Security Certificates in Public Web Sites of Banks from Balkan States

Petrov, Pavel and Dimitrov, Petar

University of Economics - Varna

24 October 2019

Security Certificates in Public Web Sites of Banks from Balkan States

Pavel Petrov, Petar Dimitrov

University of Economics - Varna, Varna, Bulgaria
petrov@ue-varna.bg, p.d.dimitrov@ue-varna.bg

Abstract. In the recent years a trend is formed to use the HTTPS protocol as the default protocol for accessing web pages and to be used by default by web applications. In order for this to be done, a valid certificate issued by authority body should be used. In the scope of the study in the spring of 2019 we examined the web sites of 20 banks licensed in Bulgaria, 24 banks licensed in Romania and 27 banks licensed in Serbia. The survey excludes the foreign bank branches, because we try to outline the "good practices" used by domestic administrators of banking websites.

Keywords. Security Certificates; Bulgarian banks; Romanian banks; Serbian banks; HTTPS; bank web site.

1. Introduction

In this comparative study we choose banks which are regulated by local central banks and are from three neighboring European countries, located on Balkan Peninsula - Bulgaria, Romania and Serbia. These countries have a lot of similarities in demographics and economics characteristics. However, from political point of view, they are not similar. Bulgaria and Romania are members of EU and NATO, while Serbia is not. From financial point of view, the countries are not using Euro as currency and their bank systems are formally independent from higher level supervision. In Table 1 are summarized some large-scale similarities which have meaning in the context of the current study.

Table 1. Some large-scale similarities between Bulgaria, Romania and Serbia

Feature	Bulgaria	Romania	Serbia
Population (circa 2019)	7.000 mil.	19.524 mil.	7.021 mil
GNI per capita (Atlas method) in 2017	7 860$	10 000$	5 180$
Monetary policy	Not members of Eurozone		
Currency	BGN	RON	RSD
Political orientation	EU, NATO		-
Credit ratings	Long term Rating, Foreign currency		
S&P Global Ratings	BBB- (2018)	BBB- (2014)	BB (2018)
Moody's Investors Service	Baa2 (2017)	Baa3 (2018)	Ba3 (2017)
Fitch Ratings	BBB (2019)	BBB- (2018)	BB (2018)

The governments have high long-term credit ratings from credit rating agencies such as Standard & Poor's, Moody's, Fitch Ratings and so on. It should be noted that Gross National Income (GNI) represents the total domestic and foreign output of an economy. The GNI per

capita, developed by the World Bank, is widely used as an indicator for the overall level of economic development.

Before the comparison, we raise the hypothesis that in such very similar countries, with similar level of living standard and penetration of information and communication technologies, it should be expected that the web technologies used in local banks' web sites should also be similar. In these institutions there is no funding issues, and there are even opportunities to use expensive proprietary software. We believe that web technologies are a key component in the banking IT infrastructure. These technologies become an integral part of every aspect of the online banking business, therefore security and performance cannot be compromised for any reason.

2. Methodology and Computational Details

In our study home pages of 20 Bulgarian, 24 Romanian and 27 Serbian banks were inspected in April 2019. The main method used in the survey includes analysis of the responses given by the web servers. Google Chrome ver.73, working under typical desktop PC - Windows 10 Professional Edition x64, was used as a web client with "Developer tools" module activated. It should be noted that this module has not been intended specifically for such kind of studies, but it is a very useful tool in such cases. The process of inspection was done manually by expert estimation. Other approaches to do the same research could include using command line tools such as "curl". In our opinion, using real web browser is more straightforward. The methodology of the study is based partially on methodology used in previous studies on web technologies used in banks, and other studies [6], [7], [8], [9].

