Privacy Protection in PKIs: A Separation-of-Authority Approach*

Taekyoung Kwon[1], Jung Hee Cheon[2], Yongdae Kim[3], and Jae-Il Lee[4]

[1] Dept. of Computer Engineering, Sejong University, Seoul 143-747, Korea
[2] Dept. of Mathematical Sciences, Seoul National Univ., Seoul 151-747, Korea
[3] Dept. of Computer Science, Univ. of Minnesota - Twin Cities, MN, USA
[4] Korea Information Security Agency, Seoul, Korea

Abstract. Due to the growing number of privacy infringement problems, there are increasing demands for privacy enhancing techniques on the Internet. In the PKIs, authorized entities such as CA and RA may become, from the privacy concerns, a big brother even unintentionally since they can always trace the registered users with regard to the public key certificates. In this paper, we investigate a practical method for privacy protection in the existing PKIs by separating the authorities, one for verifying ownership and the other for validating contents, in a blinded manner. The proposed scheme allows both anonymous and pseudonymous certificates to be issued and used in the existing infrastructures in the way that provides conditional traceability and revocability based on the threshold cryptography and selective credential show by exploiting the extension fields of X.509 certificate version 3.

1 Introduction

A Public Key Infrastructure (PKI) plays an important role in asserting the ownership of public keys for users. Both the public key and the related information including the ownership and some useful attributes, should be signed by an authorized entity as the current standard, X.509 [19,30]. During the past decade, the PKIs have been widely deployed to support various communication sessions and electronic transactions over the Internet [4]. However, when we consider the privacy infringement problems on the Internet, it may not be difficult to find that the PKI does not protect privacy well at least because of the followings.

- The signed certificate should be publicized by the authority, for example, in the directory system, in a way that discloses lots of information about users in an "authentic" manner.
- An anonymous or pseudonymous certificate [1,17,24], saying that the true identity is not included in a subject field, could enhance the privacy to some extent. However, authorized issuers such as Certification Authority (CA) and Registration Authority (RA) may become, from the privacy concerns, a

* This work was supported by grant No. R01-2005-000-11261-0 from Korea Science and Engineering Foundation in Ministry of Science & Technology.

J.K. Lee, O. Yi, and M. Yung (Eds.): WISA 2006, LNCS 4298, pp. 297–311, 2007.

big brother even unintentionally since they can always trace the registered users with regard to the public key certificates.

In this paper, we solve the problem by investigating a practical method for privacy protection in the existing PKIs by separating the authorities, one for verifying ownership and the other for validating contents, in a blinded manner. We mean by the existing PKIs that we will make use of X.509 certificates in the current deployment. Thus, the proposed scheme allows both anonymous and pseudonymous certificates to be issued and used in the existing infrastructures in the way that provides conditional traceability and revocability based on the threshold cryptography and selective credential show by exploiting the extension fields of X.509 certificate version 3.

In order to enhance privacy, plenty of work has been done since D. Chaum [10] first introduced an anonymous credential system [5,6,7,11,12,20,29]. Many schemes that anonymize the transport medium between users and service providers are not main concerns in this paper [8,16,22,25], even though they are complementary to pseudonym systems (to prevent traffic analysis). Most of the current anonymous credential systems (1) are expensive (computationally and/or spatially), and (2) are hardly applicable to the existing PKIs. Rather, our work is close to the practical schemes considered in PKIs [17,18,24] but our scheme should have much more interesting and valuable features compared to them. Recently, we have found the closest work of Benjumea, Lopez, Montenegro, and Troya [3], but still we provide more useful and practical properties.

In Section 2, the basic concept of our privacy protection method is described. In Section 3, the detailed protocol is introduced while its analysis and discussions are handled in Section 4. This paper is concluded in Section 5.

2 Privacy Protection in PKI

We define the *traceable anonymous certificate*[1] (briefly TAC or anonymous certificate in this paper) that is distinguished from the conventional pseudonymous certificate [17,19,24,30] in the fact that the certificate filled with "anonymous" or any random pseudonym in the subject name field must be *conditionally traceable and revocable*. Note that it is not simple to issue anonymous certificates when we consider conditionally-revocable and unforgeable anonymity in the legacy infrastructure. The difficulty can be observed from the following simple scenarios.

- If CA issues an anonymous certificate without verifying a true identity, it is untraceable.
- If CA issues it but with verifying the real identity, CA can anytime link it and the real identity. So, we say a big brother.

[1] A user can fill out the field with a pseudonym. However, users tend to choose their preferred pseudonyms (rather than random ones) multiple times and this may allow possible linkage between different certificates. Thus, we recommend to anonymize the subject name field or to fill it with a random pseudonym, for example, by using the base 64 encoding of the SHA1 message digest of the private key [28].

– If CA issues it but with blind signatures, CA cannot verify the contents of certificate and the certificate may be untraceable and forgeable.

