

The Study of Secure E-Will System on the Internet*

HUNG-YU CHIEN AND RU-YU LIN[†]

Department of Information Management

National Chi Nan University

Nantou, 545 Taiwan

E-mail: redfish6@ms45.hinet.net

[†]*KPMG Taiwan*

Taipei, 110 Taiwan

This is the first paper that studies the feasibility of e-will systems on the internet and designs secure e-will protocols. Traditionally, such wills usually come in the form of a paper document that has to be signed with a lawful witness and can be consigned to an attorney for safety and security. However, this traditional process with an attorney involved means a fee the general public can probably not afford. The contributions of this paper are the feasibility study of e-will system complying with the civil laws, identifying the security requirements of secure e-will protocols, and the proposed efficient solutions for e-will system.

Keywords: security, bilinear pairing, identity-based cryptosystem, signature, encryption

1. INTRODUCTION

Without a clue, the weather can sometimes change before you know it, and so can happiness turn into mishap in an instant. Our lives are so vulnerable and erratic, full of sudden changes for which we never seem to have time to get ourselves ready. Whether they come as big and unusual as the 911 terrorist attack in New York, U.S.A., and the 921 earthquake here in Taiwan, or as common as car crashes and fire accidents, the same thing that goes for every single accident is that none of the victims knows by any means what is going to happen until it does. However, full of life a person may appear at this moment, death can easily seize him/her at the next. Though this may seem like an alarmist story, if one does not write down something in advance when it is not the right time to say it now, maybe there will never be a chance for the words to get across to their due receiver(s). Indeed, preparing a will in advance is probably the only way for the deceased (or a testator) to pass his/her last messages to those who are close and dear after his/her death. By taking thorough considerations as to what valuables (real estates, antiques, bank accounts and PIN codes, for example) should be inherited, who should inherit them, how the valuables should be shared or distributed and putting all the results of the considerations down in the form of a living will, one can avoid the possible regrets over not getting ready for it when Death decides it's his/her turn now, and at the same time one can feel comfortable not letting anybody know in advance what treasures they will get until they lawfully inherit them. This way, hopefully there will not be disputes among family members as to what they are supposed to inherit, and cases where the government

Received July 2, 2007; revised December 14, 2007; accepted April 10, 2008.

Communicated by Wen-Guey Tzeng.

* A preliminary of this study has been partially published in the 16th Information Security Conference, 2006, Taichung, Taiwan, and partially supported by the National Science Council of Taiwan, R.O.C. under contract No. NSC 95- 2221-E-324-008- MY2.

takes it all when there is neither a lawful living will ordering how the valuables left behind should be distributed nor any eligible heir to naturally claim the heritage.

According to the R.O.C. Civil Laws [6], there are five kinds of prepared wills – holographic will, attested will, sealed will, ghostwritten will, and nuncupative will – and all wills take into effect upon the death of the testator. A will can be holographic or ghostwritten (that means a will can be written by the testator himself/herself or written by a ghostwriter), or can be either sealed or un-sealed. The traditional living wills are usually in the form of a paper document, which has to be signed and witnessed to confirm its validity. The will can be consigned to an attorney for safety and security. A sealed will can only be opened on occasions where the family gathers or in the courtroom. There are several disadvantages to this conventional approach. Firstly, of course the costs for gathering the witnesses and for hiring the attorney are so high that the general public cannot seem to afford. Secondly, even though the testator can decide to keep the will at hand and revise it at his/her convenience, it is technically extremely difficult to stop people from beating around the bush and to keep the will from being interpolated or even destroyed due to natural or human factors. As a result, there has never been a trend towards preparing a living will among the general public.

Nowadays, thanks to the advancement of computer technologies and the development of the internet, document management and data processing have become much easier and extremely cost-saving. Furthermore, digital signature systems and encryption mechanisms have matured and become widely standardized. It is now an era when everything gets online, and there is absolutely no reason at all why wills should be any exception. However, wills are such documents of significance and importance that perfect security should be ensured with the opening of the will happening only when the pre-defined conditions are satisfied. Based on the advancement of identity-based (ID-based) cryptosystems from bilinear pairings [2], this paper offers two e-will protocols, the holographic e-will protocol and the sealed will protocol, enabling users conveniently, securely and efficiently prepare holographic wills and sealed wills. The holographic will protocol gets the will document digitally signed by the testator and securely stores it in the system, which plays the role of a trusted third party (in practice, the court can play this role). The advantage of convenient revisions of holographic wills is retained, and the wills stored in the system can stay securely away from malicious modifications. As for the sealed will protocol, on the other hand, we delicately apply the digital signature scheme, symmetric encryption, and ID-based encryption from pairings [2-5] such that the sealed will can be securely maintained and can only be opened by the trusted third party under the pre-defined conditions. In addition to the security, the e-will systems also help save time and trouble for getting the testator, notary, and witnesses involved, and at the same time the fee for hiring an attorney to do the safekeeping of the will can be spared. With advantages including convenience, security, and low cost, this research expects to encourage the public to prepare living wills online.

1.1 Related Works

To our best knowledge, this paper is the first research that studies the feasibility and the security of e-will systems, and designs secure e-will protocols that conform to the Civil laws. Even though there are some related services on the Internet; however, these

services only provide very limited functions, and do not conform to the Civil laws. A preliminary of this study is published in [14].

The Electronic Time-Stamping service [9] provides one-line time stamping on digital documents such that the stamping can be used as evidences of the time-lines of the stamped documents. E-wills can be one kind of the documents to be stamped. Compared to this time stamp only service, our scheme provides complete functions covering all the security requirements of e-will system. The Prepare Life Service [10] provides storage for encrypted digital will documents, but it provides no non-repudiation and the clients have to securely maintain the secret key by themselves. The scheme does not consider the Civil Laws issues. Both the RC Internet Law Center [11], Your E Will [12] and Hong Kong e-law [16] provide consultant services of preparing wills, but no e-will services are provided. Taiwan Creative E-integrated service project has included the e-will service, but only the *attested will* (the attested will is one kind of wills that the will is attested by a trusty third party; we will introduce different kinds of will in section 2.1) is considered in the project [17].

