EasyChair Preprint

№ 3873

Web Security Technologies Used in Banks of Estonia, Latvia and Lithuania

Pavel Petrov

July 14, 2020

WEB SECURITY TECHNOLOGIES USED IN BANKS OF ESTONIA, LATVIA AND LITHUANIA

***Pavel Petrov*[1]**
[1] University of Economics – Varna/Department of Informatics, Bulgaria, petrov@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 this to be done a valid certificate issued by authority body should be used. In the scope of the study in the summer of 2019 we examined the web sites of banks licensed in Estonia, Latvia and Lithuania. The survey excludes the foreign bank branches, because we try to outline the "good practices" used by domestic administrators of banking websites.

Keywords: *Estonian banks; Latvian banks; Lithuanian banks; HTTPS; SSL/TLS certificates.*

INTRODUCTION

In this comparative study we choose banks which are regulated by local central banks and belong to three neighbour European countries, located in Northern Europe on the eastern coast of the Baltic Sea - the so called "Baltic states" - Estonia, Latvia, and Lithuania. These countries have a lot of similarities in demographics, economics and politics characteristics - they are members of the European Union and NATO. In their financial system they are using Euro as currency and are members of the Eurozone.

In Table 1 are summarized some overall data for countries which have general meaning in the context of the current study. It should be noted that there are some variations. For example the Gross Domestic Product per capita indicator of Estonia is the largest, but the Gini Index indicator is the lowest. This could be happen because of different metrics and the time lag in collected data. In general the three countries are very similar.

Before the comparison, we raise the hypothesis that in such very similar countries, with similar level of living standard, it should be ex-

pected that the web technologies used in local banks' web sites should be also similar. In these institutions usually there is no problem with funding, and there are opportunities to use expensive software.

Table 1

Large-scale overall comparison between the Baltic States

Feature	Estonia	Latvia	Lithuania
Population [millions]	1.3	1.9	2.8
Area [km^2]	45 339	64 589	65 300
GDP (nominal) per capita (2018) [€]	19 500	15 300	16 100
Gini Index (2015)	32.7	34.2	37.4
HDI (2018)	0.871 (Very High)	0.847 (Very High)	0.858 (Very High)

Sources: *Wikipedia 2019; Eurostat, 2019; World Bank DRG, 2019; UN HDRO, 2019.*

1. METHODOLOGY AND EMPIRICAL RESULTS

In our study home pages of 9 Estonian, 14 Latvian and 4 Lithuanian banks were inspected in August 2019. The main method used in the survey includes analysis of the responses given by the web servers. An up to date browser Google Chrome Version 76.0.3809.100 (Official Build) (64-bit), working under typical desktop PC with Windows 10 Professional Edition x64, was used as a web client with "Developer tools" module activated. 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", but using real web browser is more straightforward. The methodology of the study is based partially on methodology used in previous studies (Petrov, 2018/19) on web technologies used in banks.

The lists of banks authorized to operate in Estonia, Latvia and Lithuania (Table 2) were taken from the websites of Estonia Finantsinspektsioon, Latvia Financial and Capital Market Commission and Bank of Lithuania (see reference list at the end). In this study websites of foreign bank branches and representative offices of foreign banks operat-

ing in the local financial markets are excluded. We surveyed only domestic ones, which operate under regulation of the domestic authority body. So the websites of those banks that operate on an EU branch or on an EU cross-border basis are not included.

Table 2

HTTPS protocol usage in public web sites of banks in the Baltic States

№	Bank Name	Bank domain	HTTPS
Estonia			
1	AS Inbank	www.inbank.ee	yes
2	AS LHV Pank	www.lhv.ee	yes
3	AS Luminor Bank	www.luminor.ee	yes
4	AS SEB Pank	www.seb.ee	yes
5	AS TBB pank	www.tbb.ee	yes
6	Bigbank AS	www.bigbank.ee	yes
7	Coop Pank aktsiaselts	www.cooppank.ee	yes
8	Holm Bank AS	www.holmbank.ee	yes
9	Swedbank AS	www.swedbank.ee	yes
Latvia			
1	AS Baltic International Bank	www.bib.lv, www.bib.eu	yes
2	AS Citadele banka	www.citadele.lv	yes
3	AS LPB Bank	www.lpb.lv	**NO**
4	AS Reģionālā investīciju banka	www.ribbank.com	**NO**
5	AS Rietumu Banka	www.rietumu.lv	yes
6	AS Meridian Trade Bank	www.mtbank.eu	yes
7	AS PrivatBank	www.privatbank.lv	yes
8	AS BlueOrange Bank	www.blueorangebank.com	yes
9	AS Expobank	www.expobank.eu	yes
10	AS PNB Banka	www.pnbbanka.eu	yes
11	AS SEB banka	www.seb.lv	yes
12	Rigensis Bank AS	www.rigensisbank.com	**yes, but redirects to HTTP**