We could solve the problems simply by dividing the issuer. In other words, we could separate the functionality of verification of ownership from the validation of certificate contents. For example, we can devise a simple protocol in the current PKI model. 1) A user proves a true identity to RA (Registration Authority) and obtains a kind of token in a confidential manner. 2) The user then shows the token along with certificate contents to CA (without proving the true identity this time). 3) Finally the CA signs the certificate if the token is valid and returns the signed certificate to the user. RA and CA should keep user's true identity and the serial number of certificate, respectively, by indexing with the token. 4) When abuse is detected, CA and RA may be requested to disclose the true identity as for the corresponding certificate. They use the saved token as an index and match the result for tracing the identity. This simple protocol looks like working for PKIs. However, there still exists several limitations and problems.

– A malicious user can deceive the authorized parties easily since the token has no more than freshness and does not give any explicit connectivity between identity and contents. For example, the malicious user obtains the token in one place and gets the certificate in the other place. Note that this mixing is necessary for communicating with distinct servers subsequently. Then the malicious user can deny having gotten the certificate and assert the token was stolen. The authorized parties cannot prove the malicious user is lying.
– If the token is really compromised, the scheme fails at any phases. Say, the token is not a simple index any more and should have the same security level to secret keys. This is because the token is not intrinsically related to the corresponding session under cryptographic methods.
– The authorized parties are not extensible and scalable. Even if more than two issuers are organized, for example, one CA and multiple RAs, then two of them (one CA and one RA) can always disclose the user's true identity without the others' agreement.

Therefore, we extend the simple *separation-of-authority* idea to have more concrete system. First we describe our goal and introduce our basic model for achieving the goal from the general perspectives.

2.1 Goals and Requirements

The main goal of this paper is definitely to design a new separation-of-authority model and a specific protocol in a way that enables the traceable anonymous certificate in the existing PKIs. So, the following requirements must be satisfied.

– In appearance, the traceable anonymous certificate should be an X.509 certificate in which the subject name field is only anonymized or possibly filled out with a random pseudonym for high compatibility.
– The token must be unique and cryptographically bound to the corresponding session so that the malicious user could not deny afterwards and its compromise should not be the same as the compromise of secret keys.

- The separated authority must be scalable and allow threshold cryptography.
- The traceability and revocation must support bi-directional capability between identity and pseudonym. It should be able to trace a true identity from the anonymous certificate and vice versa, on agreement.
- The anonymous certificate must support anonymous credential system by providing a selective credential show.

2.2 Our Separation-of-Authority Model

In Table 1, we enumerate the notation to be used in the rest of this paper. Let κ be a general security parameter (say 160 bits) and ℓ be a special security parameter for public keys (1024 or 2048 bits). $\{M\}_{SIG_X}$ implies a message M along with its signature under X's signature key, while $\{M\}_{ENC_X}$ means an encrypted message under X's public key.

Figure 1 depicts our basic model, the separation-of-authority model, from the general perspectives, for issuing a traceable anonymous certificate in the current infrastructure. We define a certificate domain $CD = \{AI, BI\}$ where at least two authorized parties (AI similar to CA and BI similar to RA) work for issuing a traceable anonymous certificate. For accommodating multiple authorized parties, we allow a number of BIs in CD by re-defining $CD = \{AI, BI_i\}$ for $1 \leq i \leq n$. In abstract, a user U authenticates him or herself to the anonymous certificate issuer CD (more exactly AI and BIs) and then obtains the traceable anonymous certificate in a confidential manner. Thus, we need the following assumptions in our model.

Table 1. Notation

Participating entities			
U	User	CA	Certificate Authority
AI	Anonymous Issuer	BI	Blind Issuer
SP	Service Provider / Site	CD	Certificate Domain (AI,BI)
Cryptographic Primitives and mathematical notations			
SIG_X	Signature under X's private key	$H(\cdot)$	Strong one-way hash function
ENC_X	Encryption under X's cipher key	$\oplus$	Exclusive OR
$\leftarrow$	Inclusion	$\leftarrow_R$	Random selection
$\phi(\cdot)$	Euler totient function		
Protocol parameters			
ID_U	User's real ID	PN_U	User's subject name
pk_X	X's public key	sk_X	X's private key
apk_U	User's anonymized public key	ask_U	User's anonymized private key
e	CD's public exponent	d	CD's private exponent
d_1	BI's private exponent	d_2	AI's private exponent
N	CD's RSA modulus	r	User's blind factors
M	Anonymous certificate's contents	SN	Certificate's serial number
b	Anonymous certificate's header	c_i	Credentials
$\Rightarrow$	Send over secure channels	CT_U	User's real certificate
κ, ℓ	Security parameters	TAC_U	User's anonymous certificate

