# Application of Security Technologies in the Public Websites of Banks in Serbia

Pavel Petrov
Shabnamjit Hundal

**Abstract**

*In this publication, the collected data in the course of a survey are summarized, systemized and analyzed. The survey is conducted in the autumn of 2018 and is focused on the usage of the HTTPS protocol in the public web sites of Serbian banks. The scope of the survey is limited only to the public site of the particular bank and 27 web sites were explored. All of them belong to Serbian banks, which are licensed by the National Bank of Serbia. The HTTPS protocol in the last years is used as the default protocol by many web applications. The study shows that from all 27 Serbian banks licensed by the Serbian National Bank, 81.5% (22 banks) of the surveyed bank's sites are using HTTPS without problems, 11.1% (3 banks) are using HTTPS with some problems and 7,4% (2 banks) are not using HTTPS at all. From banks that are using HTTPS without any problems, the majority - 72.7% (16 banks) use simple Domain Validation (DV), and the rest - 27.2% (6 banks) use Extended Validation (EV) types of certificates. The most popular certification authorities are Thawte with share of 27.2% (6 banks), Go Daddy Secure Certificate Authority and GeoTrust - each with share of 18.1% (4 banks), cPanel Inc. Certification Authority - 13.6% (3 banks), and etc. One bank uses free certificate from Let's Encrypt Authority X3. The validity period varies from 3 months (typically issued from cPanel and Let's Encrypt) to 3 years (typically issued from Go Daddy). Only 7.4% (2 banks) of all Serbian banks are using the latest HTTP/2 protocol.*

*Keywords: Serbia, banks, Serbian banks, HTTPS, web site, SSL, certificates.*

*JEL Code: G21, O14, O30.*

## Introduction

In this publication, we summarize, systemize and analyze data collected in the autumn of 2018 on the use of HTTPS in the public sites of banks in Serbia. The scope of the study is limited to the public site of the particular bank, which examined the sites of all 27 Serbian banks licensed by the Serbian National Bank at the time of the survey[1]. The survey excludes only the Bank of China Srbija Akcionarsko Drustvo Beograd - Novi Beograd's Web site at www.bankofchina.com/rs, as it is not a stand-alone site but only an information webpage located on the parent bank's website. Accordingly, in this case, it cannot be inferred from the practices used by Serbian administrators of banking websites.

As it is known, when using text protocols (such as HTTP/0.9/1.0/1.1) after listening to traffic, exchanged queries and responses can easily be read, even without the use of complex technical means. In many cases the exchange of confidential information (passwords, bankcard number for payment, personal information, etc.). And for these purposes is intended protocol HTTPS (also known as "HTTP Secure", "Secure HTTP", "HTTP over SSL"[2], "HTTP over TLS"[3], etc.). The use of a secure connection increases the load on the client and the server in terms of busy CPU time and the amount of RAM usage, but in recent years, this is not considered as a serious argument given the great benefits of connection security[4]. The trend over recent years has increasingly been to use the HTTPS protocol as the default protocol for setting hyperlinks in

[1] National Bank of Serbia (NBS), List of Banks, 04.09.2018, <https://www.nbs.rs/internet/english/50/50_2.html>
[2] Hickman, K., The SSL Protocol, 1995, <https://tools.ietf.org/id/draft-hickman-netscape-ssl-00.txt>
[3] Rescorla, E. HTTP Over TLS, IETF RFC 2818, 2000, <https://tools.ietf.org/rfc/rfc2818.txt>
[4] Kuyumdzhiev, I. Controls Mitigating the Risk of Confidential Information Disclosure by Facebook: Essential Concern in Auditing Information Security. TEM Journal, 3, 2014, 2, pp.113-119.
Kuyumdzhiev, I. Backup and recovery of MongoDB database: features, state, problems. // IZVESTIA, JOURNAL OF THE UNION OF SCIENTISTS - VARNA, ECONOMIC SCIENCES SERIES, 2015, pp.125-133.

webpages and to be used by default by web applications[5].

