An Efficient Off-Line Reputation Scheme Using Articulated Certificates

Roslan Ismail[1], Colin Boyd[1], Audun Josang[2], and Selwyn Russell[1]

[1] ISRC, Queensland University of Technology, Brisbane, Australia
[2] DSTC, University of Queensland, St Lucia, Australia

Abstract. A common feature practical reputation schemes is that they are on-line which results in restrictions to both availability and scalability. In order to overcome these two problems we propose an off-line reputation scheme based on public key certificates. We introduce the idea of *articulated certificates* which use proxy signatures to increase the efficiency of reputation verification. As well as being well-suited to our problem such linked certificates may be of independent interest.

1 Introduction

Reputation schemes are systems developed to collect, analyse and propagate users' reputation [12]. They can be used for many purposes, but in the last few years have emerged as a promising means for enabling electronic transactions in e-commerce. Studies have shown that use of reputation schemes has positive effects on the efficiency and honesty of markets [1], and that the reputation of a particular agent can have positive effects on the agent's gain [13].

Most current reputation schemes, especially the practical ones, are specifically designed for on-line use, eBay being a prime example (`www.ebay.com`). This situation is not surprising as a reputation scheme must provide real time responses so that users' past behaviours can be obtained immediately. Although an on-line reputation scheme is currently preferred, it suffers two main difficulties: availability and scalability. For example, in a case of denial of service it may not be possible to access the central server and so reputation values cannot be found. If the central server is distributed to overcome such problems, then synchronisation and consistency of data will become difficult.

These problems of distributed reputation systems have much in common with the problems of distribution of public keys. In both cases there is a need for access to authenticated values distributed in a timely fashion. Public keys are usually propagated through *certificates* formed by an off-line trusted third party. It seems a natural idea to use *reputation certificates* formed in an analogous way by a trusted third party. One of the main aims of this paper is to explore how this may best be achieved.

Reputation certificates may be controlled by users themselves. The certified reputation value calculated from processed feedback is communicated to the reputation owner after completion of transactions with its counterparts. Reputation

Ismail R., Boyd C., Josang A. and Russell S. (2004).
An Efficient Off-Line Reputation Scheme Using Articulated Certificates.
In *Proceedings of the 2nd International Workshop on Security in Information Systems*, pages 53-62
DOI: 10.5220/0002660200530062

Table 1. The participants and their symbols

FT	A feedback target is the entity who is being evaluated and gains the reputation rating based on the feedback given by a feedback provider.
RP	A relying party is the entity who relies on the feedback target's reputation rating to make a decision whether to proceed in a transaction or not.
CA	The certificate authority is responsible for the registration of the feedback targets as well as to issue certificates to them.
CC/RA	The collection centre/reputation authority collects legitimate feedbacks and uses them to calculate reputation rating and update the feedback target's reputation certificate.
AA	The attribute authority is responsible for issuing and signing the attributes.

certificates can be obtained from reputation owners without the need to contact a central authority. There seem to be two natural ways to realize this proposal.

1. Employ existing identity certificate technologies, for example, X.509 [5] and PGP [15] to incorporate reputation values.
2. Employ a separate certificate specifically for the reputation value.

In the former option a reputation rating is regarded as one of the attributes in the identity certificate. As a result the implementation does not require any significant modification to the existing infrastructure. The latter, on the other hand, requires a special authority to manage the reputation rating scheme. We will compare the relative advantages of these different options later.

This paper proposes an off-line reputation scheme based on public key certificates. The solution is flexible enough to accommodate most formats of reputation rating. Different options are considered for how to bind the reputation information with the identity of the subject. Our proposal, which we call *articulated certificates*, can be applied in other situations when it is desired to augment or update certificate information without re-issuing the identity certificate.

Organisation of the paper Section 2 discusses the background of reputation schemes. Section 3 discusses three basic solutions to implement binding between identity certificates and reputation information. Section 4 describes our proposed solution, its properties and the required protocols. Section 5 discusses the relative merits with other options. Table 1 presents the notations and the symbols used throughout the paper.

2 Reputation Systems

There has been considerable interest in reputation systems in recent years and an extensive literature has developed [12]. Reputation systems may be roughly classified into two activities.

Reputation calculation is the task of obtaining reputation values from a set of feedback information. There are various properties that may be desirable for calculation engines and reputation values may take different formats. In this paper we are not concerned with how reputation values are calculated, as long as they can be represented efficiently in a bit string.

