2010 International Conference on Availability, Reliability and Security

Unified Public Key Infrastructure Supporting Both Certificate-based and ID-based Cryptography

Byoungcheon Lee
Dept. of Information Security, Joongbu University
101, Daehak-Ro, Chubu-Myeon, Geumsan-Gun, Chungnam, Korea
sultan@joongbu.ac.kr

***Abstract*—Certificate-based cryptography and ID-based cryptography have been designed under different theoretical backgrounds and they have their own advantages and drawbacks, but there have been few works which try to provide them together in an efficient way. Chen *et al.* [4] considered a hybrid scheme of public key infrastructure (PKI) and ID-based encryption (IBE), and also discussed various trust relationship among multiple authorities, but they have not discussed more in-depth implementation issues of the hybrid scheme. In ID-based cryptography issuing private keys to users in escrow-free way had been an important issue. Lee *et al.* [12], [13] proposed a unique private key issuing protocol in the *single-authority multiple-observer (SAMO)* model which can reduce the user authentication load a lot, but these schemes are subject to several attacks due to the lack of verifiable authentication of protocol messages [11].**

In this paper we show that these two problems can be solved by combining certificate-based and ID-based cryptography. In the proposed scheme certificate is issued to user for user-chosen public key and ID-based private key is issued to user through a private key issuing protocol. In the private key issuing protocol user is authenticated using the certificate and protocol messages are blinded using the certified public key of the user, thus the private key issuing protocol becomes private and also verifiable, which solves the authentication problem of [13].

We further present the concept of *unified public key infrastructure (UPKI)* in which both certificate-based and ID-based cryptosystems are provided to users in a single framework. We also show that if interactions between end users are mainly executed using ID-based cryptography, then end users don't need to manage other end users' certificates, which is a great efficiency gain than traditional PKI.

***Keywords*-Unified public key infrastructure (UPKI); Private key issuing protocol; Key generation and certification authority (KGCA); Key privacy agent (KPA); Certificate-based cryptography; ID-based cryptography; Bilinear pairing; Hybrid cryptography**

I. Introduction

A. *Certificate-based Cryptography*

In traditional certificate-based public key cryptography, user's public key generated by user is authenticated with a certificate issued by a certification authority (CA). A certificate is a digital document signed by CA which binds a public key to a specific user. It provides explicit authentication of the public key in the sense that the authenticity of the public key is convinced to anyone by verifying the certificate. Any participant who wants to use other's public key must first verify the corresponding certificate to check the authenticity of the public key. Thus users have to retrieve, verify, store, and manage other's certificates that they are communicating with. It requires large amount of storage, communication and computing to store, verify, and revoke certificates.

B. *ID-based Cryptography*

In 1984, Shamir [15] proposed the ID-based cryptography which can greatly simplify key management. In ID-based cryptography an entity's public key is derived directly from its public identity information, for example, name, e-mail address, IP address of the user, etc. The corresponding private key of the user is generated by a trusted authority called key generation center (KGC) and given to the user through a secure channel. Compared with certificate-based cryptography, ID-based cryptography is advantageous in key management, since distribution of public key is not required. A sender can send an encrypted message to a receiver using the receiver's public identity information, even before the receiver obtains his private key from KGC. If a signature is received, it can be verified immediately by using sender's public identity information.

But an inherent problem of ID-based cryptography is the key escrow problem, i.e., KGC knows user's private key. Therefore, malicious KGC can decrypt ciphertexts of the user and forge signatures with the name of the user. It also requires a secure channel between users and KGC to deliver private keys securely. Therefore, providing an escrow-free private key issuing mechanism is an important issue to make the ID-based cryptography more practical in the real world. Because of these inherent problems ID-based cryptography was considered to be suitable only for communications inside a small organization where KGC is fully trusted.

C. *Private Key Issuing in ID-based Cryptography*

In ID-based cryptography issuing private keys to users in escrow-free way had been an important issue. Recently, Lee *et al.* [12], [13] proposed a unique private key issuing protocol in the *single-authority multiple-observer (SAMO)* model, which is the first pioneering work that can reduce the

978-0-7695-3965-2/10 $26.00 © 2010 IEEE
DOI 10.1109/ARES.2010.49

identification cost in multi-authority-based key issuing protocol. In this approach a single key generation center (KGC) provides user identification and partial key issuing function and multiple key privacy agents (KPAs) provide key privacy service without additional user identification. This proposal reduced the identification cost from multiple identifications by multiple authorities to a single identification by KGC.