**1. Object of the empirical study**

The survey was conducted in the autumn of 2018. The list of banks licensed in the Republic of Serbia is taken from the site of the Serbian National Bank as well as the list of addresses of the banking websites. The summarized results of the surveyed sites are presented in Table 1.

Table 1. Use HTTPS protocol in public sites of banks in Serbia.

| № | Bank Name | URL Address | HTTPS |
|---|---|---|---|
| **1** | ADDIKO BANK AD BEOGRAD | www.addiko.rs | да |
| **2** | AGROINDUSTRIJSKO KOMERCIJALNA BANKA AIK BANKA AKCIONARSKO DRUSTVO, BEOGRAD | www.aikbanka.rs | yes |
| **3** | BANCA INTESA AKCIONARSKO DRUSTVO BEOGRAD (NOVI BEOGRAD) | www.bancaintesa.rs | **with problems** |
| **4** | BANKA POSTANSKA STEDIONICA AKCIONARSKO DRUSTVO, BEOGRAD (PALILULA) | www.posted.co.rs | yes |
| **5** | CREDIT AGRICOLE BANKA SRBIJA AKCIONARSKO DRUSTVO NOVI SAD | www.creditagricole.rs | yes |
| **6** | DIREKTNA BANKA AKCIONARSKO DRUSTVO KRAGUJEVAC | www.direktnabanka.rs | yes |
| **7** | ERSTE BANK AKCIONARSKO DRUSTVO, NOVI SAD | www.erstebank.rs | yes |
| **8** | EUROBANK AKCIONARSKO DRUSTVO BEOGRAD | www.eurobank.rs | yes |
| **9** | EXPOBANK AKCIONARSKO DRUSTVO BEOGRAD | www.expobank.rs | **with problems** |
| **10** | HALKBANK AKCIONARSKO DRUSTVO BEOGRAD | www.halkbank.rs | **no** |
| **11** | JUBMES BANKA AD BEOGRAD (NOVI BEOGRAD) | www.jubmes.rs | **no** |
| **12** | KOMERCIJALNA BANKA AD, BEOGRAD (VRACAR) | www.kombank.com | yes |
| **13** | MIRABANK AKCIONARSKO DRUSTVO BEOGRAD-NOVI BEOGRAD | www.mirabankserbia.com | yes |

[5] This trend is getting stronger since Google's search services, Gmail, and more have passed entirely to HTTPS in 2010, and by Google in 2015 Google announces that HTTPS-served websites will be given priority in indexing, compared to those using HTTP only. For more information see:
Radev, M. Proposals for changes in the rule 3-2-1 used in corporate backup strategies in the IT infrastructure. // IZVESTIA, JOURNAL OF THE UNION OF SCIENTISTS - VARNA, ECONOMIC SCIENCES SERIES, 2015, pp.134-139.
Stoev, S. Product Risk Management in Information Systems Implementation. // IZVESTIA, JOURNAL OF THE UNION OF SCIENTISTS - VARNA, ECONOMIC SCIENCES SERIES, 2016, vol.2, pp.109-116. Radev, M. Using the TOPSIS Method to Evaluate Projects for Virtualization. // IZVESTIA, JOURNAL OF THE UNION OF SCIENTISTS - VARNA, ECONOMIC SCIENCES SERIES, 2017, vol.2, pp.234-241.
Stoev, S. Integration of Risk Management Processes into the Business of IT Companies. // IZVESTIA, JOURNAL OF THE UNION OF SCIENTISTS - VARNA, ECONOMIC SCIENCES SERIES, 2017, vol.2, pp.225-233.