13	Signet Bank AS	www.signetbank.com	yes
14	Swedbank AS	www.swedbank.lv	yes
Lithuania			
1	Akcinė bendrovė Šiaulių bankas	www.sb.lt	yes
2	AB SEB bankas	www.seb.lt	yes
3	Swedbank AB	www.swedbank.lt	yes
4	UAB Medicinos bankas	www.medbank.lt	yes

The summarized results of the studied home web pages are presented in the next table (Table 3) based on the following key indicators: presence of automatic redirection to HTTPS, certificate type, the name of certification body and validity period of the SSL certificate.

Table 3

Main features in usage of the HTTPS in public web sites of banks in the Baltic States

Bank №	Automatic redirection to HTTPS	Certificate type	Certification authority body	Validity
Estonia				
1	yes	**DV**	Sectigo RSA Domain Validation Secure Server CA	2 y. 2 m.
2	yes	EV	DigiCert SHA2 Extended Validation Server CA	2 y. 3 m.
3	yes	**DV**	**Let's Encrypt Authority X3**	3 m.
4	yes	EV	GlobalSign Extended Validation CA - SHA256 - G3	1 y. 1 m.
5	**NO**	**DV**	DigiCert SHA2 Secure Server CA	2 y. 1 m.
6	yes	EV	DigiCert SHA2 Extended Validation Server CA	2 y. 2 m.
7	yes	**DV**	Amazon	1 y. 1 m.
8	yes	EV	Sectigo RSA Extended Validation Secure Server CA	1 y.
9	yes	EV	DigiCert SHA2 Extended Validation Server CA	1 y.

Latvia				
1	yes	EV	DigiCert SHA2 Extended Validation Server CA	2 y. 1 m.
2	yes	EV	Thawte EV RSA CA 2018	2 y.
5	yes	**DV**	DigiCert SHA2 Secure Server CA	2 y. 2 m.
6	yes	EV	Thawte EV RSA CA 2018	2 y. 1 m.
7	yes	**DV**	Go Daddy Secure Certificate Authority - G2	1 y. 1 m.
8	yes	**DV**	DigiCert SHA2 Secure Server CA	2 y.
9	yes	**DV**	**Let's Encrypt Authority X3**	3 m.
10	yes	**DV**	Thawte RSA CA 2018	1 y.
11	yes	**DV**	GlobalSign Organization Validation CA - SHA256 - G2	2 y. 1 m.
12	**NO**	**DV**	DigiCert SHA2 Secure Server CA	1 y. 3 m.
13	yes	**DV**	Go Daddy Secure Certificate Authority - G2	2 y.
14	yes	EV	DigiCert SHA2 Extended Validation Server CA	1 y.
Lithuania				
1	yes	**DV**	Thawte TLS RSA CA G1	1 y. 7 m.
2	yes	**DV**	GlobalSign Organization Validation CA - SHA256 - G2	2 y. 1 m.
3	yes	EV	DigiCert SHA2 Extended Validation Server CA	1 y.
4	yes	**DV**	COMODO RSA Domain Validation Secure Server CA	3 y.

2. COMPUTATIONAL DETAILS AND DISCUSSION

Three Latvian banks web sites are not using HTTPS (№3, №4 and №12) - two are not using HTTPS at all (№3 and №4) and in one case (№12) HTTPS requests are redirected to use HTTP. The number of banks web sites not using HTTPS is not high, but this situation is quite strange, because the prices for a simple DV certificate starts at around

30€ per year and also there is a free alternative. Well reputable 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, with the main goal to issue free certificates. These certificates are currently valid for 3 months. The so-called "wildcard certificates" covering all subdomains of a domain was introduced in 2018. One Estonian (№3) and Latvian (№9) banks are using free certificates from Let's Encrypt Certificate Authority.

About the case of redirecting the HTTPS requests to use HTTP (Latvian bank №12) it will be better either to support HTTPS according to the good practices or not to use HTTPS at all, because these problems could weaken the confidence of customers in the bank's capability to keep up to date its systems.

