Digital Signing Using National Identity as a Mobile ID

Emir Husni
School of Electrical Engineering & Informatics
Institut Teknologi Bandung
Bandung, Indonesia
ehusni@lskk.ee.itb.ac.id

***Abstract*— Today's implementation of digital signature consist of uniquely generated key connected with someone's digital identity (certificate). However, the current implementation of digital signature may present problem in official agreement, which needs legitimate identity information and needs to involve notary. This paper covers the method of digital signature creation which mimic physical signature in official agreement, and helps involve party being able to work with digital documents as well as working with physical documents. Using cloud computing approach, and mobile devices, we integrate signing service to user's national identity.**

Keywords— Digital Signature, Digital Certificate, Digital Documents, Notary, Electronic Legal Document component

I. INTRODUCTION

Today implementation of digital signature has consisted of uniquely generated key connected with someone's digital identity (certificate). This type of digital signature might not valid for cases which need higher trust requirement. An agreement regulated by government law needs to involve notary and official identity card of all parties.

This paper covers the method of digital signature creation which mimic physical signature in official agreement, and helps involve party being able to work with digital documents as well as working with physical documents.

II. BACKGROUND

Grow by needs of environmentally-friendly paperless document and faster document delivery push the adoption of digital documents. Popular digital document format has made an effort to produce a document which can be used in digital as well as in physical form. Digital form of signature also exists in order to guarantee a seamless transition from physical to digital document. However, the current implementation of digital signature may present problems with a document which needs legitimate identity information.

In official documents, especially which involved government, signature is often attached with identity information. The reason is that the identity information is becoming the fact of our identity guaranteed by government. Today's digital signature will not consider identity information in the key creation. Other parties cannot ensure the identity of the signer by only mean of the digital signature verification using certificates. Lack of integration between digital signatures and signer identity makes the digital signature position is weak in official agreement.

The signing process in official agreement also needs to involve notary, as stated by law. The notary is a party which does not involve in negotiation between two or more parties. The notary is appointed by government by having a license legalizing an agreement. By having notary in the signing process, the agreement has a strong position in law. This is important in case the conflicts exist in the future and this ensures secure position in present time.

III. SIGNING CLOUD DESIGN

A. Signing Cloud Definition

The National Institute of Standards and Technology (NIST) [1] define cloud computing as computing resources available through network access that can be used with minimal effort. The cloud computing usage model is a service which can be differ as Infrastructure as a Service (IaaS), Platform as a service (PaaS), and Software as a Service (SaaS).

Digital signature as a cloud service goal is that customers could integrate with their existing system (e.g. e-commerce, medical, or government) with ease and available on-demand. Using Application Programming Interface (API) and standard network protocol, the service can be used by the broad choice of client platforms.

The digital signature is a method to authenticate a message. Much like physical signature, digital signature, in document imply that the signer agrees with the content of a document. A digital signature has a property of source authentication, integrity, and non-repudiation. It is achieved by computing a hash value and encrypted it using asymmetric encryption. The hash value computed using message as input to a fixed length hash function. This hash value is then encrypted using a sender private key to produce digital signatures. In order to verify sender message, the receiver computes the hash value of the message. The sender also decrypts the digital signature using sender public key. Valid message would produce a match value of the decrypted message and hash.

The public key in X.509 standard has already contained key's owner information in the subject field. This information guaranteed by certificate authority private key. This way, we can identify who has a private key used to create digital signatures. However, it does not prove if the private key used by a person stated in the key owner information.

978-1-5090-1709-6/16/$31.00 ©2016 IEEE

Mobile ID is our implementation of signing service using mobile device and national identity card information. Design of signing cloud service is based on method explained by Kinastowski [2]. The mobile ID cloud model is Software as a service.

B. System Architecture

Mobile ID consists of infrastructure, customer and user. The system architecture is illustrated in Fig. 1. Infrastructure is the providers of signature services; user is an entity which has an identity; and customers are entities using user identity.

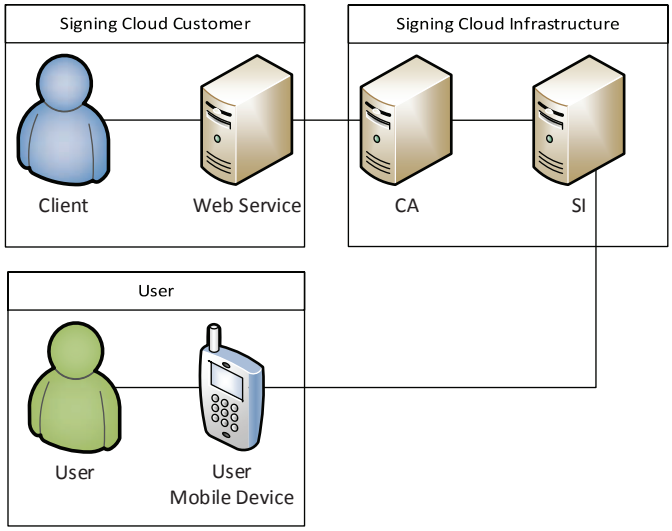


Fig. 1. Mobile ID System Architecture

Signing cloud infrastructure performs reliable signing service in a cloud environment. Signing cloud designed as a separate module. It can be deployed on one server with different port or different server. Access to infrastructure is done using the API in HTTP protocol.