| № | Bank Name | URL Address | HTTPS |
|---|---|---|---|
| **14** | MTS BANKA AKCIONARSKO DRUSTVO BEOGRAD | www.mts-banka.rs | yes |
| **15** | NLB BANKA AD, BEOGRAD | www.nlb.rs | yes |
| **16** | OPPORTUNITY BANKA AD, NOVI SAD | www.obs.rs | yes |
| **17** | OTP BANKA SRBIJA AKCIONARSKO DRUSTVO, NOVI SAD | www.otpbanka.rs | yes |
| **18** | PIRAEUS BANK AKCIONARSKO DRUSTVO BEOGRAD (NOVI BEOGRAD) | www.piraeusbank.rs | yes |
| **19** | PROCREDIT BANK AD, BEOGRAD (NOVI BEOGRAD) | www.procreditbank.rs | yes |
| **20** | RAIFFEISEN BANKA AD BEOGRAD | www.raiffeisenbank.rs | yes |
| **21** | SBERBANK SRBIJA A.D. BEOGRAD | www.sberbank.rs | yes |
| **22** | SOCIETE GENERALE BANKA SRBIJA AD, BEOGRAD | www.societegenerale.rs | yes |
| **23** | SRPSKA BANKA AD BEOGRAD (SAVSKI VENAC) | www.srpskabanka.rs | yes |
| **24** | TELENOR BANKA AD BEOGRAD (NOVI BEOGRAD) | www.telenorbanka.rs | **with problems** |
| **25** | UNICREDIT BANK SRBIJA A.D., BEOGRAD (STARI GRAD) | www.unicreditbank.rs | yes |
| **26** | VOJVODANSKA BANKA AKCIONARSKO DRUSTVO NOVI SAD | www.voban.rs | yes |
| **27** | VTB BANKA AKCIONARSKO DRUSTVO BEOGRAD | www.vtbbanka.rs | yes |

Examined bank's web sites can be divided into three main categories: HTTPS-free web sites, HTTPS-using websites and non-HTTPS-based websites (see Figure 1). The more typical of each of these categories is summarized and analyzed below.

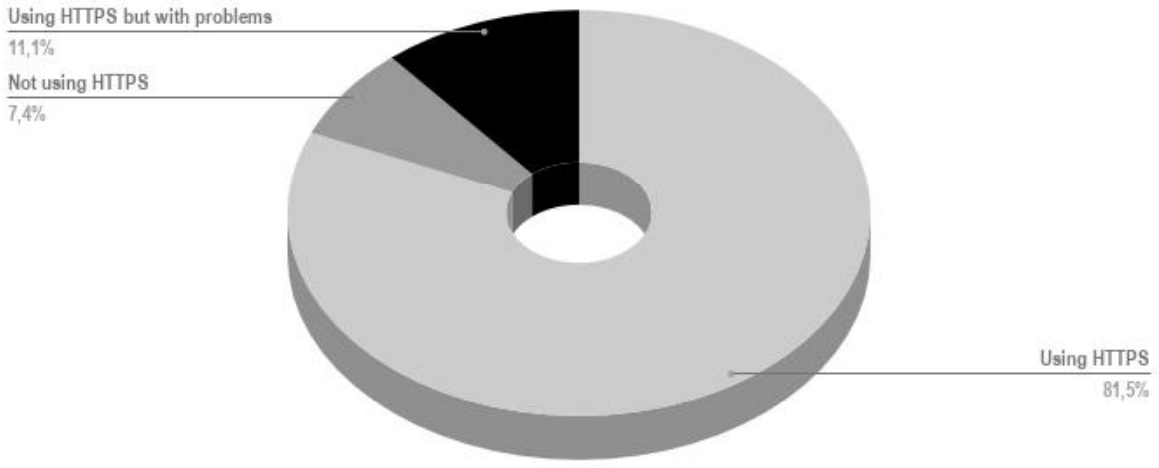


Figure 1. Relative share of Serbian bank web sites using HTTPS, not using HTTPS, and using HTTPS but with problems.

**2. Websites using HTTPS without problems**

Around 81.5% of the surveyed sites fall into this category of sites. The HTTPS protocol prevents from intercepting the traffic exchanged between the web server serving the Web site and its users. Web sites that use HTTPS without problems 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. These certification bodies sign the X.509 certificate with the digital signature methods[6], which connects the public key together with other metadata related to the owner of that key. In the case of websites, the most important is the DNS name of the site. The public key holder must be able to administer the web server serving that name accordingly. Web browsers maintain a list of trusted certification bodies and can check if a certificate is issued by such an organization.