They are three types of certificates: Domain Validated (DV), Organization Validated (OV), and Extended Validated (EV) (Cooper, 2008; Saint-Andre, 2011). 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 that 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. Because there is no sure way to tell with confidence if a SSL certificate is Domain Validated or Organization Validated, in this research we didn't provide separation between them. 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 connection is protected. In general, the DV certificate is cheaper than EV certificate, but EV certificates are more prestigious.

From the data presented in Table 3 and aggregated in Table 4, it is clear that the majority - 15 banks are using simple DV certificates, and only 10 banks are using the more complicated for issuance EV. Only in Estonia the majorities (56%) of banks are using EV certificates while in Latvia and Lithuania the situation is the opposite - the majority (57% in Latvia and 75% in Lithuania) uses DV.

Table 4

Type of the SSL certificates in public web sites of banks in the Baltic States

Certificate type	Estonia		Latvia		Lithuania	
	Count	%	Count	%	Count	%
No certificate	-	-	2	14	-	-
DV	4	44	8	57	3	75
EV	5	56	4	29	1	25
TOTAL	*9*	*100*	*14*	*100*	*4*	*100*

In two cases - one in Estonia, one case in Latvia the good practices are not followed and HTTP requests are not automatically redirect to use secure HTTPS connection.

There is a wide variety of preferences for a certification authority, but the most popular choices in Baltic States are:

- DigiCert - 10 banks;
- Thawte - 4 banks;
- GlobalSign - 3 banks;
- Sectigo/Comodo (Sectigo is formerly Comodo) - 3 banks;
- Go Daddy - 2 banks;
- Let's Encrypt (free of charge 3 months-long certificates.) - 2 banks;
- Amazon - 1 bank.

The data about certification authority which is presented in Table 3 are aggregated for convenience in Table 5 and represented on Figure 1.

Table 5

The issuers of the SSL certificates used in public web sites of banks in the Baltic States

Certification authority body	Estonia		Latvia		Lithuania	
	Count	%	Count	%	Count	%
Amazon	1	11	-	-	-	-
DigiCert	4	45	5	42	1	25

GlobalSign	1	11	1	8	1	25
Go Daddy	-	-	2	17	-	-
Let's Encrypt	1	11	1	8	-	-
Sectigo/Comodo	2	22	-	-	1	25
Thawte	-	-	3	25	1	25
TOTAL	*9*	*100*	*12*	*100*	*4*	*100*