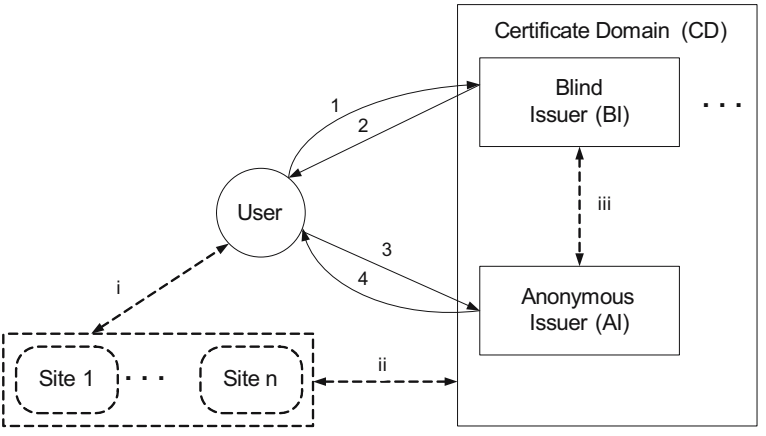

Fig. 1. A Separation-of-Authority Model

- There must be a specific method for authenticating U in steps 1 and 2. For example, U can be authenticated by showing some identification off line or by using the legacy certificate issued by CA on line. In the latter case, U is postulated to have own digital certificate in the current PKI. More weakly but conveniently, CD could accept password authentication methods afterwards.
- Secure communications channels must be established in steps 1 and 2, steps 3 and 4, and steps ii and iii, respectively. For example, we may assume the use of the current PKI and its most influential solution SSL/TLS or a kind of digital envelope for establishing secure channels. For the reasons, AI and BI are respectively postulated to have their own digital certificates in the current PKI.

We describe briefly the general procedure in our model step by step.

- Steps 1 and 2: BI verifies the true identity of U and blindly authenticates the contents of anonymous certificate. (Note: The blindly authenticated message corresponds to the token mentioned above.)
- Steps 3 and 4: AI verifies the contents of anonymous certificate without knowing the true identity and completes issuing the anonymous certificate.
- Step i: U utilizes the traceable anonymous certificate for registration or authentication to SP.
- Steps ii and iii: If abuse is detected, SP reports to AI so that AI can trace the corresponding identity by virtue of BI. If U's anonymous certificates must be revoked, BI and AI may identify them.

In step i, we can observe that no change is needed to use the anonymous certificate in the existing PKIs. The basic idea behind this model is that AI could control and verify the contents of a anonymous certificate without knowing the

user's real identity, while BI could verify the user's real identity without knowing the contents of a anonymous certificate when issuing it. This simple separation could wisely disconnect the links between the real identity ID_U and the anonymous certificate (or possibly a pseudonym) unless AI and BI collaborate.

As for the simple protocol we have mentioned above, we should have to solve problems related to the token and the extensibility. For the purpose, we enforce the user to contribute to the token, and make use of the mediated RSA-based blind signature for blinded authentication of message by multiple parties. In that sense, X.509 anonymous certificate is digitally signed by an RSA signature scheme, which is (arguably) a current de facto standard in PKIs [26]. Detailed version of our protocol and its extensions are described in Section 3.

2.3 Other Anonymous Credential Schemes

In 1981, Chaum introduced digital pseudonyms along with anonymous remailer systems [8]. Later in 1985, Chaum first introduced an anonymous credential system (also called pseudonym system) that allows users to interact with multiple organizations anonymously by using different pseudonyms in abstract [10]. Subsequently, Chaum and Evertse proposed a concrete scheme based on RSA but this required the involvement of a trusted third party in all transactions, which is undesirable in a distributed environment [11]. In 1988, Damgård proposed a credential system in which the central authority's role is very limited to ensuring that each pseudonym belongs to some valid user [14]. However, his scheme relied on quite heavy cryptographic primitives such as multi-party computations and zero-knowledge proofs. In 1995, Chen designed a practical scheme for Damgård's model by using the discrete-logarithm-based blind signatures, but her scheme overly postulated that the trusted party should refrain from transferring credentials between different users [12]. All of the above mentioned schemes did not consider protection against pseudonym sharing. In 1999, Lysyanskaya, Rivest, Sahai, and Wolf solved this problem but their scheme was again expensive because of their manipulation of one-way functions and zero-knowledge proofs [20]. In the same year, Brands proposed a discrete-logarithm-based certificate system by dealing with the privacy protected attribute certificates [4,5]. While this scheme looks infeasible to provide multi-show credentials, his scheme still remains useful. In 2001, Camenisch and Lysyanskaya first introduced an unlinkable pseudonym system that allows a user to demonstrate the possession of credentials as many times as necessary (say, multi-show) without linking each pseudonym and involving the issuing organization, and provides optional anonymity revocation [7]. They employed strong-RSA-based signature schemes and group signature schemes but are still complex due to proof of knowledge [2,13]. Subsequently, Camenisch and Herreweghen implemented their prototype called idemix (identity mix) [6]. Friedman and Resnick introduced a new method to generate a anonymous certificate through blind signatures but the centralized authority cannot verify the content of the anonymous certificate due to its blindness [15]. Verheul proposed another unlinkable scheme using self-blinding techniques constructed from bilinear map [29]. His scheme does not

provide selective demonstration of credentials and is hardly interoperable with RSA-based PKIs. It is also difficult to prevent a pseudonym abuse of malicious users.

