.	sparkasse.si	yes
5	Delavska hranilnica d.d.	delavska-hranilnica.si	yes
6	Deželna banka Slovenije d.d.	dbs.si	yes
7	Gorenjska banka d.d.	gbkr.si	yes
8	Hranilnica LON d.d.	lon.si	yes
9	Nova Kreditna banka Maribor d.d.	nkbm.si	yes
10	Nova Ljubljanska banka d.d.	nlb.si	yes
11	Primorska hranilnica Vipava d.d.	phv.si	yes
12	Sberbank banka d.d.	sberbank.si	yes
13	SID-Slovenska izvozna in razvojna banka, d.d.	sid.si	yes
14	SKB banka d.d.	skb.si	yes
15	UniCredit Banka Slovenija d.d.	unicredit.si	yes

The browser module "Web Developer Tools" has not been specifically designed for such kind of studies, but in such cases, it is a very convenient instrument. The process of examination was done manually, and expert evaluation was made. Other technique to do the same study could include using the command line online tools such as "curl", but in our opinion, using web browser is more proper in this case.

Table 4. Presence of the HTTPS protocol in public bank's web sites from Hungary

№	Bank's Name	Bank's Domain	HTTPS Support
1	BUDAPEST Hitel- és Fejlesztési Bank Zrt.	budapestbank.hu	yes
2	CIB Bank Zrt.	cib.hu	yes
3	Commerzbank Zrt.	commerzbank.hu	yes
4	DUNA TAKARÉK BANK Zrt.	dunatakarek.hu, dtbank.hu	yes
5	ERSTE BANK HUNGARY Zrt.	erstebank.hu	yes
6	GRÁNIT Bank Zrt.	granitbank.hu	yes
7	KDB Bank Európa Zrt.	kdbbank.eu	yes
8	Kereskedelmi és Hitelbank Zrt.	kh.hu	yes
9	MagNet Magyar Közösségi Bank Zrt.	magnetbank.hu	yes
10	Magyar Cetelem Bank Zrt.	cetelem.hu	yes
11	Merkantil Váltó és Vagyonbefektető Bank Zrt.	merkantil.hu	yes
12	MKB Bank Nyrt.	mkb.hu	yes
13	MTB Magyar Takarékszövetkezeti Bank Zrt.	mtb.hu	**NO**
14	OTP Bank Nyrt.	otpbank.hu	yes
15	Polgári Bank Zrt.	polgaribank.hu	yes
16	Porsche Bank Hungaria Zártkörűen Működő Rt.	porschebank.hu	yes
17	Raiffeisen Bank Zrt.	raiffeisen.hu	yes
18	Sberbank Magyarország Zrt.	sberbank.hu	yes
19	SOPRON BANK BURGENLAND Zrt.	sopronbank.hu	yes
20	TAKARÉK Kereskedelmi Bank Zrt.	takarek.hu	yes
21	Takarékbank Zrt.	takarekbank.hu	yes
22	UniCredit Bank Hungary Zrt.	unicreditbank.hu	yes

In our study websites of foreign bank branches and representative offices of foreign banks operating in Czech Republic, Slovakia and Hungary are excluded. We surveyed only domestic ones, operated under supervision of the national bank of the respective country. The websites of the banks which operated on a branch or on a cross-border basis were skipped.

3. Empirical Results and Discussion

The summarized results of the studied bank's public web pages are presented in several tables (Tables 5 – 7) based on the following key indicators: the certification body issued the certificate, the type of the SSL/TSL certificate, validity period of the SSL/TSL certificate and presence of automatic redirection to HTTPS.

Table 5. Major characteristics of the HTTPS usage in public web sites of Czech banks