For example, at the beginning of the communication, the web client who wants to connect to the respective banks' web server cannot be "sure" that he is connecting to the right one. In the course of encryption of the communication link, the bank web server sends the public key that will be used to encrypt the connection and the certificate. The browser checks the certificate if it is not expired and the DNS name matches the entry on the certificate. Normally, the certification body does not sign the certificates directly, and this is done by other intermediary organizations that carry out this activity. This results in a chain of certificates that ultimately associate intermediate bodies with a certification authority and the website certificate.

As is known, three types of certificates are used: Domain Validation (DV), Organization Validation (OV), and Extended Validation (EV). 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[7].

Table 2 shows the main features related to the use of the HTTPS protocol by the Serbian banks.

Table 2. Main features in usage of the HTTPS protocol.

| Bank № | Automatic redirection to HTTPS | HTTP/2 support | Certificate type | Certification body | Validity period |
|---|---|---|---|---|---|
| **1** | yes | no | **EV** | Thawte EV RSA CA 2018 | 11 m. |
| **2** | yes | **yes** | DV | Go Daddy Secure Certificate Authority - G2 | 1 y. |
| **4** | **no** | no | DV | Thawte RSA CA 2018 | 1 y., 2 m. |
| **5** | yes | no | **EV** | GeoTrust EV RSA CA 2018 | 1 y. |
| **6** | yes | no | DV | cPanel, Inc. Certification Authority | 3 m. |

[6] Cooper, D., Santesson, S., Farrell, S. et al. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, IETF RFC5280, 2008, <http://www.ietf.org/rfc/rfc5280.txt>

[7] Qualys SSL Labs, SSL and TLS Deployment Best Practices, <https://github.com/ssllabs/research/wiki/SSL-and-TLS-Deployment-Best-Practices>

| Bank № | Automatic redirection to HTTPS | HTTP/2 support | Certificate type | Certification body | Validity period |
|---|---|---|---|---|---|
| **7** | yes | no | DV | DigiCert Global CA G2 | 1 y. |
| **8** | yes | no | DV | Go Daddy Secure Certificate Authority - G2 | 3 y. |
| **12** | **no** | no | DV | Go Daddy Secure Certificate Authority - G2 | 3 y. |
| **13** | yes | no | DV | Thawte RSA CA 2018 | 1 y., 1 m. |
| **14** | yes | no | DV | GlobalSign Organization Validation CA - SHA256 - G2 | 2 y. |
| **15** | yes | **yes** | DV | Go Daddy Secure Certificate Authority - G2 | 2 y. |
| **16** | **no** | no | DV | **Let's Encrypt Authority X3** | 3 m. |
| **17** | yes | no | **EV** | GeoTrust EV RSA CA 2018 | 1 y. |
| **18** | yes | no | DV | GlobalSign CloudSSL CA - SHA256 - G3 | 11 m. |
| **19** | yes | no | DV | Thawte RSA CA 2018 | 1 y., 2 m. |
| **20** | yes | no | **EV** | Thawte EV RSA CA 2018 | 2 y. |
| **21** | yes | no | **EV** | GeoTrust EV RSA CA 2018 | 1 y., 2 m. |
| **22** | yes | no | DV | Thawte RSA CA 2018 | 2 y. |
| **23** | **no** | no | DV | cPanel, Inc. Certification Authority | 3 m. |
| **25** | yes | no | DV | Actalis Organization Validated Server CA G1 | 1 y. |
| **26** | yes | no | **EV** | GeoTrust EV RSA CA 2018 | 1 y. |
| **27** | **no** | no | DV | cPanel, Inc. Certification Authority | 3 m. |

From the data presented, it is clear that the majority (16 banks) use DV, and the rest (6 banks) use EV. There is a wide variety of preferences for a certification authority, but the most popular are: Thawte - 6 banks, Go Daddy Secure Certificate Authority and GeoTrust - 4 banks, cPanel, Inc. Certification Authority - 3 banks, etc. Interestingly, 1 bank uses free certificates from Let's Encrypt Authority X3. Only 2 banks use the latest HTTP/2 protocol, which shows that the penetration process of HTTPS/2 will be extended in the time.