The symmetric encryptions and the asymmetric encryptions/signatures are directly related to our works. But, naïve application of these cryptographic mechanisms does not satisfy all the security requirements of sealed e-will systems. The digital envelopes [13] that combine the techniques of symmetric encryption and asymmetric encryption can encrypt documents such that only the designated receiver can decrypt them. However, the designated receiver who owns the only private key can decrypt all documents at any time on his/her own wish. On the contrary, our e-will design facilitates each client a distinct public key to encrypt his/her will such that the corresponding private key can only be generated by trusted parties upon the death of the client. This design not only enhances the security but also facilitates the separation of the authorities among several parties when the system is implemented.

The rest of this paper is organized as follows. Section 2 reviews the five types of wills stipulated by the R.O.C. Civil Laws and introduces the cryptographic primitives of our schemes. Our e-will schemes are to be presented in section 3, and section 4 is responsible for the security analysis and performance. Finally, section 5 will be the conclusion part.

2. BACKGROUND REVIEW

2.1 Five Types of Living Will Stipulated by the Civil Laws

According to the R.O.C. Civil Laws [6], citizens above the age of 16 and not under any legal interdiction can establish a “living will” at normal times, and the will is legitimate. Living wills can be classified into five types in terms of the method by which the will is prepared and the conditions and properties the will is supposed to follow or provide. Any will that belongs into any of the five types is considered a legal will and will take effect upon the death of the testator.

1. Holographic will: the testator writes the will without the assistance of any other. After the will is written, it is dated and signed. The signature cannot be replaced with any seal or any fingerprint seal. No witness is required. Any addition to, reduction from, or modification of the content should be noted with the number of modified words

- and should be signed.
2. Attested will: the testator should dictate the content of his/her will to the attestator and 2 or more witnesses that are appointed by the testator. After the attestator records, reads, and explains the will, with the confirmation of the testator, the will is dated and signed by the attestator, witnesses, and the testator. If the testator is unable to sign the will, the reason shall be clearly noted by the attestator and the signature can be replaced by the testator's fingerprint seal. The role of the attestator can be played by a court secretariat in places where attestators are unavailable. For overseas nationals to establish a will in the place where there is an R.O.C. consulate, the consul can play the role of the attestator.
 3. Sealed will: the will is self-written by the testator, dated, signed, and finally sealed with a signature. To validate the will, the testator has to propose the application to the attestator and appoints two or more than two witnesses to state his/her application. If the will is not holographic, the name and address of the ghostwriter should be stated. The attestator notes the date of the application and jointly signs with the testator and witnesses. A sealed will, unless in a formal meeting of the testator's relatives or in the office of attestation in a courtroom, cannot be opened and revealed. When a sealed will is opened and revealed, the process should be recorded, and it should be noted whether or not the seal is intact before the opening or any other special event. The record should be signed by all the people involved.
 4. Ghostwritten will: more than three witnesses appointed by the testator are required for validating a ghostwritten will. In dictating the intent of the will, one of the witnesses should record, read, and explain the content. After approved by the testator, the will is dated, signed by the ghostwriter, and jointly signed by all the witnesses and the testator. If the testator is unable to sign the will, a fingerprint seal may apply.
 5. Nuncupative will: when the testator is a case of pending death or in another special situation, a nuncupative will can be established in accordance with the following stipulations: (1) one of more than two witnesses records the intent of the will, and dates the record, and all the witnesses jointly sign the will and the record; (2) more than 2 witnesses dictate the will and audiotape the process. The tape is sealed on site, dated, and jointly signed on the seal. A nuncupative will is invalidated three months after the testator is able to establish a will in a different way. Within 3 months after the death of the testator, one of the witnesses or interest parties can propose to hold a formal family meeting to authenticate the will. Should there be any dissidence, the case may be brought to a courtroom for legal judgment.

Because the attested will, the nuncupative will, and the ghostwritten will require the testator to dictate his/her will to the attestator and the witnesses on the spot, online applications of such wills do not seem likely now. We, therefore, choose to design our e-will systems applicable to the establishment of the holographic will and the sealed will.

2.2 Bilinear Pairing

This paper, based on ID-based cryptosystems from pairings [1-5], describes our e-willing protocols. However, any other ID-based cryptosystem can be used as building blocks in our e-will systems. The concept of ID-based cryptosystem was first proposed

by Shamir in 1984 [7]. Here, in this paper, we delicately apply the ID-based cryptosystems such that the public key for some one's death can be easily derived off-line without any ambiguity and the corresponding private key will be generated by a trusted third party only when upon the death of him/her. This arrangement not only enhances the security and but also provides more convenience to the testator. Before presenting our e-will systems, let's review the concept of bilinear pairing and the framework of an ID-based cryptosystem here.

The basics of bilinear pairings are as follows. Let G_1 and G_2 denote two groups of prime order q , where G_1 is an additive group that consists of points on an elliptic curve, and G_2 is a multiplicative group of a finite field. A bilinear pairing is a computable bilinear map between two groups. In this paper, we use this notation e to mean a general bilinear map; *i.e.*, we have $e: G_1 \times G_1 \rightarrow G_2$, which can be either the modified Weil pairing [2] or the modified Tate pairing [8] and has the following three properties:

- (1) Bilinear: If $P, Q, R \in G_1$ and $a \in Z_q^*$, $e(P + Q, R) = e(P, R)e(Q, R)$, $e(P, Q + R) = e(P, Q)e(P, R)$, and $e(aP, Q) = e(P, aQ) = e(P, Q)^a$.
- (2) Non-degenerate: There exists $P, Q \in G_1$ such that $e(P, Q) \neq 1$.
- (3) Computable: There exist efficient algorithms to compute $e(P, Q)$ for all $P, Q \in G_1$.

Several commonly believed hard problems from pairings are introduced as follows.

Definition 1 The computational Diffie-Hellman problem (CDHP) is defined as follows: Given $P, aP, bP \in G_1$, where a and b are random numbers from Z_q^* , compute $abP \in G_1$.