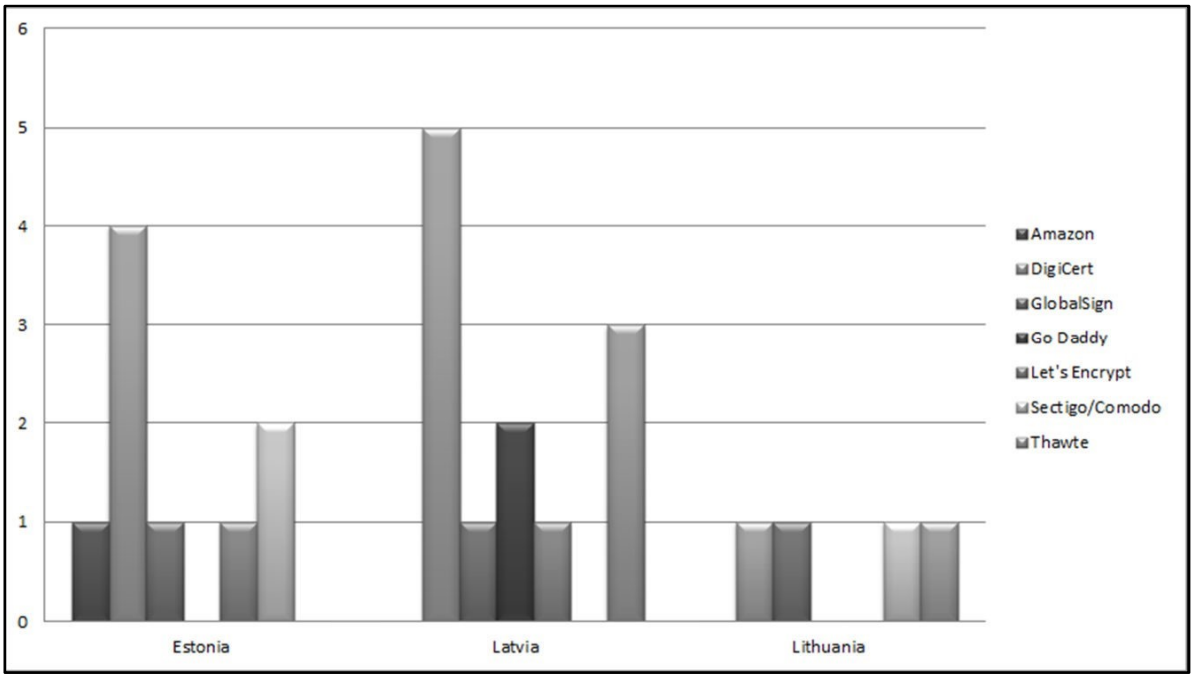

Figure 1. Certification authorities used by banks in the Baltic States

CONCLUSION

This research leads to the following conclusions. First, the banks sector in Lithuania, which is the largest Baltic state, is more consolidated that this in Estonia and Latvia. Second, as for the use of SSL certificates the most popular SSL certificate provider is DigiCert with share of 40% web sites. It is interesting that one Estonian and one Latvian bank are using free certificates from Let's Encrypt Authority. One bank in Estonia, two banks in Latvia are not redirecting automatically from unsecure HTTP to secure HTTPS connection. Three banks in Latvia are not using SSL at all or redirect secure HTTPS requests to unsecure HTTP connection. The last one we consider as a very bad practice.

The average validity of certificates is 1 year and 7 months with median - 1 year and 11 months.

The collected data are related to particular period - August 2019. The results of the study could have important practical impact for banks managers and IT specialist when evaluating options which technologies to implement in order to minimize the risk to the financial institution. Also the results reveal some good and bad practices used in the Baltic States banks. The research conducted on the use of the HTTPS protocol on the banks' public web sites covered the sites of all 9 Estonian, 14 Latvian and 4 Lithuanian banks licensed to operate on the respective country territory by the domestic National Banks or other government institution.

REFERENCES

1. BANK OF LITHUANIA (2019). Supervision of financial market participants. Banks authorised in the Republic of Lithuania. [Online] Available from: https://www.lb.lt/en/sfi-financial-market-participants ?business_form=82&market=1 [Accessed 07/08/2019].
2. COOPER, D., et al. (2008) Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. *RFC5280*. [Online] Available from: https://www.ietf.org/rfc/rfc 5280.txt [Accessed 07/08/2019].
3. ESTONIA FINANTSINSPEKTSIOON (2019). Supervised Entities. Licensed credit institutions in Estonia [Online] Available from: https://www.fi.ee/en/banking-and-credit/banking-and-credit/credit-institutions/licensed-credit-institutions-estonia [Accessed 07/08/ 2019].
4. EUROSTAT (2019), Gross domestic product at market prices. *Eurostat Database* [Online] Available from: https://ec.europa.eu /eurostat/tgm/table.do?tab=table&plugin=1&language=en&pcode=tec00001 [Accessed 07/08/2019].
5. LATVIA FINANCIAL AND CAPITAL MARKET COMMISSION (2019). Market. Credit institutions. Banks. [Online] Available from: https://www.fktk.lv/en/market/credit-institutions/banks/ [Accessed 07/08/2019].

6. PETROV, P., BUEVICH, A., DIMITROV, G., KOSTADINOVA, I. and DIMITROV, P. A Comparative Study on Web Security Technologies Used in Bulgarian and Serbian Banks. *19 International Multidisciplinary Scientific Geoconference SGEM 2019, Vol. 19, Issue. 2.1,* Sofia: STEF92 Technology Ltd., 2019, pp.3-10.
7. PETROV, P., DIMITROV, G. and 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*, Sofia: STEF92 Technology Ltd., 2019, pp.3-10.
8. SAINT-ANDRE, P. and HODGES, J. (2011) 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). *RFC6125.* [Online] Available from: https://tools.ietf.org/rfc/rfc6125.txt [Accessed 07/08/2019].
9. UN HUMAN DEVELOPMENT REPORT OFFICE (2019), Human Development Indices and Indicators. *2018 Statistical update.* [Online] Available from: http://hdr.undp.org/en/2018-update [Accessed 07/08/2019].
10. WIKIPEDIA (2019), Baltic states. *Wikipedia.org.* [Online] Available from: https://en.wikipedia.org/wiki/Baltic_states [Accessed 07/08/2019].
11. WORLD BANK DEVELOPMENT RESEARCH GROUP (2019), GINI index (World Bank estimate). *International Comparison Program database.* [Online] Available from: https://data.worldbank.org/indicator/NY.GNP.PCAP.PP.CD [Accessed 07/08/2019].