Anonymity 2.0 – X.509 Extensions Supporting Privacy-Friendly Authentication

Vicente Benjumea[1], Seung G. Choi[2], Javier Lopez[1], and Moti Yung[3]

[1] Computer Science Dept., University of Malaga, Spain
{benjumea,jlm}@lcc.uma.es
[2] Computer Science Dept., Columbia University, USA
sgchoi@cs.columbia.edu
[3] Google & Computer Science Dept., Columbia University, USA
moti@cs.columbia.edu

Abstract. We present a semantic extension to X.509 certificates that allows incorporating new anonymity signature schemes into the X.509 framework. This fact entails advantages to both components. On the one hand, anonymous signature schemes benefit from all the protocols and infrastructure that the X.509 framework provides. On the other hand, the X.509 framework incorporates anonymity as a very interesting new feature. This semantic extension is part of a system that provides user's controlled anonymous authorization under the X.509 framework. Additionally, the proposal directly fits the much active Identity 2.0 effort, where anonymity is a major supplementary feature that increases the self-control of one's identity and privacy which is at the center of the activity.

Keywords: Anonymous authentication, X.509 certificates, group signatures, ring signatures, traceable signatures.

1 Introduction

As the number of remote Internet transactions grows, the amount of personal information that organizations collect also increases. In the near future, the majority of transactions that a user can perform in her daily life will be done remotely via the Internet (e-government, e-bank, e-commerce, e-library, e-services, etc.). This, together with the fact that information systems are able to collect, store and cross reference big amounts of data, implies that the Internet will become the largest surveillance system ever devised.

Anonymity can be seen as a cornerstone in individual privacy protection in environments like the Internet. Recently, new signature schemes oriented towards providing support for anonymity have been designed from a pure cryptographic point of view. These signature schemes focus on anonymity from different point of views with many interesting features. Group signatures [10,1,14], ring signatures [30,14], traceable signatures [24,27,12], are among them. However, though they exhibit very interesting features, they have not been transferred to practical open systems yet, and no one has even studied in what available systems framework they can be well supported.

F. Bao et al. (Eds.): CANS 2007, LNCS 4856, pp. 265–281, 2007.

X.509 public key and attribute certificates [23] conform a standard and secure mean to convey users' identity and authorization information respectively. They are widely used means to convey user's information in open systems. However, they were designed to support identities and anonymity was not considered in their design, let alone the available recent new anonymous signatures.

Motivated by the above two issues, this paper presents a semantic extension to X.509 certificates aimed at incorporating the aforementioned new signature schemes. Compatibility, simplicity yet high level of applicability to many various existing anonymous schemes is at the core of the work.

This semantic extension entails that a standard framework can be applied to new scenarios where anonymity is an issue, featuring the interoperability that the standard provides. On the other hand, it allows adapting the framework to new anonymity requirements with no need to alter the standard. In a sense, its importance is in showing the robustness of the X.509 framework to basic semantical changes in its operating environment and its ability to support credentials in a much wider range than originally intended.

Moreover, we note that this semantic extension can also be applied in a similar way to other frameworks, such as SPKI [15,16] and others.

The present work is part of a broader ongoing work and a system that attempts to use these extended X.509 certificates to create a user centric system where the user is able to access system resources while controlling how and which kind of information is disclosed.

Anonymity is at the core of the system, and users are entitled to anonymously prove that they have enough privileges as for being authorized to perform a given transaction.

This process is ruled by authorization policies specified for each resource. The system fits in the X.509 framework and mixes with existing systems, supporting both identified and anonymous authorization.

In the current Identity 2.0 [21] effort the user is the center of the system, and decides what information to disclose in order to be authorized to perform a remote transaction. Under this approach, the user controls her identity and how it is used, as opposed to Identity 1.0 where service providers hold personal information in order to identify the users and make them accountable for their actions.

Anonymity is perhaps the cornerstone in a user centric point of view, since allows the user to access resources but avoids disclosing user's sensitive information. Therefore, if anonymity is joined with the user controlled disclosure of information, we find that the system fits and is one step beyond the Identity 2.0 effort.

The paper is organized as follows. Section 2 presents some related work and overviews the fundamentals which our work is built on. Then, Sect. 3 describes the main idea behind the proposed extension. Section 4 shows how the above mentioned signature schemes can be integrated into the proposed extension and describes their main properties. Section 5 describes how the X.509 public key certificate can be extended to incorporate this extension in a controlled way and how the extension also applies to X.509 attribute certificates. Section 6 presents some performance results for our implementation of traceable signatures (which is part of the overall broad system design and demonstrates its feasibility). Sect. 7 concludes the paper. Finally, the appendices give the ASN.1 specification of the certificate semantic extension.