In five cases of the banks' sites, the good practices are not followed and they do not redirect from unsecure to secure connection.

As we have said, the server and eventually the client use digital certificates to "prove" their identity. The respondent shall verify that the certificate was issued by a trusted certifying authority. Typically, browsers are distributed with an initial built-in list of similar bodies, which is then automatically updated. Additionally, the user can manually add entries to this list, indicating that he also trusted other certifying authorities.

Examination of the validity of a certificate by a browser, in addition to checking whether it is issued by a trusted authority, also includes: whether the certificate is used between the date of

activation and the expiry date of the certificate; whether the domain name specified on the certificate matches the domain to which the link is made; whether the certificate has been canceled; whether the certificate has been added to a blacklist, and etc. checks.

**3. Websites using HTTPS with problems**

This category of sites is 11.1% of the surveyed sites, namely from Table 1, those with numbers 3, 9, and 24. In our opinion, this is not a relatively high percentage, but indicates underestimation of security issues for web sites.

Table 3. Problems when using the HTTPS protocol and their description.

| Banks № | Problem description when using HTTPS |
|---|---|
| **3** | When trying to connect to HTTPS, the connection takes place and then downgrade - the browser is automatically redirected to using HTTP |
| **9** | Using a 10-year self-signed certificate for a completely different domain - marfin.gridsrv.net |
| **24** | Use of a self-signed certificate with a validity period of 5 years |

HTTPS protocol usage issues vary widely, as those on the 3-digit site may remain unnoticed by most users. However, this practice of transferring from a secure to an uncertain relationship is extremely strange. For the sites of banks number 9 and 24, we can give the recommendation either to support HTTPS according to good practices or better not to use HTTPS at all. Using self-signed certificates, incorrectly configuring the HTTPS web support server, may weaken the confidence of the financial institution's ability to keep its systems up to date.

**4. Web sites not using HTTPS at all**

About 7,4% of the sites surveyed, namely in the Table 1, those with numbers 10 and 11. This is not a high share and is not worrying factor, but given that the prices for a DV certificate start at around 30€ for a year, the only meaningful reason not to support HTTPS is to ensure compatibility with old devices. Of course, other reasons are also possible - i.e. to override some disadvantages of the HTTPS protocol. The main shortcomings of the HTTPS protocol are:

• The pages accessed through it are never cached in an intermediate cache because the connection between the web browser and the web server is encrypted and the content cannot be recognized and cached accordingly.

• Some browsers do not cache local HTTPS content.

• Because it is not recommended to mix encrypted and unencrypted content on a single page, a number of resources - pictures, icons and other accessory files are also encrypted and thus eliminates the possibility of reducing the traffic by using cache.

• Encryption and decryption require additional computing operations on both the server and the client. While this is usually not a problem for the client, it can be a problem for highly loaded web servers serving multiple HTTPS queries simultaneously.

• It is possible that an incorrectly configured firewall or proxy system does not allow access to HTTPS sites. In these cases, most traffic is usually controlled - recorded or checked for viruses.

• The use of certificates increases costs - the cost per year for a single domain certificate varies widely and can range from 30-40€ to 300-400€ or more depending on the type of certificate.

In 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. Such initiatives have a major impact on the massive switch to HTTPS worldwide, including Serbian banks that are not yet using this protocol.

**Conclusion**

The purpose of this study has been to explore the security technologies used in the public sites of banks in Serbia. The collected data are related to particular period - September-October 2018. 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 result reveals some good practices used in Serbian banks. The research conducted on the use of the HTTPS protocol on the banks' public sites in Serbia covered the sites of 27 Serbian banks licensed to operate on the country territory by the Serbian National Bank.

From all 27 Serbian banks licensed by the Serbian National Bank, 81.5% (22 banks) of the surveyed bank's sites are using HTTPS without problems, 11.1% (3 banks) are using HTTPS with some problems and 7,4% (2 banks) are not using HTTPS at all.