It is commonly believed that there is no polynomial time algorithm to solve the CDHP problem with non-negligible probability. For other related hard problems like BDHP problem and DBDH problem, please refer to [1-5].

2.3 ID-based Cryptosystems from Pairings

Our e-will schemes use the ID-based encryption scheme and the ID-based signature scheme as basic building blocks. Any secure ID-based scheme can be used in our schemes; here, for reader's convenience, we take Boneh-Franklin's ID-based encryption scheme [2] and Hess's ID-based signature scheme [4] as examples. In an ID-based scheme from pairings, a user's entity is transformed into a point on the Elliptic Curves, and the point is taken as the user's public key. The trusted authority generates a private key for the user by multiplying the point by a secret scalar value.

Suppose G_1 and G_2 are two groups of prime order q , where G_1 is a group on the elliptic curve E . Let P be a generator of G_1 , and the *MapToPoint* function H_1 [2] encodes the identity of the user to a point in the group G_1 . Assume an entity with identity ID_i , then the output point $Q_i = H_1(ID_i)$ is taken as the entity's public key. Then, let's define this cryptographic hash function $H_2: G_2 \rightarrow \{0, 1\}^l$. As defined above, e is a bilinear pairing. ID-based public key infrastructure involves a Trusted Authority (*TA*) and users. The basic operations include "Set Up" and "Private Key Extraction".

Set Up: The *TA* selects the system parameters $\{E, q, G_1, G_2, e, H_1, H_2, P\}$, chooses a ran-

dom secret $s_{TA} \in_R Z_q^*$ as its secret key, computes its public key $P_{TA} = s_{TA} \cdot P$ and finally publishes $\{E, q, G_1, G_2, e, H_1, H_2, P, P_{TA}\}$.

Private Key Extraction: For each registered user U_i with his/her identity ID_i , the public key is $Q_i = H_1(ID_i)$ and the private key is $S_i = s_{TA} \cdot Q_i$, which is sent from the TA to the user via a secure channel.

2.3.1 ID-based encryption scheme

ID-based encryption schemes [2, 4, 5] allow the private key holder to decrypt a message sent to him/her under his/her public key (the public identity), where the Boneh-Franklin scheme [2] is not adaptive chosen ciphertext secure and the techniques [3-5] could be applied to enhance the security to be adaptive chosen-ciphertext secure. To simplify our presentation, we only review the Boneh-Franklin ID-based encryption scheme [2] here, and the techniques from [3-5] could be applied to enhance the security if the adaptive chosen-ciphertext security is required.

Let U_A denote an encryptor and U_B denote a decryptor. $M \in \{0, 1\}^l$ denotes the message to be encrypted.

- (1) Encryption: U_A chooses a random number $r \in Z_q^*$, computes $R = r \cdot P$ and $V = M \oplus H_2(e(P_{TA}, Q_B)^r)$, and sends $\{R, V\}$ as a ciphertext to U_B .
- (2) Decryption: After receiving the message $\{R, V\}$, U_B computes $V \oplus H_2(e(R, S_B)) = V \oplus H_2(e(rP, s_{TA} \cdot Q_B)) = V \oplus H_2(e(P_{TA}, Q_B)^r) = M$.

2.3.2 ID-based digital signature scheme

Any secure signature scheme can be used in our scheme, and Hess's scheme [1], which we shall review here, is a good example since it has been proven secure in a formal model and is efficient. After registering as a valid user, U_i can use S_i to sign any message M . In the following, we assume U_A to be the signer and U_B any verifier.

- (1) Signature generation: U_A randomly chooses an integer k , computes $r = e(P, P)^k$, $v = H_2(M, r)$ and $u = vS_A + kP$. Then, the signature is (v, u) .
- (2) Signature verification: After receiving the signature $\{M, (v, u)\}$, U_B checks whether the equation $v \stackrel{?}{=} h_1(M, e(u, P)e(Q_A, -P_{pub})^v)$ holds. If so, he accepts the signature. To check the correctness of the equation, please refer to [4].

Please notice that, for fixed signers, the values $e(P, P)$ and $e(Q_A, -P_{pub})$ can be pre-computed, and then the computational cost for signature is one modular exponentiation and two scalar multiplication in G_1 , and the verification cost is 1 modular exponentiation and one pairing operation.

3. DESIGN OF E-WILL SYSTEM

Because the attested will, the nuncupative will, and the ghostwritten will require the

testator to dictate his/her will to the attestator and the witnesses on the spot, online applications of the establishment of such wills do not seem likely now. We, therefore, choose to design our e-will systems applicable to the establishment of the holographic will and the sealed will. The Electronic Time-Stamping service [9] would be applied in our scheme, but, to simplify the presentation, we omit the time stamping presentation in our protocol.

3.1 Entities and Notations

Entities: There are three entities involved in our e-will system:

- Trusted Authority (TA): Mainly responsible for issuing private keys to users, maintaining the wills for the testators, and managing applications for creating living wills. In practice, these functions can be shared among multiple TAs , but in our simulations one TA did all these jobs. This role is suitable for the court or an attestator to play in real life.
- Hospital (H): Responsible for providing the certificate of death of the deceased and issuing the certificate of death to the relatives. A certificate of death is a certificate that formally specifies name, sex, date of birth, blood type, date of death, cause, *etc.* of the deceased. This e-document should be signed by the doctors and the hospital.
- Witnesses (U_X and U_Y): Witnesses are appointed by the testator, and their function is to provide proof to the establishment of the will by the testator. Infant, interdicted person, heir, heir's spouse, heir's lineal relatives by blood, devisee, devisee's spouse, devisee's lineal relatives by blood, the attestator (or the deputy), the attestator's co-habitant, the attestator's assistant, the attestator's employees must not be a witness to the will.
- Testator (U_A): The party who establishes a living will.
- Relatives: Relatives to the testator by blood.

Notations: In section 2.3, we have introduced the ID-based encryption function and the ID-based signature function. Now we define the following notations to represent these functions and to simplify the presentation of our protocols.

