TELKOMNIKA, Vol.14, No.4, December 2016, pp. 1527~1533
ISSN: 1693-6930, accredited A by DIKTI, Decree No: 58/DIKTI/Kep/2013
DOI: 10.12928/TELKOMNIKA.v14i4.2915

Paper-based Verification Design of Trade Business License in Indonesia

Pizaini*[1], Sugi Guritman[2], Heru Sukoco[3]
[1]Department of Informatics Engineering, Faculty of Science and Technology,
Universitas Islam Negeri Sultan Syarif Kasim Riau - Indonesia
[2]Department of Mathematics, [2]Department of Computer Science
[2,3]Faculty of Mathematics and Natural Science, Bogor Agricultural University - Indonesia
*Corresponding author, email: pizaini@uin-suska.ac.id[1], guritman@yahoo.co.id[2], hsrkom@ipb.ac.id[3]

Abstract

The trade business license certificate (SIUP) is a paper-based license to conduct trade businesses in Indonesia issued by the government. Until today, there is no mechanism for verifying the validity of document unless to verify it manually. The current paper presents a design that allows paper-based verification of the printed trade business license. It aims to provide the verification mechanism and ensure the document validity. Our design implemented digital signature with QR Code image that placed into the document and the digital certificate issued by a certification authority (CA). The proposed scheme generated 442 Bytes of data and version 14 of QR Code to scan easily by a reader device. The experimental result indicates that our scheme is easy and feasible to implement in Indonesia with guaranteed the document integrity, authentication, and nonrepudiation.

Keywords*: digital signature, paper-based verification, QR code, trade business license*

1. Introduction

The trade business license (SIUP) is a paper-based license and the legality to carry out business activities. It issued by the government and given to businesses in the trade field. Each individual or business entity trade with small, medium or large-scale mandatory have the license issued and signed by the local government where the business is conducted. SIUP issued by a local government through official One Stop Services [1]. Until now, the government has no mechanism for verifying the validity of document unless involving official government employees to verify it traditionally. Consequently, the verification of printed trade business license is needed. The paper form is susceptible for forgery and needs an approach to verify the printed document and ensure its validity.

An approach to implement paper-based verification is by applying digital signature and QR Code. Digital signature is a data associates the message with some originating entity [2, 3]. One of the algorithms of the digital signature is digital signature algorithm (DSA) which has *O(n)* complexity [4]. DSA very much implemented such as attorney power [5] and letter of government [6]. QR Code patented by Denso [7] and so many implementations of QR Code such as for watermarking [8], it is flexible for any data type such as web address, text, etc [9].

Reference [10] introduced verification method where the user scans QR Code and gets the public key through the internet. In another word, internet connection required to verify the product validity. Reference [11] introduced an alternative of tracking product by scanning QR Code. It also required an internet connection to access product information from a server and to compare decrypted message with computed hash value. Reference [12-14] summarized that the hardcopy document can be verified by scanning the document. By scanning the printed document, an image generated and afterward extracted QR Code and document text using optical character recognition (OCR).

In this study, we proposed an approach by applying QR Code [7, 15], digital signature [16] with hash functions [17], and digital certificate to ensure the document integrity, authentication, and nonrepudiation. For verification purpose, we placed some information in QR Code and the user does not must have internet connection during verification process and

Received October 26, 2015; Revised August 9, 2016; Accepted August 28, 2016

doesn’t require any optical scanning device. This design is practically usable in Indonesia for paper-based verification of trade business license.

In general, we have learned that there are symmetric and asymmetric also hybrid cryptosystem [18]. In a public key (asymmetric) cryptosystem, the private key need be kept secret to prevent compromise the key. Further, the private key usually stored in the secret place and protected with other key such password, symmetric cryptosystem, smart card or radio frequency identification (RFID) [19]. In our prototype, we used password protection.

2. Proposed Design

Our proposed design contains signing scheme and verification. The signing scheme described as Figure 1.

