Secure Data Access Method based on electronic identity for Mobile Internet

Minghui Yang\textsuperscript{1,2}, Lijuan Xia\textsuperscript{1,2}

\textsuperscript{1}The Third Research Institute of Ministry of Public Security, Shanghai, Shanghai, 201204, China
\textsuperscript{2}Key Lab of Information Network Security, Ministry of Public Security, Shanghai, Shanghai, 201204, Country
\textsuperscript{*}Corresponding author’s e-mail: yangminghui@163.com

Abstract. Network electronic Identity is convenient and secure for citizens’ online remote authentication. With the rapid development of Mobile Internet, the pervasive use of mobile devices brings new security and privacy risks. Electronic identity will have a wider application space on the mobile Internet. This paper introduces a remote secure storage protocol as the technology of electronic Identity security function using NFC-enabled mobile devices. This protocol is security and globally accessible so as to provide strong privacy protection and key management performance, which will bring new development opportunities for application developers.

1. Introduction
With the rapid development of mobile network technology, mobile devices, such as smart phones, Pads, or other tablet computers, play an increasingly important role in people’s daily life \cite{1}. Although many mobile devices’ apps provide convenient solutions, and use mobile devices as a secure authentication channel, the leaking of users’ identities and sensitive data become more and more serious.

Electronic identity technology was introduced to China in 2010. Chinese citizens may use electronic identity in the network as remote digital identity certificates. The electronic Identity constitute a big opportunities for the government, the public, service providers and application developers \cite{2,3}. Mobile devices clearly offer a compelling proposition for governments seeking to provide citizens with secure and convenient access to online public services. During the past years, numerous mobile eID and e-signature solutions have been proposed, tested, and deployed in various European countries \cite{4-8}.

In this paper we look for a new way to use electronic identity and mobile devices to accomplish the secure electronic authentication, aiming to solve the defects of privacy. A service is defined to allow users to securely store and update their data (such as the password, key, accounts, etc.) remotely. Electronic identity cards can be used at any time to access the service. Also, the data on the server are invalid to both internal and external attackers.

2. Electronic identity technology
Electronic identity cards are the smart cards according to smartcard standards (such as ISO/IEC 14443 and GB/T 16649, etc.), which citizens can verify their self-online remotely, and achieve actual and
digital identity certification. There are identity documents in electronic identity cards, which contain the hash value of the basic identity information and personal information certificates. These certificates are signed by the Ministry of Public Security Citizen network Identification System (MCIS). The electronic identity card is secure and the access to the private key is protected with a secret PIN.

The private key $SK_{Auth}$ for certification is stored in the tamper-proof portion of the chip in electronic identity cards, which can only be activated by the PIN code. The corresponding $PK_{Auth}$ is authorized by the same certificate. Each certificate also holds the cardholder's name and a unique identification number named eID_code.

A software kit (SDK) is developed to set up the interaction between the electronic identity card and the mobile devices. SDK contains a graphical interface that allows users to read documents and certificates stored in their electronic identity cards, even to change the PIN. SDK also serves as an intermediary for other applications to access to electronic identity cards. When certificating documents, SDK will transfer the hash value of authentication information to the electronic identity card. When applications use the electronic identity card to authenticate a document, SDK will ask the user for the PIN code and send it forward to the electronic identity card. SDK can also check the validity of the certificate using CRL or OCSP. Note that the SDK is not necessary and applications can achieve the same function and interact directly with the electronic identity card.

Certificates in electronic identity cards have a layered infrastructure. Certificates for signature and certification are issued by citizen CA, and the certificates of citizen CA are issued by the root CA on the top of layers. CRL is defined which contains the revoked certificate serial numbers.

3. Symbol
The following are symbols using in this paper:

- $P_1 \leftrightarrow P_2 : \text{eID\_code} \leftarrow \text{authenticate\_eID\(_1\)}()$: An interactive protocol, which $P_1$ authenticates $P_2$ with $SK_{Auth}$ then gets the eID\_code of $P_2$;
- $P: \text{sig} \leftarrow \text{sign\_eID\(_1\)}(\text{hash}(M))$: Users sign information $M$ with the key $SK_{Sig}$ and send its hash value;
- $P: K \leftarrow \text{createSymmetricKey}($PRG$, seed$): A pair of keys $K$ are created by users using a random number generator PRG and a seed seed. The same PRG and the seed seed bring the same $K$.
- $P: \text{store(data; index)}$: Data data are stored at index index in the database.

