Comparison of Performance Analysis of Comodo SSL and Let's Encypt SSL *(Case Study: Bukalapak and Tokopedia)*

Ipung Ardiansyah[1,] Misbachul Munir [2,] Joko Dwi Santoso [3,] Sri Mulyatun [4,] Ali Mustopa [5)]

[1)] *Department of Computer Engineering Universitas Amikom Yogyakarta DI Yogyakarta, Indonesia, 2) Department of Computer Engineering Universitas Amikom Yogyakarta DI Yogyakarta, Indonesia, 3) Department of Computer Engineering Universitas Amikom Yogyakarta DI Yogyakarta, Indonesia, 4) Department of System Information Universitas Amikom Yogyakarta DI Yogyakarta, Indonesia, 5) Department of System Information Universitas Amikom Yogyakarta DI Yogyakarta, Indonesia*

Author Emails

ipung.19@students.amikom.ac.id, misbachul.munir@students.amikom.ac.id, jds@amikom.ac.id, sri.m@ amikom.ac.id, ali.m@students.amikom.ac.id

***Abstract*— The world is becoming connected with the internet, the arrival of the internet has greatly influenced new network technology. The number of internet users is increasing day by day, there is an increase in online transactions. As a growing number of websites have sprung up with easy information transmission facilities, it has been seen that it has caused a huge increase in fraud. Broad e-commerce spectrum (B2B / B2C / C2C), banking, finicial trading and others. Business applications require very high data exchange for security. Secure Sockets Layer (SSL), and its influence on web server performance. Secure SocketLayer (SSL) is the most popular protocol used on the internet to facilitate communication security through authentication, encryption, and decryption. Although the use of SSL provides adequate security, this can cause a decrease in performance compared to insecure protocols as well as a decrease in the percentage of downloads compared to insecure protocols. In this paper, we analyze the performance and impact of SSL on web performance and the type of SSL used by Bukalapak e-commerce and Tokopedia**

Keywords— SSL; Comodo SSL; Let's encrypt SSL

I. INTRODUCTION

The internet has become an important part of our daily lives, so the need for cybersecurity has also increased. The more users connected to the internet the more attractive the criminals are. Cyber security / internet security against domain web sites or servers from various forms of attack by criminals. Cyber security is very useful in every area of the world today such as the military, government, online business and even in our world of daily life. Today, everything is connected to the internet, from simple shopping to secret cyber security needs. Billions of dollars of transactions occur every hour through the internet, this needs to be protected. Destroying a small unnoticed network can cause serious damage. In every area of the Internet, whether financial, personal, or business that everyone wants to know with whom they communicate, make sure their data can be sent safely, and whether it has reached its destination correctly. Cyber security is an ongoing effort to protect electronic data and computer systems from unwanted intrusions. Transmits data through the network while requesting confidentiality, message integrity or endpoints to be approved.

II. LITERATURE REVIEW

A. SSL (Secure Socket Layer)

One of the most important components in online business or e-commerce is creating an environment where potential customers are confident in making purchases. SSL (Secure Socket layer) is used for this purpose. It was developed by Netscape Communications in the 1990s. The company wants to encrypt data in transit between its flagship Netscape Navigator browser and Web servers on the Internet to ensure sensitive data/information, such as credit card numbers, Social Security numbers, and entry credentials are protected. Thus, SSL (Secure Socket Layer) is a security layer for the security of transactions on your website with sophisticated data encryption technology.

The SSL protocol authenticates the server to clients using public-key cryptography and digital certificates. This protocol also provides client-to-server approval. The public key algorithm used is RSA, and the secret key algorithm used is IDEA, DES, and 3DES, and the hash function algorithm uses MD5. Public key verification can use certificates that are standard X.509. There are two components that make up SSL, which are SSL handshaking and SSL records. SSL Handshaking sub-protocol that establishes secure connections for communication and SSL Records are sub-protocols that use secure connections. The SSL record wraps all data sent during the connection.