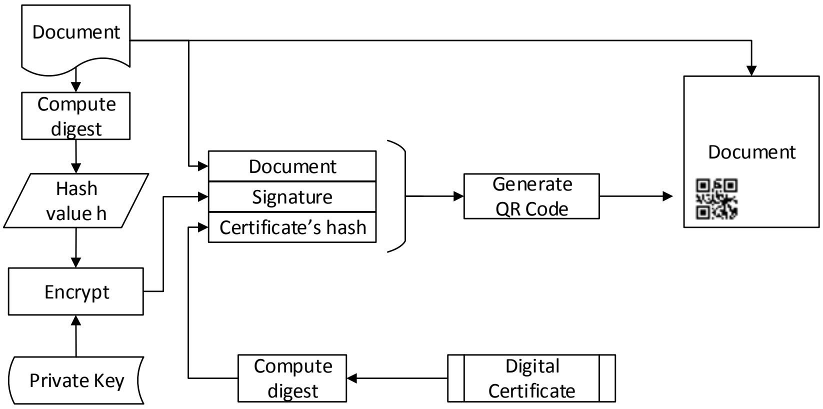


Figure 1. Proposed Signing Scheme

Based on Figure 1, head of One Stop Service as the document signatory gets the document fields contains several pieces of information (company name, company owner, address, etc) from trade business license input form. To separate one field to others, we applied abstract syntax notation (ASN.1) to format the document fields and for retrieving easily. The ASN.1 format for trade business license described as follows:

```
ASN1Siup ::= SEQUENCE{
    number UTF8String,
    companyName UTF8String,
    ownerName UTF8String,
    position UTF8String,
    address UTF8String,
    phone UTF8String,
    fax UTF8String,
    capital INTEGER,
    institutional UTF8String,
    businessCode UTF8String,
    date UTF8String,
    signatory UTF8String
}
```

The ASN.1 format above, there are 12 fields according to Trade Ministerial Regulation [1]. The digest of the formatted field computed using a hash function to ensure the document integrity. In this study, we implemented secure hash algorithm (SHA) 256 hash function. The hash value encrypted utilizing generated private key and resulted as a signature.

To ensure the public key ownership, we applied digital certificate issued by trusted third party (TTP). If the signatory does not have a valid digital certificate that binds signatory identity information with a public key, the signatory has to send certification signing request (CSR) to a trusted certification authority (CA). Furthermore, the certificate computed by the signatory using a hash function (we used SHA1) and generated a hash value of the certificate. There are three fields must be generated (document, signature, and a hash value of certificate) and collected into an ASN.1 format. The ASN.1 format for QR Code data described as follow:

```
ASN1QrData ::= SEQUENCE{
    siup ASN1Siup,
    siupSignature OCTET STRING
    signatoryCertDigest OCTET STRING
}
```

The signature value stored as octet string also the digest value of the digital certificate. The ASN1QrData encoded into base64 encoding for scanning easily and stored to QR Code generator. All data prepared and ready to generate QR Code image. The generated image will be put to the prepared template that covered all required data field of trade business license. The document is ready to be printed and given to an individual or organization.

The printed document needs to be verified to ensure document validity. Based on signing process, a verifier could verify document by scanning QR code of the printed document. To verify the printed trade business license, a verifier must have an application implemented the verification scheme on Figure 2 and a QR Code scanner. Considered a verifier scans the QR Code of printed document and afterward a verifier extracts there fields carried in the QR Code (document, signature and hash of certificate). This information will be used to verify the printed document. The hash value of certificate verified by computing the hash value of the digital certificate and compared them. If the hash values are equal, then the digital certificate is valid.

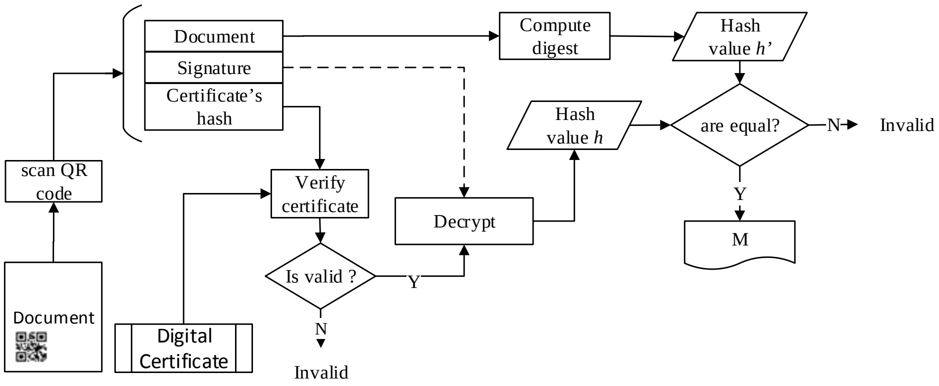


Figure 2. Proposed Verification Scheme

The digital certificate also verified (subject, issuer, valid date, revoked status, etc) to ensure the authentication. Afterward, the digital signature decrypted using a public key of the validated digital certificate and produced hash value *h*. The document fields computed using a hash function and produced hash value *h'*. Afterward, *h* and *h'* compared, if they are equals then document fields are valid, otherwise invalid. If document fields are valid, a verifier got the information of document fields from a screen of the application. By getting document fields, a verifier decided the document validity by comparing the printed document and the verified document.