2 Background

2.1 Related Work

Anonymity has been largely studied since D. Chaum introduced the problem in [7,8], yielding many privacy aware interactive systems [9,11,25,5,6,34,29]. Some studies have been oriented towards providing support for anonymous authentication in different contexts [32,33,28,3,4], and, as far as we know, only a few of them [28,3,4] have been focussed to some extend on interoperating with standard frameworks, however they are not perfectly integrated and require dedicated protocols to fulfill their aim. Moreover they only provide a fixed flavor for anonymity. In the presented proposal, many different flavors of anonymity are gently introduced into X.509 certificates, which are then transparently supported by the underlying infrastructure, with no need of dedicated extra protocols. It also provides a suitable way to incorporate new forthcoming signature schemes for anonymity into the standard framework.

2.2 X.509 Certificates

X.509 public key certificates (PKC) [22,20] have been designed to bind a public key to a subject, under the consideration that such a subject is the only one that knows the associated private key (Fig. 1). In these certificates, the certification authority, i.e. the entity that certifies the binding, is equally important. Any entity using the public key certificate will trust the binding of the subject and the public key if it trusts the entity that issued the certificate. The relationship between the subject and the public key holds as long as the associated private key is known only to the entity that the certificate subject field refers to.

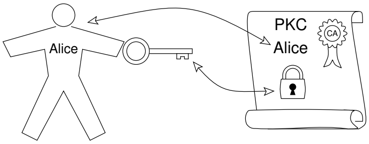

Fig. 1. Relationship between user and public key certificate

X.509 public key certificates have been proved as a very useful tool for providing authentication in many different contexts, such as electronic mail, the World Wide Web, user authentication and IPsec. Particularly, the TLS [13] (and

SSL [19]) transport layer protocol uses X.509 public key certificates to provide an authenticated secure communication channel to application layers.

X.509 attribute certificates (ATC) [23,17] bind a holder with a set of attributes, and at the same time can be linked with a X.509 public key certificate (Fig. 2). The attribute authority is the entity that certifies such bindings. The attributes can be used for authorization purposes in many different ways, providing a flexible authorization approach. The holder of the attribute certificate will be authenticated by means of the linked public key certificate to enjoy the privileges associated with the specified attribute. Here again, the authorization verifier needs to trust the certificates issuers in order to trust the bindings that they state.

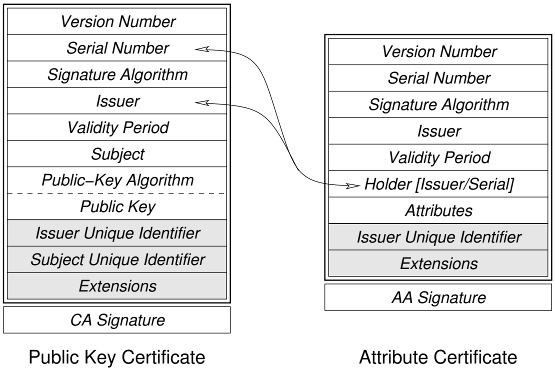

Fig. 2. Relationship between public key and attribute certificates

X.509 certificates are valid for a limited period of time that is specified in the certificates. However, under certain circumstances, the binding can be revoked, e.g. if the private key is compromised, or if the specified attribute no longer relates with the holder. If a certificate is revoked, the fact is made public by means of a *certificate revocation list* (CRL). Additionally, OCSP [26] provides an interactive way to check if a given certificate has been revoked.

2.3 Digital Signatures

Signature Schemes for Identification. These signature schemes are those ones that, when used in an adequate environment such as the X.509 framework, provide an authentication method that directly and uniquely identifies the entity that is being authenticated. They are unforgeable and provide authentication and non-repudiation features. In these schemes, one public key corresponds to a unique private key, and an adequate environment provides a correlation between the public key and the identity . Such correlation is based on the fact that only the one who knows the private key is the entity that performs the authentication. Examples of these kind of signature schemes can be DSA [18], RSA [31], and others.

Signature Schemes for Anonymity. We mean here those ones that allow the breaking of the correlation between a public key and the identity of the entity that owns an associated private key. With the work of D. Chaum and E. van Heyst [10], a new kind of signature schemes have been developed, where many different private keys correspond with one public key in a *one to many* relationship, and even in some schemes different private keys correspond with different public keys in a *many to many* relationship. These signature schemes allow to focus the anonymity from different point of views with many interesting features.

In *group signatures* [10,1], a group public key defines a group. A designated *group manager*, who owns the group private key, is responsible for joining new members. Whenever a new member is added, she gets her own private membership key that allows to sign on behalf of the group. The signature issued can be verified with the group public key and it is neither possible to distinguish which member of the group issued the signature, nor even to link the signature with any other one issued by any member. However, the group manager has the special capability to identify which member issued a given signature, providing in this way with *reversible anonymity* in the sense that if a member abuses of her anonymity, the group manager can *open* the signature and disclose the identity of its issuer.