Reputation propagation is concerned with how to distribute reputation values to parties that require to use them. This is the area addressed in this paper. There are different properties that may be important, including high availability of values and reliability. A feature that has often been neglected is privacy of reputation values; we address this partially in this paper by allowing owners of reputation certificates to control their distribution.

Off-line reputation propagation has been proposed by some recent authors [4, 3]. These schemes addressed the integrity of the submitted feedbacks against manipulation but are not suited to centralised reputation calculation. A recent proposal of Liau et al. [7] (the LZBT scheme) demonstrated the possibility of using certificates to represent a user's reputation in the off-line environment. The LZBT scheme seems promising for P2P systems because no central authority is required to operate the scheme. However, its major limitation is that the relying party has to contact one or more of the preceding feedback provider to verify the validity of reputation certificates. This creates an extra burden to the service consumers to verify the certificate.

3 Reputation certificates

Identity certificates bind the identities of users with their public keys. The certificate is issued and signed by a trusted *certificate authority* CA. Identity certificates are typically long term and contain several attributes such as subject name, public key, expiry date, issuer name, and certificate holder's name. These certificates are mainly used for authentication purposes. Attribute certificates [9], on the other hand, are mainly used to provide access controls and role permissions of an entity with regard to accessing resources. Therefore, these certificates are often employed within organizational boundaries. Attribute certificates typically do not contain the identity of an entity; instead they may contain attributes such as role, access control, expiry date, the issuer name and the issuer signature.

A reputation rating can be considered as an attribute bound to an identity. Reputation certificates therefore need to be used in conjunction with an identity certificate. There are various ways that this may be achieved. Park and Sandhu [11] discussed three techniques to bind two certificates (the identity and the attribute certificate): monolithic, autonomic and chained signatures. In the *monolithic* signature technique the identity and attribute certificate are combined to become a single certificate which is signed by an authority. The *autonomic* signature technique implements separate signatures: the identity certificate and the attribute certificate are signed by different authorities. To bind the two certificates certain attributes in the identity certificate are linked to the attribute certificate. Finally in the *chained signature* technique the signature of authority on the identity certificate is used as a connection link between the identity and the attribute certificates. In the next subsections we will consider solutions which correspond roughly to this classification.

3.1 Combined Certificates

In this solution the identity certificate and reputation certificate are the same object, and the reputation value is simply an additional attribute in the certificate. This corresponds to the monolithic certificate of Park and Sandhu [11]. Figure 1 depicts the abstract view of the solution. In this solution, the feedback target and the feedback provider are required to register with the authority. A reputation certificate is issued and signed by the reputation certificate authority. The reputation certificate should be verified by the relying party.

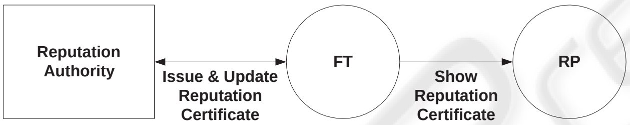
Reputation Authority
Issue & Update Reputation Certificate
FT
Show Reputation Certificate
RP

Fig. 1. Abstract view of Combined Reputation Certificate

The combined certificate offers several advantages; it requires no new infrastructure, is straightforward to implement and requires only one operation to verify the authority's signature. However, it has some drawbacks.

1. The reputation authority is required to issue and manage the certificates besides its routine task to calculate the reputation of the participants.
2. The reputation attribute becomes available to any party who has access to the identity certificate. Users may prefer to hold their reputation values privately except when needed for transactions.
3. Reputation certificates need to be updated frequently so the identity certificate also needs to be issued each time the reputation is updated.

A different way to form a combined certificate was the *smart certificate* proposed by Park and Sandhu [10]. The scheme uses the structure of the X.509 certificate as its basis and the extension fields in the original certificate are used to incorporate additional attributes. Each attribute in the certificate is managed by different authorities. Although the smart certificate has several desirable properties, a major limitation highlighted by Chadwick and Otenko [2] is that it is automatically invalid once any attribute is changed. We expect the reputation rating to change frequently and the certificate needs to be re-issued each time.

3.2 Separate Certificates

The separate certificate corresponds to the autonomic certificate of Park and Sandhu [11]. Figure 2 is a graphical representation of the solution showing the two types of certificates used. The identity certificate is issued by the certificate authority, while the reputation certificate will be issued by the reputation authority. The certificates are linked due to shared information, in particular the unique name (or X.509 *distinguished name*) from the identity certificate may be included in the attribute certificate.