Certificate authority (CA) provides user identity information and public key when needed. CA manages registration process and stores the information securely in a database. When needed, CA retrieves information from the database to be sent to the applicant. CA is also bridging communication between Web services and SI.

Signing Interface (SI) provides secure creation, storage and access of user private key. SI also performs the signing operation. The user private key is stored in encrypted form using a user PIN.

Cloud signing customer is a web service. The client is defined as someone who needs user identity. The client is using web service to initiate a signing cloud request and later receive result in web service. Web service runs on a web server and accessible to the customer and CA.

A user is someone who has an identity. The user communicates to cloud signing infrastructure using a mobile device. When there are requests to the user identity, the purpose of request will be displayed and then the user will have the option to accept or reject the request. The mobile device performs authentication of users.

The signing operation uses encryption algorithm. Factors to be considered in encryption are mainly whether the algorithm has known vulnerability, and key length which are considered as safe factors. The encryption scheme used here can be seen in Table 1.

TABLE I. ENCRYPTION SCHEME

Purpose	Algorithm
Network Protocol	HTTPS using TLS
Hash	SHA-256
HMAC	SHA-256
Asymmetric Key Pair	RSA-2048
Key Storage	AES-256

IV. SIGNING CLOUD OPERATION

In order to understand how Mobile ID is being used, functions can be separated into 3 categories: registration, basic function and main function. Registration is needed to input user information and key pair on signing cloud. The basic function is used as a building block for the main function.

A. Registration

The registration process is an important step in the signing cloud operation. It must ensure that the information in identity card is correct and legitimate. The entity that is registered must have access to government records of people's IDs.

To register, firstly user must show their identity card, then their mobile device will push an address retrieved from the mobile device application. The user will also supply PIN to SI securely using encryption key sent by push messages. After the user was registered, some files are generated. They are as follows.

1) User identity's information is stored in CA and user's device.
2) User private key is stored in SI.
3) User public key is stored in CA.

B. Basic Function

Confirmation process sends challenge to the user device to make sure that the user approves the request. The data sent are the information to be processed in SI and the user device. By replacing data with user information saved in CA and the user device, the system can use this process to verify the user information. The steps are done as follows.

1) Client initiates a request to the CA through the web service.
2) CA sends data to SI.
3) SI sends data and one time password (OTP) to the user device using Google Cloud Messaging (GCM).
4) The user receives a notification and then chooses whether to decline or accept the request by entering the PIN. Using provided OTP from SI, the user generates and sends hash where:

$$h_{data} = HMAC_{OTP}(data)$$

All data sent using HTTP secure (HTTPS).

$$Sentdata = HTTPS(h_{data} + PIN)$$

5) SI restore and compares the received information from the user device and doing calculations of HMAC.

$$h_{data} == HMAC_{OTP}(data)$$

6) SI sends the verification result to CA. If the function needs data to be signed, the step continues in the signing process. If it only needs user confirmation, CA sends the result to the client through the web service.

A signing process runs digital signature creation. The signing steps are done as follows:

1) CA sends the data to be signed to SI.
2) SI modifies data, to include signer id number and time.
3) SI accesses user private key using provided PIN in the confirmation step.

$$k_{user}^{prv} = Sym_{PIN}^{dec}(\hat{k}_{user}^{prv})$$

4) SI generates signature using user's private key.

$$data_{sign} = Sign_{k_{user}^{prv}}(data)$$

5) SI sends the signature to CA.
6) CA sends the signature to client through web service.

C. Main Function

Main function extends the basic function to provide the Mobile ID service to the client. Not only for signing process, this operation can also be used for another process which needs user's authentication in web applications. The main function consists of login, identity check, data signing and document signing. These functions are combined to be used in the cloud signing web application. The method detail about each function explains below. (Bold words indicate another function being called)

- Identity check, a function is to send identity to another person as a client for the identification or verification process. Before begin the client needs a user ID number by seeing ID card physically or using another medium. Identity check steps illustrated in Fig. 2.