But these schemes have weaknesses due to the lack of authentication of protocol messages. In these scheme KGC first checks user's identification and provides partial private key, then KPAs check KGC's user identification and provide key privacy service without any further direct identification of user. Since explicit authentication was not employed in these schemes, it's hard for KPAs to accept KGC's identification result and the overall scheme became complicated.

D. Combining Certificate-based and ID-based Schemes

Traditionally certificate-based cryptography and ID-based cryptography have been considered separately. Certificate-based cryptography and public key infrastructure (PKI) can be deployed to authenticate users in large scale, hierarchical groups, while ID-based cryptosystem is generally used to authenticate users in a closed, highly trusted group. In designing a private key issuing protocol in ID-based cryptography researchers in many literatures tried to exclude the use of certificate due to the high overhead of certificate-based scheme. It looks quite reasonable in some sense, but if we consider the case that PKI is already existent, adding ID-based cryptography to certificate-based cryptography is not a heavy load.

There have been several works which try to combine certificate-based and ID-based systems. Chen *et al.* [4] proposed a hybrid scheme of public key infrastructure (PKI) and ID-based encryption (IBE) system which merges traditional PKI with identity-based encryption system. They suggested that the combination of two schemes, PKI for global name and ID for local name, is advantageous and scalable. They further discussed various trust relationship between multiple authorities in this hybrid system. Price *et al.* [14] considered the issue of interoperation between entities in conventional PKI and entities in ID-based infrastructure. These schemes considered interoperation between two systems, but they have not discussed more in-depth implementation issues of the combined system.

In this paper we show that combining these two cryptosystems in a single framework is possible with small extra load and it has many advantages. This work can be considered as an efficient implementation example of the idea of [4], [14].

E. Motivation of Unified Public Key Infrastructure

Another critical problem of ID-based cryptography is that it is not easy to implement hierarchy of trust. Gentry *et al.* [9] showed an example of hierarchical ID-based encryption, but it is not flexible to suit to the real world requirements. Therefore, though we try to use ID-based cryptography for end users, it looks better to rely on certificate and PKI to construct upper trust hierarchy.

In this paper we introduce a new concept called *unified public key infrastructure (UPKI)* in which both certificate-based and ID-based cryptography are provided to users in a highly combined manner. Here we assume the existence of a trusted authority called *key generation and certification authority (KGCA)* who has the role of both CA and KGC. It checks identification information of user and issues a certificate for a user-chosen public key X. It also issues ID-based partial private key to the user. We also assume the existence of multiple KPAs like in [13] who provide key privacy service. In the proposed private key issuing protocol user is authenticated with certificate and user's certified public key X is used to blind the protocol messages such that only the legitimate user can retrieve the ID-based private key. This approach can solve the problems of both [12], [13] and [4], [14]. We also show that if interactions between end users are mainly executed using ID-based cryptography, then end users don't need to manage other end users' certificates, which is a great efficiency gain than traditional PKI. We further discuss various topics on UPKI.

F. Organization of Paper

The rest of the paper is organized as follows. Several related works on private key issuing protocol and hybrid system are presented in Section II. Details of the proposed certificate issuing and private key issuing protocol is described in Section III. Various discussions on UPKI are described in Section IV. Finally we conclude in Section V.

II. Related Works

A. Private Key Issuing Protocol in ID-based Cryptography

There have been lots of works to design private key issuing protocol for ID-based cryptography which does not have key escrow problem. A straightforward solution to the key escrow problem is to distribute the key issuing function to multiple authorities [2], [5]. If the master key of a KGC is distributed to multiple authorities and a private key is computed in a threshold manner [2], key escrow problem of a single KGC can be prevented. Generating a new private key by adding up multiple private keys [5] is another approach. However, these approaches requires high identification cost, because each authority has to identify the same user independently before key issuing. Considering the high cost of user identification, sometimes requires off-line interactions depending on policy, multiple independent identifications for the same user by multiple authorities is a big burden.