- $(R, V) \leftarrow IBE_{Q_i}(M)$ denotes the ID-based encryption of the message M under the decryptor's public key Q_i .
- $\{M \text{ or } \perp\} \leftarrow IBD_{S_i}(R, V)$ denotes the ID-based decryption of the ciphertext $\{R, V\}$ using the decryptor's private key S_i , which corresponds to the public key Q_i .
- $S \leftarrow IBS_{S_i}(M)$ denotes the ID-based digital signature of the message M using the signer's private key S_i .
- $\{success \text{ or } failure\} \leftarrow IBSV_{Q_i}(S, M)$ denotes the ID-based verification of the signature (S, M) . The verifier uses the signer's public key Q_i to verify the signature, and the result is either "success" or "failure". If we implement the digital signature using Chen's scheme as introduced in section 2.3, then the signature S would consist of two values of the form $\{D, h\}$.
- $E_k(M)$ denotes the symmetric encryption of the message M under the key k .
- Q_A/S_A : entity A 's general public key/private key. The private key S_A will be generated and securely distributed to A when entity A registers at the authority. $Q_A = H_1(ID_A)$,

where $ID_A = (\text{Name} \parallel \text{the social security number} \parallel \text{Date of Birth} \parallel \text{Sex})$, and U_A 's private key is $S_A = s_{TA} \cdot Q_A$.

- $Q_{A_{\text{Death}}}$: entity A 's public key of death. Any entity A can generate the public key any time without the help of the authority. However, the authority will generate the corresponding private key only when the authority has received the certificate of death of A . That is, the private key will be generated only when the entity has past away. The Household Registration office in Taiwan has plan the implementation of issuing the e-certificate of death [17]. $Q_{A_{\text{Death}}} = H_1(ID_{A_{\text{Death}}})$, where the identity $ID_{A_{\text{Death}}} = (A\text{'s Name} \parallel A\text{'s social security number} \parallel \text{gender} \parallel \text{Date of Birth} \parallel \text{the Court Name} \parallel \text{"Death"})$ specifies A 's death and the format is pre-defined and published by the court.

3.2 The Protocol of the Holographic E-Will System

Traditional holographic wills usually come to existence in the form of a paper document. Such wills are not sealed, so the testators can revise them whenever it is convenient. However, this convenience also makes traditional holographic wills vulnerable to modifications or even destructions against the testator's will due to natural or human factors. To make a difference, we have designed our Holographic E-Will System on the basis of the Internet framework and information security technologies. With our system, the testator can make sure that the testament is kept in safety and security by the trusted third party, and the merit of easy modification by the authenticated testator is still retained. All the transmissions on the Internet are protected via the Secure Socket Layer (SSL) channel, which is denoted as $\xrightarrow{\text{SSL}}$. The security requirements of the holographic

e-will system include the following properties: (1) Authenticity/non-repudiation- only the genuine testator can create/modify his/her will, and no one can deny the contents of the will; (2) Integrity- no one except the testator can modify the content of a will. Here, we ignore the implementation issue of availability; that is, the system is robust to the denial-of-service (DOS) attack. Therefore, we define the security of the holographic e-will protocol in Definition 2.

Definition 2 Secure holographic e-will protocol: A holographic e-will protocol is secure if it satisfies the following property.

1. Authenticity and non-repudiation: Since non-repudiation also implies authenticity here, we require the e-will to be existentially un-forgable under chosen message attack [3-5].
2. Integrity of e-will: Here non-repudiation also implies integrity.

The procedures of our holographic e-will system are shown in Fig. 1. Each step is detailed as follows.

1. System construction phase: TA sets up the system parameters $\{E, q, G_1, G_2, e, H_1, H_2, P, P_{TA}\}$, which are the same as those in the "set up" part in section 2.3. Then TA chooses a random integer $s_{TA} \in \mathbb{Z}_q^*$ as TA 's private key and computes the system's public key $P_{TA} = s_{TA} \cdot P$.

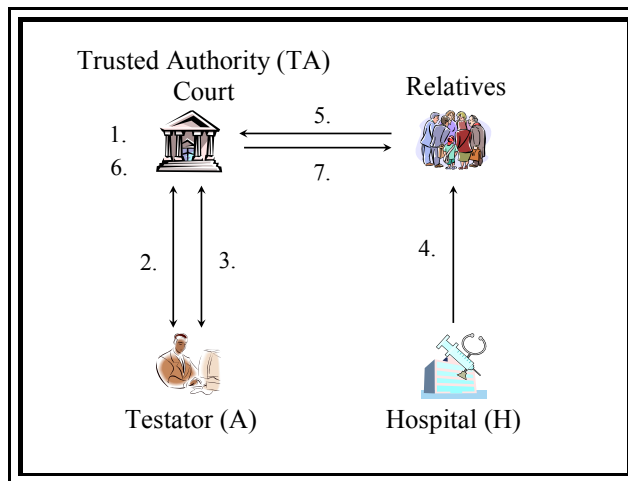


Fig. 1. The operation procedure of the holographic will system.

2. Registration phase: Each entity involved should register with TA to acquire his/her private key. The testator U_A 's public key is $Q_A = H_1(ID_A)$; where $ID_A = (\text{Name} \parallel \text{the social security number} \parallel \text{Date of Birth} \parallel \text{Sex})$, and U_A 's private key is $S_A = s_{TA} \cdot Q_A$. In addition, the court (C), the doctor (D), and the hospital (H) all have to register with TA to acquire their private keys, respectively $S_C = s_{TA} \cdot Q_C/S_D = s_{TA} \cdot Q_D/S_H = s_{TA} \cdot Q_H$, as well as their public keys $Q_C = H_1(\text{Court Name})/Q_D = H_1(\text{Doctor's Name} \parallel \text{Certificate Number})/Q_H = H_1(\text{Hospital Number} \parallel \text{Hospital Address})$. In practice, the role of the court and the trusted authority can be played by the same entity.
3. Creating a living will: Testator A fills out an application form and submits it to TA (which is assumed to be the role played by the court). After the will is established and dated, testator A is required to sign on both the will and the application form. Finally, A submits the will and the application form to TA , and TA verifies the validity of the signed will and the signed application form. If the verifications turn out positive, TA will sign the application form and return a missive to the testator to confirm the application. The procedure of creating a living will is detailed as follows:

$$(1) A \xrightarrow{SSL} TA: L', S, M, L.$$

The testator A writes an application letter L and a will M . The application letter L includes information such as name of the recipient, date of application, name of the applicant, social security number of the applicant, date of birth, gender, email, phone number, current address, registered residence address, lineal relatives by blood one generation up and down, and *etc.* The letter is linked to the plaintext will M . The will M includes the testament, date, and the digital signature of the testator. After the testator completes the application letter L and the will M , A signs on the application letter L and the will M , and obtains $S = IB_{S_A}(M)$ and $L' = IB_{S_A}(L)$, respectively. Meanwhile, the correlation between the application letter and the will is shown in Fig. 2. Finally, the testator A submits L', S, M and L to the court.

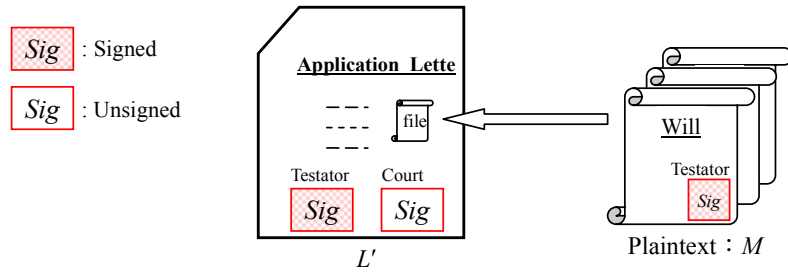


Fig. 2. The correlation between the application letter and the will.

(2) $TA \xrightarrow{SSL} A : L''$.

When the court receives the request for establishing a living will, it will apply the testator A 's public key Q_A to verify the signatures. The verification formulas are $IBSV_{Q_A}(\{L'\}, (L))$ and $IBSV_{Q_A}(\{S\}, (M))$. If the signatures are valid, the court will sign the application letter $L'' = IBS_{S_C}(L, L')$ and return a missive L'' to the testator to confirm the application.

(3) When the testator A receives the reply from the court, he/she uses the court's public key Q_C to verify whether it has been legally endorsed. The verification formula is $IBSV_{Q_C}(\{L''\}, (L, L'))$. This confirms the acceptance of the application by the court.

The testator can, after authentication, modify the will at any time on the Internet and repeat procedures (1)-(3) to establish a legal will.

4. The hospital issues the certificate of death: After the testator passes away, the doctor diagnoses the cause of death and issues a digital death certificate (DC) to the relatives. The certificate includes the doctor's signature $S^D = IBS_{S_D}(DC)$ and the hospital's seal $S^H = IBS_{S_H}(DC, S^D)$. Then, DC , S^D , and S^H are transmitted to A 's lineal relatives by blood within one generation's distance.
5. Relatives submit the DC : Relatives of the deceased submit the certificate of death $\{DC, S^D, S^H\}$ to the court and request for revelation of the will.
6. The court authenticates the DC : The court verifies whether the certificate contains the doctor's digital signature and the hospital's digital seal. The verification formulas are $IBSV_{Q_D}(\{S^D\}, (DC))$ and $IBSV_{Q_H}(\{S^H\}, (DC, S^D))$, respectively. If the certificate is legal, the court proceeds to step 7.
7. The court reveals the Will: The court delivers the will established by the deceased to his/her relatives.

3.3 The Protocol of the Sealed Will System

A conventional sealed will has to be signed, sealed, and signed again on the seal. The sealed will system we have designed takes advantage of both the Internet and information security technologies. In the system, the testator has to go through a digital signature and encryption process and appoint 2 or more than 2 witnesses to endorse the validity of the encrypted will. Please notice that the responsibility of the witnesses is to en-

dorse the establishment of the will but they are not allowed to read the content of the will. The will can be submitted to a court for attestation to acquire legitimacy. The e-will can be open only when the testator deceases and the hospital issues the certificate of death. Therefore, we define a secure sealed e-will protocol as follows.

Definition 3 Secure sealed e-will protocol: A sealed e-will protocol is secure if it satisfies the following property.

1. *Authenticity and non-repudiation*: Since non-repudiation also implies authenticity here, we require the e-will to be existentially unforgeable under chosen message attack [1, 2].
2. *Integrity of e-will*: Here non-repudiation also implies integrity.
3. *Privacy of the sealed will*: Since, for performance reason, it is reasonable to encrypt the will using a symmetric encryption scheme and protecting the encrypting key using asymmetric encryption scheme, we can define this property to both the security of the symmetric encryption and the security of the asymmetric encryption.
4. *Punctual decryption*: For a sealed will, no one can decrypt a sealed will and know the contents until the testator pass away and the authority has got the corresponding certificate of death. A certificate of death is a formal certificate that specifies one's death, date and cause, and the certificate should be signed by the corresponding authorities.

We use digital signatures, symmetric encryptions, and ID-based encryptions to secure the will. All the transmissions are done over the Secure Socket Layer (SSL) channel, denoted as \xrightarrow{SSL} . Unlike the holographic e-will system, every user in the sealed e-will system owns two sets of public keys- the ordinary public key and the public key for death. The set of ordinary public key is used for ordinary signature generation/verification while the public key for death is only used for encrypting the symmetric keys that are used to seal the content of the wills. The main idea is that the testator off-line selects a symmetric key to encrypt the wills, and uses the public key for death to encrypt the symmetric keys such that the TA will generate the corresponding private key only upon the death of the testator. Unless the specified conditions are satisfied (the testator deceases and the hospital issues the certificate of death), none of the witnesses, the court, the relatives nor any malicious attacker can open the content of the will.

The operation procedures of the sealed will system are shown in Fig. 3. Each step is detailed as follows.