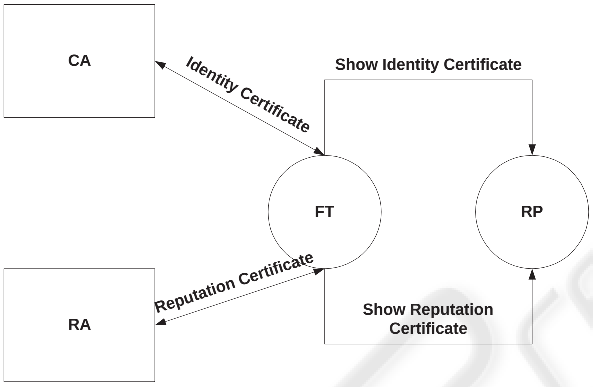

Fig. 2. Abstract view of Separate Certificate

Because there are two authorities, separation of duties can be conducted which can reduce the problem of overloading the reputation authority. The reputation authority is only responsible for the calculation of the reputation, while the certificate authority is responsible for the registration of the feedback targets. The identity certificate is used as an identity mechanism for the feedback target. Like the combined certificate solution, this solution also has its limitations.

1. It is costly to match the identity certificate and the reputation certificate especially to the relying party RP who has to do three steps of verification: first to check the validity of the identity certificate; second to check the validity of the reputation certificate; third to match between these two certificates.
2. RP cannot determine whether RA is authorized to provide reputation for FTs. This means that relying parties have to independently check the policy and practice statements for any issuers of attribute certificates.

3.3 Related Certificates

The idea of related certificates is to ensure that the attribute certificate has a functional link to the identity certificate, beyond simply referring to the same identity. This corresponds to the chained certificates of Park and Sandhu [11]. The difference from the separate certificate option is that now the binding information in the attribute certificate depends on the CA signature on the identity certificate. In other words, the attribute certificate is bound to a specific instance of the identity certificate.

Using an attribute certificate related to the identity certificate as the reputation certificate is a reasonable option. However, the drawbacks already mentioned for separate certificates still apply. Independent signature checking increases the computational burden. The issue of authorization of the RA also applies here, but with a different twist. The issuer of attribute certificate is free to act independently of the $CA$of the identity certificate. However, CAs may object to use of their certificates by third parties for purposes without their consent and may put in place legal obstacles to prevent this.

4 Articulated Certificates

From the discussion in section 3 we see that each of the previous proposals for binding identity and attribute certificates has some drawbacks when used for reputation certificates, although separate certificates or related certificates could be reasonable choices. In this section we proposed a new scheme for linking reputation and identity certificates. We called this an *articulated certificate.*

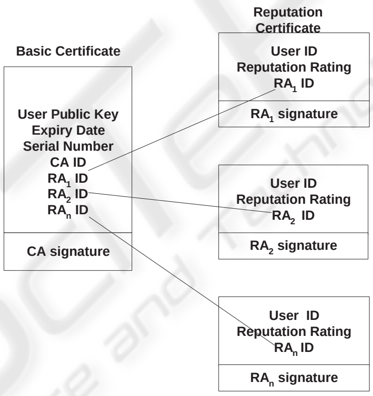

Fig. 3. Abstract View of Articulated Certificate

Figure 3 illustrates the view of the proposed scheme. The properties of articulated certificates are different from all the options considered in section 3.

- Articulated certificates can only be issued by entities that have been authorised to do so by the identity CA. Moreover, the authority to issue may be restricted for a specific purpose or particular time interval.
- The articulated certificate can be verified using the CApublic key alone – no separate certificate is required for the reputation authority.
- The identity certificate may be used either with or without the attribute certificate.

A major feature of our proposed solution is to use the concept of *delegation* to allow the certification authority to give power to the reputation authority to link to the original certificate. Delegation enables RA to update reputation rating in the certificate without invalidating the certificate. The CA delegates his signing capability to RA using the proxy signature scheme. Figure 4 shows the abstract view of the proposed architecture.

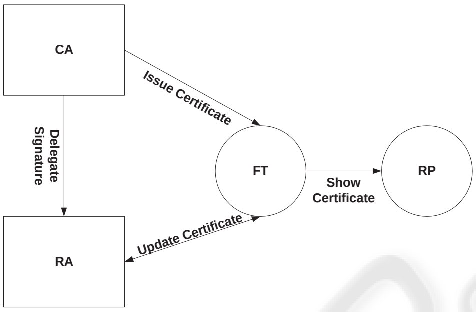

Fig. 4. Proposed Architecture

4.1 Proxy Signatures

Proxy signature schemes allow an original signer to delegate signing capability to another entity, the proxy signer. The first proxy signature scheme was introduced by Mambo et al. [8]. Subsequently a number of schemes have been proposed in the literature [14, 6]. For our purpose the scheme of Mambo et al. (MUO scheme hereafter) will be employed. However, other proxy signature schemes can also be used in our proposal. A brief review of MUO scheme follows.