Table 2. Usage of the HTTPS protocol in public web sites of banks in Bulgaria

№	Bank Name	Bank' domain	HTTPS
1	Allianz Bank Bulgaria AD	allianz.bg	yes
2	Bulgarian Development Bank AD	bdbank.bg, bbr.bg	problem
3	Bulgarian-American Credit Bank AD	bacb.bg	yes
4	Central Cooperative Bank AD	ccbank.bg	yes
5	D Commerce Bank AD	dbank.bg	yes
6	DSK Bank EAD	dskbank.bg	yes
7	Eurobank Bulgaria AD	postbank.bg	yes
8	First Investment Bank AD	fibank.bg	yes
9	International Asset Bank AD	iabank.bg	**NO**
10	Investbank AD	ibank.bg	yes
11	Municipal Bank AD	municipalbank.bg	yes
12	Piraeus Bank Bulgaria AD	piraeusbank.bg	yes
13	ProCredit Bank (Bulgaria) EAD	procreditbank.bg	yes
14	Raiffeisenbank (Bulgaria) EAD	rbb.bg	yes
15	Societe Generale Expressbank AD	sgeb.bg, expressbank.bg	yes
16	TBI Bank EAD	tbibank.bg	yes
17	Texim Bank AD	teximbank.bg	yes
18	Tokuda Bank AD	tcebank.com, tokudabank.bg	yes

19	UniCredit Bulbank AD	bulbank.bg, unicreditbulbank.bg	yes
20	United Bulgarian Bank AD	www.ubb.bg	yes

Table 3. Usage of the HTTPS protocol in public web sites of banks in Romania

№	Bank Name	Bank' domain	HTTPS
1	Alpha Bank Romania S.A.	alphabank.ro	yes
2	Banca Comerciala FEROVIARA S.A.	bfer.ro	proble m
3	Banca Comerciala Intesa Sanpaolo Romania S.A.	intesasanpaolobank.ro	yes
4	Banca Comerciala Romana S.A.	bcr.ro	yes
5	Banca de Export Import a Romaniei EXIMBANK S.A.	eximbank.ro	yes
6	Banca Romana de Credite si Investitii SA	brci.ro	yes
7	Banca Romaneasca S.A. Membra a Grupului National Bank of Greece	brom.ro, banca-romaneasca.ro	yes
8	Banca Transilvania S.A.	bancatransilvania.ro	yes
9	Bank Leumi Romania S.A.	leumi.ro	yes
10	BRD - Groupe Societe Generale S.A.	brd.ro	yes
11	CEC Bank S.A.	cec.ro	yes
12	Credit Agricole Bank Romania S.A.	credit-agricole.ro	yes
13	Credit Europe Bank (ROMANIA) S.A.	crediteurope.ro	yes
14	First Bank S.A.	firstbank.ro	yes
15	Garanti Bank S.A.	garantibank.ro	yes
16	Idea Bank S.A.	idea-bank.ro	yes
17	Libra Internet Bank S.A.	librabank.ro	yes
18	Marfin Bank (ROMANIA) S.A.	marfinbank.ro	yes
19	OTP Bank Romania S.A.	otpbank.ro	yes
20	Patria Bank S.A.	patriabank.ro	yes
21	Porsche Bank Romania S.A.	porschebank.ro	yes
22	ProCredit Bank S.A.	procreditbank.ro	yes
23	Raiffeisen Bank SA	raiffeisen.ro	yes
24	UniCredit Bank S.A.	unicredit.ro	yes

The lists of banks authorized to operate in Bulgaria, Romania and Serbia were taken from the websites of Bulgarian National Bank [10] (Table 2), Romanian National Bank [11] (Table 3) and National Bank of Serbia [12] (Table 4). In our study websites of foreign bank branches and representative offices of foreign banks operating in Bulgaria, Romania and Serbia are excluded. We surveyed only local ones, which operate under supervision of the domestic national bank. So, the websites of those banks that operate on a branch or on a cross-border basis were omitted.

The summarized results of the studied home web pages are presented in several tables (Tables 5 - 7) based on the following key indicators: presence of automatic redirection to HTTPS, certificate type, certification body and validity period of the SSL certificate.

