ANALYSIS OF SSL CERTIFICATES TRENDS AND EXTENDED VALIDATION SSL USAGE FOR E-COMMERCE WEBSITES AND INTERNET of THINGS

Valentin-Andrei MĂNESCU[1], Ramona-Alexandra NEGHINĂ[2], Andreea BARBU[3], Mihaela-Rodica GANCIU[4], Gheorghe MILITARU[5]

With the tremendous evolution of the Internet spheres such as electronic commerce and the Internet of Things (IoT), online security has become a major concern in the digital business world. The purpose of the paper is to contribute to the better understanding of Secure Socket Layer (SSL) certificate aspects such as, currently available SSL certificate types, the advantages of using an SSL certificate and best practices. The study conducted analyzes the interest granted on security solutions in digital business environment between November 2015 and October 2020. As well, the proposed study analyzes the current state of Extended Validation SSL implementation in top 50 countries or territories worldwide, selected by the criteria of most viewed 1 million websites. Finally, the research offers the perspectives of web&IoT experts regarding SSL certificates and best practices, based on a qualitative research made in April 2021.

Keywords: SSL certificates, digital business security, websites and IoT SSL

1. Introduction

Nowadays, security plays a pivotal role in digital businesses environment around the world, especially with the tremendous growth of e-commerce and IoT applications, that have brought the need to securely protect sensitive information [1]. Thus, SSL certificates are vital for encrypting data transmitted between a client and a server, especially when dealing with sensitive data such as usernames, passwords or credit card information [2]. While security threats can be a challenge for any company, no matter the size, SSL certificates can help a digital business to maintain trust among its customers [3]. Although more and more websites and IoT devices are adopting SSL technologies, it is necessary to better understand the

[1] PhD student, WEBECOM S.R.L., Bucharest, Romania, e-mail: mail@valentinmanescu.ro

[2] PhD student, WEBECOM S.R.L., Bucharest, Romania, e-mail: ramona@webecom.ro

[3] Assist. Prof., Faculty of Entrepreneurship, Business Engineering and Management, University POLITEHNICA of Bucharest, Romania, e-mail: barbu.andreea92@gmail.com

[4] PhD student, ENERGOMONTAJ S.A. of Bucharest, Romania, e-mail: mihaella.ganciu@gmail.com

[5] Prof., Faculty of Entrepreneurship, Business Engineering and Management, University POLITEHNICA of Bucharest, Romania, e-mail: gheorghe.militaru@upb.ro

current state of SSL adoption. Thus, the proposed research provides a quantitative and qualitative perspective on the use of SSL certificates, with the aid of a web and IoT technology experts group. The purpose of the paper focuses on analyzing the current state of SSL adoption and offering an in-depth view of SSL certificates from web&IoT experts experience. As well, the research aims to identify best practices for SSL certificates and how industry expert's view these best practices.

2. Working principles of secure socket layer certificates

SSL is an encryption system for transmitting data between websites, mobile apps, smart devices, emails, IoT applications and servers [4]. SSL certificates transmit encrypted data between the client and the server [5], ensuring the transmission of data thought a secure connection, in order to preserve the data integrity and confidentiality. Also, SSL certificates avoid data interception, as they the data encrypted has no value if it cannot be decoded [6].

Largely used for securing websites and e-commerce platform, SSL is also used to increase the security of IoT devices. IoT devices can be given an SSL certificate, which allows users to seamlessly and securely connect (via their smartphone or other devices) just as they would a secure website by using an SSL certificate, avoiding SSL/TLS-related warnings and errors. Conversely, an IoT device can request an SSL certificate from a user's device in order to perform particular tasks [7].

SSL represents the core of securely using the web with Hypertext Transfer Protocol Secure (HTTPS), an extension of its predecessor Hypertext Transfer Protocol (HTTP). This standard is used to guarantee security of Internet communications such as e-commerce websites, IoT applications, web basted email services or Internet Banking. The HTTPS security protocol provides authentication, integrity and confidentiality for data transmitted over the Internet and prevents unauthorized viewing of the data exchanged [8].

SSL certificates validate the identity of websites, IoT applications, computer systems and data, by connecting pairs of security keys (public and private) on Public Key Infrastructure (PKI) or public key cryptography [9]. The process of validating and an SSL certificate involves a Public Key and a Private Key, keys used to confirm the identity of a website or device. The SSL protocol works as follows: (1) the browser requests a secure connection (https://), (2) the server sends the public key of the certificate, (3) the client verifies if the SSL certificate was issues by a Certificate Authority (CA), has a validity date and if the certificate is related to the owner, (4) the client uses the public key to encrypt the data and sends it to the server, (5) the server decrypts the data using its private key, (6) the server sends back the requested data, (7) the client decrypts the data and displays the information to the user [10].

