QR code and transport layer security for licensing documents verification

A Wibiyanto, I Afrianto*
Informatics Engineering Department, Universitas Komputer Indonesia, Jl. Dipati Ukur No.112-116 Bandung, Indonesia, 40132

*irawan.afrianto@email.unikom.ac.id

Abstract. This paper aimed at licensing documents verification. Licensing can be interpreted as one form of implementation of regulatory functions and controlling nature owned by the government against activities undertaken by the community. The purpose of this research is to add QR code and transport layer security (TLS) feature to the licensing document verification system. The technologies used in the research are QR code and digital signature for the speed of access and security of licensing documents, and TLS to ensure safe communication during the process verification. QR code that is included in licensing document, contains the serial number and an access code that serves as an access key to the permission data stored in the system and then the data signed using a digital signature. The licensing document authenticity can be verified using mobile application and web page. To secure communication session between the verification application with the system, TLS is applied on the server so that all communication session is encrypted. The result of this research, licensing documents that have QR code is harder to forge and can be verified quickly, moreover, TLS complete the service by encrypting all communication session thus the communication session is more secure.

1. Introduction
The licensing document is an important document created and issued by the government. This is what causes a lot of forged documents by parties who are not responsible. [1]. QR code is a matrix barcode (two-dimensional barcode) [2], QR is short for quick response in accordance with its purpose, it used to access information quickly and get a quick response, QR code capacity is larger than one-dimension barcodes [3]. Research on QR code is done by Liu [4] which makes QR code as a verification code for goods delivery process. While Canadi research [5], has implemented Qr code in the tourism environment in order to introduce the object more informative.

This study aims to develop a security mechanism that can be inserted into a QR code because of the QR code is very easy to counterfeit [6]. Research on QR code security has been done by Harini [7] where QR code is used as media to store user's personal information such as password and fingerprint. While Warasart's research implements the security of digital signatures on paper documents, to maintain data integrity [8]. Elliptic Curve Digital Signature Algorithm (ECDSA) is selected for digital signature algorithm, selection is based on the limited availability of storage space, so algorithm need that produces short signature but secure need to be selected, ECDSA with 256-bit key size have the same level of security with RSA with 3072 bits key, signature of ECDSA with 256-bit key size is 64 bytes, while the length of signature RSA with 3072-bit key size is 384 bytes (equal to the size of RSA keys) [9].
SSL/TSL is a technology used to make secure communications sessions between two parties, all communication sessions that run on SSL are encrypted and thus more secure [10]. Secure communication is not limited to the security of inter-process communication within a single computer, but also securing communication between processes on two different computers. Even securing communication between processes on two different computers is much more important because there are more threats. For example, the largest use of SSL / TLS is to "secure session" between the web browser to the web server process that normally resides on two different computers [11]. Implementation of SSL / TLS utilization has been done in Luqman's research, which is utilizing SSL / TLS for VPN security [12]. While Castelluccia's research [13] establishes a mechanism for enhancing SSL / TSL security capabilities.

Based on existing issues and references, the licensing document is a document that needs to be protected, it is necessary to develop a QR code system as a secure verification feature based on digital signatures and TLS as a secure communication channel. Thus, the results to be achieved from this research are the licensing documents being difficult to forge, accessible, and more secure.

2. Method
The research methods used in this study include the following:

- Data Collection: Data collection methods to be used in this study are as follows: a. literature study: Data collection techniques by collecting and studying literature, journals, and papers that have links to research such as QR codes and SSL/TLS. b. observation and interview: conducted by visiting the office of BPMPPPT West Bandung regency to discuss a related licensing system that already exists.
- Analysis of current system: at this stage, an analysis of existing systems, this is because the topic of research is the development of the system, then the analysis of existing information systems become important to know the various business processes that exist, as well as business processes that must be changed to allow for new verification features.
- Designing new system architecture: At this stage, a new system architecture design will be applied to the old system. The design includes an updated business system process and an overview of how the licensing document verification feature is applied.
- Feature analysis QR code verification and security with TLS: At this stage, an analysis of how QR code can be used for verification of permissions, as well as coding flow and QR code readings used for licensing verification, and also analyzing the security of communication sessions by using TLS.
- Designing QR Code verification feature and security with TLS: at this stage, designing of QR code-based licensing verification feature and designing of communication session security using TLS.
- Implementation and testing: At this stage, the results of the design of additional features QR code and TLS will be applied and tested whether it can meet the objectives of the study.

3. Results and discussion
System Architecture
The architecture of verification features that will be added to the system can be seen in Figure 1.
Verifier accepts licensing applications and performs processing by using the system.