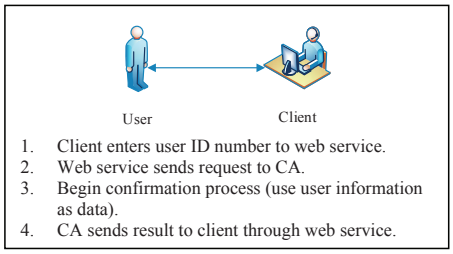


Fig. 2. Identity Check Steps

- Web login, a function to identify person in order to use specific website which require official id information. Web login steps illustrated in Fig. 3.

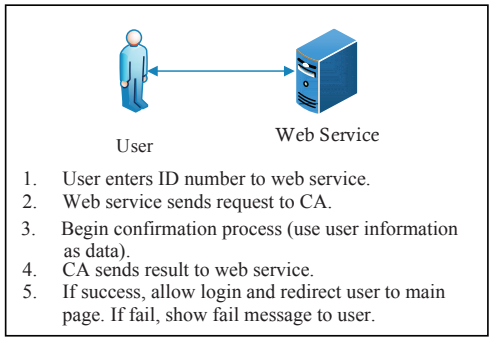


Fig. 3. Web Login Steps

- Data signing, a function to generate user signatures from simple data, such as a string generated by a web service. Data signing steps illustrated in Fig. 4.

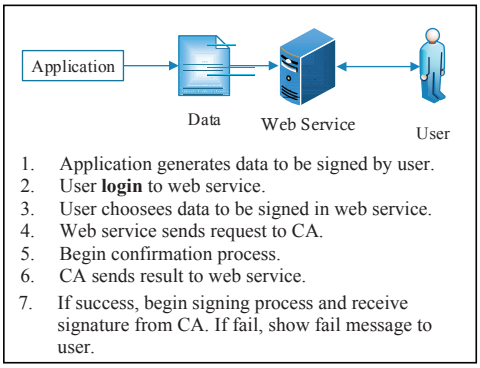


Fig. 4. Data Signing Steps

- Document signing, a function to generate user signatures from providing data. We define document format as Adobe® PDF. Document signature creation involving one client (as a notary) and at least one user. Document signing steps illustrated in Fig. 5.

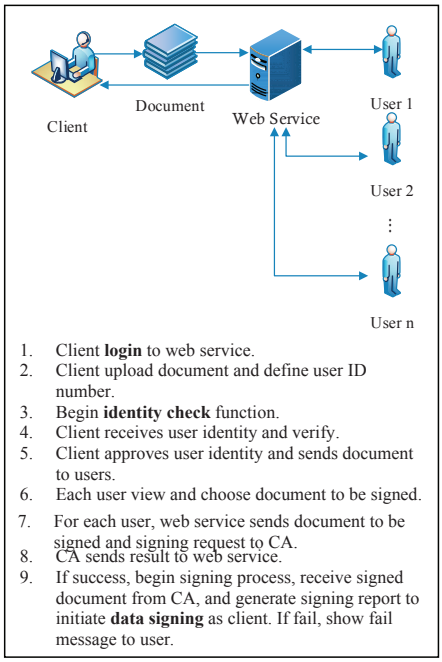
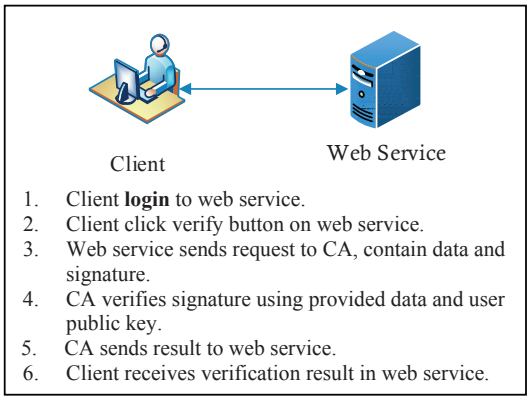


Fig. 5. Document Signing Steps

- Signature verification, a function to verify digital signatures and signature identity. Signature verification steps illustrated in Fig. 6.



1. Client **login** to web service.
2. Client click verify button on web service.
3. Web service sends request to CA, contain data and signature.
4. CA verifies signature using provided data and user public key.
5. CA sends result to web service.
6. Client receives verification result in web service.

