Network Working Group B.
Laurie
Internet-Draft
Nominet
Expires: December 16, 2006 June 14,
2006

Distributing Keys for DNSSEC
draft-laurie-dnssec-key-distribution-02

Status of this Memo

Copyright Notice

Abstract

Until DNSSEC is fully deployed, so-called "islands of trust" will exist. This will lead to a large number of keys with no method within DNSSEC to manage the keys. This proposal seeks to address that issue using existing mechanisms to allow cross-signing of root (i.e. roots of islands) keys. This cross-signing of keys creates a non-hierarchical web of trust which permits the efficient gathering and validation of trust anchors.

Table of Contents

1. Introduction

When DNSSEC signatures are validated the validators will follow a chain of authority from a pre-configured trust anchor to the data that is to be validated. The DNSSEC protocol (RFC 4033 [RFC4033], RFC 4034 [RFC4034] and RFC 4035 [RFC4035]) clearly describes how these chains of trust are to be established but does not address the issue of the distribution of the trust anchors.

This document describes how an X.509 based public key infrastructure can be used to bootstrap the configuratation of a set of trust anchors. SEP keys are stored in certificates that are signed by the registries' Certificate Authorities. The system allows registries to indicate levels of trust which allows for prudent cross-signing.

The Certificate Authority and the certificates are discussed in Section 2 and Section 3. Section 4 and Section 5 describe how the certificates are published. Section 6 describes how the certificates are used to establish the trust-anchors.

In this document the term secure entry point (SEP) key is used to describe the (sub)set of public key(s) that is intended as a secure entry point into the zone [RFC3757]. The term Island of security, or island for short, is used for a zone for which one of the SEP keys are used as a trust-anchor and which is therefore the start of a chain of authority.

2. Island CAs

The root of each island will publish an X.509 CA certificate. This will be a long-term, self-signed certificate, known as the Island Root CA (IRCA). This CA will then be used to create two subsidiary CAs, each with a shorter expiry, known as the High Assurance Island CA and the Low Assurance Island CA. The High and Low Assurance CA certificates will each contain an X.509v3 extension indicating their role.

Each island will have a set of requirements for cross-signing, one for low assurance and one for high assurance. The reason for having two is to allow cross-signing of keys that the island's operators do not have high confidence in without exposing them to accusations of insufficient prudence.

3. Key Signing

Each island will issue a certificate signed by the Island Root CA for

each of its own SEPs. The public key in the certificate will be the same public key as used by the SEP.

For each other island that meets the island's requirements for cross-signing, the island will issue a certificate for their IRCA signed by either the Low or High Assurance Island CA, as appropriate. That is, the certificate will have the same subject name and public key as the IRCA being signed, but the issuer will be one of this island's subsidiary CAs. This could be done using the cross-certification protocol from RFC 2510 [RFC2510]

Each certificate issued will contain an X.509v3 extension with the name of the domain associated with the signed public key.

4. Publication of Certificates

Each island will maintain a URL (known as the Island Publication URL or IPU) where all current certificates issued by any of its CAs are available. This URL may also have a collection of certificates issued by other island CAs and also the CA certificates themselves of other islands. Note, however, that the presence of a certificate does not indicate any kind of trust in it - that is done purely by the certificate signatures.

5. Location of Island Publication URL

The location of each IPU will be held in the IRCA using an X.509v3 certificate extension registered for the purpose.

6. Use of Certificates

A resolver wishing to bootstrap its collection of trust anchors need only choose a small set of IRCAs to trust (or, with luck, a single one). Once it has done so, it can extract the IPU from the CA certificate, use HTTP to retrieve the certificate collection available there, check their (chained) signatures, extract the public keys from the certificates and use these as the initial set of SEPs for the domains named in the certificates.

Once the initial set of certificates has been retrieved, this process can be followed recursively for other IRCAs retrieved. Also, the set

of trusted IRCAs could be expanded to include some or all of the retrieved IRCAs.

After the set of trusted trust anchors have been established, in-band

mechanisms can be used to keep them up to date. If for some reason the set of trust anchors becomes too stale to update (for example, because the device has been offline for an extended period), then the process can be repeated from the start.

7. Verification of Certificates

Once the collection of certificates is complete, the resolver uses the trusted IRCAs to verify the certificate of each SEP. Because of the use of cross-certification, the X.509 verification must be capable of trying multiple paths to verification, as specified in RFC 3280 [RFC3280].

Users may choose to restrict the verification path, for example by requiring certificate chains to be below some length, or not permitting verification through Low Assurance CAs.

Once the set of verified SEPs has been established, then the public keys are extracted from each one and associated as trust anchors for DNSSEC with the corresponding domain.

8. Variations

Instead of a URL, the certificate could contain a domain name and socket number.

Certificates could be published in the DNS [I-D.ietf-dnsext-rfc2538bis].

Rather than using X.509 for signing, OpenPGP [RFC2440] could be used instead.

9. Security Non-issues

Note that DNSSEC is not required to secure the domain names used for certificate retrieval, since the signature of the selected IRCA(s) will be sufficient to validate the retrieved certificates.

10. Acknowledgements

Thanks to Olaf Kolkman for comments on early drafts and Russ Housley for explaining how to use X.509 the way I wanted to.

11. Requirements notation

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].

12. Security Considerations

13. References

13.1. Normative References

[I-D.ietf-dnsext-rfc2538bis] Josefsson, S., "Storing Certificates in the Domain Name System (DNS)", draft-ietf-dnsext-rfc2538bis-09 (work in progress), October 2005.

[RFC2440] Callas, J., Donnerhacke, L., Finney, H., and R. Thayer, "OpenPGP Message Format", RFC 2440, November 1998.

[RFC2510] Adams, C. and S. Farrell, "Internet X.509 Public Key Infrastructure Certificate Management Protocols", RFC 2510, March 1999.

[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.

13.2. Informative References

[RFC2026] Bradner, S., "The Internet Standards Process -- Revision 3", BCP 9, RFC 2026, October 1996.

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

[RFC2418] Bradner, S., "IETF Working Group Guidelines and Procedures", BCP 25, RFC 2418, September 1998.

[RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, March 2005.

[RFC4034] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Resource Records for the DNS Security Extensions",

RFC 4034, March 2005.

[RFC4035] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Protocol Modifications for the DNS Security Extensions", RFC 4035, March 2005.

Author's Address

Ben Laurie
Nominet
17 Perryn Road
London W3 7LR
England

Phone: +44 (20) 8735 0686
Email: ben@algroup.co.uk

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

Funding for the RFC Editor function is currently provided by the

Internet Society.