3. Types of secure socket layer certificates

Due to a growing demand for SSL certificates, CA have diversified certificate validation levels. Some organizations use SSL certificate just for encryption, while other organizations want to reassure their customers that they are a trusted company. According to each organization's needs, have resulted in different certificate validation types.

Also, SSL certificates can be classified depending on how many domain names and/or subdomains are being validated by the same SSL certificate as follows: single domain (validates one domain name), wildcard (validated a base domain and its subdomains) and multi domain certificates (validates up to 100 domains and subdomains). Depending on the CA's validation levels, SSL certificates are classified in the paragraphs below. The features of each SSL types are listed in Table 1.

Table 1

Features of SSL types according to CA validation levels [11]

	Domain Validation SSL	Organization Validation SSL	Extended Validation SSL
Activates green HTTPS in browser address bar	✓	✓	✓
Dynamic site seal	x	✓	✓
Verified company name displayed in certificate details and a dynamic site seal	x	✓	✓
Basic business vetting	x	✓	✓
Advanced business vetting	x	x	✓
Displays verified company's name next to URL	x	x	✓

Domain Validation SSL Certificates (DV SSL) - For DV SSL Certificates, the CA verifies only the domain ownership but does not guarantee the organization's identity. This SSL certificate type validates only one domain name [12]. This type of SSL certificates offers a minimal encryption and is used mainly for blogs or informational websites.

Organization Validation SSL Certificates (OV SSL) - This type of SSL certificate implies a more rigorous verification by the CA. The CA will contact the company that applies for an OV SSL and make extended verifications of the company in order to issue an OV SSL. An OV SSL displays the company's name and address in the certificate details, making the SSL certificate more trustworthy [13].

Extended Validation SSL Certificates (EV SSL) - involve a complete vetting of a company by the CA [11], in order to assure the legal, physical and operational existence of the company and if the identity of the company matches official records [14]. Due to the CA's extended validation process for EV SSL's, this type of SSL is more trustworthy than DV and OV certificates. Websites such as financial institutions, large companies and e-commerce websites will usually opt for an EV SSL, due to the fact that these types of websites process customer sensitive data such as login credentials, credit card details or personal information.

4. Best practices for SSL

The study continued with a state-of-the-art literature overview of the best practices for SSL certificates, that will be followed by a qualitative analysis addressed to web&IoT experts.

A. ***Use Current SSL/TLS Protocols*** – Old protocol versions are vulnerable, thus, in order to be secure and always up to date with the latest security protocols, a website should implement the newest protocol versions of SSL/TLS [15]. Currently TLS 1.2 is the most used version of the SSL/TLS protocol. The latest version is TLS 1.3 and it is already supported by most major web browsers [16].

B. ***HSTS (HTTP Strict Transport Security)*** is a policy mechanism that protects websites from man-in-the-middle attacks and allows web servers to declare that web browsers should automatically use only HTTPS connections, even if a user enters a HTTP URL in the browser address bar [17]. It also tells search engines (such as Google, Yahoo, Bing) to server only search results that use HTTPS, minimizing the risk of unsecured content [15].

C. ***Make sure the certificate is registered on the correct domain name and all hostnames are covered –*** One of the most common mistakes is purchasing an SSL certificate with an incorrect name, thus the domain name should be always doubled checked. Furthermore, always verify an SSL certificate is valid for all host names of a website [16], in order to avoid invalid certificate warnings, that will confuse visitors and weaken their confidence into the website [18]. For example, if an SSL certificate only covers www.domainname.com, visitors that access a website using just domainname.com (without the "www." prefix) will be blocked by a certificate name mismatch error [15].

D. Check SSL expiration date - The website owner or webmaster should make sure that the SSL certificate is always up to date, in order to avoid security risks. SSL certificates should be renewed in a timely manner. It is recommended to renew a certificate at least 15 days before the expiration date, in order to have time for testing and fixing any issues [18].

***E. Use relative URLs* –** another best practice is to use relative URLs for URLs that reside on the same secure domain (for example: /urlname.htm instead of www.domainname.com/urlname.htm) [19].

F. ***Use 301 redirects from HTTP to HTTPS -*** When migrating a website from HTTP to HTTPS, server side 301 redirects should be used in order to avoid lower visitors' numbers. The 301 redirect will redirect users and search engines to the HTTPS page or resource [15].

