Models for Certificate Path Validation

L. Lo Iacono [1], S. Müller [2], M. Schneider [3]

1 C&C Research Laboratories, NEC Europe Ltd.

2 Institute for Data Communications Systems, University of Siegen (Germany)

3 Department of Information Technology, Districtal Environmental Authority Siegen (Germany)

Abstract: Before a certificate can be used, it must be validated. In order to validate such a certificate, a chain of certificates or a so-called certification path between the certificate and an established point of trust must be constructed, and every certificate within that path must be checked. This process is referred to as certification path processing.

In general, certification path processing consists of two phases: certificate path construction and certificate path validation. The article focuses on certificate path validation and describes the different models discussed in literature. It compares the different properties and discusses the possibilities of using them in accordance of the German digital signature law.

1. Introduction

Public Key Infrastructure (PKI) supports a number of security-related services, including data confidentiality, data integrity, and end-entity authentication. Fundamentally, these services are based on the proper use of public/private key pairs. The public component of this key pair is issued in the form of a public key certificate and, in association with the appropriate algorithm(s), it may be used to verify a digital signature, encrypt data, or both[1].

Before a certificate can be used, it must be validated. In order to validate such a certificate, a chain of certificates or a so-called certification path between the certificate and an established point of trust must be constructed, and every certificate within that path must be checked. This process is referred to as certification path processing.

In general, certification path processing consists of two phases:

1. **Path construction** involves "building" certification paths.
2. **Path validation** includes making sure that each certificate in the path is within its established validity period, has not been revoked, has integrity, et cetera; and any constraints levied on part or all of the certification path are honored (e.g., path length constraints, name constraints, policy constraints).

The article focuses on the path validation step only whereas some issues on path constructing are also mentioned.

2. Discussed Models

The 4th Edition of X.509 [1] and the Internet certificate and certificate revocation list profile as defined in RFC3280 [2] provide the most recent specifications for certification path validation. In these specifications the following two discussed models are included.

- The **shell model** checks the validity of every certificate in the path at the current date and time.
- The **modified shell model** checks the validity of the first certificate at the time the target document has been signed. Every following verification will be based on this time.

In Germany the **chain model** has been developed. It adapts the time for every single certificate check to the time the previous certificate has been issued. This model is not standardized in any form

3. Conformance to German Digital Signature Law

The German Digital Signature Law defines requirements for the validations of certificate paths. It is analyzed which of the introduced models is in conformance to these legal requirements. The modified shell model as well as the chain model fulfill all requirements and are therefore suitable for applications which have to consider these legal aspects.

References

[1] ITU-T Recommendation X.509, *Information Technology—Open Systems Interconnection—The Directory: Public Key and Attribute Certificate Frameworks*, March 2000 (equivalent to ISO/IEC 9594-8, 2000).

[2] R. Housley, W. Ford, W. Polk, and D. Solo, *Internet X.509 Public Key Infrastructure: Certificate and CRL Profile*, Internet Request for Comments 3280, April 2002.

[1] 1 It should be recognized that there are several reasons that separate key pairs should be used for digital signature and confidentiality, including differing requirements associated with key backup/recovery and long-term handling of keying material, and the ability to use different algorithms for each (e.g., DSA could be used for the digital signature and RSA could be used for symmetric key exchange).