Table 4. Usage of the HTTPS protocol in public web sites of banks in Serbia

№	Bank Name	Bank' domain	HTTPS
1	Addiko Bank AD Beograd	addiko.rs	yes
2	Agroindustrijsko Komercijalna Banka AD, Beograd	aikbanka.rs	yes
3	Banca Intesa AD Beograd (Novi Beograd)	bancaintesa.rs	yes
4	Banka Postanska Stedionica AD, Beograd (Palilula)	posted.co.rs	yes
5	Credit Agricole Banka Srbija AD Novi Sad	creditagricole.rs	yes
6	Direktna Banka AD Kragujevac	direktnabanka.rs	yes
7	Erste Bank AD, Novi Sad	erstebank.rs	yes
8	Eurobank AD Beograd	eurobank.rs	yes
9	Expobank AD Beograd	expobank.rs	problem
10	Halkbank AD Beograd	halkbank.rs	**NO**
11	Jubmes Banka AD Beograd (Novi Beograd)	jubmes.rs	**NO**
12	Komercijalna Banka AD, Beograd (Vracar)	kombank.com	yes
13	Mirabank AD Beograd-Novi Beograd	mirabankserbia.com	yes
14	MTS Banka AD Beograd	mts-banka.rs	yes
15	NLB Banka AD, Beograd	nlb.rs	yes
16	Opportunity Banka AD, Novi Sad	obs.rs	yes
17	OTP Banka Srbija AD, Novi Sad	otpbanka.rs	yes
18	Piraeus Bank AD Beograd (Novi Beograd)	piraeusbank.rs, direktnabanka.rs	yes
19	Procredit Bank AD, Beograd (Novi Beograd)	procreditbank.rs	yes
20	Raiffeisen Banka AD Beograd	raiffeisenbank.rs	yes
21	Sberbank Srbija A.D. Beograd	sberbank.rs	yes
22	Societe Generale Banka Srbija AD, Beograd	societegenerale.rs	yes
23	Srpska Banka AD Beograd (Savski Venac)	srpskabanka.rs	yes
24	Telenor Banka AD Beograd (Novi Beograd)	telenorbanka.rs	yes
25	Unicredit Bank Srbija A.D., Beograd (Stari Grad)	unicreditbank.rs	yes
26	Vojvodanska Banka AD Novi Sad	voban.rs	yes
27	VTB Banka AD Beograd	vtbbanka.rs, apibank.rs	yes

3. Empirical Results and Discussion

Around 5% of the Bulgarian and 7.4% of the Serbian bank web sites surveyed are not using HTTPS at all. In our opinion this is not a high percentage, but it is strange, because the prices for a simple DV certificate starts at around 30€ annual fee. Also, there is a free alternative. For example, in the recent years, major organizations and companies, such as the Electronic Frontier Foundation, Mozilla, Akamai, Cisco, IdenTrust, and others, have

collaboratively set up a certifying authority, Let's Encrypt, to issue free certificates. These certificates are currently valid for 90 days. Since the beginning of 2018, the so-called "wildcard certificates" covering all subdomains of a domain was introduced.

One Bulgarian, one Romanian and one Serbian bank web sites are using HTTPS with issues. Bulgarian bank №2 (from Table 2) is using expired in 2012 self-signed certificate for "localhost.localdomain". Romanian bank №2 (from Table 3) is using certificate which hostname does not match the main domain but only the subdomain bcfonline.bfer.ro. Serbian bank №9 (from Table 4) is using self-signed certificate for "marfin.gridsrv.net" with validity period of 10 years - until 2027. In these cases, we can give the following recommendation: either to support HTTPS according to good practices or better not to use HTTPS at all, because these problems could weaken the confidence of customers in the financial institution's ability to keep its systems up to date.