In *ring signatures* [30,14], a ring is made up of the public keys of the entities that compose the ring. These entities do not need to be aware of the existence of the ring, since their public keys are freely available. Any entity in a ring is able to produce a signature that can be verified with the ring public key, but no one is able to distinguish which entity issued the signature, or even to link it with any other signature produced by any entity in the ring. They offer similar features as group signatures, but ring signatures can not be *opened* to disclose the identity of its issuer. Thus, they provide *irreversible anonymity.*

Traceable signature schemes [24,27,12] are group signature schemes with additional tracing capabilities, what makes them very suitable for real-world applications. In addition to group signature properties such as indistinguishability, unlinkability, and the ability of the group manager to open a signature issued by any member of the group, a user is able to claim that a given signature has been issued by herself. Additionally, it is possible, with the help of the group manager that provides a member trapdoor, to identify which signatures within a set were issued by a given member with no other disclosure of information. These additional capabilities make this scheme very suitable for real world applications, since the tracing capability is necessary in many real situations. Some performance results are described in section 6.

3 Extending the Semantic of X.509 Certificates

Though not explicitly stated, X.509 public key certificates were originally designed for public key algorithms where one public key corresponds with one private key and where the public key is bound to the identity of that one who knows the corresponding private key.

With the advent of new signature schemes, such as group signatures, ring signatures, traceable signatures and others, the aforementioned semantic becomes too restrictive to allow the integration of these signature schemes with X.509 public key certificates, thus avoiding the X.509 framework to enjoy the numerous advantages that the new schemes offer.

3.1 Semantic Extension

While keeping the same structure, we can extend the semantic of X.509 certificates to additionally allow the use, as public key algorithms, of aforementioned signature schemes in those environments where their use could be appropriate.

Because in some of the new signature schemes, one public key can correspond with several different private keys (each one owned by different entities), we can define a *X.509 public key certificate with extended semantic* as a X.509 public key certificate where *the public key is not bound to a single entity but it is bound to a concept.* In the traditional semantic, the concept relates to a single entity, such as a system or a person, that owns the unique private key corresponding with the public key in the certificate (and the public key algorithm is a one-to-one scheme). However, in the extended semantic, the concept can be a more abstract definition where all entities that own a private key that can be verified with the certificate public key share the concept stated in the certificate. Each private key must be unforgeable, unique and not shared with other entities. Note that the extended semantic is a superset of the traditional one. In other words, an extended X.509 public key certificate binds a public key with a concept and, therefore, binds the concept with every entity that owns a private key that is publicly verifiable with the public key in the certificate (Fig. 3), which also specifies the public key algorithm to be used for such verification.

This extended semantic entails the use of standard extension fields defined for that purpose in the X.509 specification. Additionally, by means of these standard extension fields it is possible to control and restrict the usage of X.509 public key certificates in those scenarios where this is required (Sect. 5).

This broader semantic for public key certificates directly affects to X.509 attribute certificates. Since an attribute certificate binds a set of attributes with

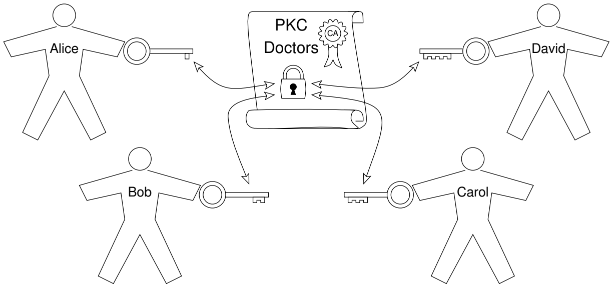

Fig. 3. X.509 public key certificate with extended semantic

a public key certificate, the represented concept in the public key certificate and related entities are able to enjoy the privileges associated with the bound attributes.

3.2 Entity Authentication – Identification and Anonymous Authentication

Up to now, *entity authentication* was usually considered equivalent to *identification*. However, in the context of this extended semantic, identification is a special kind of entity authentication where the concept in the public key certificate identifies a single entity. Entity authentication has now a broader semantic, since now the entity being authenticated by means of a public key certificate might not be directly related with his real identity, as in the case of these new signature schemes. Therefore, we can define the concept of *anonymous authentication* as a special kind of entity authentication where an anonymous entity becomes authenticated as a valid subject of the concept stated in the certificate. This authentication can be performed as usual by proving knowledge of a private key verifiable with the public key in the certificate.