B. Algorithm RSA

The RSA algorithm is a public key algorithm that is popularly used and is even still used today. The strength of this algorithm lies in the exponential process and factoring into 2 prime numbers which until now requires a long time to factoring. This algorithm is named after its inventors, Ron Rivest, Adi Shamir and Adleman (Rivest-Shamir-Adleman),

published in 1977 at MIT, answering the challenges posed by the Diffie Hellman key exchange algorithm.

The RSA scheme itself adopts a block cipher scheme, where before encryption, the existing plaintext is divided into blocks of the same length, where the plaintext and ciphertext are integers between 1 to n, where n is usually 1024 bit, and the length of the block itself is smaller or equal to log (n) +1 with base 2.

C. Algorithm SHA-256

The Secure Hash Algorithm (SHA) is a one-way hash function algorithm created by NIST and used with DSS (digital signature standards). SHA is based on MD4 made by Ronald L. Divest. SHA is called (safe) because it is designed in such a way so that it can find messages that correspond with messages in the given gest. The SHA algorithm takes messages that are less than 264 bits long and produces a 160-bit digest message. This algorithm is slower than MD5, but larger digest messages are safer from Bruteforce collisions and inversion attacks. There are many versions of SHA. There are SHA-0, SHA-1, SHA-2. Meanwhile, SHA-2 is divided into SHA-224, SHA-256, SHA-34, and SHA-512.

SHA-256 is a cryptographic hash function with a digest length of 256 bits. This is a keyless hash function; that is, MDC (Detection Code Manipulation). A message is required with 512 blocks = 16 × 32 bits, each block requires 64 rounds.

D. SSL Certificate

An SSL certificate is a small data file that digitally contains cryptographic keys to organizational details. When installed on a web server, this activates the padlock and https protocol and allows a secure connection from the webserver to the browser. An SSL certificate is tied to the domain name, server name or host name, organizational identity and location. SSL certificates have two combinations, namely public key and private key. The public key uses an asymmetric algorithm that converts messages into an unreadable format. Someone who has a public key can encrypt messages addressed to a specific recipient. Recipients with private keys can only decode messages that have public key encrypted. Keys are available through directories that can be accessed by the public. Whereas the private key is the secret key used to decrypt messages. In the traditional method, the private key is only shared in a communicator to enable message encryption and decryption, but if the key is lost the system will become invalid. To avoid this, the *PKI (Public Key Infrastructure)* provides a policy where the public key can be used together with the private key. PKI allows internet users to exchange information securely using *public keys* and *private keys*.

Types of SSL certificates are divided into 3 major groups namely Domain Validation (DV), Organizational Validation (OV) and Extended Validation (EV).

1) Domain Validation (DV) :- Domain validated certificates include your domain name in the certificate (not your business or organization name). These certificates are cheaper and usually issued in minutes as the Certificate authority validates your domain by looking at the WHOIS information for your domain. However, these certificates provide less assurance to customers.
2) Organization Validation (OV):- Organizational certificates are Trusted. Organizations are strictly authenticated by real agents against business registry databases hosted by governments. Documents may exchange and personnel may be contacted during validation to prove the right of use. OV certificates therefore contain legitimate business information. This is the standard type of certificate required on a commercial or public facing website. OV certificates conform to the X.509 RFC standards and thus contain all the necessary information to validate the organization.
3) Extended Validation (EV):- Nothing provides more trust and security than Symantec Extended Validation Certificates. It is used by most of the world's leading organizations. They have found that switching from OV to EV certificates increases online transactions and improve customer confidence. It is no longer a luxury but a necessity. Sites protected with a EV SSL Certificate display a green browser bar to quickly assure visitors that the organization's legal and physical existence was verified according to strict industry standards.

The choice of SSL certificate is not based on the brand used, but the selection of the type of SSL that is tailored to the needs of the approved company and document fulfillment of certificate validation requirements. The higher the level of transaction transactions on the website, the better the use of SSL with a higher level of encryption. Based on brands, there are two brands that are very strong in marketing in Indonesia's online business, namely Comodo SSL and Let's Encrypt.