Table 5. Main features in usage of the HTTPS in public web sites of Bulgarian banks

Bank №	Automatic redirection to HTTPS	Certificate type	Certification authority body	Validity in
1	Yes	**DV**	RapidSSL RSA CA 2018	9
3	Yes	EV	COMODO RSA Extended Validation Secure Server CA	26
4	Yes	EV	COMODO RSA Extended Validation Secure Server CA	24
5	Yes	EV	GeoTrust EV RSA CA 2018	14
6	Yes	EV	DigiCert SHA2 Extended Validation Server CA	13
7	Yes	EV	GeoTrust EV RSA CA 2018	24
8	Yes	EV	COMODO RSA Extended Validation Secure Server CA	26
10	**NO**	**DV**	COMODO ECC Domain Validation Secure Server CA 2	6
11	Yes	EV	GeoTrust EV RSA CA 2018	24
12	Yes	EV	DigiCert SHA2 Extended Validation Server CA	24
13	**NO**	**DV**	DigiCert SHA2 Secure Server	24
14	yes	EV	COMODO RSA Extended Validation Secure Server CA	24
15	yes	**DV**	COMODO RSA Domain Validation Secure Server CA	24
16	yes	EV	GeoTrust EV RSA CA 2018	24
17	yes	EV	GeoTrust EV RSA CA 2018	24
18	yes	EV	GeoTrust EV RSA CA 2018	9
19	yes	**DV**	Let's Encrypt Authority X3	3
20	yes	EV	DigiCert SHA2 Extended Validation Server CA	24

Around 90% of the Bulgarian, 96% of the Romanian and 89% of the Serbian bank web sites are using HTTPS without major issues. They use certificates from recognized certification authorities (CAs) that certify the connection between the public key used to encrypt the connection and the domain name stored on DNS servers (Tables 5, 6, 7).

Table 6. Main features in usage of the HTTPS in public web sites of Romanian banks

Bank №	Automatic redirection to HTTPS	Certificate type	Certification authority body	Validity in months
1	yes	EV	DigiCert SHA2 Extended Validation Server CA	14
3	yes	EV	GeoTrust EV RSA CA 2018	26
4	yes	EV	DigiCert SHA2 Extended Validation Server CA	12
5	yes	**DV**	GeoTrust RSA CA 2018	26
6	yes	EV	GeoTrust EV RSA CA 2018	14
7	yes	EV	DigiCert SHA2 Extended Validation Server CA	5
8	yes	EV	DigiCert SHA2 Extended Validation Server CA	13
9	yes	EV	DigiCert Global CA G2	13
10	yes	**DV**	Let's Encrypt Authority X3	3
11	yes	EV	DigiCert SHA2 Extended Validation Server CA	14
12	yes	EV	DigiCert Global CA G2	22
13	yes	**DV**	Thawte RSA CA 2018	27
14	yes	**DV**	GeoTrust RSA CA 2018	24
15	yes	**DV**	DigiCert SHA2 Secure Server CA	12
16	yes	**DV**	DigiCert SHA2 Secure Server CA	14
17	yes	EV	DigiCert SHA2 Extended Validation Server CA	24
18	**NO**	EV	DigiCert Global CA G2	13
19	yes	EV	GeoTrust EV RSA CA 2018	14
20	yes	**DV**	COMODO RSA Domain Validation Secure Server CA	24
21	yes	**DV**	Let's Encrypt Authority X3	3
22	yes	**DV**	Go Daddy Secure Certificate Authority - G2	12
23	yes	**DV**	DigiCert SHA2 Secure Server CA	26
24	yes	EV	Actalis Extended Validation Server CA G1	12

Three types of certificates are used: Domain Validation (DV), Organization Validation (OV), and Extended Validation (EV) [13], [14]. When validating a domain (DV), the certification authority checks to see if the applicant can use a specific domain name. No company identity checks are performed, and no other information is displayed in the browser, unless the connection is secure. Upon Validation of Organization (OV), the Certifying Authority additionally conducts a survey of the organization that appears when examining the certificate. In the Extended Validation (EV), the Certification Body carries out an in-depth verification of the organization with regard to the legal form of existence, real address, and right to use a particular domain, where the name of the organization is displayed in the browser along with the information that the link is protected. In general, the DV certificate is cheaper than EV certificate.