System Settings: Global system parameters consist of a large prime p, a prime factor q of $p-1$, and an element $g \in Z_p^*$ of order q. Computations take place in Z_p^* unless indicated otherwise. Entity A denotes the original signer and B denotes the proxy signer. Assume that x_A is a private key for A and the corresponding public key $y_A = g^{x_A}$ and m_w is a statement about delegation which typically contains some particulars including the proxy signer identification. A one way hash function $\mathcal{H}()$ is used. The scheme can be divided into four phases; generation of a proxy key, verification of the proxy key, signing using the proxy key and verifying the proxy signature. A small modification is made to the original of MUO scheme to include the hash of m_w.

Generation of a proxy key. A chooses a random number, $k \in_R Z_q^*$ and computes $r = g^k$. He proceeds to compute $s_P = x_A\mathcal{H}(m_w) + kr \bmod q$ and then sends (s_P, r) to B securely.

Verification of the proxy key. Upon receiving (s_P, r), B verifies $g^{s_P} \stackrel{?}{=} y_A^{\mathcal{H}(m_w)} r^r$. If this equation holds B accepts it is a valid proxy key.

Signing using the proxy key. B signs message m using the proxy key s_P. The signed message is $S(m), r$ where $S()$ is any discrete log signature generation algorithm.

Verifying of the proxy signature. A verifier first calculates $y_P = y_A^{\mathcal{H}(m_w)} r^r$ and checks the validity of the proxy signature $V(y_P, message) \overset{?}{=} true$ where $V()$ is a the signature verification algorithm.

Since MUO scheme is employed, the properties of the scheme of MUO are automatically inherited into our proposal.

1. **Unforgeablity** Besides CA, only RA can create a valid proxy signature. The third parties who are not designated as a proxy signer cannot create a valid proxy key.
2. **Verifiability** RP can be convinced of the original signer agreement on the signed message.
3. **Identifiability** Anyone can determine the identity of the proxy signer from a proxy signature.
4. **Undeniability** Once the proxy signer creates a valid proxy signature he cannot repudiate it.

4.2 Protocol of the Scheme

The protocol consists of six phases as follows. Execution of the phases is not necessarily in sequential order, except that the delegation and registration phases have to be executed prior to the other phases. Some phases may need to be executed more than once, such as updating certificate, showing certificate and validating certificate.

- **Delegation** CA delegates signing capability to RA so that RA can update the certificate of FT with a new reputation rating. It is assumed that both parties CA and RA have already agreed upon the terms and conditions of delegation beforehand which are encoded in m_w. To delegate, CA executes the generation phase of the MUO scheme by choosing a random number k and computes $r_{RA} = g^k$. This is followed by computing $s_{RA} = x_{CA}\mathcal{H}(m_w) + kr_{RA} \bmod q$ and sends (s_{RA}, r_{RA}) to RA securely. On receiving this pair RA verifies $g^{s_{RA}} \overset{?}{=} y_{CA}\mathcal{H}(m_w) r_{RA}^{r_{RA}}$. If this holds RA accepts it is a valid proxy key.
- **Registration** FT creates a public key y_{FT} and the corresponding private key x_{FT}. y_{FT} and ID_{FT} are securely sent to CA for registration. A typical certificate format of the basic certificate may be as follows:

Sig_{CA}	FT	y_{FT}	Exp	CA	RA

  where Sig_{CA} denotes the CA's signature and Exp denotes expiry date of the certificate, On receiving FT's particulars, CA verifies their validity. The certificate is signed by CA using his private key x_{CA} and is sent to FT.

Notice that it is not essential to include the identity of the reputation authorities with the identity certificate, as shown above. Instead, the RA may be identified separately to the relying party by the certificate owner.

- **Sending Identity Certificate** FT is required to send his identity certificate to RA for the initial contact. It can then be recorded in a database maintained by RA until a new identity certificate is issued.
- **Updating Reputation Certificate**
To prevent unnecessary updating, statistics of activity of the feedback target may be used to determine when the reputation rating should be updated. An active user may be given a short expiry date while an inactive user has a longer one. To issue a new reputation certificate RA signs it using the proxy private key s_{RA}. The certificate is sent to FT. A typical certificate format of the articulated certificate may be as follows.