Another approach to solve the key escrow problem is issuing user's private key through an interactive protocol between user and KGC using some user-chosen secret information [8], [1]. Gentry [8] proposed a certificate-based encryption (CBE) scheme where private key is computed using user-chosen secret information, but it became a certificate-based scheme losing the advantage of ID-based cryptography. Al Riyami *et al.* [1] successfully removed the necessity of certificate (they named it certificateless public key cryptography) in a similar design using user-chosen secret information, but their scheme provides only implicit authentication of the public key. The random-looking public key generated by the user is not certified in any way. Thus any participant who wants to use the public key for the first time cannot be convinced whether the public key indeed belongs to the user.

Recently, Lee *et al.* [12], [13] proposed a unique private key issuing protocol in the *single-authority multiple-observer (SAMO)* model, which is the first pioneering work that can reduce the identification cost in multi-authority-based key issuing protocol. In this approach a single key generation center (KGC) provides user identification and partial key issuing function and multiple key privacy agents (KPAs) provide key privacy service without additional user identification. This proposal reduced the identification cost from multiple identifications by multiple authorities to a single identification by KGC. [12] is not efficient and not robust since it uses serial key privacy service by multiple KPAs. [13] improves [12] in efficiency and robustness by using secret sharing among multiple KPAs and threshold cryptography in key privacy service. But these schemes are subject to various attacks by malicious KGC and attackers [11]. The main reason of the weakness is that user is not authenticated using standard way and the correctness of protocol cannot be verified publicly.

Gangishetti *et al.* [6] proposed another private key issuing protocol. In this scheme user registration stage and key issuing stage are separated. In user registration stage KGC chooses a random number and gives it to the user through a secure channel, thus key escrow problem is not solved and secure channel is required. This scheme uses a public key directory to save user's key and registration information, but it is well known that public key directory is subject to various forgery attack. Kumar *et al.* [7] proposed a new key issuing protocol to solve the key escrow problem of [6] by using user-chosen randomness, but it still depends on the use of public key directory.

In this paper we try to solve the authentication problem of [12], [13] by using certificate. Since certificate provides explicit authentication of user, it can be used to authenticate user explicitly in multi-authority-based private key issuing protocol. By using the certified public key to blind the protocol messages in the private key issuing protocol, we achieve both privacy and verifiability of the protocol messages.

B. *Combining PKI and ID-based Schemes*

There have been several works which try to combine PKI and ID-based systems. [4] proposed a hybrid PKI/IBE system which merges traditional PKI with identity-based encryption system. To create an efficient hierarchy of multiple trust authorities they considered various combinations of PKI and ID-based systems. In an example of email system they suggested that the combination of using PKI for global name and using ID for local name is advantageous. [14] considered the issue of interoperation between entities in conventional PKI infrastructure and entities in ID-based infrastructure. These schemes assumed the existence of hybrid scheme, but they have not discussed more in-depth implementation issues like key escrow problem in ID-based system.

Our proposal in this paper can be considered as an efficient implementation example of hybrid system. Moreover, we propose the concept of unified public key infrastructure (UPKI) and provide further discussion on various issues and advantages of UPKI.

III. Certificate Issuing and Private Key Issuing Protocol

In this section we present the proposed certificate issuing and private key issuing protocol, first in generic model and second in pairing-based model. Generic model shows the overview of the proposed scheme in generic cryptosystems, while pairing-based model shows an efficient implementation of the proposed scheme in pairing-based cryptosystems. This efficiency comes from the fact that ID-based cryptography is implemented mainly in pairing-based setting and certificate-based cryptography is also possible in this setting.

A. *Entities and Their Roles*

We use the same SAMO model as in [12], [13]. In this paper we assume the existence of a key generation and certification authority (KGCA) which has the role of both key generation center (KGC) and certification authority (CA). We also assume the existence of multiple key privacy agents (KPAs) who provide key privacy service. The entities participating in the protocol and their roles are as follows.