TABEL 1. COMPARISON COMODO SSL AND LET'S ENCYPT SSL

COMODO SSL	LET'S ENCRYPT
Paid	Free
Supports the overall browser version	Lack of compatibility with legacy browsers
The validity period is 1 year	The validity period is 90 days
The security insurance is available starting at $10,000	Security insurance does not exist
The process of reissuing or publishing SSL is faster	The SSL publishing process is slow

E. E-Commerce(Electronic Commerce)

E-Commerce is a process of selling and purchasing products or services that are done electronically via a computer network or the internet. The meaning of e-commerce is the use of digital information and communication technology in conducting business transactions to create, change and redefine new relationships between sellers and buyers

Models in e-commerce are divided into 7 with different characteristics as follows:

1) Business-to-Business (B2B):- Both sellers and buyers are business organizations. For example: indotrading.com, ralali.com
2) Business-to-Consumer (B2C):- Sellers are organizations, and buyers are individuals. For example: bhineka.com, lazada.co.id
3) Consumer-to-Consumer (C2C):- Individuals sell products or services to others. For example: olx.co.id, bukalapak.com, tokopedia.com
4) Consumer-to-Business (C2B):- The seller is an individual, and the buyer is an organization.
5) Business-to-Administration (B2A):- e-commerce which includes all transactions made online between companies and public administration. For example: tax.go.id, allianz.com
6) Consumer-to-Administration (C2A):- e-commerce which is all electronic transactions carried out between individuals and public administration. For example, bpjs-online.com
7) Online-to-Offline (O2O):- e-commerce that attracts customers from online channels to physical stores. For example: Kudo and Mataharimall