G. ***Check SSL installation or issues with security tools*** – After implementing an SSL certificate or make any configuration changes, always make sure that is configurated correctly and the system is secured. A variety of online tools and applications are available for checking an SSL certificate, tools such as SSL Shopper's, SSL Checker. Another method for checking an SSL certificate issues (such as mixed content of HTTP and HTTPS URLs) is the built-in developer tools that comes by default with most used web browsers (Google Chrome, Mozilla Firebox, Safari, Opera, Microsoft Edge) [16].

H. ***Use SSL for better Search Engine Optimization (SEO) -*** In august 2014, Google officially announced that they use HTTPS as a ranking signal for indexing websites, in order to encourage all website owners and webmasters to switch from HTTP to HTTPS to keep everyone safe on the web. Thus, using an SSL certificate is one of the best practices for SEO [19].

I. ***Update Google Search Console sitemap*** – After implementing an SSL certificate, the website owner or webmaster should set the new HTTPS sitemap to Google Search Console. Google Search Console is a tool that accelerates the process of web indexing treats HTTP and HTTPS separately [15].

J. ***Generate and protect new private keys for each SSL compromised or renewed*** – Private keys are important SSL assets and should be generated on a trusted server with restricted access for as few employees as possible [18]. When renewing an SSL, never reuse a CSR because it will automatically reuse the private key, increasing the risk of a compromised SSL [20]. If a private key is compromised, revoke the SSL certificate and generate a new key pair [16].

K. ***Obtain a reliable CA generated SSL -*** furthermore, Google's best practices for enabling HTTPS, strongly advice to obtain an SSL issued by a reliable CA that uses domain verification steps, in order to assure that that the web domain actually belongs to the organization, thus protecting customers from man-in-the-middle attacks [15]. A reliable CA should offer great customer service and technical support [16].

5. Analysis of secure layer socket certificates usage and trends

In order to analyze the perceived importance of SSL certificates, statistical data available on Google Trends during November 2015 – October 2020 was used. Google Trends offers access to samples of actual searches make in Google, in order to display interest in a particular topic from around the world or specific geographical areas. The data obtained from Google Trends reflects search queries people make on Google every day, the data obtained is anonymized, categorized and aggregated. Some data retrieved from Google searches is filtered by Google Trends as follows: search terms with a low frequency is eliminated, duplicate searches made by the same person over a short period of time is eliminated, queries that uses apostrophes or other special characters are as well eliminated [21].

In the initial iteration, the interest of Google users in "Business Security" was compared to the term SSL, in order to understand if users are more interested in general aspects of business security or the specific term of SSL is more frequently searched. The analysis was made exclusively on the Google data category "Business & Industrial". Fig. 1 shows the evolution of Google searches on business security, compared to the interest in SSL certificates. By analyzing the diagram, it can be observed how the interest in “Business Security” decreases as the number of searches on SSL increases in some timeframes. The decrease of search volumes on business security can represent that user’s attention shifts form business security to digital solutions (SSL certificates).

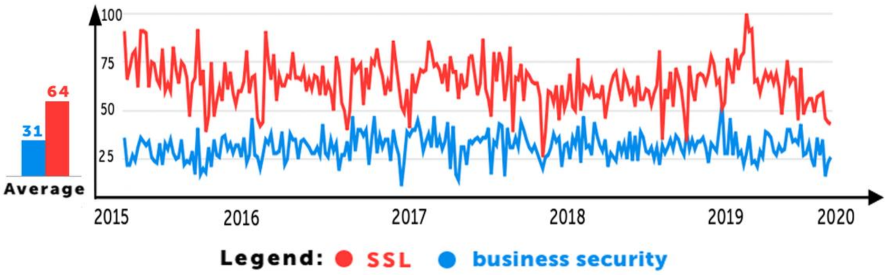

Fig. 1. Interest in keyword searches during November 2015- October 2020 for SSL and business security in Google Trends

By using the same tool, the research continued to analyze business security, SSL and the security activities of a website or an IoT system, in order to better understand if the general public interest targets general terms such as business security, secure website, secure IoT or SSL as a specific search term.

As it can be observed in Fig. 2, the interest in SSL technology is significantly higher than the term of business security, which demonstrates that it is very popular and impactful in the search volumes of “Business & Industrial” Google category selected for the research. At the other end of the spectrum, the interest in securing a website or an IoT system, is of relatively low interest, probably because it is destined for specialists who use these technologies.