1. System construction phase: This phase is basically the same as the first phase of the holographic will system. The trusted authority (TA) chooses a random integer $s_{TA} \in \mathbb{Z}_q^*$ as TA 's private key and computes the system's public key $P_{TA} = s_{TA} \cdot P$.
2. Registration phase: It is the same as the registration phase in the holographic will system. The testator U_A 's ordinary public key is $Q_A = H_1(ID_A)$, where $ID_A = (\text{Name} \parallel \text{social security number} \parallel \text{Date of Birth} \parallel \text{Sex})$, and U_A registers with TA to acquire a private key $S_A = s_{TA} \cdot Q_A$. In addition, the court (C), doctor (D), and hospital (H) respectively register with the trusted authority to acquire a private key $S_C = s_{TA} \cdot Q_C / S_D = s_{TA} \cdot Q_D / S_H = s_{TA} \cdot Q_H$, as well as a public key $Q_C = H_1(\text{Court Name}) / Q_D = H_1(\text{Doctor's Name} \parallel \text{Certificate Number}) / Q_H = H_1(\text{Hospital Number} \parallel \text{Hospital Address})$.

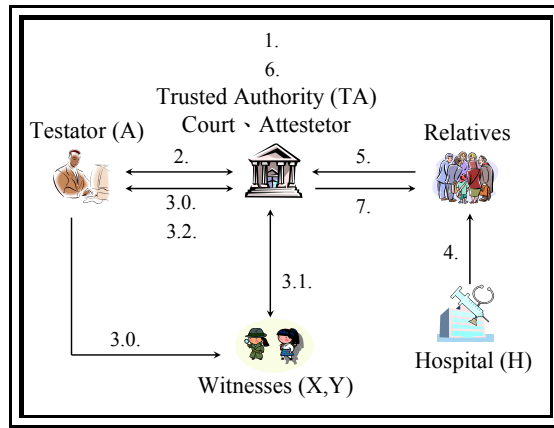


Fig. 3. The operation procedures of the sealed will system.

3.0 Creating a living will: Testator A fills out an application form and uses a symmetric key k to encrypt the content of the will. After that, what testator A has in hand is now a sealed will. The symmetric key k is further encrypted using asymmetric key encryption algorithm under the public key for his/her death. Then, A signs both the application form and the sealed will, and submits the encrypted will, the encrypted symmetric key and the application form to the court. Besides the testator him-/herself, more than two witnesses appointed by the testator have to sign on the sealed will and the application form too. Upon receiving the sealed will and the application form both properly signed by the testator and the witnesses, the court validates the signatures on the sealed will and the application. The procedures of creating a living will are shown as follows:

$$(1) A \xrightarrow{SSL} TA : L, L', C, IBE_{Q_{A_{Death}}}(k).$$

The testator A writes an application letter L and a will M , where the application letter L includes such information as name of the recipient, date of application, name of the applicant, social security number, date of birth, gender, email, phone number, current address, registered residence address, lineal relatives by blood no remoter than one generation away, witness' names, witness' social security numbers, witness' dates of birth, gender(s), emails, and *etc.* The letter is linked to the sealed will and the encrypted symmetric key $IBE_{Q_{A_{Death}}}(k)$. The will $M = (m \parallel S)$ includes a statement (m), date, and the digital signature (S) of the testator. After the testator completes an application letter and the will, he/she signs the will m and obtains $S = IBS_{S_A}(m)$. The testator chooses a random number $k \in Z_q^*$ as a symmetric key and uses the key to encrypt the signed will and get the sealed will $C = E_k(M)$. Then, the testator A follows the court's pre-defined format and computes the public key for death as $Q_{A_{Death}} = H_1(ID_{A_{Death}})$, where the identity $ID_{A_{Death}} = (A's \text{ Name} \parallel A's \text{ social security number} \parallel \text{gender} \parallel \text{Date of Birth} \parallel \text{the Court Name} \parallel \text{"Death"})$ specifies A 's death and the format is pre-defined and published by the court. The private key $S_{A_{Death}}$ corresponding to the public key of A 's death, $Q_{A_{Death}}$, will be generated only when the testator A dies and the court receives the certifi-

cate of death from the hospital. Please notice that such a design allows the testator to access his/her public key of death $Q_{A_{Death}}$ and use this key to encrypt data at any time, but the corresponding private key for the purpose of decryption can only be generated by TA after the death of the testator. Finally, A signs the application letter L to get $L' = IBS_{S_A}(L)$. Meanwhile, the correlation between the application letter and the will is shown in Fig 4. Now the testator A submits L, L', C and $IBE_{Q_{A_{Death}}}(k)$ to the court. The plaintext will is not transmitted to the court.

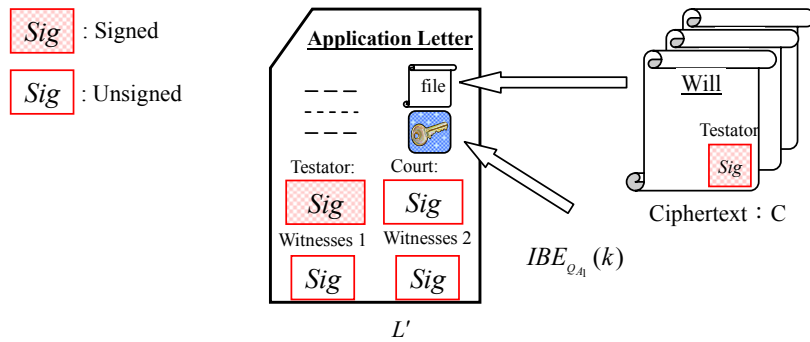


Fig. 4. The correlation between the application letter and the will.

(2) $TA \xrightarrow{SSL} X, Y : L, L', C$.

When the court receives the application, it first verifies whether the signatures on the application letter and the sealed will are valid by checking out $IBSV_{Q_A}(\{L'\}, (L, C))$. And then, the court delivers the application letter and related data to the appointed witnesses (X and Y).