4 Integrating New Signature Schemes into Extended X.509 Public Key Certificates

This section overviews how the new signature schemes can be added to the X.509 public key certificates. Though we only overview group, ring and traceable signature schemes, the semantic extension is not only restricted to those ones, but it is also open to others, even future ones. A summary of the properties of the aforementioned signature schemes is depicted in table. 1.

Table 1. Properties of some signature schemes

	Anon	One2Many	Unlink	Reversible	Traceable	MRevoc	SRevoc	Fair	NRep	MultiG	DShar
Ring sign.	●	●	●			●					
Group sign.	●	●	●	●					●		
Traceable sign.	●	●	●	●	●	●	●				

4.1 Ring Signatures

A ring can be made public and available by issuing a public key certificate with the ring public key being linked to the concept that such a ring represents. As rings do not need managers, a certification authority can create the ring public key from the sequence of the public keys of the members.[1] Of course it is up to the certification authority to decide in advance which members compose the ring. Members of the ring are able to be authenticated as holding such certificate

[1] In [30] the ring public key is the sequence of the public keys of the members, however in [14] the ring public key is created from the public keys of the members.

and to enjoy the associated privileges. In this case, the ring signature does not need to convey the public keys of the members of the ring, as specified in [30], since such information is held in the ring public key certificate. In [30] the size of both, the ring public key as well as the ring signature, are proportional to the number of members that compose the ring, however in [14] the size of the ring public key is proportional to the number of members, but the size of the signature is constant.

When a member of a public ring is authenticated by using her private key, her real identity becomes concealed. Thus, the member authentication is unlinkable and anonymous among the set of members of the ring. This scheme provides *irreversible anonymity* to the X.509 framework since no entity is able to correlate the authentication (a ring signature) with the real identity of the involved user. The ring public key certificate may be revoked as any other certificate, yielding in this way with the revocation of the whole ring and all its members. The certification authority can add and remove members to/from a concept represented by a ring by means of revoking the ring public key certificate and re-issuing a new one with the public keys of the members that now compose the concept represented by the ring. Note that users do not need to be aware of this fact except for using a fresh certificate that has not been revoked. However, the scheme seems more suitable for static rings with occasional modifications during its lifetime.

4.2 Group Signatures and Traceable Signatures

As with ring signatures, a public key certificate can define a group by binding the group public key to the concept that the group represents. The certification authority must verify that the group manager is suitable to manage such a public group and that the policy for joining new members to the group is suitable with respect to the aim of the certificate. New members can be joined to the group at any time, and as result they get their private membership keys. These members can be authenticated as holders of the group public key certificate and are able to enjoy its associated privileges. In these schemes, the size of both, the group public key and signatures, are constant.

When a member of a public group is authenticated by means of her private membership key, her real identity becomes concealed. Thus, the member authentication is unlinkable and anonymous among the set of members of the group. However, under certain circumstances, the group manager may consent to open a given authentication (a signature) and to disclose the real identity of the user involved. Additionally, as traceable signatures offer some extra features, the group manager can disclose a trapdoor for a given member, and some designated entities are able to identify, from within a set of anonymous authentications, which ones were performed by such member of the group. Moreover, a member of the group is able to claim that a given anonymous authentication was performed by herself.

The whole group can be revoked by revoking the public key certificate. Additionally, in case of traceable signatures, by means of the member trapdoor, it is possible to revoke individual members of a traceable group. There should be a trusted entity that holds a record with the private trapdoors of revoked members. Whenever a member is authenticated, in addition to check if the whole group has been revoked, the signature issued for authentication is sent to this trusted entity to be checked against the list of revoked member trapdoors.

These signature schemes provide *reversible anonymity* and *reversible, traceable and revocable anonymity* to the X.509 framework respectively.

5 The X.509 Public Key Certificate Extension

System security, authentication and authorization protocols make use of X.509 public key and attribute certificates to convey authentication and authorization information. Though the X.509 semantic extension explained in Sect. 3 uses the standard fields to convey the main information (issuer, subject, public key algorithm and public key), it also entails (for a proper usage), new semantic information to be added to the extension fields of the X.509 public key certificate (see appendix A for the specification in ASN.1).

The extensions field allows addition of new fields to the certificate without modification to the definition. An extension field consists of an extension identifier, a criticality flag, and an encoding of a data value of a type associated with the identified extension. If an extension is marked as *critical*, then any processing entity that does not recognize the extension will reject the certificate. On the contrary, if an extension is marked as *non–critical*, then any processing entity that does not recognize the extension will simply ignore it.

The X.509 standard has already defined some extension fields, though many others may be added. Among the extension fields defined by the standard, we highlight: *key usage* indicates the purpose of the key contained in the certificate; *certificate policies* indicates the policy under which the certificate has been issued and the purposes for which the certificate may be used; and *authority information access* indicates how to access certificate information and services for the issuer of the certificate.