- CA: A certification authority is a trusted authority in certificate-based model who checks user's identification according to his business rule and then issues a certificate for user-chosen public key.
- KGC: A key generation center is a trusted authority in ID-based model who checks user's identification according to his business rule and then issues a partial private key for user's ID.
- KGCA: A key generation and certification authority is a trusted authority in the unified model who has the role of both KGC and CA. KGCA checks user's identification according to his business rule, and then issues a certificate for user-chosen public key and a

partial private key for user's ID. KGCA's work is a public process in the sense that all certificates and partial private keys he issues can be published and their correctness can be verified publicly.

- n-KPAs: Multiple key privacy agents are honest observers who provide key privacy service for user's ID-based private key. They have a common public key and share the corresponding secret key using the t-out-of-n verifiable secret sharing (VSS) scheme [10]. For a given partial private key they provide key privacy service with their signatures. In the key privacy service KPAs don't need to check user's identification by themselves, but they provide services only for correct requests. KPA's work is a public process in the sense that its service can be published safely.
- User: A user with identity ID has long term private/public key pair (x, X). User gets a certificate for his public key X and use it for certificate-based cryptosystems. Using a private key issuing protocol, user finally gets an ID-based private key for ID in an escrow-free way.

Here KGCA (or KGC) and KPAs share a master private key for ID-based cryptosystem as shown in [13].

B. Generic Model

The proposed scheme consists of three protocols, certificate issuing, partial key issuing, and key privacy service. In generic model any cryptosystem which is suitable to implement these protocols can be used.

1) Certificate issuing: A user with identity ID chooses long term private/public key pair (x, X). User identifies himself/herself to CA and requests certificate issuing by sending (ID, X) and proof of possession of x. Then CA checks user's identification according to his business rule and proof of possession of x, and then issues a certificate $Cert(ID, X)$ for user-chosen public key X. Here the standard X.509 [16] certificate can be used.
2) Partial private key issuing: User requests partial key issuing to KGC by sending ID, $Cert(ID, X)$ and proof of possession of x. KGC verifies the validity of user's certificate and checks the proof of possession of x. If user's identity is verified correctly, KGC issues a partial private key sk'_{ID} for ID. Here sk'_{ID} can be published such that it's correctness can be verified by anyone.
3) Key privacy service: User requests key privacy service to n-KPAs by sending ID, $Cert(ID, X)$, proof of possession of x, and sk'_{ID}. Each KPA verifies the validity of $Cert(ID, X)$, proof of possession of x, and sk'_{ID}. If they are verified correctly, KPA signs sk'_{ID} with its private key and sends it to user through a secure channel. To build a secure channel, any secure key agreement protocol can be used. By collecting valid t signatures of KPAs user can retrieve his/her ID-based private key sk_{ID}.

Now user has both certified key pair (x, X) with certificate $Cert(ID, X)$ and ID-based key pair (sk_{ID}, pk_{ID}), where $pk_{ID} = H(ID)$. User can use both cryptosystems according to application needs. Here we described the proposed scheme in a way that the roles of KGC and CA are separated, but they can be easily integrated into a single authority as will be shown below.

C. Pairing-based Model

In this subsection we describe certificate issuing and private key issuing protocol using pairing-based cryptosystem. To obtain an efficient implementation, we use the following optimization.

1) We use pairing-based cryptosystems both for certificate-based and ID-based cryptography. Since ID-based cryptography is mainly implemented in pairing-based cryptosystems and certificate-based cryptography is also possible in this setting, using the same cryptosystem for both purposes is a good choice for efficiency.
2) We use a single KGCA rather than independent KGC and CA. Since user identification is a common basic function for KGC and CA, a single entity, KGCA, can provide both services more efficiently. Moreover, if a single authority provides both service, then certificate issuing and partial private key issuing can be provided in a single logical step.
3) We use an efficient construction of secure channel using one-way key agreement technique as shown in [12], [13]. Using this technique n-KPAs can send a protected message to the user without any prior arrangement.