Table 7. Main features in usage of the HTTPS in public web sites of Serbian banks

Bank №	Automatic redirection to HTTPS	Certificate type	Certification authority body	Validity in months
1	yes	EV	Thawte EV RSA CA 2018	11
2	yes	**DV**	Go Daddy Secure Certificate Authority - G2	14
3	yes	**DV**	Entrust Certification Authority - L1K	24
4	**NO**	**DV**	Thawte RSA CA 2018	14
5	yes	EV	GeoTrust EV RSA CA 2018	12
6	yes	**DV**	cPanel, Inc. Certification Authority	3
7	yes	**DV**	DigiCert Global CA G2	12
8	yes	**DV**	Go Daddy Secure Certificate Authority - G2	36
12	yes	**DV**	Go Daddy Secure Certificate Authority - G2	37
13	yes	**DV**	Thawte RSA CA 2018	13
14	yes	**DV**	GlobalSign Organization Validation CA - SHA256 - G2	25
15	yes	**DV**	COMODO RSA Domain Validation Secure Server CA	24
16	**NO**	**DV**	Let's Encrypt Authority X3	3
17	yes	EV	GeoTrust EV RSA CA 2018	14
18	yes	**DV**	cPanel, Inc. Certification Authority	3
19	yes	**DV**	Thawte RSA CA 2018	14
20	yes	EV	Thawte EV RSA CA 2018	24
21	yes	EV	GeoTrust EV RSA CA 2018	14
22	yes	**DV**	Thawte RSA CA 2018	24
23	**NO**	**DV**	cPanel, Inc. Certification Authority	3
24	**NO**	**DV**	Let's Encrypt Authority X3	3
25	yes	**DV**	Actalis Organization Validated Server CA G1	12
26	yes	EV	GeoTrust EV RSA CA 2018	14
27	yes	**DV**	cPanel, Inc. Certification Authority	3

Table 8. Certificate type of the SSL certificates

Certificate type	**Bulgaria**		**Romania**		**Serbia**	
	Count	**%**	**Count**	**%**	**Count**	**%**
No certificate or problem	2	10	1	4	3	11
DV	5	25	10	42	18	67
EV	13	65	13	54	6	22
TOTAL	***20***	***100***	***24***	***100***	***27***	***100***

From the data presented in Tables 5, 6 and 7, in the Bulgaria the majority (13 banks) uses EV, and the rest (5 banks) use DV. In Romania the situation is the same - the majority

(13 banks) uses EV, and the rest (10 banks) use DV. But in Serbia is the opposite - the majority (18 banks) uses DV, and the rest (6 banks) use EV (Table 8, Fig. 1).