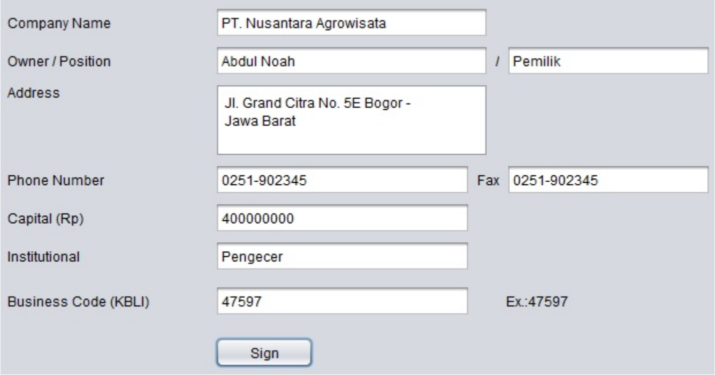
3. Experimental Result

In this paper, we implemented the schemes according to proposed signing and verification process above. The software developed as a desktop application utilizing Java to implement digital signature and QR Code. This experimental used the digital signature algorithm (DSA) with parameters *p*=2048 bits and *q*=256 bits. Thus, the hash function is SHA-256. Google

ZXing library provided QR Code process such as creation and reading QR Code with specific options. Apache PdfBox was used to generate and manipulate pdf also embed QR Code to the license document.

The prototype provided the digital certificates that generated three levels chain of trust namely root, intermediate CA, and user. In the real world, the digital certificate of the signatory issued by trusted CA. In Indonesia, the national root CA is Ministry of Communication and Informatics. The signatory of trade business license is individual of the official local government. Therefore, the digital certificate should be issued by legal CA under center government. This certification aims to ensure the authentication of the signature and the public key.

On Figure 3, we created the input form and filled data then processed for signing procedure. There are nine inputs of the form namely the company name, owner of the company, office position, address, phone number, fax number, capital (Indonesian currency), institutional, and business code. All filled data will be completed with more three fields namely the document signatory, valid date, and license number. Then, the completed field formatted into ASN.1 as described above. After obtaining the formatted document fields, the digital signature generated using DSA and SHA-256. A signatory also generates the hash value of digital certificate issued by CA using SHA1.



Company Name	PT. Nusantara Agrowisata		
Owner / Position	Abdul Noah	/	Pemilik
Address	Jl. Grand Citra No. 5E Bogor - Jawa Barat		
Phone Number	0251-902345	Fax	0251-902345
Capital (Rp)	400000000		
Institutional	Pengecer		
Business Code (KBLI)	47597		Ex.:47597