Now we introduce the notation for the pairing-based cryptosystems. Let G_1 be an additive group of prime order q and G_2 be a multiplicative group of the same order. Let P denote a generator of G_1. The discrete logarithm problem (DLP) in these groups is believed to be hard. A bilinear pairing is a map $e : G_1 \times G_1 \rightarrow G_2$ with the following properties:

1) Bilinear: $e(aQ_1, bQ_2) = e(Q_1, Q_2)^{ab}$, where Q_1, $Q_2 \in G_1$ and $a, b \in Z_q^*$.
2) Non-degenerate: $e(P, P) \neq 1$ and therefore it is a generator of G_2.
3) Computable: There is an efficient algorithm to compute $e(Q_1, Q_2)$ for all $Q_1, Q_2 \in G_1$.

We also use the following two hash functions.

1) $H : \{0, 1\}^* \rightarrow G_1$ (extract point from ID).
2) $H' : \{0, 1\}^* \rightarrow Z_q^*$ (hash to the finite field).

First of all, KGCA and n-KPAs have to work together to set up system public key. KGCA picks his master private key $s_0 \in Z_q^*$ at random and publishes his public key $P_0 =$

s_0P. KGCA's master key s_0 is used to issue certificates and P_0 is used to verify certificates. n-KPAs share the KPA's secret key s_K in t-out-of-n fashion using the verifiable secret sharing (VSS) scheme such that cooperation of more than t KPAs is required to provide key privacy service. KPA_i has a secret share s_i and publishes a public share $P_i = s_iP$. KPA's public key $P_K = s_KP$ is computed and published. Then KGCA computes the system public key

$$Y = s_0P_K = s_0s_KP$$

and publishes it, which will be used as a system public key for ID-based cryptosystems. Anyone can verify the validity of Y by $e(Y, P) \overset{?}{=} e(P_K, P_0)$.

Now we describe the certificate issuing and private key issuing protocol in the following two steps.

Step 1. Certificate Issuing and Partial Private Key Issuing.

A user with identification information ID chooses a random number $x \in Z_q^*$ and computes $X = xP$. He will use (x, X) as a long-term private/public key pair for certificate-based cryptosystems. From KGCA user gets a certificate $Cert(ID, X)$ for X and a partial private key D_0 for the identity ID as follows.

1) User generates a signed certificate request $\sigma = xH(ID, X)$ using the short signature scheme [3]. He requests certificate issuing and partial private key issuing service by sending $\langle ID, X, \sigma\rangle$ and appropriate identification information. Here σ represents user's proof of possession of the private key x corresponding to the public key X.
2) When KGCA receives a certification request, he first checks user's identification information according to his business rule and checks the validity of σ by $e(\sigma, P) \overset{?}{=} e(H(ID, X), X)$. If user identification is correct, KGCA signs a certification document using a short signature scheme with the master private key s_0 and issues a certificate $Cert(ID, X) = s_0H(ID, X)$ according to the X.509 standard [16]. KGCA also computes user's ID-based public key $Q_{ID} = H(ID)$ and then he computes a partial private key by $D_0 = s_0Q_{ID}$. KGCA sends $Cert(ID, X)$ and D_0 to the user through a public channel (or publishes in a public place).
3) User checks the validity of $Cert(ID, X)$ by verifying KGCA's short signature with the public key P_0 by $e(P, Cert(ID, X)) \overset{?}{=} e(H(ID, X), P_0)$. User also checks the validity of D_0 by $e(D_0, P) \overset{?}{=} e(Q_{ID}, P_0)$.

In this step user gets a certificate $Cert(ID, X)$ which can be used for certificate-based cryptography. Here D_0 is only a partial private key and it is of no use by itself, thus it can be published safely. Now user has to get a key privacy service from KPAs to obtain a complete private key D_{ID}.

Step 2. Key Privacy Service.

In this protocol KPAs identify user with the certificate $Cert(ID, X)$ issued by KGCA. The protocol messages from KPAs to user is blinded using the certified public key X. Now user is involved in the key privacy service with multiple KPAs as follows.