Our proposed semantic extension entails the use of aforementioned extension fields, and define a new extension field that states the features of certificates with extended semantic.

The main important contribution to public key certificates is the support of the new signature schemes as public key algorithms (new OIDs should identify them). Then, new semantic information should be added to standard fields:

– A new extension field, *certificateFeatures*, should be added to X.509 public key certificates, stating some features of the certificate. These features depend on the public key algorithm properties and on the certificate issuing method. This new extension field must be marked as *critical* if present. It is a bit string defining flags for different properties. The following flags should be considered, though new flags can be added as required by other signature schemes.

Extended: The certificate is defined with extended semantic. This flag should be activated if any of the following flags is activated.

One2Many: The public key in the certificate corresponds to many different private keys.

Anonymous: There is no a direct way to know the identity of the entity being authenticated with the certificate.

Unlinkable: It is not possible to link different signatures as being performed by the same entity.

Reversible: There is an indirect way to know the identity of the entity being authenticated with the certificate.

Traceable: It is indirectly possible to identify, within a set, which signatures were issued by a given entity.

MemberRevocable: It is possible to revoke a specific entity, even if the public key algorithm is a *one2many* scheme.

AuthRevocable: If it is possible to revoke the entity that was involved in a given authentication process, even if the public key algorithm is a *one2many* scheme.

Fairness: There exists a *trusted third party* that guarantees that special disclosure actions are performed when it is appropriate to do so.

MultiGroup: There exists a mechanism that guarantees that the same real user actually belongs to several groups.

DeterSharing: There exists a mechanism that dissuades anonymous users from sharing the certificate private key.

OneLevelAnon: The identity of the user can be disclosed in just one anonymity backtracking, i.e. if the policy requires an identified user to be joined to the group.

Note that these properties are somehow inherited from the public key algorithm, however they depend on the way they are managed by the environment. For example, if the public key algorithm is a group signature scheme which provides reversibility, and the member joined the group either being identified or by means of a reversible anonymous authentication, then the certificate property should specify that the anonymity is reversible. However, if it was allowed that the member joined the group by using a irreversible authentication, then the certificate property should reflect that the anonymity is irreversible.

- The subject field of the certificate should contain the concept description, which in the case of group signatures or ring signatures specifies either the ring or group identification, which is composed by either the ring or group name and the identification (distinguished name) of the ring or group manager. New OIDs for both *ring name* and *group name* have to be added as attribute type to distinguished names.
- In the key usage extension field the *digitalSignature* flag should be asserted. In this case, such flag state that entity authentication is allowed. If the user joined the group by means of a non-repudiable authentication and the certificate public key algorithm provides non-repudiation, then the *nonRepudiation* flag should also be asserted because it is possible, under certain

circumstances, to identify the member that issued a given signature and that the member can not deny such action.

- The certificate policies extension field indicates the policy under which the certificate has been issued, its meaning, the conditions required to create the ring, or to join the group, the conditions required to be threw out of the group, and the conditions under which a member's identity would be disclosed, etc.
- Regarding public key certificate revocation, the same support as for normal public key certificates is required, that is, the *CRL distribution points* extension can be used. Additionally, if OCSP is used as a mean to access revocation information, then the *authority information access* extension should be used.
- If it is possible to revoke individual members of a given group, this is done by storing in a private database the group public key certificate together with a list containing the member trapdoors for every member that has been revoked from the group. By using an OCSP-like protocol, the client queries if a given member has been revoked (providing the group and signature used for authentication). The identification of this member revocation manager is specified in the *authority information access* extension field. A new accessMethod OID should be defined for this case.
- If some fairness authorities guarantee that the disclosure of restricted information is performed when it is appropriate to do so, then the identification of these entities are specified in the *authority information access* extension field. A new accessMethod OID should be defined for this case.

Note that this semantic extension provides new features to applications willing to use them, however it is harmless to unaware applications since public key certificates with unrecognized critical extensions are kindly rejected. Additionally, if an application does not support the public key algorithm then it also rejects the certificate.

5.1 Attribute Certificates

When issuing an attribute certificate to be bound to a public key certificate with extended semantic, it means that any entity able to be authenticated with such a public key certificate can enjoy the specified privilege. Therefore, the policy to get an attribute certificate must be tightly linked with the policy required to join the associated group or ring.

If unlinkability is a property exhibited by a public key certificate, then all entities being authenticated with such a PKC must share the same certificate and the same attribute certificates bound to it. That is, for a given attribute and public key certificate, the same certificates are shared among all the entities. The figure 4 shows how several entities, that can be authenticated with a public key certificate, all share the same attribute certificates.