III. Results and Discussion

A. *Algorithm*

1) Bukalapak

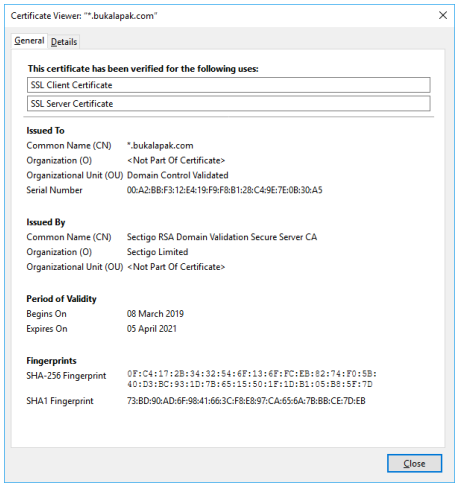

Fig.1 General Certificate Bukalapak

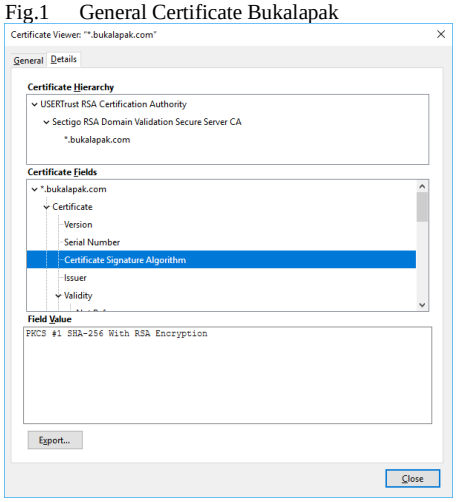

Fig.2 Certificate Signature Algorithm

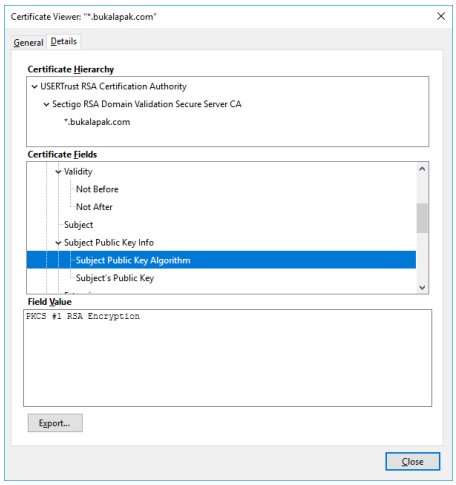

Fig.3 Subject Public Key Algorithm

Bukalapak uses SSL provided by Sectigo RSA Domain Validation Secure Server CA version 3. The key used for the public key is the RSA 2048 algorithm which is used for the algorithm using SHA-256. Tokopedia and Bukalapak use different SSL certificates of service but differ from SHA-256 with RSA 2048 Bit.

2) Tokopedia

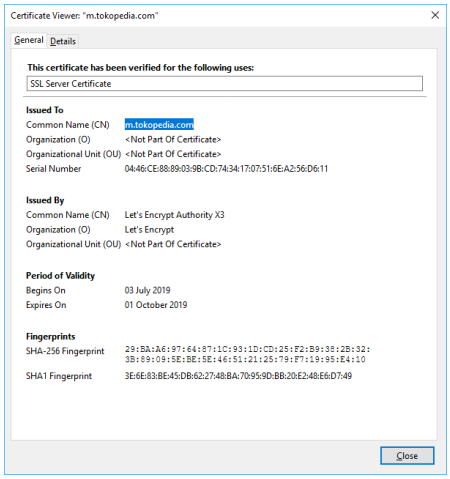

Fig.4 General Certificate Tokopedia

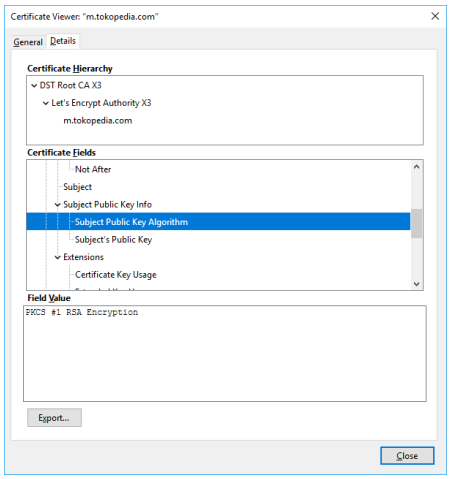

Fig.5 Subject Public Key Algorithm

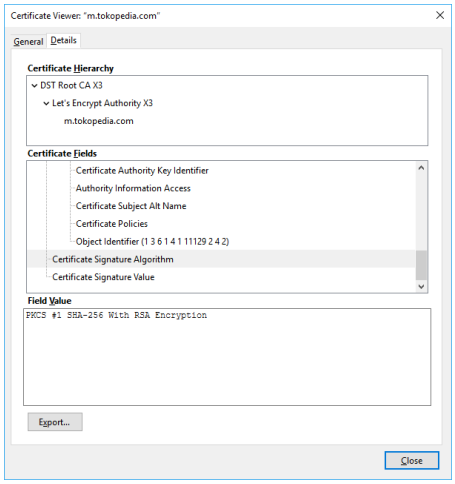

Fig.6 Certificate Signature Algorithm

Tokopedia uses SSL provided by let's encrypt version 3. The key used for the public key is the RSA 2048 Bits algorithm while for the signature algorithm it uses SHA-256

B. Performance

1) Bukalapak

Performance Results (Median Run)

	Load Time	First Byte	Start Render	Speed Index	Last Painted Hero	First Interactive (beta)	Document Complete Time	Document Complete Requests	Document Complete Bytes In	Fully Loaded Time	Fully Loaded Requests	Fully Loaded Bytes In	Cost
First View (Run 1)	15.460s	2.305s	4.000s	4.823s	11.100s	> 17.195s	15.460s	190	3,453 KB	19.226s	219	3,788 KB	$$$$$
Repeat View (Run 2)	6.738s	1.649s	2.500s	3.066s	6.500s	9.723s	6.738s	65	368 KB	13.184s	80	456 KB	