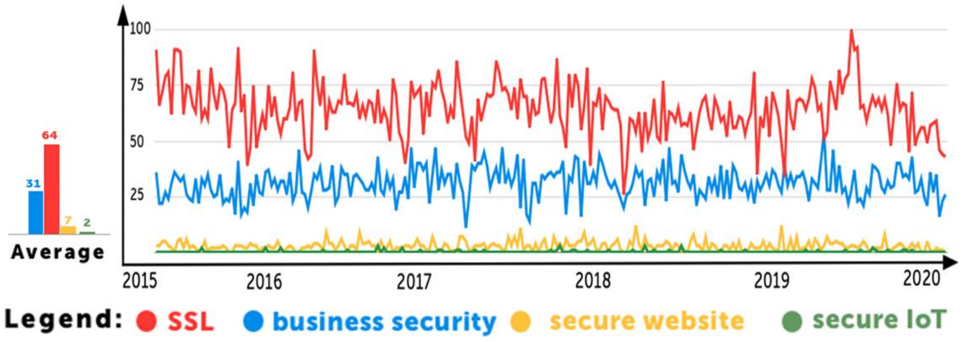

Fig. 2. Interest in keyword searches during November 2015 – October 2020 for SSL, business security, secure website and secure IoT in Google Trends

Fig. 3. indicates the comparative interest between data protection and the other factors. In May- June 2018 a significant increase can be observed due to enforcement of the General Data Protection (GDPR) on 25th of May 2018, which means that there was a great interest in protecting personal data. GDPR is a regulation in the European Union law on data protection and privacy in the European Union and the European Economic Area.

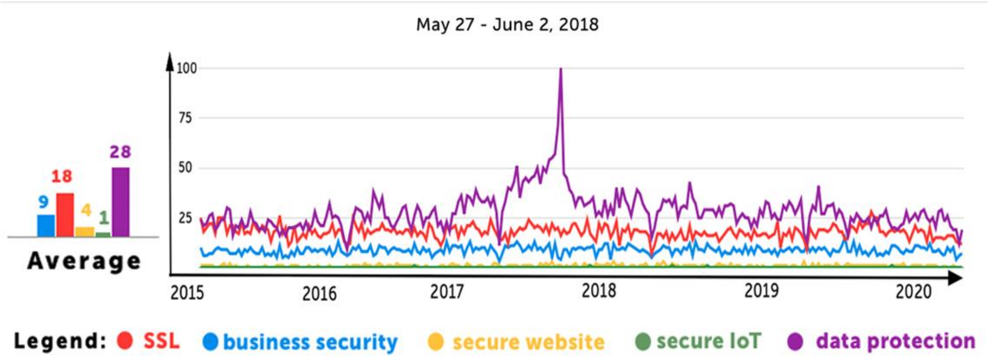

Fig. 3. Interest in keyword searches during November 2015 – October 2020 for SSL, business security, secure website, secure IoT and data protection in Google Trends

The research conducted continued by refining the SSL certificates used for both personal and business purposes. Thus, the authors considered it necessary to make an analysis of EV SSL certificates implemented worldwide. Thus, the most visited 1 million websites worldwide were analyzed and the top 50 countries or territories as number of EV SSL certificates implemented were selected. Subsequently, the authors have identified for each country or territory selected, how many EV SSL certificates exist, in order to observe the companies that manifest an increased interest in securing their digital assets. Table 2 shows the number EV SSL certificate, sorted in descending order. For the analysis, the data considered includes the most viewed 1 million websites [22].

