Network Working Group	P. Faltstrom	
Internet-Draft	Cisco	
Intended status: Informational	J. Schlyter	
Expires: October 10, 2009	Kirei AB	
	April 08, 2009	

TOC

Validation of the root trust anchor for the DNS
draft-faltstrom-root-trust-anchor-validation-00

Status of this Memo

Copyright Notice

Abstract

This document describes practical requirements and needs for automatic validation of the root trust anchor for the DNS. It also proposes a mechanism using PGP and/or S/MIME that can be used to fulfil the requirements.

Table of Contents

---

1. Introduction

TOC

In deployment of DNSSEC (Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, “DNS Security Introduction and Requirements,” March 2005.) [RFC4033], the root zone will have one or more Key Signing Keys (KSK) each having a private and public part. The public part is to be used for verification of the trust chain and because of that distributed to and trusted by every resolver that want to verify DNSSEC signed responses.
As the distribution of the public part of the KSK is made using electronic communication mechanisms, and replaced frequently, it is important that the distribution made in a way so that the integrity of the KSK can be verified. The simplest way to manage this is to sign the public part of the KSK, and have the digital signature of the KSK, and therefore the public part of the key that signs the KSK, be what is trusted by the resolver.
To be able to handle changes in the KSK in an automated fashion, while at the same time allow external organisations to audit the KSK management, and give the ability for parties that is to trust the KSK to automatically do so, it is proposed to have a recommended way of managing this distribution of the public part of the KSK.
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 (Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels,” March 1997.) [RFC2119].

---

2. Terminology

TOC

KSK Key Signing Key

ZSK Zone Signing Key

TAR Trust Anchor Repository

TAR Signee An entity signing the TAR

TAR Consumer An entity using the contents of the TAR as DNSSEC trust anchors, possibly based on the signatures created by the TAR signees.

---

3. Proposed Architecture

TOC

It is proposed that the public key signing keys (KSKs) for the root zone are distributed in the form of a trust anchor repository (TAR) signed by multiple parties.
To be able to put trust in the KSKs, and therefore in the root zone signing process, the TAR signees should be able to audit the root signing policies and procedures.
The signing mechanisms should be such that the TAR can be signed by more than one entity. It should be possible to for each signee to sign the TAR separately form other signees.
After the entities have signed the TAR, it is to be distributed. In some cases by the entities that sign it, in other cases by third parties. It is up to the TAR distributor to bundle the TAR with the signatures made by the TAR signees. A TAR distributor might choose to not include all signatures in the distribution.
Someone that receive such a signed TAR can verify the signatures and that way ensure two things - that the contents of the TAR has not changed during transmission and that the current process used for managing the keys that forms the TAR is trusted by the TAR signee.
It is suggested that the lifetime of the signatures on the TAR is potentially shorter than the administrative lifetime of the TAR contents (e.g. keys and fingerprints). This enables the ability for the signee to do the audit of the root signing policies and procedures repeatedly over time.
If the consumer of the TAR cannot validate enough signatures, it is recommended that the contents of the TAR should not be used to configure the validating DNSSEC resolver.

---

4. Trust Anchor Repository Signatures

TOC

The signees may sign the TAR using a detached signature created using either OpenPGP (Callas, J., Donnerhacke, L., Finney, H., Shaw, D., and R. Thayer, “OpenPGP Message Format,” November 2007.) [RFC4880] or S/MIME (Ramsdell, B., “Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification,” July 2004.) [RFC3851].

---

5. IANA Considerations

TOC

This document does not require any IANA actions.

---

6. Security Considerations

TOC

DNSSEC adds data origin authentication and data integrity to the DNS. Because of this, DNSSEC is almost certainly necessary for any application mechanism that stores authorization data in the DNS.
If the signature(s) on the TAR does not validate, the content of the TAR is not to be used for configuration of the DNSSEC verifying

resolver. This might lead to the resolver ignoring all DNSSEC signed data that can not be verified using a trust chain to some other trust anchor, and because of this it might lead to it not returning any responses to queries that reaches it. A signature on the TAR that is not renewed might because of this lead to DNS resolution not work (from the client perspective). Local policy in the resolver is to be carefully tuned to take care of these situations.
The mechanisms described in this document does not introduce any new security implications than what traditionally is the case for detached signatures for PGP and/or S/MIME.

7. Acknowledgements

TOC

The authors gratefully acknowledges, in no particular order, the contributions of the following persons:

Patrik Wallstrom

8. References

TOC

8.1. Normative References

TOC

[RFC1034]	Mockapetris, P., “Domain names - concepts and facilities,” STD 13, RFC 1034, November 1987 (TXT).
[RFC2119]	Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels,” BCP 14, RFC 2119, March 1997 (TXT, HTML, XML).
[RFC3851]	Ramsdell, B., “Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification,” RFC 3851, July 2004 (TXT).
[RFC4033]	Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, “DNS Security Introduction and Requirements,” RFC 4033, March 2005 (TXT).
[RFC4880]	Callas, J., Donnerhacke, L., Finney, H., Shaw, D., and R. Thayer, “OpenPGP Message Format,” RFC 4880, November 2007 (TXT).

8.2. Informative References

TOC

[RFC4034]	Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, “Resource Records for the DNS Security Extensions,” RFC 4034, March 2005 (TXT).
[RFC4035]	Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, “Protocol Modifications for the DNS Security Extensions,” RFC 4035, March 2005 (TXT).

Authors' Addresses

TOC

	Patrik Faltstrom
	Cisco
	Ledasa
	Lovestad SE-273 71
	Sweden
Email:	paf@cisco.com
	Jakob Schlyter
	Kirei AB
	P.O. Box 53204
	Goteborg SE-400 16
	Sweden
Email:	jakob@kirei.se