                  X.509 Certificate Extension for
   Secure/Multipurpose Internet Mail Extensions (S/MIME) Capabilities

Status of This Memo

   This document specifies an Internet standards track protocol for the
   Internet community, and requests discussion and suggestions for
   improvements. Please refer to the current edition of the "Internet
   Official Protocol Standards" (STD 1) for the standardization state
   and status of this protocol. Distribution of this memo is unlimited.

Abstract

   This document defines a certificate extension for inclusion of
   Secure/Multipurpose Internet Mail Extensions (S/MIME) Capabilities in
   X.509 public key certificates, as defined by RFC 3280. This
   certificate extension provides an optional method to indicate the
   cryptographic capabilities of an entity as a complement to the S/MIME
   Capabilities signed attribute in S/MIME messages according to RFC
   3851.

1. Introduction

   This document defines a certificate extension for inclusion of S/MIME
   Capabilities in X.509 public key certificates, as defined by RFC 3280
   [RFC3280].

   The S/MIME Capabilities attribute, defined in RFC 3851 [RFC3851], is
   defined to indicate cryptographic capabilities of the sender of a
   signed S/MIME message. This information can be used by the recipient
   in subsequent S/MIME secured exchanges to select appropriate
   cryptographic properties.

   However, S/MIME does involve also the scenario where, for example, a
   sender of an encrypted message has no prior established knowledge of
   the recipient's cryptographic capabilities through recent S/MIME
   exchanges.

   In such a case, the sender is forced to rely on out-of-band means or
   its default configuration to select a content encryption algorithm
   for encrypted messages to recipients with unknown capabilities. Such
   default configuration may, however, be incompatible with the
   recipient's capabilities and/or security policy.

   The solution defined in this specification leverages the fact that
   S/MIME encryption requires possession of the recipient's public key
   certificate. This certificate already contains information about the
   recipient's public key and the cryptographic capabilities of this
   key. Through the extension mechanism defined in this specification,
   the certificate may also identify the subject's cryptographic S/MIME
   capabilities. This may then be used as an optional information
   resource to select appropriate encryption settings for the
   communication.

   This document is limited to the "static" approach where asserted
   cryptographic capabilities remain unchanged until the certificate
   expires or is revoked. Other "dynamic" approaches, which allow
   retrieval of certified dynamically updateable capabilities during the
   lifetime of a certificate, are out of scope of this document.

1.1. Terminology

   The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT",
   "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this
   document are to be interpreted as described in RFC 2119 [STDWORDS].

2. S/MIME Capabilities Extension

   This section defines the S/MIME Capabilities extension.

   The S/MIME Capabilities extension data structure used in this
   specification is identical to the data structure of the
   SMIMECapabilities attribute defined in RFC 3851 [RFC3851]. (The
   ASN.1 structure of smimeCapabilities is included below for
   illustrative purposes only.)

      smimeCapabilities OBJECT IDENTIFIER ::=
         {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1)
         pkcs-9(9) 15}

      SMIMECapabilities ::= SEQUENCE OF SMIMECapability

      SMIMECapability ::= SEQUENCE {
         capabilityID OBJECT IDENTIFIER,
         parameters ANY DEFINED BY capabilityID OPTIONAL }

All content requirements defined for the SMIMECapabilities attribute
in RFC 3851 apply also to this extension.

There are numerous different types of S/MIME Capabilities that have
been defined in various documents. While all of the different
capabilities can be placed in this extension, the intended purpose of
this specification is mainly to support inclusion of S/MIME
Capabilities specifying content encryption algorithms.

Certification Authorities (CAs) SHOULD limit the type of included
S/MIME Capabilities in this extension to types that are considered
relevant to the intended use of the certificate.

Client applications processing this extension MAY at their own
discretion ignore any present S/MIME Capabilities and SHOULD always
gracefully ignore any present S/MIME Capabilities that are not
considered relevant to the particular use of the certificate.

This extension MUST NOT be marked critical.

3. Use in Applications

Applications using the S/MIME Capabilities extension SHOULD NOT use
information in the extension if more reliable and relevant
authenticated capabilities information is available to the
application.

It is outside the scope of this specification to define what is, or
is not, regarded as a more reliable source of information by the
application that is using the certificate.

4. Security Considerations

The S/MIME Capabilities extension contains a statement about the
subject's capabilities made at the time of certificate issuance.
Implementers should therefore take into account any effect caused by
the change of these capabilities during the lifetime of the
certificate.

Change in the subject's capabilities during the lifetime of a
certificate may require revocation of the certificate. Revocation
should, however, only be motivated if a listed algorithm is
considered broken or considered too weak for the governing security
policy.

Implementers should take into account that the use of this extension
does not change the fact that it is always the responsibility of the
sender to choose sufficiently strong encryption for its information
disclosure.

5. Normative References

   [STDWORDS] Bradner, S., "Key words for use in RFCs to Indicate
              Requirement Levels", BCP 14, RFC 2119, March 1997.

   [RFC3280] Housley, R., Polk, W., Ford, W., and D. Solo, "Internet
              X.509 Public Key Infrastructure Certificate and
              Certificate Revocation List (CRL) Profile", RFC 3280,
              April 2002.

   [RFC3851] Ramsdell, B., "Secure/Multipurpose Internet Mail
              Extensions (S/MIME) Version 3.1 Message Specification",
              RFC 3851, July 2004.

Author's Address

   Stefan Santesson
   Microsoft
   Tuborg Boulevard 12
   2900 Hellerup
   Denmark

   EMail: stefans@microsoft.com

Full Copyright Statement

Intellectual Property

Acknowledgement