Bank №	Certification authority body	Certificate type	Period of Validity /months/	Automatic redirection to HTTPS
1	DigiCert SHA2 Extended Validation Server CA	EV	26	yes
2	Thawte EV RSA CA 2018	EV	26	yes
3	Thawte EV RSA CA 2018	EV	26	yes
4	DigiCert SHA2 Extended Validation Server CA	EV	14	yes
5	DigiCert SHA2 Extended Validation Server CA	EV	24	yes
6	Thawte EV RSA CA 2018	EV	12	yes
7	DigiCert SHA2 Extended Validation Server CA	EV	24	yes
8	Thawte EV RSA CA 2018	EV	22	yes
9	Thawte RSA CA 2018	**DV**	14	yes
10	GeoTrust EV RSA CA 2018	EV	27	yes
11	Thawte EV RSA CA 2018	EV	26	yes
12	–	–	–	NO
13	Thawte TLS RSA CA G1	**DV**	37	yes
14	DigiCert Global CA G2	EV	12	yes
15	COMODO ECC Domain Validation Secure Server CA 2	**DV**	6	yes
16	DigiCert Global CA G2	EV	12	yes
17	Thawte EV RSA CA 2018	EV	26	yes
18	Thawte EV RSA CA 2018	EV	12	yes
19	DigiCert SHA2 Extended Validation Server CA	EV	14	yes
20	Thawte EV RSA CA 2018	EV	26	yes
21	Actalis Organization Validated Server CA G2	DV	12	yes
22	Thawte EV RSA CA 2018	EV	26	yes

One of the surveyed Czech bank's public web sites is not using HTTPS properly (bank №12 uses certificate intended for another domain – member.icbc.com.cn). This is rather a small number, but it is a strange security practice, because the cost for a simple DV SSL/TSL certificate starts as low as 30 Euro per year. Also, there is a free alternative. For example, in the last years, prominent companies and organizations, such as Akamai, Cisco, Mozilla, IdenTrust, Electronic Frontier Foundation and others, collaboratively set up Let's Encrypt – a certifying authority with the main aim to issue free of charge SSL/TSL certificates. Currently these certificates had period of validity of 3 months (90 days). It is also possible "wildcard certificate" to be used, which purpose is to cover not only the main domain but also all subdomains.

The rest of the surveyed Czech bank's public web pages (95.5%) are using SSL/TSL certificates from reputable certification authorities (CAs). This guarantees that the public key used to encrypt the network connection corresponding to the domain name stored in DNS servers. The most preferable type of SSL/TSL certificate from Czech banks is EV – 77.3%, which is very good practice.

In general, three types of SSL/TSL certificates exist: Extended Validation (EV) certificate, Organization Validation (OV) certificate, and Domain Validation (DV) certificate [11], [12].

In case of DV, the certification authority (CA) checks is that the applicant can manage the stated domain name. Identity checks for the company are not performed, and no information about the company is displayed in the browser. Only the sign that the connection is secure is shown. Validation of organization (OV) means that the CA should conducts an additional brief survey of the organization which requested the certificate. In the case of EV, the certification authority performs an in-depth survey of the applying organization in regard of the real address, legal form of existence and the right of use the domain. In the last two cases – OV and EV, the browser shows the name of the organization next to the sign that the connection is secured – usually it is icon with green padlock. In case of DV certificate usage, only information that the connection is secured is shown in the URL bar of the browser. Because of this extra effort for in-depth survey of the applying organization, the EV certificate is much expensive than DV certificate.

Table 6. Major characteristics of the HTTPS usage in public web sites of Slovakian banks

Bank №	Certification authority body	Certificate type	Period of Validity /months/	Automatic redirection to HTTPS
1	DigiCert SHA2 Extended Validation Server CA	EV	25	yes
2	GeoTrust EV RSA CA 2018	EV	15	yes
3	DigiCert SHA2 Secure Server CA	**DV**	25	yes
4	COMODO RSA Domain Validation Secure Server CA	**DV**	24	yes
5	Thawte EV RSA CA 2018	EV	25	yes
6	Entrust Certification Authority - L1K	**DV**	24	yes
7	DigiCert SHA2 Secure Server CA	**DV**	24	yes
8	Thawte RSA CA 2018	**DV**	18	yes
9	GeoTrust EV RSA CA 2018	EV	10	yes
10	Entrust Certification Authority - L1M	EV	24	yes
11	**Let's Encrypt Authority X3**	**DV**	**3**	yes
12	GeoTrust RSA CA 2018	**DV**	14	yes
13	DigiCert SHA2 Secure Server CA	**DV**	24	NO
14	Thawte EV RSA CA 2018	EV	15	yes
15	Actalis Organization Validated Server CA G2	**DV**	12	yes

All the surveyed Slovakian bank's public web sites are following good practices and use HTTPS and SSL/TSL certificates. Unfortunately, the most preferable type of SSL/TSL certificate is DV – 60%, which is not good practice. The rest 40% of the banks are using EV SSL/TSL certificates. The free of charge Let's Encrypt SSL/TSL certificate is used by one bank.