3 Traceable Anonymous Certificate Protocols

We introduce our basic protocol for handling the traceable anonymous certificate and its extensions in this section.

3.1 Basic Protocol

Protocol Setup. As assumed in Section 2.2, we defined the following protocol setup for running the basic protocol.

- User Authentication
  - U has an ordinary digital certificate issued by CA under U's true identity. This may be used for user authentication.
  - Otherwise, U should face BI in order to show his or her identification off line (in Step 1).

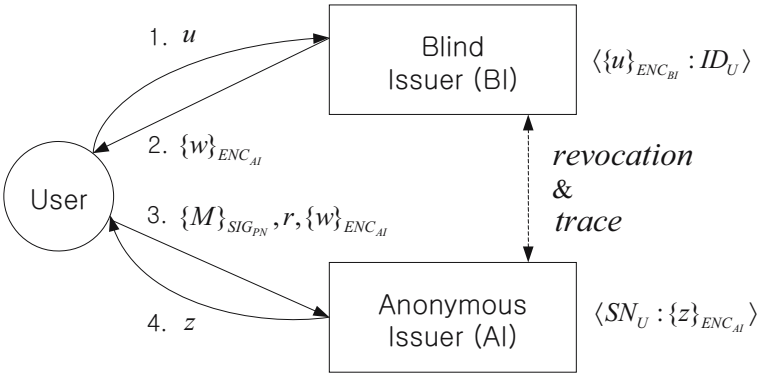

Fig. 2. Anonymous Certificate Protocol (Note: Channels are assumed secure.)

- Secure Communications Channel
  - AI and BIs have respective digital certificates issued by CA. Respective public keys are used for establishing secure sessions.
  - For establishing SSL/TLS sessions, the certificates are used along with server (AI and BIs, respectively) authentication.
  - Simply we can construct a digital enveloped message: $\{M\}_{ENC_K}$, $\{K\}_{ENC_{AI}}$. It means that a large message M is encrypted under symmetric encryption key K while K is encrypted under the certified public key of AI.

- Certification Public Key
  - All authorized parties in CD should share the same public key parameters that will be used for certification. This is different from the ones used for establishing secure communications channels. We focus on using RSA for wide acceptance and define that AI and BI share the same public key $\langle e, N\rangle$ for certification.
  - As for the RSA private exponent d of CD, we split it into two shares in the way that AI and BI should hold d_2 and d_1 respectively where $d = d_1 d_2 \mod \phi(N)$, for generating partial signatures.
  - We could apply a threshold digital signature scheme [27] for BI 's partial signatures by deploying a number of BIs (see Section 3.2.1)
- User's Knowledge
  - U knows at least three public key certificates of servers such as CD, AI, and BI respectively, as we mentioned above.

Anonymous Certificate Issuing. U proceed with the following steps (See Figure 2) for obtaining a traceable anonymous certificate, and repeat this protocol to acquire more anonymous certificates. Remind that $\Rightarrow$ means a secure channel that must be encrypted under a proper encryption key.

1. $\mathbf{U} \Rightarrow \mathbf{BI}:$ $\mathbf{u}$
   U sets $PN_U =$ "*anonymous*" or with a random pseudonym, and generates a new key pair $\langle apk_U, ask_U\rangle$. U also computes $SN_U = H(CD, apk_U, \rho)$ by choosing a κ bit random number ρ. U then constructs an X.509 certificate skeleton by composing $b \leftarrow \langle SN_U, PN_U,\ apk_U\rangle$ and $M \leftarrow \langle b, (c_i)\rangle$. U subsequently computes $h = H(M)$. Finally U computes $u = h \cdot r^e \mod N$ where $r \leftarrow_R \{0,1\}^\kappa$ and sends u to BI.
   At this stage, U must be authenticated by BI, for example, by establishing SSL/TLS channel with full authentication.
   Upon receiving u, BI computes $w = u^{d_1} \mod N$ and records $\langle \{u\}_{ENC_{BI}} : ID_U\rangle$ in its stable storage. Note that U's true identity ID_U was obtained by user authentication, for example, from the U's certificate. Finally BI computes $\{w\}_{ENC_{AI}}$ and sends it back to U.
2. $\mathbf{BI} \Rightarrow \mathbf{U}:$ $\{\mathbf{w}\}_{\mathbf{ENC_{AI}}}$
   Upon receipt of this message, U computes $\langle \{M\}_{SIG_{PN}},\ r,\ \{w\}_{ENC_{AI}}\rangle$ and sends it to AI. Note that $\{M\}_{SIG_{PN}}$ means message M and its signature under ask_U rather than sk_U.
3. $\mathbf{U} \Rightarrow \mathbf{AI}:$ $\{\mathbf{M}\}_{\mathbf{SIG_{PN}}}$, $\mathbf{r}$, $\{\mathbf{w}\}_{\mathbf{ENC_{AI}}}$
   Upon receiving this message, AI should abort unless $\{M\}_{SIG_{PN}}$ is valid. After computing $z = w^{d_2} \mod N$, AI should abort unless $z \cdot r^{-1} \mod N$ is verified by $\langle M, e, N\rangle$. Finally AI records $\langle SN_U : \{z\}_{ENC_{AI}}\rangle$ in its stable storage, and responds with z.
4. $\mathbf{AI} \Rightarrow \mathbf{U}:$ $\mathbf{z}$
   Upon receiving z, the user U recovers $h^d \mod N$ by computing $z \cdot r^{-1} \mod N$. U should abort unless $h^d \mod N$ is verified under $\langle M, e, N\rangle$. If it is verified, U can hold $\langle M, h^d \mod N\rangle$ as a new traceable anonymous certificate.