Fig.7 Performance Bukalapak

Request Details

Before Start Render | Before On Load | After On Load

Request Details

#	Resource	Content Type	Request Start	DNS Lookup	Initial Connection	SSL Negotiation	Time to First Byte	Content Download	Bytes Downloaded	Certificates	Error/Status Code	IP
1	http://www.bukalapak.com/	text/html	0.31 s	26 ms	263 ms	-	264 ms	-	-	-	301	103.117.82.28
2	https://www.bukalapak.com/	text/html	1.396 s	-	260 ms	555 ms	909 ms	297 ms	47.2 KB	-	200	103.117.82.28
3	https://www.bukalapa...s/promoted-brand.jpg	image/jpeg	2.461 s	-	-	-	291 ms	567 ms	166.3 KB	-	200	103.117.82.28
4	https://www.bukalapak.com/.webp	text/html	2.478 s	-	-	-	847 ms	6 ms	32.1 KB	-	404	103.117.82.28
5	https://www.google-a...es.com/jsa/la/gpt.js	text/javascript	2.562 s	26 ms	29 ms	57 ms	57 ms	19 ms	11.5 KB	-	200	172.217.15.66
6	https://www.google-a...ics.com/analytics.js	text/javascript	2.574 s	27 ms	32 ms	64 ms	53 ms	47 ms	17.3 KB	-	200	172.217.164.174
7	https://dev.visualwe...=9.920730386793582	application/javascript	2.574 s	26 ms	36 ms	69 ms	102 ms	1 ms	0.6 KB	-	200	50.97.40.233
8	https://www.google-a...gtm.js?id=GTM-THCD83	application/javascript	2.574 s	27 ms	36 ms	74 ms	98 ms	61 ms	29.0 KB	-	200	172.217.15.104
9	https://s4.bukalapak...6597c7ac6852124.css	text/css	2.574 s	51 ms	32 ms	100 ms	132 ms	2 ms	1.1 KB	-	200	96.17.189.52
10	https://s2.bukalapak...Foto_Amber.jpg.webp	image/webp	2.704 s	-	-	-	111 ms	2 ms	1.0 KB	-	200	96.17.189.52
11	https://s2.bukalapak...09m__Black.jpg.webp	image/webp	2.704 s	-	-	-	115 ms	3 ms	1.7 KB	-	200	96.17.189.52
12	https://s0.bukalapak...bukamall/logo@2x.png	image/png	2.704 s	-	-	-	119 ms	3962 ms	6.3 KB	-	200	96.17.189.52
13	https://s1.bukalapak...8410ec39c39899f.css	text/css	2.717 s	-	-	-	167 ms	206 ms	96.0 KB	-	200	96.17.189.52
14	https://s1.bukalapak...51cc52af2b6c55.css	text/css	2.717 s	-	-	-	453 ms	289 ms	80.2 KB	-	200	96.17.189.52

Fig.8 SSL Negoitate

2) Tokopedia

Load Time	First Byte	Start Render	Visually Complete	Speed Index	Last Painted Hero	First Interactive (beta)	Result (error code)
13.261s	0.565s	1.900s	17.100s	7.115s	17.100s	> 13.680s	99999

Fig.9 Performance Tokopedia

Request Details

#	Resource	Content Type	Request Start	DNS Lookup	Initial Connection	SSL Negotiation
1	http://www.tokopedia.com/	-	0.09 s	27 ms	32 ms	-
2	https://www.tokopedia.com/	text/html	0.224 s	-	30 ms	58 ms
3	https://fonts.google...00,400,400italic,600	text/css	0.76 s	29 ms	34 ms	57 ms
4	https://ecs7.tokoped...da31abb6b31e5463.css	text/css	0.958 s	239 ms	32 ms	46 ms

