Proceedings of the EDI Trusted Third Party Workshop, Barcelona, Spain, 8-10 February 1995.

Revocation and Revocation Certificates

Rainer A. Rueppel

r3 security engineering ag, Zürichstrasse 151, CH-8607 Aathal, Switzerland
email: rueppel@r3.ch

Abstract
In this paper we discuss certificates and revocation. A new type of certificate, the revocation certificate, is proposed. The revocation certificate is an attempt to overcome some of the drawbacks of the black list approach used in current systems. The concept of revocation certificates has been adopted in the TEDIS Project FAST.

Keywords: Trusted Third Parties, Certification, Revocation

1 Introduction

The traditional business process is based on paper and handwritten signatures. As our information society begins to rely more and more on electronic data processing and interchanges, an electronic equivalent to handwritten signatures is needed in order to allow for fully electronic business processes. In general, handwritten signatures are easy to forge and hard to verify. Digital signatures based on modern public key technology are hard to forge and easy to verify. However, digital signatures introduce new qualities that cause some uneasiness:

- you can have more than one signature at a time
- you may change your signature
- your signature may be „broken“
- your signature is performed by a device

In order to obtain general recognition of digital signatures (in an open systems point of view) we need a management infrastructure which addresses the registration, certification and revocation of signatures (or more precisely, of the corresponding public keys). The following figure illustrates the functions of a Public Key Management Infrastructure.

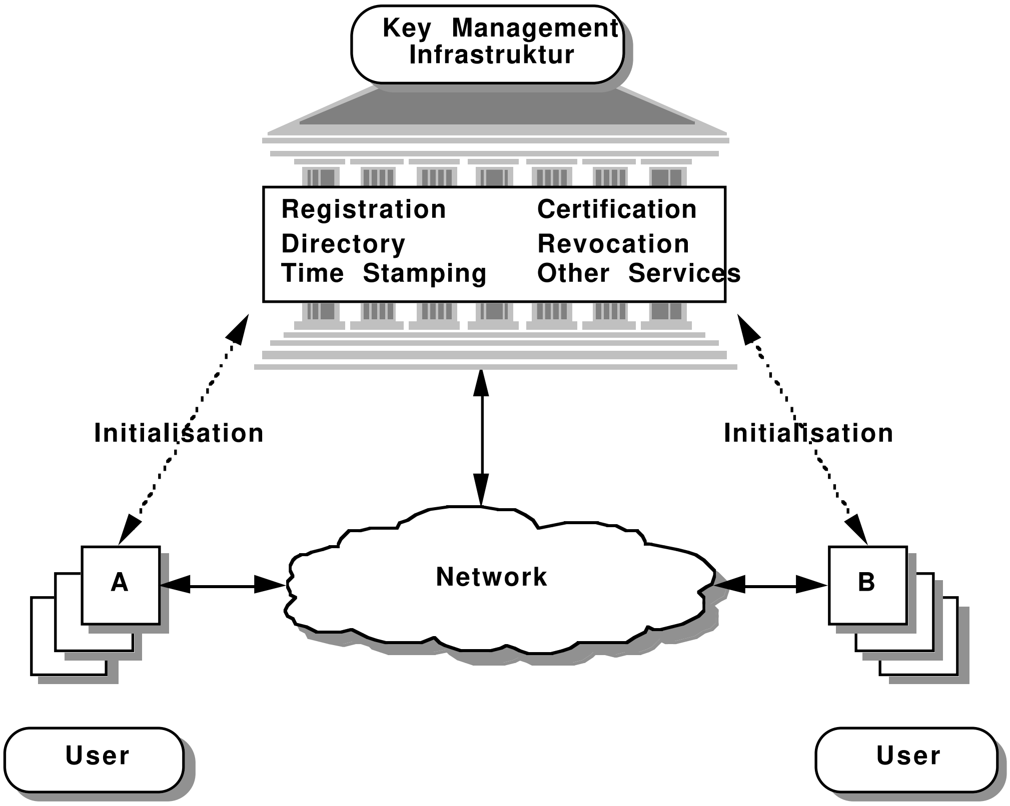

Figure 1 - Public Key Management Infrastructure

The Public Key Management Infrastructure must provide the following services

- secure registration of the users and their public keys
- certification of the public keys
- secure distribution of the public keys
- controlled revocation or change of registered public keys
- time-stamping of electronic documents, and other services

2 Certificate-based Systems

There are different types of certificates: public key certificates, attribute certificates, etc.

2.1 Public Key Certificates

For the management of public keys we have the following business requirements:

1. In order to verify the signatures of an entity we need the public verification key of that entity. It is crucial that the entity's public key is distributed in an authenticated fashion.
2. Manual signatures shall be replaced by digital signatures. It is crucial that a trusted party vouches for the legitimacy of the entity's public verification key.