1) User requests key privacy service to KPAs by sending $\langle ID, X, \sigma, Cert(ID, X), D_0\rangle$.
2) KPA$_i$ checks the validity of $Cert(ID, X)$ and D_0 by checking KGCA's signatures. KPA$_i$ also checks the validity of σ by $e(\sigma, P) \overset{?}{=} e(H(ID, X), X)$. If they are verified correctly, KPA$_i$ computes
$$D'_i = H'(ID, X, P_i, s_iX)s_iD_0.$$
He sends D'_i to the user through a public channel (or publish in a public place).
3) User computes $D_i = D'_i/H'(ID, X, P_i, xP_i)$ and checks its validity by $e(D_i, P) \overset{?}{=} e(D_0, P_i)$. If more than t valid D_is are collected, he can compute
$$D_{ID} = \sum_{i\in\Lambda} \lambda_{i,\Lambda}D_i = s_Ks_0Q_{ID},$$
where $\lambda_{i,\Lambda} = \prod_{l\in\Lambda\setminus\{i\}} \frac{l}{l-i}$ is the appropriate Lagrange coefficient and Λ is a subset of t valid D_is.
4) User checks the validity of D_{ID} by checking $e(D_{ID}, P) \overset{?}{=} e(Q_{ID}, Y)$. D_{ID} is an ID-based private key of the user corresponding to the public key $Q_{ID} = H(ID)$.

Here $H'(ID, X, P_i, s_iX) = H'(ID, X, P_i, xP_i)$ is a secret blinding factor shared between user and KPA$_i$ using the one-way key agreement technique. In this way KPAs can send blinded messages to user without any prior arrangement. Anyone except the legitimate user cannot extract private key information from the protocol messages.

Now we analyze some features of the proposed scheme.

- KPAs authenticate users using certificates issued by KGCA, thus it is hard for any attacker to impersonate other user to get illegal private key.
- Since the key privacy service by KPAs are protected by using a secret blinding factor generated with user's certified public key, anyone except the legitimate user cannot extract private key information from the protocol messages.
- Since the private key s_K is shared among n-KPAs using the t-out-of-n VSS scheme, the secrecy of user's private key D_{ID} is achieved assuming the honesty of at least $n - t + 1$ KPAs. This protocol is robust against partial unavailability of KPAs.
- Since KGCA and KPAs provide their services in public processes, they cannot provide illegal service to illegitimate users. KGCA's partial private key issuing is published and its correctness is publicly verifiable, thus malicious KGCA cannot try to impersonate a user by

himself or issue private key to illegitimate user without being detected. If malicious KPAs provide key privacy service for incorrect request, it will be detected and punished. If any illegal activity of KGCA or KPAs is published, they cannot keep on their business.

IV. Unified Public Key Infrastructure

A. Necessity of UPKI

Traditionally certificate-based cryptography and ID-based cryptography have been considered separately. Certificate-based cryptography and PKI is widely employed in the real world. It can provide explicit authentication of users, even in large scale groups with complex hierarchy. On the other hand ID-based cryptography is advantageous in key management, but it has the inherent key escrow problem. Thus, it is considered to be used in a small, but highly trusted, group. If key escrow problem is solved in reasonable way, it can be used in general environment. Another drawback of ID-based cryptography is that it is not scalable in the sense that it is hard to construct and manage the hierarchy of trust.

Thus, it looks a promising approach to combine these two cryptosystems such that the hierarchy of trust is managed by the traditional PKI mechanism and end users can utilize the advantages of ID-based cryptography. Note that many real world examples are operated in this way. As an example, employee ID card shows that a corporation certifies that the specified person is an employee of the corporation. When you check other's employee ID card, you first check the trustedness of the corporation in many possible ways, and then accept that the person with the ID is an employee of the corporation. As shown in [4], email system is another good example. If you receive an email from a stranger, you first check whether the email server or the corporation is a trusted one, and then try to check sender's ID and message. In an electronic world corporation can be verified using PKI mechanism and its member can be implicitly verified by the published ID.

In this section we show that this ideal combination is possible using the proposed certificate issuing and private key issuing protocol. We call it *unified public key infrastructure (UPKI)* in the sense that both certificate-based and ID-based cryptography are provided in a single framework more efficiently.

B. Proposed UPKI

To provide UPKI scheme, we assume that traditional PKI is already existent. One modification is that end CAs who issue certificates to end users are executing the role of KGCA as described in section III, i.e., KGCA issues both certificates and ID-based partial private keys to end users. We also assume the existence of multiple KPAs who provide key privacy service to users. Note that KPAs are honest public service, thus they can exist at the outside of the trust hierarchy.