Table 2

Extended validation certificates usage rate in 2020

No.	Country	SSL	EV SSL	Ratio	No.	Country	SSL	EV SSL	Ratio
1	United States	47439405	130438	0,27%	26	Vietnam	428749	736	0,17%
2	Netherlands	1401629	9817	0,70%	27	Poland	769105	708	0,09%
3	Germany	4357176	8044	0,18%	28	Chile	148600	659	0,44%
4	Canada	1416920	6011	0,42%	29	Mexico	286276	630	0,22%
5	Australia	1139324	5399	0,47%	30	Greece	303624	628	0,21%
6	Colombia	521608	4479	0,86%	31	Norway	16949	617	3,64%
7	France	1510491	3694	0,24%	32	British Indian Ocean Territory	416419	579	0,14%
8	Switzerland	411593	3266	0,79%	33	Malaysia	105406	529	0,50%
9	Japan	1758052	3245	0,18%	34	UAE	7467	524	7,02%
10	Italy	971318	2557	0,26%	35	Portugal	116429	451	0,39%
11	Belgium	278459	2045	0,73%	36	Turkey	306417	449	0,15%
12	Spain	845185	1994	0,24%	37	Philippines	74495	424	0,57%
13	South Africa	468825	1983	0,42%	38	Romania	191536	401	0,21%
14	Sweden	345678	1968	0,57%	39	Peru	74611	394	0,53%
15	India	1128725	1942	0,17%	40	Hong Kong	218875	359	0,16%
16	China	1074851	1824	0,17%	41	Argentina	188605	345	0,18%
17	Finland	160989	1713	1,06%	42	Indonesia	301644	344	0,11%
18	Denmark	214116	1188	0,55%	43	Slovakia	121815	341	0,28%
19	Brazil	1140436	1106	0,10%	44	Hungary	222856	336	0,15%
20	Russia	3656466	1097	0,03%	45	Ireland	112771	331	0,29%
21	South Korea	37058	1096	2,96%	46	Tuvalu	16512	264	1,60%
22	Singapore	127834	1007	0,79%	47	Taiwan	303439	257	0,08%
23	United Kingdom	3881160	905	0,02%	48	Ukraine	340597	241	0,07%
24	Austria	333173	854	0,26%	49	Thailand	124978	209	0,17%
25	New Zealand	155700	744	0,48%	50	Nigeria	90104	207	0,23%
Average rate		**0,61%**							

6. Method

In order to gain better insight of how web&IoT experts perceive SSL certificates, the study continued by conducting a qualitative primary research. The method used for conducting the research was the structured interview method. The interviews were conducted online, via Zoom or Skype with an average duration of 45 minutes for each interview.

The targeted interviewees were 8 web&IoT experts from 4 Romanian companies that offer eCommerce and IoT solutions (eCommerce platform development, IoT development, web design, online marketing, web hosting and consultancy services). The respondents job titles are divided into 2 categories: online marketing specialists (4 respondents) and web&IoT developers (4 respondents), 1 online marketing specialist and 1 web&IoT developer from each of the 4 companies. Each respondent has a considerable experience, between 3 to 16 years of experience. Due to privacy reasons, the companies’ names and respondents’ names were anonymized.

The interview had 3 sections and 23 questions. The first 4 questions were addressed for profiling each expert. The second section of the interview had 8 open questions regarding SSL certificates which followed topics such as: views on SSL certificate types, benefits of EV SSL certificates, increasing trust and notoriety of a brand or company by using SSL, issues encountered with SSL certificates, the contribution of SSL certificates to SEO and legal norms such as GDPR and the European Union (EU) directive on security of networks and information systems for cybercrime (NIS). The last part of the interview referred to SSL best practices previously identifies in the research. For measuring the respondent's perceptions, the 7 points Likert Scale was used.

7. Results

As for the results, 8 respondents chose EV SSL over DV or self-signed SSL because they consider that EV SSL are more trustworthy especially for end users. Some arguments referred to the guarantees of the company vetting process as an extra caution measure compared to a simple web domain ownership validation of DV SSL. Three respondents mentioned that DV SSL would suffice as well for smaller businesses that don't use sensitive data. Neither of the respondents would recommend or choose a self-signed SSL because it is a certificate for non-commercial use and does not offer any guarantees in case of security breaches, compared to DV and EV SSL that offer financial guarantees.

For the main benefits and advantages that EV SSL brings, most web&IoT developers interviewed mentioned the safety of data and encryption mechanisms, compatibility with most popular web browsers, protection against cyber-attacks such as phishing or man-in-the-middle attack. The online marketing specialists focused more on benefits such as better positions in search results, better brand and company image, increasing the trust of end users and higher credit card payment rate for online orders. Regarding the problems encountered with SSL certificates, the web&IoT experts' answers focused on server-side problems, initial installation or high acquisition costs. More specific, some of the problems mentioned were: incorrect server settings, problems when renewing an SSL certificate on a server that already has a valid SSL for the same domain name, failure to correct source codes that were not designed to be compatible with SSL, mixed content (HTTP and HTTPS), incorrect domain name due to human error.

As for increasing the trust and notoriety of a brand by using SSL, all respondents agreed and argued, especially in the case of businesses with important data or in the case of digital educated and experienced users. Other arguments mentioned that an EV SSL is a proof of a detailed vetting process of companies, thus increasing the trustworthiness of a brand or a company. Another interesting point of view was from an online marketing specialist who mentioned that an EV

SSL denotes a greater involvement of the website owner to create a secure environment (validation being more difficult) and an assumption that the brand is authentic. As for obtaining a better position in search engines by using an EV SSL certificate, all the respondents answered affirmative and referred more often to Google results and the fact that Google has announced that it will penalize websites that do not use SSL, through weaker positions in organic results.