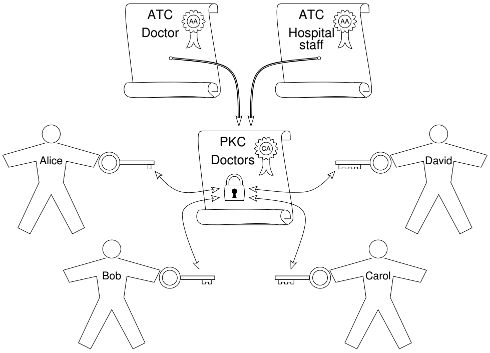

Fig. 4. Extended X.509 public key and attribute certificates

6 Traceable Signatures Performance Results

This section briefly shows some statistical results for the *traceable signature scheme*, but they can also be taken as a reference point for group signatures and alike ones. However, there is still room for optimization, since the implementation is based on [24], where some other proposals, such as [27,12] based on *bilinear pairings*, claim better efficiency.

Table 2 shows performance statistics for the basic *traceable signature* primitives. They are taken in an off-line environment where the host machine was an Intel Pentium Centrino running at 2.00GHz the Debian GNU/Linux Operating System and Sun's J2SDK 1.4.2 as Java runtime. The performance results, in milliseconds, show the arithmetic mean after several executions. A security parameter of 1024 bits was defined for Traceable Signatures and SHA-1 has been used as secure hash function.

Note that group creation and group joining depend on the search of suitable random primes, therefore their timings may vary. Group creation is an expensive operation, but it is usually performed off-line, so its cost has minor influence in system performance. The joining procedure may be speeded up by using pre-computed values for suitable random primes at group manager side. The reveal primitive just take a stored value and does not need any extra computation.

Table 2. Traceable Signature Primitives

	millisec
Create-Group	23680.2
Join-to-Group	1764.2
Sign	460.6
Verify	548.1
Open	55.8
Reveal	0.0
Trace	23.4
Claim	35.4
VerifyClaim	39.3

7 Conclusions

A new semantic extension have been proposed for X.509 certificates which provides enhanced features to both X.509 public key and attribute certificates. It has been explained how new signature schemes can be incorporated into the X.509 certificates with new extended semantic. In this way, the X.509 framework can benefit their very interesting features. As result, new anonymity features can to be added to the X.509 framework.

This semantic extension entails a new concept for entity authentication: identification and anonymous authentication. One very important advantage that this extended semantic provides is the fact that both identification and anonymous authentication coexist under a common entity authentication and, where allowed, the same protocols, data structures, etc. are valid for both. That is, there is no need to separate both authentication modes, a simple policy may discriminate between them if discrimination is required, or both can be accepted under the common entity authentication. This simple fact simplifies very much architecture and system design.

The presented work is part of a system that provides support for a user centric authorization model, where identified as well as anonymous authorization are supported. The system fits into the X.509 framework and into the Identity 2.0 initiative, being the user the core of the system. Additionally, anonymity increases the strength of the user in this approach.

Finally, some performance results for a prototype of a traceable signature scheme have been presented, which can be taken as a reference point for group signatures and derived ones, and in some way show their feasibility.

7.1 Future Work

Though ring, group and traceable signatures provide very interesting properties with respect to anonymity, there are some real world scenarios where they are not completely suitable for supporting anonymity. These signature schemes seem suitable to support anonymity in real world applications, since in these kind of scenarios, it is usually covenient that the user is accountable for her actions, and it is also very interesting the capability to trace anonymous transactions performed by a given user under suspicion. However, some real world scenarios motivate us for searching for new digital signatures.

(i) Though the group manager may be trusted with respect to joining new members to the group, in some scenarios, the group manager is not usually trusted with respect to safeguard the anonymity of the members, since in many cases the group manager is an interested party. Therefore it is necessary to split the duties of joining new members on the one hand, and disclosing sensitive information such as open/reveal/trace on the other hand. This capability of breaking anonymity should be as distributed as possible.

(ii) Additionally, it is common to prove that a user simultaneously belongs to several groups in order to be authorized to carry out some transaction. Then it is interesting to incorporate multi–group [2] features that enable the user to prove that the same real user does indeed simultaneously belongs to the required groups. This feature guarantees the verification entity that the proof has not been collected from different anonymous users.

(iii) Public key authentication systems are based on the fact that private keys are only known by just one entity, however an anonymous scenario may increase the temptation to share the private keys that allow to prove membership to groups, a case that would subvert the basis on which the whole system security relies. Therefore, it is also desirable to incorporate some mechanisms to dissuade users from sharing her private keys.

A signature scheme that enjoys all the aforementioned features, as well as those ones from group and traceable signatures would be very convenient for supporting a wide range of anonymous transactions in real world open systems.