In this setting a user gets a certificate $Cert(ID, X)$ for user-chosen long-term public key X from KGCA. Then user can use X as a long-term certified public key for certificate-based cryptography. User also gets an ID-based private key D_{ID} corresponding to the public key $Q_{ID} = H(ID)$ through an interactive protocol with KGCA and KPAs. Now user has a certified key pair (x, X) and an ID-based key pair (D_{ID}, Q_{ID}), and he/she has a choice of cryptosystem, either certificate-based or ID-based cryptography, according to application requirement. For example, users can choose cryptosystems according to the following guideline.

- ID-based cryptography: If a user interacts with other end users, then uses ID-based cryptography. Interactions between end users can be done more efficiently using ID-based cryptography. In this case end users don't need to manage other users' certificates.
- Certificate-based cryptography: If a user interacts with authorities such as CAs, governmental office, who requires explicit online presentation of prior authentication, then certificate-based cryptography has to be used. If the interacting entity requires explicit authentication with certificate, then certificate-based cryptography can be used.

Let's consider a case that two users in different KGCA domains are interacting using ID-based cryptography. A sender A is in $KGCA_A$'s domain with system parameter $param_A$ and a receiver B is in $KGCA_B$'s domain with system parameter $param_B$. A signed a document with his ID-based private key and sent it to B. Then the receiver B verifies the signature through the following two steps.

1) Verify the validity of $KGCA_A$ using the PKI mechanism and gets an authentic copy of the system parameter $param_A$.
2) Verify A's signature using the sender's ID and $param_A$.

C. Efficiency Comparison

Many researchers who tried to design escrow-free private key issuing protocol excluded the possibility of using certificate because introducing certificate and PKI just to aid ID-based cryptography is obviously a heavy overhead. But if we assume that PKI is already existent and try to add the functionality of ID-based cryptography additionally, we can make it possible with efficient combination as shown above.

If end user interaction is mainly done using ID-based cryptography and certificate is not used for end user interaction, then we can achieve huge efficiency gain.

- End users don't need to retrieve, store, and verify other users' certificates. End users only need to treat authorities' certificates to verify upper certification tree. End users only need to keep their own certificates. This is a great efficiency gain compared with traditional PKI.
- Since end user certificates are not used frequently, the number of certificate revocation is reduced and

CRL becomes much more lightweight. Note that end users don't need to care about CRL. If user certificates are used only for interactions with authorities, then authorities can try to use more efficient revocation mechanism than CRL.

One may criticize the inefficiency of introducing multiple KPAs, but they are necessary and indispensible entities to solve the key escrow problem of ID-based cryptography. Note that their services can be provided automatically and publicly. Therefore, the existence of KPAs is not a big obstacle.

D. Further Discussion on ID Revocation

One of the criticism about ID-based cryptography is the revocation problem. Since an ID is a fixed information given for a person, like name, it's hard to revoke ID. A straightforward solution to revoke ID is using ID revocation list (IRL) like CRL in certificate-based systems, but in this case a fixed ID cannot be used again and the person with the ID cannot participate in the domain again. Also it requires heavy management load of IRL. Another solution is using flexible ID, for example, combination of fixed ID and validity period can be used as a new ID. By using short-term validity period, we can remove the use of revocation list. In this case users have to interact with KGCA and KPAs more frequently to renew private key. Further study is required for the ID revocation problem.

V. Conclusion

In this paper we considered the advantages of using ID-based cryptography for user-to-user interaction and proposed an efficient implementation of combined cryptosystems where both certificate-based and ID-based cryptography are provided to end users. Assuming that traditional PKI is already existent, we have shown how to add ID-based cryptography in an escrow-free way. As a result, we provided an escrow-free private key issuing protocol and solved the authentication problem of [13] by using certificate. Our proposal is an efficient implementation example of the idea of [4].

In the proposed UPKI environment end users don't need to manage other users' certificate, which is a great efficiency gain. To the best of our knowledge this is the first efficient implementation of combined cryptosystem which supports both certificate-based and ID-based cryptography in a single framework with escrow-free private key issuing. More detailed deployment issues of UPKI will be our further research topic.