When asked about the usefulness of EV SSL to legal compliance norms, such as GDPR or the EU NIS directive, some of the respondents were convinced that an EV SSL contribute to these legal norms but they did not know all legal implications. At the same time, some respondents considered that using an SSL is just a step-in data protection and preventing cybercrime requires more involvement from many parties (website owner, users, web developers, webserver administrators). Regarding the web experts' evaluation of SSL best practices, Fig. 4 presents the average values of each best practice previously identified.

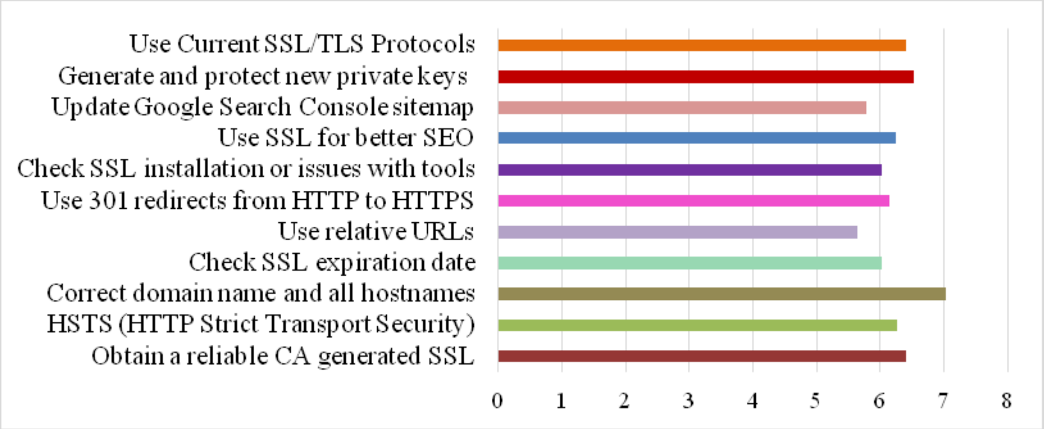

Fig. 4. SSL best practices average rates

8. Conclusions

According to the Google Trends comparative analysis, during November 2015 – October 2020, SSL and security had a constant level of interest, except for data protection which had a significant spike during May-June 2018. This spike of increased popularity is due to the enforcement of GDPR on 25th of May 2018. Given the fact that eCommerce websites and IoT devices collect, use and store huge amounts of sensitive personal data, it is highly recommended to use EV SSL certificates because GDPR implies a better protection of personal data. Most websites, especially eCommerce platforms need an SSL certificate in order to be more GDPR compliant and in order to diminish the risks of data breaches.

Fig. 5. presents the distribution ratio of the Google Trends keyword terms during November 2015 – October 2020. As it can be observed, the term of data protection accounts for 46%, followed by SSL which account for 30%. On the opposite side, secure IoT is an unpopular term, probably due to its lower adoption rate and its relative novelty in Information and Communications Technology (ICT).