- The system compiles data that will be included in a QR code which is a combination of the access code, licensing document serial number and digital signature of the data to be encoded in QR code that will be included in licensing document that will be printed, which included QR code that serves as a medium for fast access to licensing data stored in the database system.
- Licensing document verification is done by scanning the QR code using a mobile application, if the QR code is legible and valid, the application sends the data to the system. If the QR code cannot be read, verification could be done using verification web page, verification is done by entering the licensing document serial number and access code printed on licensing document.
- The system validates input data and transmits licensing data that can be used by verifiers as reference data for verification the licensing document.

**QR code data and digital signature analysis**

The analysis QR code data is done to determine the data to be included in a QR code that will be used as a medium for verification of licensing document, the data to be included in the result of a merger of a licensing document serial number and access code, every kind of licensing document had different length of serial number, which described as shown in table 1:

| Type | Serial Number        | Length     |
|------|----------------------|------------|
| SIUP | 00408/10-17/PK/IX/2012 | 22 Character |
| TDP  | 103134601437          | 12 Character |

Serial number and access codes are combined with the separator character ';'; (semicolon) to form the data that will be included in the QR code. Total length character of data for SIUP licensing is 31 characters shows in figure 2.
Data generated from the merging process of a serial number and access code, hereinafter referred as preliminary data, the initial data is not the data included in the QR code, we should first add a digital signature that will be used to maintain the authenticity of the data.

The first step is to check whether the private key exists, if the private key not existed then do the process of generating the private key and public key of ECDSA using secp256k1, once generated private key and a public key stored in the database system, for the record this process is only done once, because key pair that is used for signing must be preserved, the private key is stored in the database of system to prevent access by unauthorized people, while the public key in addition to stored is also distributed in mobile applications to be used for validating the signature. Hash value calculation is done on preliminary data using SHA256 algorithms on (serial number and an access code) [14]. The resulted hash value has a size of 32 bytes and represented using hexadecimal numbers (64-character hexadecimal) shows in figure 3.

Figure 3. The hash value of preliminary data.

Do signing operation on the hash value of the preliminary data by using the private key that has been generated in the previous process, this process generates a digital signature. Signature of ECDSA algorithm with secp256k1 is 64 bytes long, the signature is encoded with ASN.1 notation and written in DER format so it has a size of ± 71 byte (144 hexadecimal numbers) [15]. Do the preparation of the final data by combining the initial data and digital signatures using the following rule, shown in figure 4. Before merging signature with the preliminary data, the signature is encoded using base64 encoding to reduce the length of the signature shows in figure 5. Then the data is merged using ”;” separator as a final data signature shows in figure 6.

Figure 4. Signature of SIUP preliminary data.

Figure 5. Example of signature (base64 coded).

Figure 6. Final data signature.

Session securing using TLS
Licensing document verification is done through the internet, therefore, need to be a consideration in terms of the Internet security, the protocol can be used to secure communications on the Internet, the following are the results of the analysis [16]:

- Determining Key Size
  Selected key size is 2048 bit RSA key that is signed using SHA256, RSA 2048 with the SHA256 private key is the key type recommended to use.
• Determining TLS Version
The lowest client to be supported is Android 4.1.x, Android version 4.1.x only supports TLSv1 protocol, based on that information protocol version supported by the server is specified, the protocol version that used are TLSv1, TLSv1.1, TLSv1.2.

• Cipher suite selection
Cipher suite selected based on modern TLS configuration issued by the Mozilla Foundation, with a few changes which are the addition of TLSv1 protocol to supports Android 4.1.x and disabling ECDSA cipher, because the key that used is RSA key.

• HSTS
HSTS is an HTTP header that is sent from the server to the client, this header indicates the website is only accessible via HTTPS, the header that is sent from the server in the form of max-age that indicate when a header expire, headers is expressed in the format of seconds, commonly used value is 15724800 seconds or 6 months.

4. Verification feature test

Verification via the web page
The results of verification via web page test are described in table 2.

| Input | Expected Behavior | Observation | Conclusion |
|-------|-------------------|-------------|------------|
| Serial number and/or access code is invalid | Displaying error page “licensing data not found” | Displaying error page “licensing data not found” | Accepted |
| Serial number access code is valid | Displaying related licensing data | Displaying related licensing data | Accepted |

Verification via mobile application
In the first test, the scenario is assumed invalid. QR code data and digital signature show in figure 7 and the result shown in figure 8.

Figure 7. First test QR code.

Figure 8. First test application response.
The output from the application is error message shows in figure 8 "Verifikasi tanda tangan digital gagal, QR code perizinan terindikasi palsu ", which means the QR code had an invalid signature and indicated false documents, the result of the test for second test scenario is accepted.