Table 7. Major characteristics of the HTTPS usage in public web sites of Hungarian banks

Bank №	Certification authority body	Certificate type	Period of Validity /months/	Automatic redirection to HTTPS
1	DigiCert SHA2 Extended Validation Server CA	EV	16	yes
2	DigiCert Global CA G2	EV	24	yes
3	GlobalSign Extended Validation CA - SHA256 - G3	EV	26	yes
4	NetLock Üzleti (Class B) Tanúsítványkiadó	**DV**	24	yes
5	NetLock Üzleti (Class B) Tanúsítványkiadó	**DV**	24	yes
6	NetLock Üzleti (Class B) Tanúsítványkiadó	**DV**	12	yes
7	NetLock Közjegyzői (Class A) Tanúsítványkiadó	**DV**	24	yes
8	DigiCert SHA2 Extended Validation Server CA	EV	24	yes
9	NetLock Közjegyzői (Class A) Tanúsítványkiadó	**DV**	24	yes
10	DigiCert SHA2 High Assurance Server CA	**DV**	12	yes
11	NetLock Üzleti (Class B) Tanúsítványkiadó	**DV**	24	yes
12	Sectigo RSA Extended Validation Secure Server CA	EV	24	yes
13	–	**–**	–	NO
14	DigiCert SHA2 Extended Validation Server CA	EV	12	yes
15	**Let's Encrypt Authority X3**	**DV**	**3**	yes
16	**Let's Encrypt Authority X3**	**DV**	**3**	yes
17	GeoTrust EV RSA CA 2018	EV	23	yes
18	NetLock Üzleti (Class B) Tanúsítványkiadó	**DV**	24	yes
19	RapidSSL RSA CA 2018	**DV**	26	yes
20	Sectigo RSA Domain Validation Secure Server CA	**DV**	12	yes
21	**Let's Encrypt Authority X3**	**DV**	**3**	yes
22	Actalis Organization Validated Server CA G2	**DV**	12	yes

One of the surveyed Hungarian bank's public web sites is not using HTTPS at all (bank №13). The most preferable type of SSL/TSL certificate is DV – 63.6%, which is not good practice. Only 31.8% of the banks are using more expensive and more advanced EV SSL/TSL certificate. Three banks are using Let's Encrypt SSL/TSL certificate which is free of charge.

Based on the presented data in Table 5, 6 and 7 we grouped the results of our research in two tables. The types of the SSL/TSL certificates used by Czech, Slovakian and Hungarian banks are given on Table 8. Table 9 represents the shares of issuers of the SSL/TSL certificates.

Table 8. Type of the SSL/TSL certificates

Type of certificate	Czech Republic		Slovakia		Hungary	
	Count	%	Count	%	Count	%
No certificate	1	4.5	0	0	1	4.5
DV	4	18.2	**9**	**60.0**	**14**	**63.6**
EV	**17**	**77.3**	6	40.0	7	31.8
TOTAL	*22*	*100*	*15*	*100*	*22*	*100*

We find out that in the Czech Republic the large part of the banks is using EV – 77.3%; in Slovakia the share of the banks using EV is 40%; and in the Hungary the share of the banks using EV is 31.8%. The relation between indicators for economic development such as GDP per capita and GNI per capita, and the share of EV SSL/TSL certificates is revealed on Figure 1.

There is direct relation between the level of economic development and the usage of the more advanced and more expensive EV certificates. In Czech Republic which is most economically developed state compared to the other two countries the usage of EV certificates is highest. In Hungary which is less economically developed than other two countries the usage of EV certificates is lowest. In Slovakia which is in the middle of economic development between the other two countries the usage of EV certificates is also on the middle level.

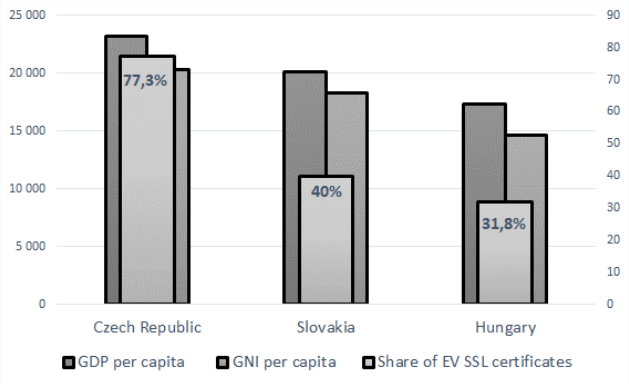

Figure 1. Relationship between GDP/GNI per capita and the share of EV SSL/TSL certificates

Based on the data in Table 9 we could conclude that there is direct relation between the level of economic development and the usage of free of charge Let's Encrypt SSL/TSL certificates. In more economically developed Czech Republic, no banks are using free of charge SSL/TSL certificates. In less economically developed Hungary three banks are using free of charge SSL/TSL certificates. In Slovakia one bank is using free of charge SSL/TSL certificate.

