IETF PKIX WG
Internet Draft
Intended Status: Standard Track
Updates: 4055 (once approved)
Expires: September 9, 2009

Sean Turner, IECA
Daniel Brown, Certicom
Kelvin Yiu, Microsoft
Russ Housley, Vigil Security
Tim Polk, NIST
March 9, 2009

Update for RSAES-OAEP Algorithm Parameters
draft-ietf-pkix-rfc4055-update-02.txt

Status of this Memo

Copyright Notice

Abstract

This document updates RFC 4055. It updates the conventions for using the RSA Encryption Scheme - Optimal Asymmetric Encryption Padding (RSAES-OAEP) key transport algorithm in the Internet X.509 Public Key Infrastructure (PKI). Specifically, it updates the conventions for algorithm parameters in an X.509 certificate's subjectPublicKeyInfo field.

Conventions used in this document

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 [RFC2119].

Discussion

This draft is being discussed on the 'ietf-pkix' mailing list. To subscribe, send a message to ietf-pkix-request@imc.org with the single word subscribe in the body of the message. There is a Web site for the mailing list at <http://www.imc.org/ietf-pkix/>.

1. Introduction

RFC 4055 specifies conventions for using the RSA Encryption Scheme - Optimal Asymmetric Encryption Padding (RSAES-OAEP) key transport algorithm in the Internet X.509 Public Key Infrastructure (PKI). It provides algorithm identifiers and parameters for RSAES-OAEP.

This document updates the conventions for RSAES-OAEP parameters in the subjectPublicKeyInfo field of an X.509 certificate. The PKIX WG Elliptic Curve Cryptography (ECC) design team recommended that Key Derivation Functions (KDFs) should not be constrained within a certificate; rather, KDF constraints should be negotiated in

protocols that need to employ certificates.

Only two paragraphs in [RFC4055] discuss RSAES-OAEP parameters in X.509 certificates: the second paragraph of section 4 and the first paragraph of section 4.1. This document only updates these two

paragraphs. Section 3 updates the second paragraph in section 4 while section 3 updates the second paragraph in section 4.1. "Old:" prefaces the text to be replaced and "New:" prefaces the replacement text.

This document also replaces incorrect references to the publicKeyAlgorithms field in Section 3 with references to the parameters field in the subjectPublicKeyInfo algorithm field. No other changes are made to the RSASSA-PSS sections.

2. Changes to Section 3 2nd and 3rd Paragraph

This change clarifies the placement of RSASSA-PSS-params in the signature, signatureAlgorithm, and subjectPublicKeyInfo fields for CA and EE certificates. It also clarifies the placement of RSASSA-PSS-params in the signatureAlgorithm field in CRLs.

Old:

CAs that issue certificates with the id-RSASSA-PSS algorithm identifier SHOULD require the presence of parameters in the publicKeyAlgorithms field if the cA boolean flag is set in the basic constraints certificate extension. CAs MAY require that the parameters be present in the publicKeyAlgorithms field for end-entity certificates.

CAs that use the RSASSA-PSS algorithm for signing certificates SHOULD include RSASSA-PSS-params in the subjectPublicKeyInfo algorithm parameters in their own certificates. CAs that use the RSASSA-PSS algorithm for signing certificates or CRLs MUST include RSASSA-PSS-params in the signatureAlgorithm parameters in the TBSCertificate or TBSCertList structures.

New:

When the id-RSASSA-PSS object identifier appears in the TBSCertificate or TBSCertList signature algorithm field, then the

RSASSA-PSS-params structure MUST be included in the TBSCertificate or TBSCertList signature parameters field.

When the id-RSASSA-PSS object identifier appears in the TBSCertificate subjectPublicKeyInfo algorithm field of CA certificates, then the parameters field SHOULD include the RSASSA-PSS-params structure. When the id-RSASSA-PSS object identifier appears in the TBSCertificate subjectPublicKeyInfo algorithm field of EE certificates, then the parameters field MAY include the RSASSA-PSS-params structure.