Now the user can access any service providers or sites (called SPs), with his or her anonymous certificate as (s)he does with a real identity certificate. The anonymous certificate can also be revoked, for example, by using a CRL or OCSP. This property makes our scheme conform to the legacy systems very easily.

Mandatory Revocation and Trace. Abuse of anonymity or pseudonymity is a problem that must not be neglected even if it is weak anonymity. When one's abuse is detected, SP can ask mandatory revocation and trace functions to AI by submitting SN_U of the corresponding certificate in step ii. Then AI and BI may run the following protocol. Remind again that $\Rightarrow$ implies a secure channel.

iii. $\mathbf{AI \Rightarrow BI:}$ $\mathbf{z}$
Upon obtaining SN_U, AI could retrieve $\langle SN_U : \{z\}_{ENC_{AI}} \rangle$ from its storage, in order to recover z. AI then sends z to BI.
Upon receiving z, BI can raise it to e and derive u. Finally, BI encrypts u under its own public key, and retrieves $\langle \{u\}_{ENC_{BI}} : ID_U \rangle$ from its storage so as to obtain a real identity ID_U.

As a result, the true identity ID_U can be disclosed.

On the other hand, when all anonymous certificates owned by a specific user must be revoked, for example, a certain user U' is known to be a criminal or spy, another protocol is necessary. In this case, AI and BI may run the following protocol.

iii'. $\mathbf{BI \Rightarrow AI:}$ $\mathbf{w_1, \cdots, w_i}$
Upon the identity $ID_{U'}$, BI could retrieve all records $\langle \{u\}_{ENC_{BI}} : ID_{U'} \rangle$ from its storage, and aggregates all corresponding u values. BI then computes $w = u^{d_1} \mod N$ for all aggregated values. Subsequently BI sends all w values to AI.
Upon receiving the list of w values, AI may raise the respective w values to d_2 so as to obtain corresponding z values. AI then encrypts respective z values under its own key, and retrieves $\langle SN_{U'} : \{z\}_{ENC_{AI}} \rangle$ from its storage. Finally AI is able to obtain the corresponding $SN_{U'}$ values.

As a result, all anonymous certificates of U' can be disclosed.

3.2 Extended Protocols

Threshold Schemes. We can apply an RSA (L, k)-threshold signature scheme by Shoup [27] to split the BI's secret d_1 into L members $BI_1, BI_2, \ldots, BI_L$ so that k members out of L members can jointly generate the BI's partial signature. In the basic scheme, we assumed that the dealer generates d_1 and d_2 and provide them to BI and AI, respectively. In this stage, instead of sending d_1 to one BI she generates L distinct shares for BI_1, BI_2, ..., BI_L and sends each share to each BI member. The shares are distinct points of a $(k-1)$-degree polynomial with the constant term d_1.