Table 9. The issuers of the SSL/TSL certificates used by Czech, Slovakian and Hungarian banks

Certification authority	Czech Republic		Slovakia		Hungary	
	Count	%	Count	%	Count	%
Actalis	1	4.5	1	6.7	1	4.5
COMODO	1	4.5	1	6.7	–	–
DigiCert	**7**	**31.8**	**4**	**26.7**	**5**	**22.7**
Entrust	–	–	2	13.3	–	–
GeoTrust	1	4.5	**3**	**20.0**	1	4.5
GlobalSign	–	–	–	–	1	4.5
Let's Encrypt	–	–	1	6.7	3	13.6
NetLock	–	–	–	–	**7**	**31.8**
RapidSSL	–	–	–	–	1	4.5
Sectigo	–	–	–	–	2	9.1
Thawte	**11**	**50.0**	**3**	**20.0**	–	–
–	1	4.5	–	–	1	4.5
TOTAL	*22*	*100*	*15*	*100*	*22*	*100*

There are several preferences for the certification body, but in Czech Republic the market is most consolidated – 81.9% of banks are using one of the following two certificate authorities – DigiCert (31.8%) and Thawte (50%) as issuers of SSL/TSL certificates. In Slovakia the market is less consolidated – 66.7% of banks are using 3 certificate authorities: DigiCert (26.7%), Thawte (20%) and GeoTrust (20%).

In Hungary the market is least consolidated with the greatest number of certificate authorities. It is strange that in this market Thawte is not presented. Instead the domestic certificate authority NetLock is the market leader with 31.8% of the issued SSL/TSL certificates. On the second place is the DigiCert with 22.7% market share and on the third place is the free of charge Let's Encrypt with share 13.6%.

The average period of validity of SSL/TSL certificates per country are as follow: in Czech Republic is 1 year and 8 months; in Slovakia is 1 year and 7 months; and in Hungary is 1 year and 6 months. Such difference is due to 3 months period of validity of Let's Encrypt SSL/TSL certificates.

4. Conclusion

This research leads to several conclusions.

First, the SSL/TSL certificate market in Czech Republic is more consolidated than this in Slovakia and Hungary.

Second, as for the use of SSL/TSL certificates, in Hungary there is more diversity – 8 SSL/TSL certificate providers, while in Czech Republic – they are only 5, in Slovakia – 7. In Czech Republic the most popular SSL/TSL certificate provider is Thawte with market share of 50% bank's web sites. In Slovakia the most popular is DigiCert with 26.7% share. In Hungary the most popular is the domestic certificate authority NetLock with 31.8% share.

Third, a relation is revealed between indicators for economic development such as GDP per capita and GNI per capita, and the type of the SSL/TSL certificates. The level of economic development impacts the usage of the more advanced and more expensive EV certificates. In Czech Republic the usage of EV certificates is the highest. In Slovakia the usage of EV certificates is in the middle level. In Hungary the usage of EV certificates is the lowest. The order by using GDP per capita and GNI per capita is the same – most economically developed state is Czech Republic, followed by Slovakia and then Hungary.

Fourth, a relation is revealed between the level of economic development and the usage of free of charge Let's Encrypt SSL/TSL certificates. In the most economic developed Czech Republic, no one of the banks are using free of charge SSL/TSL certificates. In Slovakia 1 bank is using free of charge SSL/TSL certificate. In least economically developed Hungary 3 banks are using free of charge SSL/TSL certificates.

Fifth, due to the short period of validity of the free of charge Let's Encrypt SSL/TSL certificates – 3 months, in less developed countries the the average period of validity is less. In Czech Republic it is 1 year and 8 months; in Slovakia is 1 year and 7 months; and in Hungary is 1 year and 6 months.