To satisfy these requirements we may let a trusted party (digitally) sign the name and the public key of an entity. The result is the public key certificate; it binds the public key to the entity. Legally, it certifies that the entity's manual signature may be replaced by the corresponding digital signature.

A public key certificate typically contains the following generic parts.

Certificate part	Function and Responsibility	Examples
Credentials	The credentials are presented by the entity to the registration authority in its application. The RA is responsible for processing the entity's application, for validating the entity's credentials and for assigning a distinguished name to the entity.	distinguished name
Public key	The entity is responsible for generating an asymmetric key pair for signatures and for submitting the public verification key to the RA (or in some cases to the CA).	the entity's public key
RA supplied data	The registration authority is responsible for adding registration specific data required for the proper functioning of the overall system.	date of registration name of RA validity period
CA supplied data	The certification authority is responsible for adding certification specific data required for the proper functioning of the overall system.	certificate serial number signature algorithm identifier name of CA certificate format version
CA signature	The signature of the certification authority binds the public key to the entity's name.	

Generic Certificate Structure

To verify a user public key certificate we still need the CA’s public verification key. Hence, we have pushed the public key distribution problem from the user level (say, N users in a domain) to the CA level (one CA in a domain). A CA’s public key may in turn be certified by a higher-level Certification Authority.

2.2 Attribute Certificates

It may be useful to certify other attributes of an entity (besides the public key). There are attributes which directly relate to the public key certificate, such as

- method of delivery of the credentials,
- method of identification of the entity, entity type (e.g. individual, corporation, government, device, etc.),
- information on trusted third parties involved in the registration,
- information on domains and cross-certification.

There are other attributes which relate to the signing capabilities of an entity, such as

- authorized signatory (formal authorization of individuals to sign for the organisation),
- transaction limit (maximum monetary value of a message which the entity may sign),
- transaction type (transaction types which the entity may sign),
- time of day (during which signatures of the entity are considered valid),
- location (from which signatures of the entity are considered valid),

- pre-approved counter party (to indicate with which parties the entity can conduct signed transactions),
- delegation control (indicate the amount of authority that the entity may delegate to some other entity).

These attributes could be included in the basic public key certificate. However, a number of reasons suggests that they are not:

- the attributes are not needed in every transaction,
- the attributes would increase the size of the basic certificate,
- attributes may vary much more often than the basic certificate information, which would require a reissuance of the certificate at each change.

Existing standards (such as X.500) assume that these attributes are not included in the basic public key certificate. Rather these attributes shall be carried in a separate structure called the attribute certificate. To emphasize that the attribute certificate need not be generated by the same CA as the basic public key certificate, we use the notion of attribute certification authority (ACA).

Example 1 - Attribute Certificate Information

The attribute certificate is signed by the ACA.

Attribute Certificate Information	Explanation
baseCertificateID	issuer and serial number of the associated public key certificate
issuer	distinguished name of the ACA
serialNumber	serial number of the attribute certificate
validity	validity period of the attribute certificate
attributes	a set of attributes to be certified
IssuerUniqueID	unique identifier of the ACA's public key (optional)

Structure of ANSI X9.30-3 Attribute Certificate Information

ANSI X9.30-3 assumes that the signature algorithm executed by the ACA is the same as the one used to produce the basic public key certificate and that the attribute certificate is only to be used in combination with the basic public key certificate.

To be more general, one could allow the specification of the entity's distinguished name and of the signature algorithm used by the ACA. That would make it possible to use attribute certificates independently of the basic public key certificate (and include attributes beyond those related to the certificate or the signature of the entity).

3 Revocation of Certificates

Certificates typically have a fixed validity period. However, there is a number of reasons why a certificate may have to be declared invalid before the end of that validity period (this process is called revocation):

User level:

1. compromise of the entity's private key (suspected or verified)
2. change of the certificate information

3. termination of the entity's operation

CA level[1]:

1. compromise of the CA's private key (suspected or verified)
2. change of the CA's certificate information
3. termination of the CA's operation
4. change of policy

and others. Revocation is a very serious process since it could potentially result in desastrous business consequences. There must be utmost care in verifying the authenticity of a revocation request.

We distinguish the following phases in the revocation process:

1. Revocation request
   - Who has the authority to request the revocation of a certificate?
   - Under what conditions can or must a certificate be revoked?
   - How to prove and verify a revocation request
2. Revocation
   - Who performs the revocation?
   - How is a certificate revoked?
   - Can certificates be on alert or on hold?
3. Revocation notification
   - How to notify users (and other relevant entities) about the revocation of a certificate?
   - How to prevent misuse of revoked certificates?
   - Access to and legal status of a revoked certificate?

3.1 Black List Approach

In current systems, the revocation process is approached in a different way than the certification process. In the certification process, the Certification Authority issues public key certificates as self-contained electronic documents, aimed to provide legal status. In the revocation process, the certificate serial number is included in a black list (also called Certificate Revocation List CRL). The black list is made available to users on a periodic basis. The following two examples illustrate the black list approach.