Sig_{RA}	ExpR	FT	RA	FT Rating

where Sig_{RA} is the signature of RA and ExpR denotes the expiry date of the reputation rating,

- **Showing Certificate** Before any engagement with the intended RP, FT may be required to show his reputation certificate to RP so that his reputation can be evaluated.
- **Validating Reputation Rating** Prior to accepting the rating in the reputation certificate, RP calculates y_{RA} and verifies the certificate validity based on signature to the conditions in m_w. If so RP accepts the reputation rating as a valid reputation rating.

5 Discussion

There are several advantages held by our scheme compared to other schemes.

- Only one operation is required to verify the reputation certificate, as only the RA's signature needs to be checked by the relying party while the validity of the identity certificate is verified by RA. This advantage is also shared by the basic certificate. Separate certificates and related certificates, on the other hand, require three computations to verify the validity of both certificates.
- There is a separation of duties between the identity CA and reputation authority. This is generally a good security practice, and ensures that neither is overloaded with management tasks.
- Our scheme implements tightly-coupled binding between the identity and reputation certificates because a single identity certificate may be mapped to multiple reputation certificates. This advantage is shared by the combined certificate while the separate certificate implements loosely-coupled solution.
- Our proposal has high reusability because changes to the reputation certificate or the identity certificate cannot invalidate the reputation certificate. This is shared by the separate certificate while the basic reputation and the related certificates have low reusability because any changes invalidate them.

References

1. G. Bolton, E. Katok, and A. Ockenfels. How Effective are Online Reputation Mechanisms? Discussion Papers on Strategic Interaction 25-2002, Max-Planxk-Institut, 2002.
2. D. W. Chadwick and A. Otenko. The permis X.509 role based privilege management infrastructure. *Future Generation Computer Systems*, 19(2):277–289, February 2003.
3. D. Fahrenholtz and W. Lamersdorf. Transactional security for a distributed reputation management system. In *Proceedings of the 3rd International Conference on Electronic Commerce and Web Technologies*, volume 2455 of LNCS, pages 214–223. Springer-Verlag, 2002.
4. M. Gupta, P. Judge, and M. Ammar. A reputation system for peer-to-peer networks. In *ACM 13th International Workshop on Network and Operating Systems Support for Digital Audio and Video (NOSSDAV 2003)*, pages 144–152. ACM Press, June 1-3 2003.
5. ITU-T. Recommendation X.509 Information technology - Open systems Interconnection - The Directory : Authentication framework, 1997.
6. B. Lee, H. Kim, and K. Kim. Strong proxy signature and its applications. In *SCIS'2001*, pages 603–608, Jan 23-26 2001.
7. C. Y. Liau, X. Zhou, S. Bressan, and K.-L. Tan. Efficient distributed reputation scheme for peer-to-peer systems. In *The 2nd International Human.Society@Internet Conference*, volume LNCS 2713, pages 54–63. Springer-Verlag, 2003.
8. M. Mambo, K. Usuda, and E. Okamoto. Proxy signatures for delegating signing operation. In *Proceedings of the 3rd ACM conference on Computer and communications security*, pages 48–57. ACM Press, 1996.
9. R. Oppliger, G. Pernul, and C. Strauss. Using attribute certificates to implement role-based authorization and access controls. In *Proceedings of the 4. Fachtagung Sicherheit in Informationssystemen (SIS 2000), Zürich (Switzerland)*, pages 169–184, October 5-6, 2000.
10. J. S. Park and R. Sandhu. Smart certificates: Extending X.509 for secure attribute service on the web. In *Proceedings, 22nd National Information Systems Security Conference*, pages 337–348, October 18-21 1999.
11. J. S. Park and R. Sandhu. Binding identities and attributes using digitally signed certificates. In *16th Annual Computer Security Applications Conference (ACSAC)*, pages 120–127, December 11-15 2000.
12. P. Resnick, R. Zechauser, E. Friedman, and K. Kuwabara. Reputation systems. *Communication of the ACM*, 43(12):45–48, December 2000.
13. P. Resnick, R. Zeckhauser, J. Swanson, and K. Lockwood. The value of reputation on eBay: A controlled experiment. In *Working paper presented at the ESA conference*, June 2002.
14. S. P. S. Kim and D. Won. Proxy signatures, revisited. In *Proc. of ICICS'97, International Conference on Information and Communications Security*, volume LNCS 1334, pages 223–232. Springer, 1997.
15. P. R. Zimmermann. *The Official PGP User's Guide.* MIT Press, Cambridge, MA, USA, 1995. Available at http://www-mitpress.mit.edu/mitp/recent-books/comp/pgp-user.html.