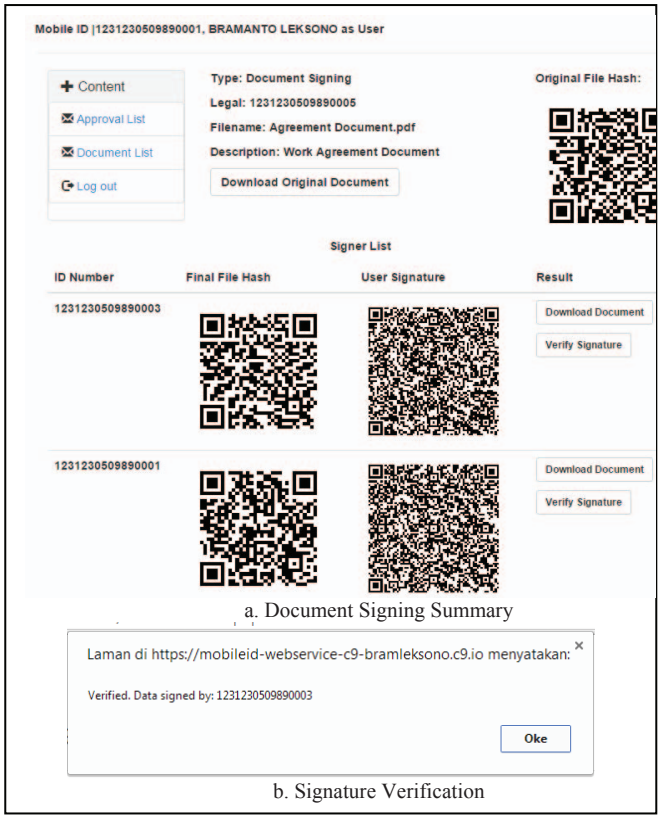
Fig. 6. Signature Verification Steps

V. Implementation

Mobile ID application consists of a web application and mobile application. The web application was built using.

- Apache web server.
- PHP programming.
- PostgreSQL database.
- OpenSSL cryptography library.

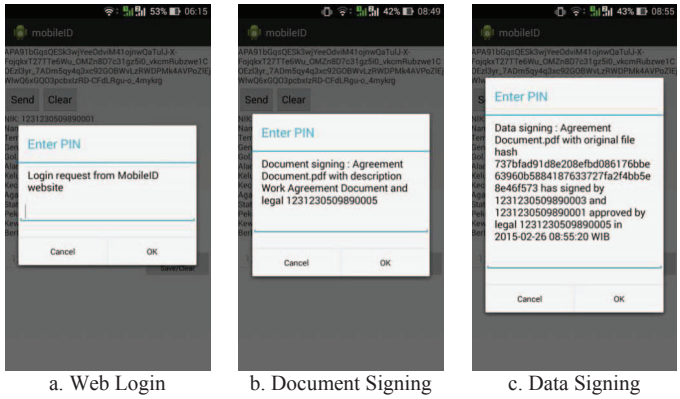
For mobile application, it was built using Google Android SDK version 19 and Google Play Services.



a. Document Signing Summary

b. Signature Verification

Fig. 7. Web Service Application Results



a. Web Login b. Document Signing c. Data Signing

Fig. 8. Mobile Device Messages

Figs. 7-8 show web service application results and mobile device messages respectively. Using Mobile ID, the action of a user (login, signing, and verification) in a web application can be associated with national identity. In contrast, username and password authentication method has no direct correlation between user records and user identity. It can assume that the mentioned user did the action based on other factors such as time, IP address, and other associated data.

Mobile ID is also effective in the signing process which needing the notary involvement. The notary can verify signer identity, monitor signing progress (whether a document has been signed by an individual user), save signing process results, and verify signed document in the future.

The Mobile ID application is modular and it communicates using HTTP API. Therefore, it can be expanded into different purposes without much effort. The other web service can use the same cloud signing infrastructure or host their private signing infrastructure by using the same API request.

VI. Conclusion

Mobile ID results show cloud signing concept has been built as expected. In addition, the advantages of Mobile ID are:

- Integrate web application user to national identity.
- Involve notary in digital document signing.
- Easy to integrate to other purpose.

References

[1] P. M. Mell and T. Grance, “SP 800-145. The NIST Definition of Cloud Computing,” National Institute of Standards & Technology, Gaithersburg, MD, United States, 2011.

[2] W. Kinastowski, “Signing Cloud: Towards Qualified Electronic Signature Service in Cloud,” in 2013 IEEE 5th International Conference on Cloud Computing Technology and Science (CloudCom), 2013, vol. 2, pp. 224–227.

[3] E. B. Barker, W. C. Barker, W. E. Burr, W. T. Polk, and M. E. Smid, “SP 800-57. Recommendation for Key Management, Part 1: General (Revision 3),” National Institute of Standards & Technology, Gaithersburg, MD, United States, 2012.

[4] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 5 edition. Boston: Prentice Hall, 2010.

[5] J. A. Buchmann, E. Karatsiolis, and A. Wiesmaier, *Introduction to Public Key Infrastructures*. Springer Science & Business Media, 2013.