References

1. Ateniese, G., Camenish, J., Joye, M., Tsudik, G.: A practical and provably secure coalition-resistant group signature scheme. In: Bellare, M. (ed.) CRYPTO 2000. LNCS, vol. 1880, pp. 255–270. Springer, Heidelberg (2000)
2. Ateniese, G., Tsudik, G.: Some open issues and new directions in group signatures. In: Franklin, M.K. (ed.) FC 1999. LNCS, vol. 1648, pp. 196–211. Springer, Heidelberg (1999)
3. Benjumea, V., Lopez, J., Montenegro, J.A., Troya, J.M.: A first approach to provide anonymity in attribute certificates. In: Bao, F., Deng, R., Zhou, J. (eds.) PKC 2004. LNCS, vol. 2947, pp. 402–415. Springer, Heidelberg (2004)
4. Benjumea, V., Lopez, J., Troya, J.M.: Anonymous attribute certificates based on traceable signatures. Internet Research 16(2), 120–139 (2006)
5. Brands, S.A.: Rethinking Public Key Infrastructures and Digital Certificates Building in Privacy, The MIT Press, Cambridge (August 2000)
6. Camenisch, J., Lysyanskaya, A.: Efficient non-transferable anonymous multi-show credential system with optional anonymity revocation. In: Pfitzmann, B. (ed.) EUROCRYPT 2001. LNCS, vol. 2045, pp. 93–118. Springer, Heidelberg (2001)
7. Chaum, D.: Blind signatures for untraceable payments. In: Chaum, D., Rivest, R., Sherman, A. (eds.) CRYPTO 1982: Advances in Cryptology, pp. 199–203. Plenum Press, Santa Barbara, CA (August 1983)
8. Chaum, D.: Security without identification: Transaction systems to make big brother obsolete. Communications of the ACM 28(10), 1030–1044 (1985)
9. Chaum, D., Evertse, J.H.: A secure and privacy-protecting protocol for transmitting personal information between organizations. In: Odlyzko, A.M. (ed.) CRYPTO 1986. LNCS, vol. 263, pp. 118–170. Springer, Heidelberg (1987)
10. Chaum, D., van Heyst, E.: Group signatures. In: Davies, D.W. (ed.) EUROCRYPT 1991. LNCS, vol. 547, pp. 257–265. Springer, Heidelberg (1991)
11. Chen, L.: Access with pseudonyms. In: Dawson, E.P., Golić, J.D. (eds.) Cryptography: Policy and Algorithms. LNCS, vol. 1029, pp. 232–243. Springer, Heidelberg (1996)
12. Choi, S.G., Park, K., Yung, M.: Short traceable signatures based on bilinear pairings. In: Yoshiura, H., Sakurai, K., Rannenberg, K., Murayama, Y., Kawamura, S. (eds.) IWSEC 2006. LNCS, vol. 4266, pp. 88–103. Springer, Heidelberg (2006)
13. Dierks, T., Rescorla, E.: RFC-4346. The Transport Layer Security (TLS) Protocol. The Internet Society (April 2006)