4. Sensitive data access protocol
Information Society is full of sensitive data access from different locations. Sensitive data (such as personal information, bank accounting, etc.) must be securely stored on a remote server accessible, so protecting the sensitive data safety is the basic function of sharing sensitive information resource. Before being stored on the server, data are encrypted by the owner. Encrypted data are of no use both to the server or any attacker. This section discusses the electronic identity-based secure storage mode of sensitive data via NFC-enabled or Bluetooth-enabled mobile devices. For example, user places mobile devices on NFC reader and enters secret PIN at PIN-card terminal (or on the phone). Server reads all necessary information from the user's mobile devices/ID card (via NFC/Internet connection).

The most direct solution is to use the public key of the certificate to encrypt data and use the corresponding private key to decrypt data. However, encryption and decryption using the electronic identity card is not possible. When the card is lost, encrypted information earlier cannot be decrypted at present. Therefore, this paper proposes a new solution using the electronic identity card as a starting program. The symmetric key is generated from the electronic identity card signature, which is used to encrypt the data before storing. When the user wants to restore its encrypted information, access to encrypted information from the server, decrypt, regenerate the same data using electronic identity card. The following will detail the protocol about how to store and recover sensitive data.
4.1. Storage Protocol

Figure 1 shows the steps of sensitive data storage protocol. Electronic identity users (U) provide the data they wish to store and a private tag as the name or alias of the data, that is \texttt{storeSensitiveData(data,tag)}.

The steps are as follow:

1. Message header is generated with the `KEYGEN`, \texttt{eID_code}, electronic identity card number and other specific user information. The hash value $H_{\text{keyGen}}$ of fixed format message is calculated using the SDK.

2. Sign $H_{\text{keyGen}}$ with the signature key in electronic identity card to get a 1024/2048-bit signature $\text{sig}$. Fixed format message can prevent an attacker using forged requesting signatures to get $\text{sig}$. In addition to this protocol, any message signed by the electronic identity card is not conform to this format. Usually, $\text{sig}$ is the seed to generate two symmetric keys $K_S$ and $K_D$.

3. - (4) In order to generate the same key regardless of platform, a special pseudo-random number generator PRG is called in \texttt{createSymmetricKey} function. As the same time, the hash function is also fixed. $K_S$ is used to encrypt the private tag that associated with data and $K_D$ is used to encrypt the data. The key is passed by the hash value of $\text{sig}$. Encrypted tag $E_{\text{tag}}$ is used in step 10 which transfers index to the server database.

4. When the data is stored (i.e. calling the protocol), a new random number $R$ is generated to associated with it.

5. The encryption key $K_D$ is transferred via the hash value of $R$ and $\text{sig}$.

6. The data is encrypted and the cipher text is $E_{\text{data}}$. In order to prevent the accession between the same encrypt data in different positions, each time calling the \texttt{storeSensitiveData} function will use a new key to encrypt data.

7. Encrypted data $E_{\text{data}}$ are stored in remote server $S$. Only the electronic identity card owner $U$ can restore his data after $U$ achieves identity authentication through the electronic identity card.

8. $U$ sends encrypted tag $E_{\text{tag}}$ and ciphertext $E_{\text{data}}$ to remote server $S$. 

![Figure 1. Protocol of remote sensitive data storage.](image-url)
(10) Server $S$ calculates the hash value of $E_{tag}$ and $eID\_code$ together as the index where $E_{data}$ will be stored in the database. $NRN$ will be public during the identity authentication. For different $E_{tag}$ will generate different $index$, $index$ is specific. In another words, using encrypted tag $E_{tag}$ can protect the privacy of $U$. If $S$ is credible and $eID\_code$ and $E_{tag}$ are not stored, $index$ is safe from exponent attack. Even if the attacker can access all database, the users’ data cannot be visited.

(11) Encrypted data and the random number $R$ are both stored at index in the database. $R$ is necessary for the data owner to transmit the key to decrypt $E_{data}$.

(12) $U$ receives a receipt from the server to prove that the encrypted data is stored well.

4.2. Restoration Protocol
When the sensitive data is stored on a remote server, it can be restored from any location by the owner. Figure 2 shows the restoration process.

1. Regenerate hash value $H_{keyGen}$.
2. Sign $H_{keyGen}$ with electronic identity card.
3. Regenerate key $K_S$ with $sig$.
4. Private tag is encrypted by $K_S$.
5. User is authenticated with the electronic identity card.
6. Send encrypted tag $E_{tag}$ to the remote server $S$ and request the corresponding records.
7. The record consists of encrypted data and the random number. The database on $S$ selects the matched records at the index $index$ and sends the records to the data owner $U$.
8. $U$ gets specific key $K_D$ from the hash value of $sig$ and $R$.
9. $U$ uses $K_D$ to decrypt $E_{data}$.