- 3.1 The witnesses sign the sealed will: upon receiving the request from the court, the witnesses first verify their personal data and A 's signature of the sealed will, and then they use their private keys to sign the application to get $S^X = IBS_{S_X}(L' \parallel L \parallel C)$ and $S^Y = IBS_{S_Y}(L' \parallel L \parallel C)$. Finally, they return their signatures S^X and S^Y to the court.
- 3.2 The court informs the testator that the application has been accepted. In this stage, the court verifies the witnesses' signatures S^X and S^Y . If the signatures are valid, the court signs the application letter (already signed by the testator and the witnesses) to get $L'' = IBS_{S_C}(L, L', C, S^X, S^Y)$ and returns a missive L'' to the testator to confirm the application. When A receives the missive L'' , he/she verifies the court's endorsement (signature) by checking out $IBSV_{Q_C}(\{L''\}, (L, L', C, S^X, S^Y))$.
After authentication, the testator can update the will at any time on the Internet by repeating procedures 3.0 through 3.2.
4. The hospital issues the certificate of death: after the testator passes away, the doctor diagnoses the cause of death and issues a digital death certificate (DC) to the relatives. The certificate includes the doctor's signature $S^D = IBS_{S_D}(DC)$ and the hospital's seal $S^H = IBS_{S_H}(DC, S^D)$. DC, S^D , and S^H are transmitted to A 's lineal relatives by blood one generation away.
5. The relatives submit DC : the relatives of the deceased submit the certificate of A 's death $\{DC, S^D, S^H\}$ to the court and request the revelation of the will.

6. The court verifies the *DC*: the court validates the certificate after checking the doctor's digital signature and the hospital's digital seal, namely $IBSV_{Q_D}(\{S^D\}, (DC))$ and $IBSV_{Q_H}(\{S^H\}, (DC, S^D))$, respectively. If the certificate is legal, the court proceeds to step 7.
7. The court reveals the will: when the *DC* is verified by the court, *TA* generates the private key $S_{A_{Death}} = s_{TA} \cdot Q_{A_{Death}}$, where $Q_{A_{Death}} = H_1(ID_{A_{Death}})$ is *A*'s public key of death. The court (*TA*) uses the private key $S_{A_{Death}}$ to decrypt the encrypted symmetric key k by computing $k = IBD_{S_{A_{Death}}}(IBD_{Q_{A_{Death}}}(k))$. Afterwards, the symmetric key k will be used to disclose the sealed will C , and the plaintext will and the signature $M = (m \parallel S)$ are delivered to the testator's relatives.

Even though it seems more efficient for the testator to sign only on the application letter which contains the hash value of the will, it pays extra cost and in-convenience when it comes to the time for the relatives to verify the will but not the application letter. Second, the arrangement of distinct signatures on the will and on the application letter is required to comply with the legal obligations and liabilities in real life.

4. SECURITY ANALYSIS, PROOFS AND PERFORMANCE EVALUATION

4.1 Security Analysis and Proofs

To begin with, all the transmissions are performed over SSL channels and are therefore under proper protection. No attackers can derive any information from the transmissions. The security of our holographic e-will system and sealed e-will system are summarized as follows.

Theorem 1 The proposed holographic e-will system is secure (it satisfies Definition 2) if the underlying digital signature scheme is existentially unforgeable under chosen message attack.

Proof: In our scheme, the testator should sign on the will M and the application letter L , where the application letter is tightly bound to the will, and the application letter is also endorsed by the *TA*. Therefore, the authenticity and the non-repudiation of the will are ensured (being existentially unforgeable under chosen message attack). \square

Theorem 2 The proposed sealed e-will system is secure (it satisfies Definition 3) if the off-line *TA* is trusted, the underlying digital signature is existentially unforgeable under chosen message attack, the symmetric encryption is indistinguishably secure against chosen plaintext attack, the underlying ID-based encryption is indistinguishably secure against adaptively chosen cipher text attack, and the CDHP is hard.

Proof:

1. Authenticity, non-repudiation and integrity. The proposed scheme satisfies these properties since the underlying digital signature scheme is existentially unforgeable under chosen message attack.

2. Privacy of the sealed will. Since the underlying symmetric encryption is indistinguishable under chosen plaintext attack and the underlying asymmetric encryption is indistinguishable under adaptive chosen cipher-text attack, the proposed scheme satisfies this property.
3. Punctual decryption. If the off-line TA is trusted, then the corresponding private key for death is generated by the TA under the authorized conditions- the TA has received the certificate of death of the testator. Therefore, to compute the corresponding private key for death, one should face the $CDHP$ problem (given $P, P_{TA} = s_{TA} \cdot P, Q_{A_{Death}} = H_1(ID_{A_{Death}})$, to compute $S_{A_{Death}} = s_{TA} \cdot Q_{A_{Death}}$ is a $CDHP$ problem). \square

Table 1. Functional comparison of related works.

	the proposed holographic will system	the proposed sealed will system	on-line will consultant [11, 16]	e-integrated service [17]	prepare life [10]
security properties	authenticity, integrity, non-repudiation	authenticity, integrity, non-repudiation, punctual decryption	only consultant services	only the attested will	only provide a storage service
comply with civil laws	yes	yes	not applicable	unknown ¹	no

¹According to the civil laws, the attested will requires that the testator should dictate the content of his/her will to the attestator and two more witnesses *on the spot*, and the attestator should record, read and explain the will, with the confirmation of the testator. We, therefore, doubt the attested will project [17] would comply with the civil laws.