Fig.10 SSL Negoitate

IV. CONCLUSION

From the results of our research, it can be concluded that the two SSL Providers used by Tokopedia and Bukalapak have the same security by using SHA 256 and RSA Algorithm as encryption. In both SSL significant differences, namely in the cost, EV (Extended Validation) and SSL validity period. In Letsencrypt to use it only need to install an app to create a new certificate from Letsencrypt itself without any cost (free) but the validity period is very short in a few months generally 3 months and after that, the SSL certificate must be extended again and there is no EV option Green bar SSL certificate and compatible with platforms such as Blackberry, Nintendo 3Ds, and various other platforms while at Comodo the costs incurred according to the company with the choice of various types of SSL with a certain validity period and the price is quite expensive, in addition to the validity period is long enough, in general, can be more than 1 year and support from the company when there is a problem with SSL purchased with a money-back guarantee and there is an EV certificate SSL certificate and is compatible on all platforms.

The SSL performance section of the e-commerce web shows that for the initial connection section (Introduction to TCP with SSL Handshake) and the DNS Lookup section and the Speed Index (Speed Index) section needed by Comodo (Bukalapak) is faster than Let's Encrypt (Tokopedia). While in the SSL negotiation process which is a client server handshake in SSL certificate Tokopedia (Mari Encryption) is faster than Bukalapak (Comodo). Broadly speaking, Comodo SSL is more compatible and is very responsible for use on security websites compared to Let's Encrypt SSL.

V. REFERENCE

[1] M. A. Alnatheer, '*Secure Socket Layer (SSL) Impact on Web Server Performance'*, J. Adv. Comput. Netw., vol. 2, no. 3, pp. 211–217, 2014.

[2] C. Castelluccia, E. Mykletun, and G. Tsudik, '*Improving secure server performance by re-balancing*

SSL/TLS handshakes', in Proceedings of the 2006 ACM Symposium on Information, computer and communications security - ASIACCS '06, Taipei, Taiwan, 2006, p. 26.

[3] D. H. P. Dewa, E. S. Pramukantoro, and D. P. Kartikasari, *'Analisis Mekanisme Keamanan Antara TLS/SSL Dan Crypto Pada Komunikasi IoT Middleware Dengan Subscriber Berbasis Protokol HTTP'*, p. 7.

[4] R. Esposito and D. P. Radicioni, *'CarpeDiem: an algorithm for the fast evaluation of SSL classifiers*', in Proceedings of the 24th international conference on Machine learning - ICML '07, Corvalis, Oregon, 2007, pp. 257–264.

[5] A. Goldberg, R. Buff, and A. Schmitt, '*Secure Web Server Performance Dramatically Improved by Caching SSL Session Keys'*, p. 8.

[6] E. P. Kaur and E. G. Kaur, *'Review of Role of SSL in Cyber Security'*, Int. J. Adv. Res. Comput. Sci., p. 4, 2017.

[7] Li Zhao, R. Iyer, S. Makineni, and L. Bhuyan, 'Anatomy and Performance of SSL Processing', in IEEE International Symposium on Performance Analysis of Systems and Software, 2005. ISPASS 2005., Austin, TX, USA, 2005, pp. 197–206.

[8] N. Lim, S. Majumdar, and V. Srivastava, *'Engineering SSL-based systems for enhancing system performance',* in Proceeding of the second joint WOSP/SIPEW international conference on Performance engineering - ICPE '11, Karlsruhe, Germany, 2011, p. 469.

[9] D. Naylor et al., *'The Cost of the "S" in HTTPS',* in Proceedings of the 10th ACM International on Conference on emerging Networking Experiments and Technologies - CoNEXT '14, Sydney, Australia, 2014, pp. 133–140.

[10] S. Puangpronpitag and N. Sriwiboon, *'Simple and Lightweight HTTPS Enforcement to Protect against SSL Striping Attack'*, in 2012 Fourth International Conference on Computational Intelligence, Communication Systems and Networks, Phuket, Thailand, 2012, pp. 229–234.