In the second test, the scenario is assumed the application scan the QR code that has valid structure, a valid signature data, and the licensing data is found on the database of the system which means its valid licensing document shows in table 9.

![QR Code](image)

**Figure 9.** Second test QR code.

Testing is done by scanning the QR code using a mobile application, the response can be seen in Figure 10.

![Application Response](image)

**Figure 10.** Second test application response.

The output from the application is licensing data of the related QR code, the result of the test for second test scenario is accepted.

**TLS Configuration Test**

Testing is done by evaluating the TLS configuration that has been implemented, SSL Qualsys test server is a service that can be used to evaluate the configuration of SSL / TLS on a server, based on the server rating guidelines issued by Qualsys SSL, the configuration got A+ grade.

The next test is performed to determine whether the communication session after application of TLS is more secure, testing is done by using Wireshark, Wireshark could be used to monitor traffic data on the network so that it could be seen whether a communication session is encrypted or not, shows in Figure 11 (a) and 11 (b).
5. Conclusion

Addition of verification feature at system made the licenses harder to counterfeit and the licensing document could be verified quickly and accurately can be implemented. The inclusion of QR code that’s secured using digital signature made the licensing document significantly harder to forge. Licensing document can be verified quickly and accurately by using the mobile application or web page. The implementation of SSL/TSL on the web server made the communication more secure. The configuration that implemented on the server gets A+ grade according to Qualsys SSL server rating. All communication session is encrypted thus more secure.

Acknowledgements

Authors acknowledged to BPMPT Kabupaten Bandung Barat for supporting this research as a place for testing and implementation of the developed system.

References

[1] Prakananda M 2012 Rancangan Penerapan Teknologi RFID untuk Mendukung Proses Identifikasi Dokumen dan Kendaraan di Samsat In Seminar Nasional Aplikasi Sains & Teknologi (SNAST) III Yogyakarta 12 2 p 1-10
[2] Denso Corporation 2011 QR Code Essentials Denso 3 2 p 1-10
[3] Lorenzi D, Vaidya J S, Chun, Shafiq B and Atluri V 2014 Enhancing the government service experience through QR codes on mobile platforms Gov. Inf. Q. 31 1 p 6–16
[4] Liu Z, Zeng Q C, Wang and Lu Q 2011 Application research of QR code barcode in validation of express delivery in Communications in Computer and Information Science 143 CCIS no PART 1 p 346–351
[5] Canadi M, Höpken W and Fuchs M 2010 Application of QR codes in online travel distribution Information and Communication Technologies in Tourism 2010 p 137-148
[6] Afrianto I, Heryandi A and Finandhita A 2012 Pemanfaatan QR code Sebagai Akses Cepat Verifikasi Ijazah UNIKOM in Seminar Nasional Teknologi Informasi dan Komunikasi (SNASTIKOM 2012) p 9-16
[7] Harini N and Padmanabhan T R 2013 2CAuth: A new two factor authentication scheme using QR-code International Journal of Engineering and Technology 5 2 p 1087-1094
[8] Warasart M and Kuacharoen P 2012 Based document authentication using digital signature and QR code In 4th International Conference on Computer Engineering and Technology International Proceedings of Computer Science and Information Technology p 94-98
[9] Bernstein D J, Duif N, Lange T, Schwabe P and Yang B Y 2012 High-speed high-security
signatures Journal of Cryptographic Engineering 2 2 p 77-89
[10] Blake-Wilson S, Nystrom M, Hopwood D, Mikkelsen J and Wright T 2006 Transport layer security (TLS) extensions (No. RFC 4366) 9 1 p 1-10
[11] Granjal J, Monteiro E and Sa Silva J 2013 End-to-end transport-layer security for Internet-integrated sensing applications with mutual and delegated ECC public-key authentication IFIP Netw. Conf. p 1–9
[12] Luqman K 2014 Implementasi dan Analisis SSL VPN sebagai Solusi Keamanan Jaringan (Doctoral dissertation, Program Studi Teknik Informatika FTI-UKSW) 8 1 p 1-5
[13] Castelluccia C, Mykletun E and Tsudik G 2006 Improving secure server performance by re-balancing SSL/TLS handshakes In Proceedings of the 2006 ACM Symposium on Information, computer and communications security p 26-34 ACM
[14] International Standar Organization 2000 Decoding Procedure Overview in International Standard ISO/IEC 18004, Geneva, ISO p 59
[15] Josefsson S 2006 RFC4648 - The Base16, Base32, and Base64 Data Encodings The Internet Engineering Task Force
[16] Kromodiemoeljo 2009 SSL/TLS in Teori & Aplikasi Kriptografi, SPK IT Consulting p 335-340