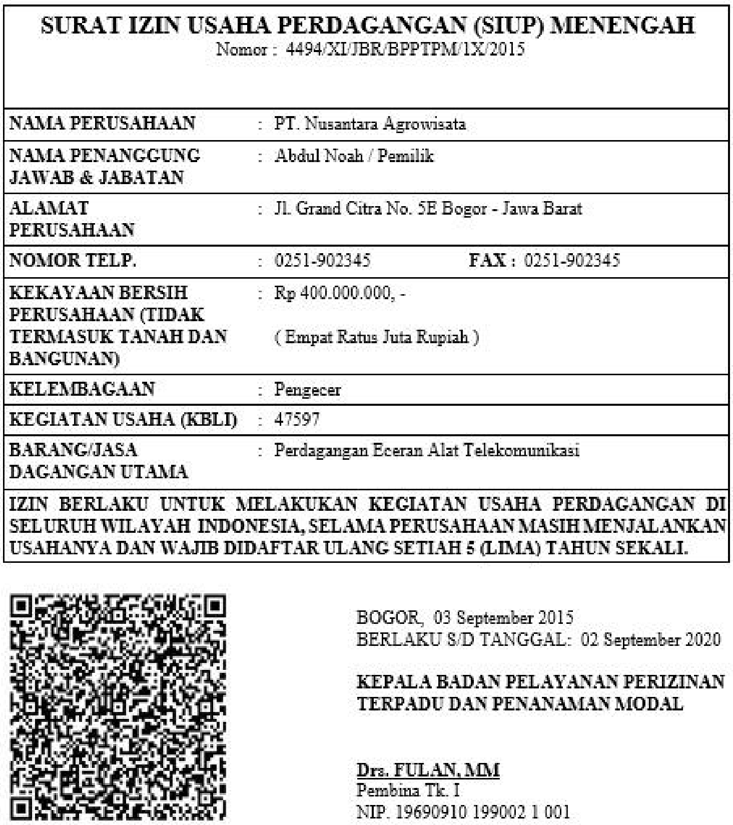
Figure 3. Prototype of Input Form

The result of ASN1QrData:

```
Sequence
   UTF8String(4494/XI/JBR/BPPTPM/1X/2015)
   UTF8String(PT. Nusantara Agrowisata)
   UTF8String(Abdul Noah)
   UTF8String(Pemilik)
   UTF8String(Jl. Grand Citra No. 5E Bogor - Jawa Barat)
   UTF8String(0251-902345)
   UTF8String(0251-902345)
   Integer(400000000)
   UTF8String(Pengecer)
   UTF8String(47597)
   UTF8String(2015-09-03)
   UTF8String(Drs. Fulan, MM)
DER Octet String[70]
DER Octet String[20]
```

The formatted document field, signature, and hash value of the certificate are formatted into base64 encoding. This aims to encode easily by QR Code generator and by the scanner / reader. The formatted base64 stored in and generated a QR Code using ZXing library. In this prototype also prepared document template of the trade business license in PDF format. This template will be completed with document fields, afterward the QR Code image embedded in the PDF document and finally the document is ready to be printed.

The result of the printed Indonesia's trade business license described as Figure 4.



SURAT IZIN USAHA PERDAGANGAN (SIUP) MENENGAH
Nomor : 4494/XI/JBR/BPPTPM/1X/2015

NAMA PERUSAHAAN	: PT. Nusantara Agrowisata
NAMA PENANGGUNG JAWAB & JABATAN	: Abdul Noah / Pemilik
ALAMAT PERUSAHAAN	: Jl. Grand Citra No. 5E Bogor - Jawa Barat
NOMOR TELP.	: 0251-902345 **FAX :** 0251-902345
KEKAYAAN BERSIH PERUSAHAAN (TIDAK TERMASUK TANAH DAN BANGUNAN)	: Rp 400.000.000, - (Empat Ratus Juta Rupiah)
KELEMBAGAAN	: Pengecer
KEGIATAN USAHA (KBLI)	: 47597
BARANG/JASA DAGANGAN UTAMA	: Perdagangan Eceran Alat Telekomunikasi

IZIN BERLAKU UNTUK MELAKUKAN KEGIATAN USAHA PERDAGANGAN DI SELURUH WILAYAH INDONESIA, SELAMA PERUSAHAAN MASIH MENJALANKAN USAHANYA DAN WAJIB DIDAFTAR ULANG SETIAH 5 (LIMA) TAHUN SEKALI.

BOGOR, 03 September 2015
BERLAKU S/D TANGGAL: 02 September 2020

KEPALA BADAN PELAYANAN PERIZINAN
TERPADU DAN PENANAMAN MODAL

Drs. FULAN, MM
Pembina Tk. I
NIP. 19690910 199002 1 001

Figure 4. Prototype of Printed Trade Business License

Figure 4 shows that the printed document contains all the document fields. Therefore, a verifier can verify easily by scanning the printed QR Code using an application implemented verification scheme. A verifier scanned the QR Code and decoded the formatted data then extracted into three important information namely signature, formatted document fields, and a hash of the certificate. Then, the hash of certificate verified by comparing hash value computed from application's certificate using SHA1. If they are equal, then the digital certificate is verified. The digital signature verified utilizing the public key of verified certificate. If the digital signature is verified, then the document fields on QR Code are verified.

The verified document displayed by application and lets the verifier decides and compares between printed document and verified QR Code. The document fields compared such as a number of license, company name, address, business code, date, etc. If found the unmatched printed field, a verifier decides that the printed document is invalid.

Table 1 shows the size and version of QR Code in several different document. It shows that the data size stored in QR Code is 442 Bytes and the version of QR Code is 14 in maximum. It proves that the generated QR Code image can be placed into the document with size 250x250 pixels for scanning easily. Verification process runs as expected and the QR Code data decoded properly. It is because the QR Code has an error correction that can restore up to 30% of damaged data.

Table 1. The Result of Document Signing

Documents	QR Code Result	
	Data Size (Bytes)	Version
Document 01	312	11
Document 02	350	12
Document 03	298	11
Document 04	380	13
Document 05	342	12
Document 06	442	14
Document 07	311	11
Document 08	410	13
Document 09	390	13
Document 10	438	14

4. Comparison to Previous Scheme

In this section, we compared our proposed scheme with the prior scheme in the light of QR Code content, verification requirement, and cryptography guarantee. According to Table 2, our scheme more effective and usable for trade business license in Indonesia. In our prototype, we have tested to input several data of trade business license. Furthermore, QR Code image generated under version 15. It indicates that QR Code content in our scheme is applicable for paper-based verification.