From banks that are using HTTPS without any problems, the majority - 72.7% (16 banks) use simple Domain Validation (DV), and the rest - 27.2% (6 banks) use Extended Validation (EV) types of certificates. The most popular certification authorities are: Thawte with share of 27.2% (6 banks), Go Daddy Secure Certificate Authority and GeoTrust - 18.1% (4+4 banks), cPanel, Inc. Certification Authority - 13.6% (3 banks), etc. Interestingly, 1 bank uses free certificates from Let's Encrypt Authority X3. The validity period varies from 3 months (i.e. cPanel and Let's Encrypt) to 3 years (i.e. Go Daddy). Only 7.4% (2 banks) of all Serbian banks are using the latest HTTP/2 protocol that shows that the penetration process of HTTPS/2 will be extended in the time.

The quality of banking and strategic management has strong relation[8] and in this day's web technologies plays more and more important role in bank's operations.

**References**

1. Cooper, D., Santesson, S., Farrell, S. et al. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, IETF RFC5280, 2008, <http://www.ietf.org/rfc/rfc5280.txt>
2. Hickman, K., The SSL Protocol, 1995, <https://tools.ietf.org/id/draft-hickman-netscape-ssl-00.txt>
3. Kuyumdzhiev, I. Backup and recovery of MongoDB database: features, state, problems. // IZVESTIA, JOURNAL OF THE UNION OF SCIENTISTS - VARNA, ECONOMIC SCIENCES SERIES, 2015, pp.125-133.
4. Kuyumdzhiev, I. Controls Mitigating the Risk of Confidential Information Disclosure by Facebook: Essential Concern in Auditing Information Security. TEM Journal, 3, 2014, 2, 113-119.
5. National Bank of Serbia (NBS), List of Banks, 04.09.2018, <https://www.nbs.rs/internet/english/50/50_2.html>

[8] Zafirova, T., Stavreva, G. Quality of banking and strategic management after entrance foreign capital in bank organizations. The case SG Expressbank. Strategijski menadžment, 2002, 1, 12-17.

6. Qualys SSL Labs, SSL and TLS Deployment Best Practices, <https://github.com/ssllabs/research/wiki/SSL-and-TLS-Deployment-Best-Practices>
7. Radev, M. Proposals for changes in the rule 3-2-1 used in corporate backup strategies in the IT infrastructure. // IZVESTIA, JOURNAL OF THE UNION OF SCIENTISTS - VARNA, ECONOMIC SCIENCES SERIES, 2015, pp.134-139.
8. Radev, M. Using the TOPSIS Method to Evaluate Projects for Virtualization. // IZVESTIA, JOURNAL OF THE UNION OF SCIENTISTS - VARNA, ECONOMIC SCIENCES SERIES, 2017, vol.2, pp.234-241.
9. Rescorla, E. HTTP Over TLS, IETF RFC 2818, 2000, <https://tools.ietf.org/rfc/rfc2818.txt>
10. Stoev, S. Integration of Risk Management Processes into the Business of IT Companies. // IZVESTIA, JOURNAL OF THE UNION OF SCIENTISTS - VARNA, ECONOMIC SCIENCES SERIES, 2017, vol.2, pp.225-233.
11. Stoev, S. Product Risk Management in Information Systems Implementation. // IZVESTIA, JOURNAL OF THE UNION OF SCIENTISTS - VARNA, ECONOMIC SCIENCES SERIES, 2016, vol.2, pp.109-116.
12. Zafirova, T., Stavreva, G. Quality of banking and strategic management after entrance foreign capital in bank organizations. The case SG Expressbank. Strategijski menadžment, 2002, 1, 12-17.

**Contacts**
Assoc. Prof. Pavel Petrov, PhD
University of Economics - Varna
petrov@ue-varna.bg

Senior Lecturer Shabnamjit Hundal
JAMK University of Applied Sciences, Jyväskylä, Finland
Shabnamjit.Hundal@jamk.fi