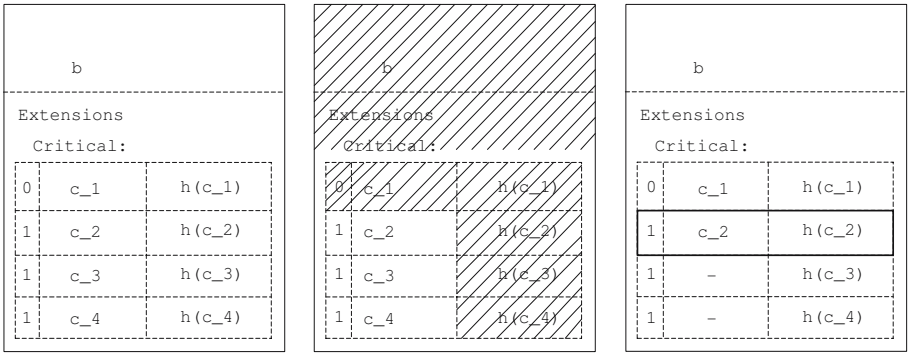

Fig. 3. Selective Credential Show in Anonymous Certificate

One difference from the original RSA threshold scheme is that d is split into d_1 and d_2. In our scheme, k BI members generate their signature shares and combine them to obtain $w = u^{d_1 \Delta}$ by Lagrange Interpolation. While $\Delta = 4(L!)^2$ can be removed in the original scheme, the BIs can not since they do not know d_2. In Step 5, after receiving (u, w), the AI computes $z' = w^{d_2}$ which satisfies $z'^e = u^{\Delta}$. Since $\gcd(e, \Delta) = 1$, the AI can easily compute z such that $z^e = u$: Find integers f and g with $fe + g\Delta = 1$ using Euclidean Algorithm. Take $z = z'^g u^f$. Then $z^e = u^{g\Delta} \cdot u^{fe} = u$.

Since Shoup's scheme is efficient as well as secure, it does not reduce the efficiency of our scheme significantly: When generating BI's partial signature, we need two exponentiations for each k members of BIs and $L-1$ multiplications for combining shares, and two more exponentiations are needed from the AI side. Also the restriction on the system parameter is small: e should be a prime larger than L and a modulus N is a product of two strong pseudoprimes p and q where both $(p-1)/2$ and $(q-1)/2$ are distinct primes. For more details, refer to [27].

Selective Credential Show. We can extend our anonymous certificate to one that provides selective demonstration of credentials by very little modification only. Figure 3 shows how to manipulate digital credentials in our anonymous certificate for selective show. While b means a header (say, remaining fields except extensions), user's digital credentials can be placed as depicted in Figure 3-(a). In other words, each credential c_i and its hashed value $h(c_i)$ are stored along with a flag denoting whether c_i is selective (1) or mandatory (0), in each semi-record of the critical extension fields, say, $\langle flag, c_i, h(c_i) \rangle$. In Figure 3-(b), we give a little modification to the certifying system so that a CD should certify all semi-records of which flag is 0 but a hashed value only for all with flag 1 in the critical extension fields. The shadowed area implies the parts that are all hashed and digitally signed by CD in Figure 3-(b). We can see the values c_2, c_3, and c_4 are excluded. Any SP who verifies the corresponding anonymous certificate

should consider it and do the verification just in the same way. As a result, a user who owns the anonymous certificate is able to choose some credentials of which flags are 1s, and show them selectively as Figure 3-(c) depicts. We can see that c_3 and c_4 are eradicated by the user. SP could validate the selective credentials by computing their hashed values and comparing them to the original ones, after verifying the CD's certification on the shadowed area. For example, SP should compare a hashed value of c_2 to the value $h(c_2)$ of the certificate after verifying the validity of the certificate.

4 Analysis and Discussions

4.1 Properties

It is explicit that our scheme satisfies the requirement stated in Section 2.1. Note that we do not consider the unlinkability in multi-show but only in single-show scenario due to digitally signed X.509 certificate. Since the *anonymous certificate* is an X.509 certificate except that a pseudonym is used in the subject identifier field, *authenticity* and *accountability* can be achieved easily under the pseudonym. *Revocation* and *multi-show* can also be manipulated by using a Certificate Revocation List (CRL) or Online Certificate Status Protocol (OCSP) [19,21]. We are able to define some *credentials* (which can even be selectively demonstrated in an extended scheme) in the anonymous certificate by exploiting the extension fields of X.509 version 3. We also achieve *protection against pseudonym forgery* by careful manipulation of our issuing protocol. Amongst all, our system will provide *conditional traceability* in order to revoke pseudonymity with authority, for example, when its abuse is detected or all pseudonyms of a specific user must be revoked. Finally, in our extensions, a *threshold cryptography* among the authorities and a *selective credential show* are considered for allowing diverse setup.

As we summarized briefly, our system is extremely simple but can provide many valuable features for pseudonyms in practical ways, even without any change in the existing infrastructure such as CAs and various service providers in the legacy PKIs.

4.2 Security Analysis

Anonymity. Anonymity comes from unlinkability between pk_U and apk_U in our system. In Step 3, an RSA-based blind signature [9] is requested to BI to generate an anonymous certificate for apk_U only when a real identity certificate of pk_U is verified. Since BI has witnessed neither the anonymous certificate nor its hashed value, BI cannot link pk_U and apk_U. On the other hand, AI knows only apk_U, not pk_U. Unless AI and BI cooperate, apk_U and pk_U are unlinkable.

As we mentioned already, our system provides weak anonymity only. In case the same certificate is used multiple times, the transactions are linked through the same structure of certificate (say, SN, apk_U, and so on). However, the user's identity is still hidden.

To achieve strong anonymity by allowing unlinkability among certificates, the user just issues a number of pseudonyms through distinct protocols. Since each certificate is generated independently, one can not find a link between pseudonyms unless anonymity (unlinkability between a real identity and a pseudonym) is broken.