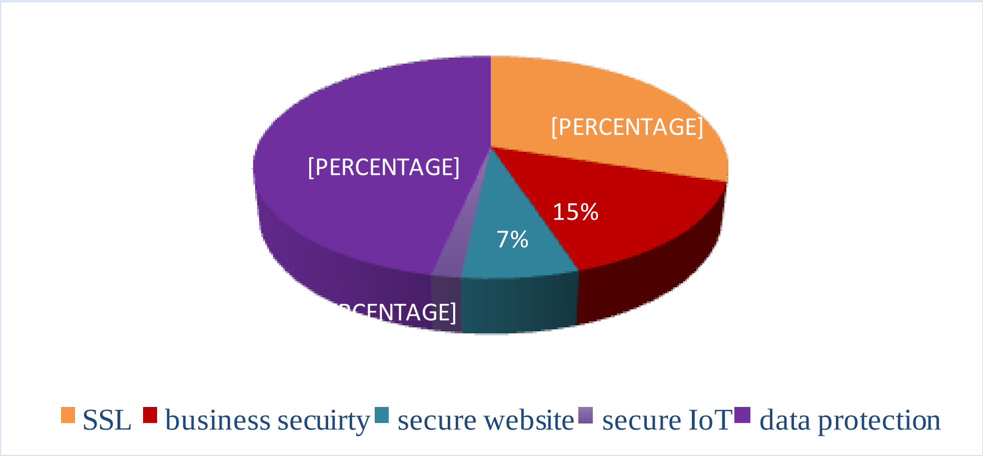

Fig. 5. Google Trends keyword ratio during November 2015 – October 2020

Following the research on top most viewed 1,000,000 websites worldwide, the authors have noticed that there are more SSL certificates than websites, probably due to the fact that a website or an IoT application can use more security certificates. However, in top 50 countries and territories in the world (by the number of SSL certificates), very few companies use EV SSL certificates, more exactly only 0.61% of companies use EV SSL certificates. According to the quantitative analysis conducted, it can be observed that the most visited 1 million websites in the world, have a below average rate, namely 0.55%. In Table 3 and Fig.6 it can be observed that the rate of EV SSL certificates increases in more popular websites, probably due to the fact that popular websites want to increase customers trust by using an EV SSL that implies a vetting process of the company. According to the final results, only 0.04% of all websites on the Internet (155,765,854) where traffic data was available, have EV SSL certificates.

Table 3

Extended validation certificate distribution ratio in 2020

Sample sites	SSL Certificates	Extended SSL	Extended SSL Ratio
Top 1.000.000 sites by traffic	1.712.404	9.477	0,55%
Top 100.000 sites by traffic	239.064	2.583	1,08%
Top 10.000 sites by traffic	30.915	477	1,54%
Entire Internet	155.765.854	63.367	0,04%

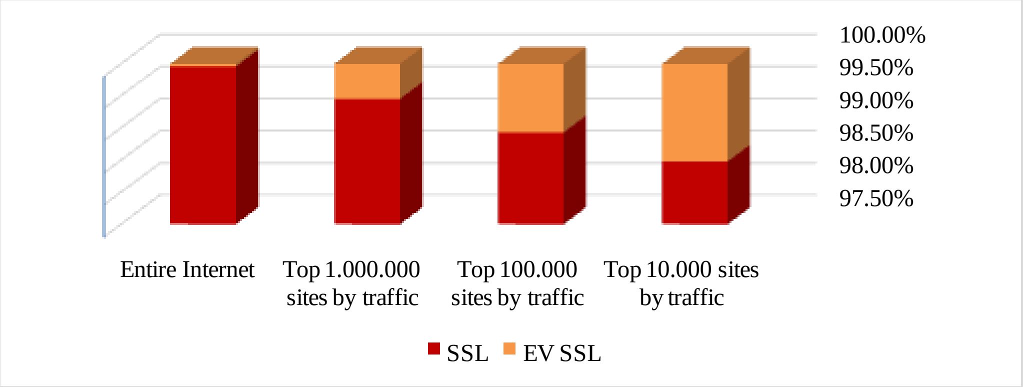

Fig. 6. EV SSL distribution ratio across most popular websites worldwide by traffic in 2020

As for the qualitative primary research conducted, by the interview method addressed to 8 experts (web&IoT developers and online marketing specialist), EV SSL were highly recommended by the respondents, due to a detailed vetting process of companies, increasing brand ad company credibility and trust. The top 3 best practices chosen by the online experts were: making sure an SSL is registered on the correct web domain and all hostnames are covered, obtain a reliable CA generated SSL and use current SSL/TLS protocols.

The original elements of this paper are provided by analyzing the interest granted on security solutions for digital businesses over November 2015-October 2020 on Google Trends and analyzing the usage rate of EV SSL in top most visited website worldwide. Also, the study conducted includes a qualitive research on how specialists perceive the importance of SSL certificates, compared to state-of-the-art literature which offers an in-depth technical view. The research conducted has an applicability in increasing the adoption of SSL EV certificates in the digital environment, because the obtained results denote an early usage stage of these data security systems, thus creating opportunities for increasing trust and security amongst companies and end users.

Further research can identify the top CA that issued EV SSL certificates, the geographical distribution of SSL certificates and especially the distribution of free or paid SSL certificates, as well as a in depth quantitative analysis on what end users know about EV SSL and its benefits.

Acknowledgment

This work has been funded by the European Social Fund from the Sectoral Operational Program Human Capital 2014-2020, through the Financial Agreement with the title "Scholarships for entrepreneurial education among doctoral students and postdoctoral researchers (Be Antreprenor!)", Contract no. 51680/09.07.2019 - SMIS code: 124539.