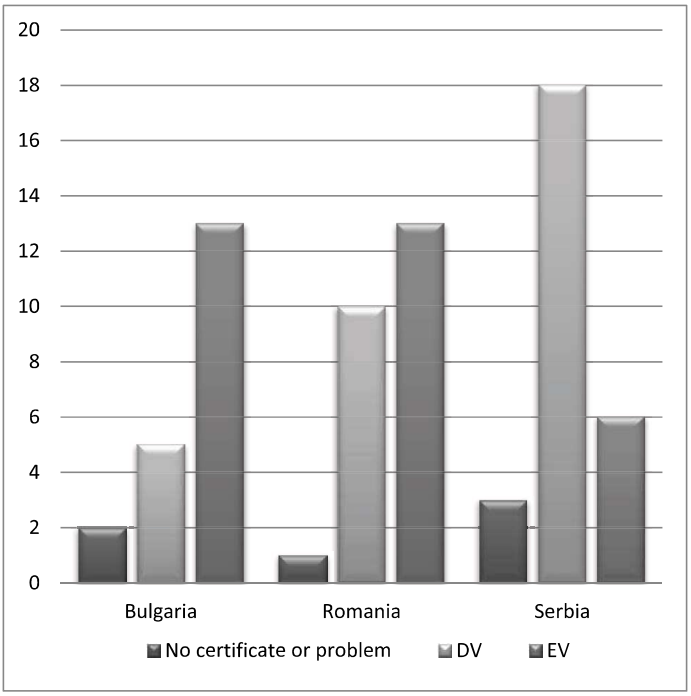

Fig. 1. Shares of certificate types.

In two cases in Bulgaria, one case in Romania and four cases in Serbia of the banking websites, the good practices are not followed, and they do not automatically redirect from unsecure to secure connection.

Table 9. The issuers of the SSL certificates used by Bulgarian and Serbian banks

Certification authority body	**Bulgaria**		**Romania**		**Serbia**	
	Count	**%**	**Count**	**%**	**Count**	**%**
Actalis	-	-	1	4	1	4
COMODO	6	33	1	4	1	4
cPanel	-	-	-	-	4	17
DigiCert	4	22	12	52	1	4
Entrust	-	-	-	-	1	4
GeoTrust	6	33	5	22	4	17
GlobalSign	-	-	-	-	1	4
Go Daddy	-	-	1	4	3	13
Let's Encrypt	1	6	2	9	2	8
RapidSSL	1	6	-	-	-	-
Thawte	-	-	1	4	6	25
TOTAL	***18***	***100***	***23***	***100***	***24***	***100***

There is a wide variety of preferences for a certification authority, but the most popular choices in Bulgaria are: Comodo and GeoTrust - 6 banks, DigiCert - 4 banks. It should be noted that RapidSSL is owned by GeoTrust, so actually the real leader is the GeoTrust. In Romania the most popular choice is DigiCert - 12 banks, followed by GeoTrust - 5 banks. In Serbia the most popular choices are other market players, which are not presented in Bulgaria and poorly presented in Romania: Thawte - 6 banks, cPanel - 4 banks, Go Daddy - 3 banks. The only large common player is GeoTrust - 4 banks (Table 9).

One bank in Bulgaria and two banks in Romania and Serbia are using free of charge 3 months-long Let's Encrypt certificates.

4. Conclusion

This research leads to several conclusions. First, the bank sector in Bulgaria is more consolidated that this in Romania and Serbia. Second, as for the use of SSL certificates, in Serbia there is more diversity - ten SSL certificate providers, while in Bulgaria - they are only five, in Romania - seven. In Serbia the most popular SSL certificate provider is Thawte with share of 25% web sites. In Bulgaria the most popular is GeoTrust with 39% share (if taking into account RapidSSL). In Romania the most popular choice is DigiCert with 52% market share. It is interesting that one Bulgarian and two Romanian and Serbian banks are using free certificates from Let's Encrypt Authority. Two banks in Bulgaria, one bank in Romania and four banks in Serbia are not redirecting automatically from unsecure HTTP to secure HTTPS connection. Two banks in Bulgaria, one bank in Romania and three banks in Serbia are not using SSL or have some problem with the certificates. In Bulgaria the average validity of certificates is 19 months (median - 24 months), while in Romania and Serbia - more shorted - around 16 and 15 months (median - 14 months).

The collected data are related to period April 2019. The results of the study could have important practical impact for bank managers and IT specialists when evaluating options which technologies to implement in order to minimize the risk to the financial institution. Also, the results reveal some good practices used in Bulgarian, Romanian and Serbian banks. The research conducted on the use of the HTTPS protocol on the banks' public web sites covered the sites of all 20 Bulgarian, 24 Romanian and 27 Serbian banks licensed to operate on the respective country territory by the domestic National Banks.