The data used in this study are collected in specific time period – from 1 July to 31 August 2019. IT specialist and bank's managers could use the results of the study when estimate different alternatives in regard of what technology to put into practice in order to maximize the benefits and in the same time to minimize the hazards for the financial institution. Our study finds out some good practices used in Czech, Slovakian and Hungarian banks. The study was focused on the HTTPS protocol used in the bank's public web sites and covered all 22 Czech, 15 Slovakian and 22 Hungarian banks which are licensed to operate on the respective country under the supervision of the domestic central banks.

Acknowledgements

This research was partially supported by NPI 9/2017 from University of Economics - Varna Science Fund.

References

[1]. World Bank (2019). *National accounts data and OECD National Accounts data files.* The World Bank Group.

[2]. Eurostat (2019). *Key figures on enlargement countries.* Publications Office of the European Union. DOI: 10.2785/542953

[3]. UNDP (2018). *Human Development Indicators and Indices: 2018 Statistical Update Team.* Human Development Report Office.

[4]. Country Economy (2019). Electronic resource. *Sovereigns Ratings List.* Retrieved from: https://countryeconomy.com/ratings [accessed: 19 March 2019].

[5]. Petrov, P., & Hundal, S. (2018). Application of Security Technologies in the Public Websites of Banks in Serbia. *Izvestia Journal of the Union of Scientists-Varna. Economic Sciences Series, 7*(2), 298-305.

[6]. Petrov, P., Krumovich, S., Nikolov, N., Dimitrov, G., & Sulov, V. (2018, September). Web Technologies Used in the Commercial Banks in Finland. In *Proceedings of the 19th International Conference on Computer Systems and Technologies* (pp. 94-98). ACM.

[7]. Petrov, P., Dimitrov, G., & Ivanov, S. (2018). A Comparative Study on Web Security Technologies Used in Irish And Finnish Banks. *International Multidisciplinary Scientific GeoConference: SGEM: Surveying Geology & mining Ecology Management, 18*, 3-10.

[8]. CNB (2019). *Banks and branches of foreign banks*. Czech National Bank.

[9]. BSI (2019). *Institutions under supervision. Banks in Slovenia.* Banka Slovenije.

[10]. MNB (2019). *The register of the financial service providers*. Magyar Nemzeti Bank.

[11]. Rajakumar, J., & Subrahmanya, K. N. (2019). Overview of TLS Certificate Revocation Mechanisms. *International Journal of Advanced Research in Computer Science, 10*(3), 54-59.

[12]. Tian, C., Chen, C., Duan, Z., & Zhao, L. (2019). Differential Testing of Certificate Validation in SSL/TLS Implementations: An RFC-guided Approach. *ACM Transactions on Software Engineering and Methodology (TOSEM), 28*(4), 24.

[13]. Hametner, M., Kostetckaia, M., Setz, I., Bley, S. J., Gebhard, F., Mayer, C., … & Steurer, A. (2019). *Sustainable development in the European Union. Overview of progress towards the SDGs in an EU context (2019 edition)*. Luxembourg: Publications Office of the European Union. DOI: 10.2785/58838

[14]. Panayotova, G., Dimitrov, G. P., Petrov, P., & Os, B. (2016, September). Modeling and data processing of information systems. In *2016 Third International Conference on Artificial Intelligence and Pattern Recognition (AIPR)* (pp. 154-158). IEEE.

[15]. Vasilev, J., Turygina, V. F., Kosarev, A. I., & Nazarova, Y. Y. (2016). Mathematical optimization in environmental economics. Algorithm of gradient projection method. *International Multidisciplinary Scientific GeoConference: SGEM: Surveying Geology & mining Ecology Management*, *3*, 349-355.

[16]. Berg, D., Demina, M., Isaichik, K., Panachev, A., Popkov, V., & Parusheva, S. (2018, November). Competition of payment systems in Russia: Numerical analysis. In *AIP Conference Proceedings* (Vol. 2040, No. 1, p. 050014). AIP Publishing.

[17]. Kachhwaha, R., & Purohit, R. (2019). Relating vulnerability and security service points for web application through penetration testing. In *Progress in Advanced Computing and Intelligent Engineering* (pp. 41-51). Springer, Singapore.

[18]. Calzavara, S., Focardi, R., Nemec, M., Rabitti, A., & Squarcina, M. Postcards from the Post-HTTP World: Amplification of HTTPS Vulnerabilities in the Web Ecosystem. In *Postcards from the Post-HTTP World: Amplification of HTTPS Vulnerabilities in the Web Ecosystem*. IEEE.