REFERENCES

[1]. *S. Waite,"* Securing online business with SSL", in Network Security, **vol, 3**, 2006, pp. 10-12

[2]. *N.Vratonjic, J. Freudige, V.Bindschaedler and J.P. Hubaux*,"The Inconvenient Truth About Web Certificates" in Economics of Information Security and Privacy III, ***vol 3***, July 2012, pp. 79-117

[3]. *S.A. Thomas*, "SSL and TLS essential", Wiley Computer Publishing, New York, 2000, pp. 150-152

[4]. *V. Krishna, S. Misra, D. Joshi, A. Gupta and M. Obaidat*, (2014) "Secure socket layer certificate verification: a learning automata approach" in Security and Communication Networks, **vol. 7**, no. 1, November 2014, pp. 1712-1718

[5]. *D. Gheorghică, V. Croitoru,* "FIREWALL POLICY MANAGEMENT USING SECURE WEB SYSTEM" in The Scientific Bulletin of University Politehnica of Bucharest, *Series C* **vol. 72**, no. 3, 2010, pp. 227-238

[6]. *I. Ristic*, "Bulletproof SSL and TLS: Understanding and Deploying SSL/TLS and PKI to Secure Servers and Web Applications", Feisty Duck, London, 2014, pp. 50-52

[7]. *S. Bocetta*, "Secure Your IoT Network with SSL Certificates" Retrived from https://openprovider.com/secure-your-iot-network-with-ssl-certificates/, August 2019

[8]. *D. Naylor, A. Finamore, I. Leontiadis, Y. Grunenberger, M. Munafò, K. Papagiannaki and, P. Steenkiste* "The Cost of the "S" in Proceedings of the 10th International Conference on emerging Networking EXperiments and Technologies (CoNEXT), Sydney, Australia, pp. 133–140, 2014

[9]. *C. Fei, W. Kehe C. Wei and Z. Qianyuan* "The Research and Implementation of the VPN Gateway Based on SSL" in 2013 International Conference on Computational and Information Sciences, Shiyang, China, IEE, pp. 1376-1379, 2013.

[10]. *F. Martin*, "SSL Certificates HOWTO", Independently published, ISBN-10 1707213488, 2019

[11]. *The SSL Store*, "Inspire Trust with SSL/ TLS How OV and EV SSL Certificates help you boost trust" Retrived from https://www.thesslstore.com/new-to-ssl/inspire-trust-ssl.aspx, May 2020

[12]. *N. Leavitt "Internet Security under Attack: The Undermining of Digital Certificates* in Computer, **vol. 44,** no 12, 2011, pp. 17-20

[13]. *Cloudflare*, "Types of SSL Certificates | SSL Certificate Types Explained" Retrived fromhttps://www.cloudflare.com/learning/ssl/types-of-ssl-certificates/, August 2019

[14]. *R. Biddle, C. van Oorschot, A. S. Patrick, J. Sobey and T. Whalen, "Browser interfaces and extended validation SSL certificates"* in Proceedings of the first ACM Cloud Computing Security Workshop, DBLP, Chicago, IL, USA, 2009

[15]. *Google LLC*, "*Secure your site with HTTPS"*, Retrived from https://developers.google.com/search/docs/advanced/security/https, September 2020

[16]. *A. Rusell*, "SSL/TLS Best Practices for 2021", Retrived from https://www.ssl.com/guide/ssl-best-practices/, Januarry 2021

[17]. *I. Dolnák and J. Litvik*, "*Introduction to HTTP security headers and implementation of HTTP strict transport security (HSTS) header for HTTPS enforc"*, in Proceedings of the 15th International Conference on Emerging eLearning Technologies and Applications (ICETA), IEEE, pp. 1-4, 2017

[18]. *Qualys, Inc* "*SSL and TLS Deployment Best Practices"*, Retrived from https://github.com/ssllabs/research/wiki/SSL-and-TLS-Deployment-Best-Practices, January 2020

[19]. *Google LLC*, “*HTTPS as a ranking signal”*, Retrived from https://developers.google.com/search/blog/2014/08/https-as-ranking-signal, August 2014

[20]. *DigiCert Inc*, “*TLS BEST PRACTICES”*, Retrived from https://www.digicert.com/resources/tls-best-practices-ebook-en-2020.pdf, October 2020

[21]. *Google LLC*, “*FAQ about Google Trends data”*, Retrived from https://support.google.com/trends/answer/4365533?hl=en, June 2015

[22]. *BuiltWith Pty Ltd*, “*SSL Usage Distribution in the Top 1 Million Sites”* Retrived from https://trends.builtwith.com/ssl, June 20