Traceability or Anonymity Revocation. When AI and BI cooperate, the proposed protocol enables traceability between a real identity and an anonymized certificate. If one combines AI holding $\langle d_2, SN_U, z\rangle$ and BI holding $\langle d_1, ID_U, u\rangle$ where $z^e \equiv u \mod N$, one can obtain the link between SN_U and ID_U. One possible failure on tracing is that the user gives a wrong blind factor r to AI, but it is avoided in our system. To prevent the user from manipulating r after its commitment to BI, we encrypt the partial signature from BI by the AI's public key. Since the user can not obtain signature pairs from the encryption, she can not generate a fake partial signature or its encryption.

Certificate Forgery Protection. Protection against certificate forgery relies on the RSA blind signature. Further, AI checks the contents M and the user's possession of her private key before signing. Thus as long as the signature scheme is secure, one must alter the contents M before BI completes the signature to get a certificate for unauthorized pseudonyms. However, it is hard if the hash function is collision-resistant as pointed out before.

4.3 Practical Considerations

An anonymous certificate issued by our system can be used for various applications, especially that need to maintain a history of users while providing privacy for individuals, for instance, various web sites, reputation systems, P2P file sharing systems and bulletin boards.

- The most interesting feature of our scheme, from the practical perspectives, is that we follow the current PKI. In that sense, CA and RA can take the roles of AI and BI, respectively. This will cause easy migration for the existing system.
- It may be considered inconvenient for users to carry their private keys and certificates for accessing every service. Thus, there are various approaches for supporting the roaming users' mobility but they are out of scope in this paper. Any PKI roaming scheme can be applied to our system since we follow the standard PKI.
- The most widely used user authentication method in the present Internet is password authentication by which users can access services at different locations with passwords only. However, at registration for obtaining the ID and password pair, users are providing too much information to the service sites. In this existing system, the anonymous certificate can be applied for registration only if the service sites have required password authentication. The anonymous certificate can be constructed so as to minimize the private

information and to control it, for example, by the selective credentials. After the registration, the service sites can maintain the registration data including SN_U, and allow users to use their preferred ID and password pair as usually without leaking their private information.
- For enhancing anonymity of each pseudonym (say unlinkability in each use), we can 1) obtain and use many anonymous certificates at once or 2) utilize our anonymous certificate as means to access another unlinkable anonymous credential system. The latter implies an improvement of the existing anonymous credential systems by not giving a real identity at an initial phase.
- Before sending an initial message to BI, we can let U submit her basic information such as a use (for example, pseudonym identity, prescription, etc.), sex or age, so that AI can choose an appropriate BI for the user[2].
- In practice, we can give the respective roles of AI and BI (or BIs) to various entities. For example, an web site (or a CA designated by the web site) can play the role of AI, while (a group of) court, bank, social security office, civil organization or other government agencies may have a role of BI. This is quite natural setting: Web sites only needs to verify if the new joining member is certified by trusted agencies and can be traceable in case of illegal activities. On the other hand, agencies representing the role of BI play the role of mediator between the user and the web site in case of legal disputes.

We believe our scheme is useful for any e-commerce application, since it provides 1) privacy of the client, 2) conditional traceability in case of misuse, 3) full compatibility with X.509 standard, and 4) very simple and efficient.

5 Conclusion

In this paper, we investigate a practical method for privacy protection in the existing PKIs by separating the authorities, one for verifying ownership and the other for validating contents, in a blinded manner. It is explicit that our scheme satisfies the requirement stated in Section 2.1. The proposed scheme allows both anonymous and pseudonymous certificates to be issued and used in the existing infrastructures in the way that provides conditional traceability and revocability based on the threshold cryptography and selective credential show by exploiting the extension fields of X.509 certificate version 3.

We could observe that most of the current anonymous credential systems 1) are expensive (computationally and/or spatially), and 2) are not simply applicable to the existing PKIs (in particular where an RSA signature scheme is solely supported). The major difference from the other related work is that our scheme considers adding new properties such as conditional traceability and weak anonymity to the existing X.509 certificate (in particular signed by RSA). The related previous attempts such as [3,17,18,24] were also compared with our scheme.

[2] We can consider a set of BIs, each of which has a different role in verifying users with their identity information, for example, male or female only, adult only, prescription only and so forth. It is also considerable that AI sets a credential c_i with that information in the skeleton. The final result can also be verified by AI in step 3.