![Figure 2. Restore the encrypted data remotely.](image)

4.3. Restoration of key
The proposed solution takes the advantage of the property that the determinate signature is calculated in the electronic identity card. When a signature is created with electronic identity card, the same $H_{keyGen}$ always get the same signature $sig$. Thus, the same PRG and the same hash function($hash_A,\ldots,hash_D$) will regenerate the same keys $K_S$ and $K_D$ regard to the same random number.
If the electronic identity card is lost or updated, $PK_{Sig}$, $SK_{Sig}$ and card number will be changed. In this condition, a different $sig^*$ is gained instead of $sig$, which prevent the stored message to be localized and decrypted. To protect important data, it will create a security backup when the signature $sig$ is generated at the first time. In case that the electronic identity card is lost or updated, the signature $sig$ is stored repeatedly from the backup, and the key is also can be restored. The guaranteed backup is provided by the third-party key services.

5. Analysis and conclusions
The discussed extended safety function above indicates the new opportunities of electronic identity technology. The electronic identity card not only can be used for digital signatures and authentication, but also can be used to store and recover sensitive data. Users can simply use the electronic identity card via NFC-enabled mobile devices to access the encrypted data stored at the remote server. However, the attacker still can send continuous defiant information to the electronic identity card in order to get the key. To avoid this threat, the signature in the electronic identity card is used in this given solution. PIN code is required for each signature, but authenticate key only need PIN code once. In addition, the fixed format of the message is also can prevent Trojans or malicious applications that request user's signature.

To support the recovery of sensitive data when the electronic identity card is lost or updated, a secure backup is created as signature $sig$ is generated at the first time. However, users still have to be responsible for security backup. Another method is to set a key escrow system. Using secret sharing algorithm separates signature $sig$ into $n$ parts. Each part is stored on a different hosting server. To rebuild confidential content, it is necessary to get $n$ parts from the hosting server and combine them to the complete data. In order to make sure that users only get their own key, these hosting servers will get to verify through electronic identity card. Further, the hash value of eID_code and electronic identity card serial number could add to the head of confidentiality contents. And every citizen can inquiry his current and previous electronic identity card number from the registration or management of electronic identity online.

This paper reveals the extended and reusable technology of electronic identity card with which users can access remote storage service securely at anywhere and manage their sensitive data securely, also brings new development opportunities for application developers.

Acknowledgments
This work is supported by the National Key Research and Development Program of China under Grant 2017YFB0802302, in part by the project of 2014EG153068 and in part by Shanghai Excellent Technology Leader Fund 16XD1420200.

References
[1] China Internet Network Information Centre (2019). The 43rd statistic report of China Internet network development state [R]. http://www.cac.gov.cn/2019-02/28/c_1124175677.htm
[2] Hu, C.P., Zou, X., Yang, M.H. (2014) Global Network Identity Management: Current Status and Development. Posts and Telecom Press, Beijing.
[3] Wikipedia. Identity management [J/OL]. (2019) http://en.wikipedia.org/wiki/Identity_management.
[4] Alix, M. (2013) Finnish Mobile ID: A Lesson in Interoperability. https://www.gsma.com/identity/wp-content/uploads/2013/03/GSMA_Mobile-Identity_Finnish_Case_Study.pdf
[5] Swisscom. (2013) Swisscom Mobile ID Client Reference guide. http://documents.swisscom.com/product/filestore/lib/b79870f2-7297-45a5-90f4-935c4ebd35a7/mobile-id-client-reference-guide-v-2-9[1].pdf
[6] GSMA and SIA. (2015) Mobile Identity - Unlocking the Potential of the Digital Economy. https://www.gsma.com/identity/wp-content/uploads/2014/10/GSMA-SIA-paper_FINALNov-2014.pdf

[7] Chen, B.D., Roscoe, A.W.. (2015) Mobile Electronic Identity: Securing Payment on Mobile Phones. https://www.cs.ox.ac.uk/files/3884/mobileElectronicIdentity.pdf

[8] Hewlett Packard Enterprise. (2018) Implementing mobile electronic identity: A Hewlett Packard Enterprise approach based on hardware token microSD card. http://www.securitydocumentworld.com/creo_files/upload/article-files/4AA6-8167ENW-Implementing-mobile-electronic-identity_update.pdf