Table 2. Comparison to Previous Scheme

	Reference [12]	Reference [14]	Reference [11]	Our scheme
QR Code content	Hash value of the document	Compressed message and digital signature	Link and digital signature	Business trade license, digital signature, hash value of the digital certificate
Verification requirement	QR Code and OCR scanner	QR Code and OCR scanner	Internet connection to access the server	QR Code and digital certificate
Cryptography guarantee	Integrity	Integrity, authentication, nonrepudiation	Integrity, authentication, nonrepudiation	Integrity, authentication, nonrepudiation

In the verification process, required a digital certificate to ensure integrity, authentication, and nonrepudiation. The verification also required a QR Code scanner or an application implemented QR Code and a digital certificate. Is does not require OCR scanning or internet connection to verify the document. Thus, this scheme is effective and feasible to implement in Indonesia.

5. Conclusion

Paper-based verification design of trade business license is easy and feasible to implement in Indonesia. The scheme of signing and verification can ensure the integrity of a document, authentication, and nonrepudiation. Since the license is signed by a head of One Stop Service, a document signatory cannot deny that the document has signed. Anyone can verify the document and this scheme ensure the authentication of the signatory and the ownership of the trade business license.

References

[1] Regulation of Minister Trade of The Republic of Indonesia Number 36/M-DAG/PER/9/2007 about Publishing Trade Business License. 2007.

[2] Menezes A, Oorschot P Van, Vanstone S. Handbook of Applied Cryptography. CRC Press, Inc. 1996.

[3] Schneier B. Applied Cryptography: Protocols, Algorithms, and Source Code in C. 2nd ed. New York, USA: John Wiley & Sons. 1996.

[4] Situmorang K. Security and Performance Analysis Algorithm Digital Signature Algorithm (DSA) on the Formation Process and Verification of Digital Signatures. Undergraduate Thesis: Bogor Agricultural University; 2006

[5] Sholihah W. Electronic Power of Attorney Protocol by Using Digital Signature Algorithm. Graduate Thesis: Bogor Agricultural University; 2013.

[6] Somad WA. Online Digital Signature System for Official Letter using DSA (Digital Signature Algorithm) Algorithm. Undergraduate Thesis: Bogor Agricultural University; 2013.

[7] ISO/IEC 18004. Information Technology - Automatic Identification and Data Capture Technique - QR Code 2005 Barcode Symbolic. 2005.

[8] Cho DJ. *Study on Method of New Digital Watermark Generation Using QR-Code*. Eighth Int Conf Broadband Wirel Comput Commun Appl. 2013: 585-588.

[9] Narayanan AS. QR Codes and Security Solutions. *Int J Comput Sci Telecommun*. 2012; 3(7): 1-4.

[10] Seino K, Kuwabara S, Mikami S, Takahashi Y, Yoshikawa M, Narumi H, et al. *Development of the traceability system which secures the safety of fishery products using the QR code and a digital signature*. Ocean '04 MTS/IEEE Techno-Ocean. 2004.

[11] Melgar MEV, Santander LAM. *An alternative proposal of tracking products using digital signatures and QR codes*. IEEE Colomb Conf Commun Comput, IEEE. 2014: 1-4.

[12] Salleh M, Yew T. Application of 2D Barcode in Hardcopy Document Verification System. *Adv Inf Secur Assur*. 2009; 5576: 644-651

[13] Eldefrawy MH, Alghathbar K, Khan MK. *Hardcopy Document Authentication Based on Public Key Encryption and 2D Barcodes.* Int Symp Biometrics Secur Technol, IEEE. 2012: 77-81

[14] Warasart M, Kuacharoen P. *Paper-based Document Authentication using Digital Signature and QR Code*. 4th Int Conf Comput Eng Technol. 2012; 40: 94-98.

[15] Denso. QR Code Essentials. 2011: 1-12.

[16] National Institute of Standards and Technology. Digital Signature Standard (DSS). FIPS-PUB.2013: 186-184.

[17] National Institute of Standards and Technology. Secure Hash Standard (SHS). FIPS- PUB. 2012: 180-184.

[18] Mantoro T, Zakariya A. Securing E-Mail Communication Using Hybrid Cryptosystem on Android-based Mobile Devices. *TELKOMNIKA Telecommunication Computing Electronics and Control*. 2012; 10(4): 807-814.

[19] Naser M, Aldmour I, Budiarto R, Peris-lopez P. SLRV : An RFID Mutual Authentication Protocol Conforming to EPC Generation-2 Standard. *TELKOMNIKA Telecommunication Computing Electronics and Control*. 2015; 13(3): 1054-1061