References

1. C. Adams and M. Just, "PKI: Ten Years Later," the 3rd Annual PKI R&D Workshop, NIST, 2004.
2. G. Ateniese, J. Camenisch, M. Joye, and G. Tsudik, "A practical and provably secure coalition-resistant group signature scheme," CRYPTO '00, Lecture Notes in Computer Science, vol. 1880, Springer-Verlag, pp.255-270, 2000.
3. V. Benjumea, J. Lopez, J. Montegegro, and J. Troya, "A first approach to provide anonymity in attribute certificates," PKC 2004, Lecture Notes in Computer Science, vol. 2947, Springer-Verlag, pp.402-415, 2004.
4. S. Brands, *Rethinking public key infrastructures and digital certificates - Building in Privacy*, PHD thesis, Eindhoven Institute of Technology, Eindhoven, The Netherlands, 1999.
5. S. Brands, "A technical overview of digital credentials," Manuscript, 2002.
6. J. Camenisch and E. Herreweghen, "Design and implementation of the Idemix anonymous credential system," ACM Conference on Computer and Communications Security, pp.21-30, 2002.
7. J. Camenisch and A. Lysyanskaya, "Efficient non-transferable anonymous multishow credential system with optional anonymity revocation," Eurocrypt '01, Lecture Notes in Computer Science, vol. 2045, Springer-Verlag, pp.93-118, 2001.
8. D. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," Communications of the ACM, vol. 4, no. 2, February 1981.
9. D. Chaum, "Blind signature system," CRYPTO '83, Plenum Press, page 153, 1984.
10. D. Chaum, "Security without identification: Transactions systems to make big brother obsolete," Communications of the ACM, vol. 28, no. 10, pp.1035-1044, 1985. Revised version, "Security without identification: Card computers to make big brother obsolete," available at `http://www.chaum.com/`.
11. D. Chaum and J. Evertse, "A secure and privacy-protecting protocol for transmitting personal information between organizations," CRYPTO '86, Lecture Notes in Computer Science, vol. 263, Springer-Verlag, pp.118-167, 1987.
12. L. Chen, "Access with pseudonyms," Cryptography: Policy and Algorithms, Lecture Notes in Computer Science, vol. 1029, Springer-Verlag, pp.232-243, 1995.
13. R. Cramer and V. Shoup, "Signature schemes based on the strong RSA assumption," ACM Conference on Computer and Communications Security, pp.46-52, 1999.
14. I. Damgård, "Payment systems and credential mechanism with provable security against abuse by individuals," CRYPTO '88, Lecture Notes in Computer Science, vol. 403, Springer-Verlag, pp.328-335, 1988.
15. E. Friedman, and P. Resnick, P. "The Social Cost of Cheap Pseudonyms". Journal of Economics and Management Strategy vol. 10, no. 1, pp. 173-199, 2001.
16. D. Goldschlag, M. Reed, and P. Syverson, "Onion routing for anonymous and private internet connections," Communications of the ACM, vol. 42, no. 2, pp.84-88, February 1999.
17. J. Graaf and O. Carvalho, "Reflecting on X.509 and LDAP, or How separating identity and attributes could simplify a PKI," WSEG 2004, pp. 37-48.
18. R. Grimm and P. Aichroth, "Privacy Protection for Signed Media Files: A Separation-of-Duty Approach to the Lightweight DRM (LWDRM) System," ACM MM&Sec'04, pp. 93-99, 2004
19. R. Housley, W. Polk, W. Ford, and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile," IETF Request for Comments 3280, April 2002.

20. A. Lysyanskaya, R. Rivest, A. Sahai, and S. Wolf, "Pseudonym systems," Selected Areas in Cryptography, Lecture Notes in Computer Science, vol. 1758, Springer-Verlag, 1999.
21. M. Myers, R. Ankney, A. Malpani, S. Galperin, C. Adams, "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP," IETF Request for Comments 2560, June 1999.
22. A. Pfitzmann, B. Pfitzmann, and M. Waidner, "Isdnmixes: Untraceable communication with very small bandwidth overhead," Manuscript, 1991.
23. A. Pfitzmann and M. K̈ohntopp, "Anonymity, Unobserbability, and Pseudonymity - A Proposal for Terminology," International Workshop on Design Issues in Anonymity and Unobservability, Lecture Notes in Computer Science, vol. 2009, Springer-Verlag, pp.1-9, 2000.
24. S. Rafaeli, M. Rennhard, L. Mathy, B. Plattner, and D. Hutchison, "An Architecture for Pseudonymous e-Commerce," AISB'01 Symposium on Information Agents for Electronic Commerce, pp. 33-41, 2001.
25. M. Reiter and A. Rubin, "Crowds: anonymity for Web transactions," ACM Transactions on Information and System Security, vol. 1, no. 1, pp.66-92, 1998.
26. R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signature and public-key cryptosystems," Communications of the ACM, vol. 21, no. 2, pp.120-126, 1978.
27. V. Shoup, "Practical threshold signatures," EUROCRYPT 2000 , Lecture Notes in Computer Science, vol. 1087, Springer-Verleg, pp. 207-220, 2000.
28. F. Siebenlist, "Is there life after X.509?," Security Workshop of the Globus World 2004 Conference, 2004.
29. E. Verheul, "Self-blindable credential certificates from the Weil pairing," Asiacrypt '01, Lecture Notes in Computer Science, vol. 2248, Springer-Verleg, pp.533-551, 2001.
30. X.509, "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks," ITU-T Recommendation X.509, March 2000. Also avaiable at ISO/IEC 9594-8, 2001.