IETF PKIX WG
Internet Draft
Intended Status: Proposed Standard
Updates: 3161 (once approved)
Expires: April 29, 2010
October 26, 2009

Stefan Santesson
(3xA Security)
Nick Pope
(Thales)

ESSCertIDv2 update for RFC 3161
draft-ietf-pkix-rfc3161-update-09

Status of this Memo

Copyright and License Notice

Abstract

This document updates RFC 3161 [RFC3161]. It allows the use of ESSCertIDv2 defined in RFC 5035 [ESSV2] to specify the hash of a signer certificate when the hash is calculated with a function other than SHA-1 [SHA1].

Table of Contents

1 Introduction

The time stamping protocol defined in RFC 3161 [RFC3161] requires that the CMS SignedData [RFC3852], used to apply a digital signature on the time-stamp token, include a signed attribute that identifies the signer's certificate.

This identifier only allows SHA-1 to be used as hash algorithm to generate the identifier value.

The mechanism used in [RFC3161] employed ESSCertID from RFC 2634 [ESS]. RFC 5035 [ESSV2] updated ESSCertID with ESSCertIDv2 to allow the use of any hash algorithm.

The changes to RFC 3161 [RFC3161] defined in this document allows ESSCertIDv2 to be used to include an identifier of the signing certificate as defined in RFC 5035 [ESSV2].

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 [RFC2119].

2 Updates to RFC 3161

2.1 Changes to section 2.4.1 Request Format

Last paragraph on page 5.

Old:

> If the certReq field is present and set to true, the TSA's public key certificate that is referenced by the ESSCertID identifier inside a SigningCertificate attribute in the response MUST be provided by the TSA in the certificates field from the SignedData structure in that response. That field may also contain other certificates.

New:

> If the certReq field is present and set to true, the TSA's public key certificate that is referenced by the ESSCertID [ESS] field inside a SigningCertificate attribute or by the ESSCertIDv2 [ESSV2] field inside a SigningCertificateV2 attribute in the response MUST be provided by the TSA in the certificates field from the SignedData structure in that response. That field may also contain other certificates.

2.2 Changes to Section 2.4.2 Response Format

2.2.1 signature of time stamp token

5th paragraph on page 8, just before the definition of TSTInfo.

Old:

> The time-stamp token MUST NOT contain any signatures other than the signature of the TSA. The certificate identifier (ESSCertID) of the TSA certificate MUST be included as a signerInfo attribute inside a SigningCertificate attribute.

New:

> The time-stamp token MUST NOT contain any signatures other than the signature of the TSA. The certificate identifier (either ESSCertID [ESS] or ESSCertIDv2 [ESSV2]) of the TSA certificate MUST be included as a signerInfo attribute inside a SigningCertificate attribute.
>
> Note: As mentioned in RFC 5035 [ESSV2], the SigningCertificateV2 attribute MUST be used if any algorithm other than SHA-1 is used and SHOULD NOT be used for SHA-1.
>
> Note: For backwards compatibility, in line with RFC 5035, both ESSCertID and ESSCertIDv2 MAY be present. Systems MAY ignore ESSCertIDv2 if RFC 5035 has not been implemented.

2.2.2 verifying the time stamp token

3rd paragraph on page 11.

Old:

The purpose of the tsa field is to give a hint in identifying the name of the TSA. If present, it MUST correspond to one of the subject names included in the certificate that is to be used to verify the token. However, the actual identification of the entity that signed the response will always occur through the use of the certificate identifier (ESSCertID Attribute) inside a SigningCertificate attribute which is part of the signerInfo (See Section 5 of [ESS]).

New:

The purpose of the tsa field is to give a hint in identifying the name of the TSA. If present, it MUST correspond to one of the subject names included in the certificate that is to be used to verify the token. However, the actual identification of the entity that signed the response will always occur through the use of the certificate identifier (ESSCertID inside a SigningCertificate attribute or ESSCertIDv2 inside a SigningCertificateV2 attribute) which is part of the signerInfo (See Section 5 of [ESS] and Section 3 of [ESSV2]).

3 Security Considerations

This draft incorporates the security considerations of RFC 5035 [ESSV2] with further explanations in this section.

ESSCertID provides a means based on the SHA-1 hash algorithm for identifying the certificate used to verify the signature on a time stamp. The use of ESSCertIDv2 aims to enable implementers to comply with policies that require phasing out all uses of the SHA-1 algorithm.

The update provided by this draft is motivated by reasons of interoperability and migration to other hash algorithms rather than mitigating new security issues.

4 IANA Considerations

This draft requires no actions by IANA.

5 References

5.1 Normative References

[RFC2119] S. Bradner, "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[ESS] Hoffman, P., "Enhanced Security Services for S/MIME", RFC 2634, June 1999.

[ESSV2] Schaad, J., "Enhanced Security Services (ESS) Update: Adding CertID Algorithm Agility", RFC 5035. August 2007.

[RFC3161] Adams, C., Cain, P., Pinkas, D. and Zuccherato, R. "Time-Stamp Protocol (TSP)", RFC 3161. August 2001.

[RFC3852] R. Housley, "Cryptographic Message Syntax (CMS)", RFC 3852, July 2004.

5.2 Informative References

[SHA1] Secure Hash Standard. FIPS Pub 180-1. National Institute of Standards and Technology. 17 April 1995.

Author's Addresses

Stefan Santesson
3xA Security AB
Sweden

Email: sts@aaa-sec.com

Nick Pope
Thales Information Systems Security
Long Crendon, Aylesbury
United Kingdom

Email: nick.pope@thales-esecurity.com