Acknowledgment

This work was supported by the Korea Research Foundation Grant funded by the Korean Government (MOEHRD, Basic Research Promotion Fund) (KRF-2007-521-D00472).

References

[1] S. Al-Riyami, K. Paterson, "Certificateless public key cryptography", Advances in Cryptology – Asiacrypt 2003, LNCS 2894, Springer-Verlag, pages 452–473, 2003.

[2] D. Boneh, and M. Franklin, "Identity-based encryption from the Weil pairing", Advances in Cryptology – Crypto 2001, LNCS 2139, Springer-Verlag, pages 213–229, 2001.

[3] D. Boneh, H. Shacham, and B. Lynn, "Short signatures from the Weil pairing", J. of Cryptology, Vol. 17, No. 4, pages 297–319, 2004.

[4] L. Chen, K. Harrison, A. Moss, D. Soldera, and N.P. Smart, "Certification of Public Keys within an Identity Based System, "ISC 2002, LNCS 2433, Springer-Verlag, pages 322–333, 2002.

[5] L. Chen, K. Harrison, N. P. Smart, D. Soldera, "Applications of multiple trust authorities in pairing based cryptosystems", InfraSec 2002, LNCS 2437, Springer-Verlag, pages 260–275, 2002.

[6] R. Gangishetti, M. C. Gorantla, M. L. Das, A. Saxena, "Threshold Key Issuing in Identity-based Cryptosystems", Computer Standards & Interfaces, Vol. 29, pages 260–264, 2007.

[7] K. P. Kumar, G. Shailaja, A. Saxena, "Secure and Efficient Threshold Key Issuing Protocol for ID-based Cryptosystems", Cryptology ePrint 2006/245, 2006.

[8] C. Gentry, "Certificate-based encryption and the certificate revocation problem", Advances in Cryptology - EUROCRPYT 2003, LNCS 2656, Springer-Verlag, pages 272 – 293, 2003.

[9] C. Gentry, A. Silverberg, "Hierarchical ID-Based Cryptography", Asiacrypt 2002, LNCS 2501, Springer-Verlag, pages 548-566, 2002.

[10] R. Gennaro, S. Jarecki, H. Krawczyk, T. Rabin, "Secure Distributed Key Generation for Discrete-Log Based Cryptosystems", Advances in Cryptology Eurocrypt '99, Lecture Notes in Computer Science, Vol. 1592, Springer-Verlag, pages 295–310, 1999.

[11] S. Kwon, S. Lee, "Security Analysis and Improvement for Key Issuing Schemes in ID-Based Cryptography", TrustBus 2006, LNCS 4083, Springer, pages 203-212, 2006.

[12] B. Lee, C. Boyd, E. Dawson, K. Kim, J. Yang and S. Yoo, "Secure Key Issuing in ID-Based Cryptography", In ACSW Frontiers 2004 - Second Australasian Information Security Workshop (AISW2004), volume 26 of Australian Computer Science Communications, pages 66–74. Australian Computer Society, January 2004.

[13] B. Lee, E. Dawson, S. Moon, "Efficient and Robust Secure Key Issuing Protocol in ID-based Cryptography", Preproceedings of the 6-th International Workshop on Information Security Applications (WISA 2005), pages 267-280, Ramada Plaza Jeju Hotel, Korea, Aug. 22-24, 2005.

[14] G. Price and C. J. Mitchell, "Interoperation between a conventional PKI and an ID-based infrastructure,"EuroPKI 2005, Canterbury, UK, June 30 – July 1, 2005. Revised Selected Papers, Springer-Verlag, LNCS 3545, pages 73-85, 2005.

[15] A. Shamir, “Identity based cryptosystems and signature schemes”, Advances in Cryptology - Crypto’84, LNCS 196, Springer-Verlag, pages 47–53, 1984.

[16] RFC 2459, “Internet X.509 Public Key Infrastructure Certificate and CRL Profile”, IETF, 1999, http://www.ietf.org/dyn/wg/charter/pkix-charter.html