4.2 Performance Evaluation

The *functional* comparisons among related works are summarized in Table 1. The e-will services like [11, 12, 16] only provide on-line consultant service, and the Prepare Life scheme [10] only provide a storage maintenance service for users to store their wills. These schemes are not e-will systems. The Taiwan Creative E-integrated services project initiated by Taiwan Research Development and Evaluation Commission Executive Yuan has covered the design of the attested e-will service [17]; however, the system is not yet implemented and no designed protocol is published. Table 2 summarizes the computational cost and the communication cost of the proposed schemes. Here T_{sig} denotes the computational cost for one signature operation, T_{ver} denotes that for one signature verification, T_{ENC}/T_{DEC} denotes that for one symmetric encryption/decryption, and T_{IBE}/T_{IBD} respectively denotes that for one identity-based encryption/identity-based decryption. Likewise, L_{app} denotes the length of one application letter, L_{will} denotes that of one e-will, L_{sig} denotes that for one signature, L_{DC} denotes that for one death certificate, and L_{G_1} denotes the length of presentation of one point in G_1 . If we adopt Hess's signature scheme, then T_{sig} require one modular exponentiation and 2 scalar multiplications in the G_1 field, T_{ver} requires one modular exponentiation and one pairing, and L_{sig} takes one point in G_1 and one hash. If we adopt Boneh-Franklin identity-based encryption scheme, then T_{IBE} requires one scalar multiplication in G_1 , one symmetric encryption and one pairing, and

T_{IBD} requires one pairing and one hash. From Table 2, we can see that our proposed schemes are efficient, because the schemes fully comply with the process in the real life and only require the necessary operations that are regulated by the civil laws.

Table 2. Computational complexity and communication cost of the proposed schemes.

	holographic e-will system	the sealed e-will system
Comput. Cost/comm. cost of testator in the e-will creation phase	$2T_{sig} + 1T_{ver}$ $1L_{app} + 1L_{will} + 2L_{sig}$	$2T_{sig} + 1T_{ver} + (L_{will}/L_{key}) T_{ENC} + 1T_{IBE}$ $1L_{app} + 1L_{will} + 1L_{sig} + 1L_{key} + 1L_{G_1}$
Comput. Cost/comm. cost of trusted authority in the e-will creation phase	$1T_{sig} + 2T_{ver}$ $1L_{sig}$	$1T_{sig} + 3T_{ver}$ $3L_{sig}$
Comput. Cost/comm. cost of hospital in the e-will open phase	$2T_{sig}$ $1L_{DC} + 2L_{sig}$	$2T_{sig}$ $1L_{DC} + 2L_{sig}$
Comput. Cost of trusted authority in the e-will open phase	$2T_{ver}$	$2T_{ver} + 1T_{DEC} + 1T_{IBD}$

5. CONCLUSIONS

In this research, we have studied the living will preparation methods ratified in the R.O.C. Civil Laws and have pointed out the inconvenience and high costs involved in the preparation of conventional wills in the form of paper documents. In order to make the establishment of a living will cheaper, securer and more convenient, we have proposed two e-will schemes – the holographic e-will system and the sealed e-will system. The security of the schemes is based on the primitives, namely SSL, ID-based signature, ID-based encryption and secure symmetric encryption. With these advantages, this research is expected to encourage more people to prepare a living will online, shortening the time and reducing the cost for the arrangement of the valuables left behind after death, saving trouble for both the family and the government. A prototype system based the library from NUI Maynooth Crypto Group [15] is now under development.

REFERENCES

1. F. Hess, "Efficient identity based signature schemes based on pairings," in *Proceedings of the 9th Annual International Workshop on Selected Areas in Cryptography*, LNCS 2595, 2002, pp. 310-324.
2. D. Boneh and M. Franklin, "Identity based encryption from the Weil pairing," in *Proceedings of Advances in Cryptology – CRYPTO*, LNCS 2139, 2001, pp. 213-229.
3. H. Y. Chien, "Selectively convertible authenticated encryption in the random oracle model," *The Computer Journal*, Vol. 51, 2008, pp. 419-434.
4. R. Canetti, S. Halevi, and J. Katz, "Chosen-ciphertext security from identity-based encryption," in *Proceedings of Advances in Cryptology – EUROCRYPT*, LNCS 3027, 2004, pp. 207-222.

5. X. Boyen, Q. Mei, and B. Waters, "Direct chosen ciphertext security from identity-based techniques," in *Proceedings of the 12th ACM Conference on Computer and Communications Security*, 2005, pp. 320-329.
6. R.O.C. Civil Laws, correction in June 26, 2002, laws and regulations database: <http://law.moj.gov.tw/fn.asp>.
7. A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proceedings of Advances in Cryptology – CRYPTO*, LNCS 196, 1985, pp. 47-53.
8. G. Frey, M. Muller, and H. Ruck, "The Tate pairing and the discrete logarithm applied to elliptic curve cryptosystem," *IEEE Transactions on Information Theory*, Vol. 45, 1999, pp. 1717-1719.
9. Electronic Time-Stamping, <http://www.e-timestamping.com/chi/about/app/app1.html>.
10. Prepare Life Service, <http://www.geocities.com/preparelife/>.
11. RC Internet Law Center, <http://www.rclaw.com.tw/>.
12. Your E Will, <http://www.yourewill.com/added.html>.
13. Digital Envelops, <http://www.windowsitpro.com/Windows/Article/ArticleID/2698/2698.html>, <http://www.rsasecurity.com/products/bsafe/overview/Article5-SignEnv.pdf>.
14. H. Y. Chien and R. Y. Lin, "The design of sealed e-will system," in *Proceedings of the 16th Information Security Conference*, 2006. pp. 139-146.
15. NUI Maynooth Crypto Group: <http://www.crypto.cs.nuim.ie/software/eyebee/>.
16. Hong Kong e-law services, <http://www.hkelaw.com/>.
17. Taiwan Creative E-integrated services, <http://egov.iii.org.tw/>.



Hung-Yu Chien (簡宏宇) received the B.S. degree in Computer Science from National Chiao Tung University, Taiwan, 1988, the M.S. degree in Computer and Information Engineering from National Taiwan University, Taiwan, 1990, and the doctoral degree in Applied Mathematics at National Chung Hsing University, 2002. He was an assistant researcher at TL, MOTC, Taiwan, during 1992-1995. He was the director of Computer Center at Nan-Kei College. He was an associate professor of Chaoyang University of Technology during 2003-2006/08. Now he is a professor of National Chi Nan University, a member of the Chinese Association for Information Security, an IEEE member. His research interests include cryptography, networking and network security.



Ru-Yu Lin (林茹玉) received the M.S. degree at the Department of Information Management of Chaoyang University of Technology. Her research interests include cryptography, and network security. Now she is a security auditor at KPMG Taiwan.