14. Dodis, Y., Kiayias, A., Nicolosi, A., Shoup, V.: Anonymous identification in Ad Hoc groups. In: Cachin, C., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 609–626. Springer, Heidelberg (2004)
15. Ellison, C.: RFC-2692. SPKI requirements. IETF SPKI Working Group (September 1999)
16. Ellison, C., Frantz, B., Lampson, B., Rivest, R., Thomas, B., Ylonen, T.: RFC-2693. SPKI certificate theory. IETF SPKI Working Group (September 1999)
17. Farrel, S., Housley, R.: RFC-3281. An Internet Attribute Certificate Profile for Authorization. The Internet Society (April 2002)
18. FIPS 186. Digital Signature Standard. U.S. Department of Commerce/N.I.S.T., National Technical Information Service, Springfield, Virginia (1994)
19. Freier, A., Karlton, P., Kocher, P.: The SSL Protocol. Netscape (November 1996)
20. Housley, R., Polk, W., Ford, W., Solo, D.: RFC-3280. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. The Internet Society (April 2002)
21. Identity 2.0, http://www.identity20.com/
22. ITU-T Recommendation X.509. Information Technology - Open systems interconnection - The Directory: Authentication Framework (June 1997)
23. ITU-T Recommendation X.509. Information Technology - Open systems interconnection - The Directory: Public-key and attribute certificate frameworks (March 2000)
24. Kiayias, A., Tsiounis, Y., Yung, M.: Traceable signatures. In: Cachin, C., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 571–589. Springer, Heidelberg (2004)
25. Lysyanskaya, A., Rivest, R., Sahai, A., Wolf, S.: Pseudonym systems. In: Heys, H.M., Adams, C.M. (eds.) SAC 1999. LNCS, vol. 1758, Springer, Heidelberg (2000)
26. Myers, M., Ankney, R., Malpani, A., Galperin, S., Adams, C.: RFC-2560. X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP. The Internet Society (June 1999)
27. Nguyen, L., Safavi-Naini, R.: Efficient and provably secure trapdoor-free group signature schemes from bilinear pairings. In: Lee, P.J. (ed.) ASIACRYPT 2004. LNCS, vol. 3329, pp. 372–386. Springer, Heidelberg (2004)
28. Persiano, P., Visconti, I.: A secure and private system for subscription-based remote services. ACM Trans. on Information and System Security 6(4), 472–500 (2003)
29. Persiano, P., Visconti, I.: An efficient and usable multi-show non-transferable anonymous credential system. In: Juels, A. (ed.) FC 2004. LNCS, vol. 3110, pp. 196–211. Springer, Heidelberg (2004)
30. Rivest, R., Shamir, A., Tauman, Y.: How to leak a secret. In: Boyd, C. (ed.) ASIACRYPT 2001. LNCS, vol. 2248, pp. 552–565. Springer, Heidelberg (2001)
31. Rivest, R.L., Shamir, A., Adleman, L.: A method for obtaining digital signatures and public key cryptosystems. Communications of the ACM 21(2), 120–126 (1978)
32. Schechter, S., Parnell, T., Hartemink, A.: Anonymous authentication of membership in dynamic groups. In: Franklin, M.K. (ed.) FC 1999. LNCS, vol. 1648, pp. 184–195. Springer, Heidelberg (1999)
33. Stubblebine, S.G., Syverson, P.F., Goldschlag, D.M.: Unlinkable serial transactions: Protocols and applications. ACM Trans. on Information and System Security 2(4), 354–389 (1999)
34. Verheul, E.R.: Self-blindable credential certificates from the weil pairing. In: Boyd, C. (ed.) ASIACRYPT 2001. LNCS, vol. 2248, pp. 533–551. Springer, Heidelberg (2001)

A ASN.1 Specification of Anonymity Extensions for X.509v3 Certificates

This appendix describes the ASN.1 specification of the proposed extensions for X.509v3 certificates. The following OIDs and structures should be incorporated to the extensions of X.509v3 certificates. The new OIDs are members of the anonymity extensions arc, `id-ae`[2], that is under the standard private extensions arc `id-pe`.

```
id-ae   OBJECT IDENTIFIER ::= { id-pe 32 }
```

New OIDs should be defined for ring, group and traceable signature schemes.

The subject field in standard X509v3 certificates is a sequence of distinguished names, which is a set of attribute type and value pairs. New OIDs are defined to identify ring, group, traceable–group and fair–traceable–group names for attribute types:

```
id-ae-at   OBJECT IDENTIFIER ::= { id-ae 2 }

id-ae-at-ringName     AttributeType ::= { id-ae-at 1 }
id-ae-at-groupName    AttributeType ::= { id-ae-at 2 }
id-ae-at-tGroupName   AttributeType ::= { id-ae-at 3 }
```

and the syntax for the respective values:

```
RingName    ::= X520name
GroupName   ::= X520name
TGroupName  ::= X520name
```

The *certificateFeatures* extension MUST be marked critical, with the following OID and value syntax:

```
id-ae-ef   OBJECT IDENTIFIER ::= { id-ae 3 }

id-ae-ef-certificateFeatures  OBJECT IDENTIFIER ::= { id-ae-ef 1 }

CertificateFeatures ::= BIT STRING {
    extended         (0),
    one2Many         (1),
    anonymous        (2),
    unlinkable       (3),
    reversible       (4),
    traceable        (5),
    memberRevocable  (6),
    authRevocable    (7),
```

[2] Note that the number of this arc is a suggestion, and should be defined to avoid conflicts.

```
    fairness        (8),
    multiGroup      (9),
    deterSharing    (10),
    oneLevelAnon    (11)
}
```

The authority information access extension in standard X509v3 certificates is defined as a sequence of access description, which is composed of an access method identifier and access location that specifies the URI for the corresponding method. The new OIDs for the new *member revocation access* and *fairness authorities* access methods are as follows:

```
id-ae-aia   OBJECT IDENTIFIER ::= { id-ae 4 }

id-ae-aia-am   OBJECT IDENTIFIER ::= { is-ae-aia 1 }

id-ae-aia-am-memberRevAccess    OBJECT IDENTIFIER ::= { is-ae-aia-am 1 }
id-ae-aia-am-fairnessAuthority  OBJECT IDENTIFIER ::= { is-ae-aia-am 2 }
```