All certificates and CRLs signed by a CA that supports the id-RSASSA-PSS algorithm MUST include the RSASSA-PSS-params in the signatureAlgorithm parameters in Certificate and CertList structures, respectively.

3. Changes to Section 4 2nd Paragraph

This change prohibits the inclusion of RSAES-OAEP-params in the subjectPublicKeyInfo field. This was done because a) it does not affect interoperability b) aligns with PKIX practice to not include limitations on how the public key can be used in subjectPublicKeyInfo. A poll of implementers was taken and there were no objections to this change as it did not affect current implmentations.

Old:

CAs that issue certificates with the id-RSAES-OAEP algorithm identifier SHOULD require the presence of parameters in the publicKeyAlgorithms field for all certificates. Entities that use a certificate with a publicKeyAlgorithm value of id-RSA-OAEP where the parameters are absent SHOULD use the default set of parameters for RSAES-OAEP-params. Entities that use a certificate with a publicKeyAlgorithm value of rsaEncryption SHOULD use the default set of parameters for RSAES-OAEP-params.

New:

CAs that issue certificates with the id-RSAES-OAEP algorithm identifier MUST NOT include parameters in the subjectPublicKeyInfo algorithm field.

4. Changes to Section 4.1 1st Paragraph

This change prohibits the inclusion of parameters in the subjectPublicKeyInfo field. This was done because a) it does not affect interoperability b) aligns with PKIX practice to not include limitations on how the public key can be used in subjectPublicKeyInfo. A poll of implementers was taken and there were no objections to this change as it did not affect current implmentations.

Old:

When id-RSAES-OAEP is used in an AlgorithmIdentifier, the parameters MUST employ the RSAES-OAEP-params syntax. The parameters may be either absent or present when used as subject public key information.

The parameters MUST be present when used in the algorithm identifier associated with an encrypted value.

New:

When id-RSAES-OAEP is used in an AlgorithmIdentifier, the parameters MUST employ the RSAES-OAEP-params syntax. The parameters MUST be absent when used in the subjectPublicKeyInfo field. The parameters MUST be present when used in the algorithm identifier associated with an encrypted value.

5. Security Considerations

The security considerations from [RFC4055] apply.

If the RSAES-OAEP-params are negotiated, then the negotiation mechanism needs to provide integrity for these parameters. For example, an S/MIME Agent can advertise their capabilities in the SMIMECapabilities attribute, which is either signed attribute [RFC3851bis] or a certificate extension [RFC4262].

6. IANA Considerations

None

{{Please remove this section prior to publication as an RFC.}}

7. References

7.1. Normative References

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

[RFC4055] Schaad, J., Kaliski, B., and R. Housley, "Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 4055, June 2005.

7.2. Informative References

[RFC4262] S. Santesson, "X.509 Certificate Extension for Secure/Multipurpose Internet Mail Extensions (S/MIME) Capabilities", RFC 4262, December 2005.

[RFC3851bis] Turner, S., Farrell, S., and R. Housley, "An Internet Attribute Certificate Profile for Authorization", draft-ietf-pkix-3281update-04.txt, work-in-progress.

/*** RFC EDITOR: Please replace RFC3851bis with RFCXYAZ when draft-ietf-pkix-3281update is published.

Author's Addresses

Sean Turner

IECA, Inc.
3057 Nutley Street, Suite 106
Fairfax, VA 22031
USA

EMail: turners@ieca.com

Kelvin Yiu

Microsoft
One Microsoft Way
Redmond, WA 98052-6399
USA

Email: kelviny@microsoft.com

Daniel R. L. Brown

Certicom Corp
5520 Explorer Drive #400
Mississauga, ON L4W 5L1
CANADA

EMail: dbrown@certicom.com

Russ Housley

Vigil Security, LLC
918 Spring Knoll Drive
Herndon, VA 20170
USA

EMail: housley@vigilsec.com

Tim Polk

NIST
Building 820, Room 426
Gaithersburg, MD 20899
USA

EMail: wpolk@nist.gov