From banks that are using HTTPS without major problems, in Bulgaria the majority (13 banks) uses Extended Validation (EV) types of certificates, and the rest (5 banks) use Domain Validation (DV). In Romania the situation is the same - the majority (13 banks) uses EV, and the rest (10 banks) use DV. But in Serbia is the opposite - the majority (18 banks) uses DV, and the rest (6 banks) use EV. We suppose that one of the reasons for this is because DV certificates is usually cheaper than EV certificates.

As it is known, when using text protocols (such as HTTP/0.9/1.0/1.1) the so called "man in the middle" could be listening to all traffic and exchanged queries and responses between clients and servers. Network packets can easily be read, even without the use of complex tools. In many cases confidential information is exchanged, e.g. passwords, bankcard numbers for payment, personal information, etc. In those cases, the best option is to use the specially intended for this purposes protocol HTTPS, also known as "HTTP Secure", "Secure HTTP", "HTTP over SSL", "HTTP over TLS", etc. The use of a secure connection increases the processing load on the client and on the server in terms of busy CPU time and the amount of RAM, but in recent years, this is not considered a serious argument given the great benefits of communication security.

References

1. National Statistical Institute (2018). *Population by districts, municipalities, place of residence and sex as of 31.12.2018* <http://www.nsi.bg/en/content/6704/ population-districts-municipalities-place-residence-and-sex>
2. National Institute of Statistics (2018). *Population* <http://www.insse.ro/cms/sites/default/files/com_presa/com_pdf/poprez_ian2018e.pdf>
3. Statistical Office of the Republic of Serbia (2017). *Estimated population*, <http://www.stat.gov.rs/en-us/vesti/20180629-procene-stanovnistva-2017/?s=1801>
4. The World Bank Group, GNI per capita, Atlas method (current US$), <https://data.worldbank.org/indicator/ NY.GNP.PCAP.CD>
5. Sovereigns Ratings List, <https://countryeconomy.com/ratings> (20.04.2019)
6. Petrov, P., et al. (2018). Web Technologies Used in the Commercial Banks in Finland. *CompSysTech'18*, University of Ruse, Bulgaria, ACM, 94-98.
7. Petrov, P., Dimitrov, G. & Ivanov, S. (2018). A Comparative Study on Web Security Technologies Used in Irish and Finnish Banks. *18 International Multidisciplinary Scientific Geoconference SGEM*, Vol. 18, Issue 2.1, 3-10.
8. Petrov, P. (2013). Trends In The Use Of Web Server Software In Bulgarian Banks. *International Conference On Application Of Information And Communication Technology And Statistics In Economy And Education (ICAICTSEE-2012)*, UNWE, 359-364.
9. Petrov, P. & Hundal, S. (2018) Application of Security Technologies in the Public Sites of Banks in Serbia. Izvestia Journal of the Union of Scientists - Varna. Economic Sciences Series, Union of Scientists - Varna, Vol.7, Iss.2, pp.298-305.
10. BNB, Banks Licensed in the Republic of Bulgaria as of 11.02.2019, <http://www.bnb.bg/ BankSupervision/BSCreditInstitution/BSCIRegisters/BS_CI_REG_BANKSLIST_EN>
11. Banca Naţională a României, REGISTRUL INSTITUTIILOR DE CREDIT LA DATA 18-01-2019, PARTEA I - Sectiunea I - Banci, <http://www.bnr.ro/files/d/RegistreBNR/InstitCredit/ban1_raport.html>
12. National Bank of Serbia (NBS), List of Banks as of 22.03.2019, <https://www.nbs.rs/internet/english/ 50/50_2.html>
13. Cooper, D., et al. (2008) RFC5280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, <https://www.ietf.org/rfc/rfc5280.txt>
14. Saint-Andre, P., Hodges, J. (2011) RFC6125, Representation and Verification of Domain-Based Application Service Identity within Internet Public Key Infrastructure Using X.509 (PKIX) Certificates in the Context of Transport Layer Security (TLS), <https://tools.ietf.org/rfc/rfc6125.txt>