Example 2 - Certificate Revocation List

The certificate revocation list contains a header and a sequence of revocation entries. The CRL is signed by the CA and published and distributed on a periodic basis.

CRL-Part	Contained information
CRL Header	signature algorithm identifier
	issuer name
	issuer unique identifier (optional)
	CRL number
	last update

[1] It must be distinguished between user level and CA level, since the compromise of a CA's private key may require the revocation and subsequent re-certification of all user keys in a domain.

	next update
CRL Entry	certificate serial number
	revocation date
	reason

Structure of ANSI X9.30-3 Certificate Revocation List

The reason of revocation may be one of the following: key compromise, CA compromise, changed affiliation, superseded by new certificate, termination and other.

Example 3 - Revocation Notice

The CA may wish to inform other entities directly of individual revocations. The Revocation Notice is a message signed by the CA and containing the following information.

Part	Contained information
Revocation Notice header	name of issuer
	unique identifier of issuer (optional)
Components of CRL entry	certificate serial number
	revocation date
	reason

Structure of ANSI X9.30-3 Revocation Notice

3.2 Business Requirements

There are several business requirements which cannot be satisfied by the black list approach:

1. It might be required to have access to a revoked certificate in order to perform verifications with the revoked public key. Such a situation may occur when a document was signed long before the revocation but has to be verified after the revocation.
2. It seems inadequate to request users to download the complete black list in order to find out about individual revocations. In addition, the black list typically gives only the serial numbers of revoked certificates. Therefore, these black lists are only useful to check the status of certificates which have been obtained through some other means.
3. One might wish to check the history of a user for the reasons and frequencies of revocations.
4. It seems desirable to have a legally binding status for revoked certificates. The same way as the CA certifies the association between an entity and its public key, the CA should certify the revocation of a certificate in a self-contained manner.
5. Periodically issued CRLs do not allow for non-repudiation. Given the currently valid black list (say, from last month) and a business partner signature that was computed after the issuance of the black list, the recipient does not have assurance of the validity of the signature (and hence, no non-repudiation).

3.3 Revocation Certificates

To satisfy the outlined business requirements, we propose the concept of revocation certificates. The revocation certificate is issued by a CA. It consists of the original certificate information and additional information about the revocation such as date and reason of revocation, the date of known or suspected compromise, the party who requested the revocation, and the name of the CA who performed the revocation. The CA then signs the revocation information and thereby creates a self-contained revocation certificate. Such revocation certificates can be stored and handled in the same way as public key certificates are. Legally, they also have a self-contained status.

3.4 Structure of a Revocation Certificate

The following table shows the proposed structure of a revocation certificate.

Part	Contained information
certificate	the original certificate (or certificate serial number)
signature	signature algorithm identifier
issuer	CA who performed the revocation
revocation date	date when certificate has been revoked
reason	reason why the certificate has been revoked[2]
compromise date	date of suspected compromise (optional)
initiator	party who requested the revocation (optional)

Structure of Revocation Certificate

In case of private key compromise, it might be useful to include the the date and time of known or suspected compromise (which need not coincide with the time of revocation). This would help in auditing the systems and messages. The party who requested the revocation (initiator) need not be the user itself, it may, for instance, be the employer or a trusted third party.

To be completely general, one may logically separate the functionality of certification from the functionality of revocation and introduce a separate revocation authority. Note that this does not mean that the two functions have to be performed by physically different authorities.

3.5 Applications of Revocation Certificates

The concept of revocation certificates has been adopted in the TEDIS Project FAST (First Attempt to Secure Trade). The certificate segment has been extended by the following newly introduced data elements:

Number	Description	M/C	Format	Special notes
???	CERTIFICATE TYPE	C	an..3	1 for regular certificate 2 for revocation certificate
S501	SECURITY DATE AND TIME	C		Certificate revocation date
0515	Date and time qualifier	M	an..3	Code = 5 for CRD
0502	Date	C	n8	YYYYMMDD
0504	Time	C	n6	HHMMSS
0506	UTC offset	C	an..5	XHHMM where X is either P for plus or M for minus.
???	KEY COMPROMISE	C	an..3	1 for Yes 2 for No

[2] In some countries, data privacy laws prevent the use of detailled revocation reason codes.

4 References

ANSI X9.30 199x, "Public Key Cryptography Using Irreversible Algorithms for the Financial Services Industry, Part 3: Certificate Management for DSA".

Michael S. Baum, „Federal Certification Authority Liability and Policy“, NIST-GCR-94-654.

FAST, „First Attempt to Secure Trade“, TEDIS Phase II, T1.1 „Credentials, Attributes and Certificates“, April 1994.

X.509 (1992) Authentication Framework