DNSOP
Internet-Draft
Expires: July 19, 2005

G. Guette
IRISA / INRIA
O. Courtay
Thomson R&D

January 18, 2005

Requirements for Automated Key Rollover in DNSSEC
draft-ietf-dnsop-key-rollover-requirements-02.txt

Status of this Memo

Copyright Notice

Abstract

This document describes problems that appear during an automated rollover and gives the requirements for the design of communication between parent zone and child zone during an automated rollover process. This document is essentially about in-band key rollover.

Table of Contents

1. Introduction

The DNS security extensions (DNSSEC) [4][6][5][7] uses public-key cryptography and digital signatures. It stores the public part of keys in DNSKEY Resource Records (RRs). Because old keys and frequently used keys are vulnerable, they must be renewed periodically. In DNSSEC, this is the case for Zone Signing Keys (ZSKs) and Key Signing Keys (KSKs) [1][2]. Automation of key exchanges between parents and children is necessary for large zones because there are too many changes to handle.

Let us consider for example a zone with 100000 secure delegations. If the child zones change their keys once a year on average, that implies 300 changes per day for the parent zone. This amount of changes is hard to manage manually.

Automated rollover is optional and resulting from an agreement between the administrator of the parent zone and the administrator of the child zone. Of course, key rollover can also be done manually by administrators.

This document describes the requirements for a protocol to perform the automated key rollover process and focusses on interaction between parent and child zone.

2. The Key Rollover Process

Key rollover consists of renewing the DNSSEC keys used to sign resource records in a given DNS zone file. There are two types of rollover, ZSK rollovers and KSK rollovers.

During a ZSK rollover, all changes are local to the zone that renews its key: there is no need to contact other zones administrators to propagate the performed changes because a ZSK has no associated DS record in the parent zone.

During a KSK rollover, new DS RR(s) must be created and stored in the parent zone. In consequence, data must be exchanged between child and parent zones.

The key rollover is built from two parts of different nature:

o An algorithm that generates new keys and signs the zone file. It can be local to the zone,

o the interaction between parent and child zones.

One example of manual key rollover [3] is:

o The child zone creates a new KSK,

- the child zone waits for the creation of the DS RR in its parent zone,
- the child zone deletes the old key,
- the parent zone deletes the old DS RR.

This document concentrates on defining interactions between entities present in key rollover process.

3. Basic Requirements

This section provides the requirements for automated key rollover in case of normal use. Exceptional case like emergency rollover is specifically described later in this document.

The main condition during a key rollover is that the chain of trust must be preserved to every validating DNS client. No matter if this client retrieves some of the RRs from recursive caching name server or from the authoritative servers for the zone involved in the rollover.

Automated key rollover solution may be interrupted by a manual intervention. This manual intervention should not compromise the security state of the chain of trust. If the chain is safe before the manual intervention, the chain of trust must remain safe during and after the manual intervention

Two entities act during a KSK rollover: the child zone and its parent zone. These zones are generally managed by different administrators. These administrators should agree on some parameters like availability of automated rollover, the maximum delay between notification of changes in the child zone and the resigning of the parent zone. The child zone needs to know this delay to schedule its changes and/or to verify that the changes had been taken into account in the parent zone. Hence, the child zone can also avoid some critical cases where all child key are changed prior to the DS RR creation.

By keeping some resource records during a given time, the recursive cache servers can act on the automated rollover. The existence of recursive cache servers must be taken into account by automated rollover solution.

Indeed, during an automated key rollover a name server could have to retrieve some DNSSEC data. An automated key rollover solution must ensure that these data are not old DNSSEC material retrieved from a recursive name server.

4. Messages authentication and information exchanged

This section addresses in-band rollover, security of out-of-band mechanisms is out of scope of this document.

The security provided by DNSSEC must not be compromised by the key rollover, thus every exchanged message must be authenticated to avoid fake rollover messages from malicious parties.

Once the changes related to a KSK are made in a child zone, there are two ways for the parent zone to take this changes into account:

- o the child zone notify directly or not directly its parent zone in order to create the new DS RR and store this DS RR in parent zone file,
- o or the parent zone poll the child zone.

In both cases, the parent zone must receive all the child keys that need the creation of associated DS RRs in the parent zone.

Because errors could occur during the transmission of keys between child and parent, the key exchange protocol must be fault tolerant. Should an error occured during the automated key rollover, an automated key rollover solution must be able to keep the zone files in a consistent state.

5. Emergency Rollover

Emergency key rollover is a special case of rollover decided by the zone administrator generally for security reasons. In consequence, emergency key rollover can break some of the requirement described above.

A zone key might be compromised and an attacker can use the compromised key to create and sign fake records. To avoid this, the zone administrator may change the compromised key or all its keys as soon as possible, without waiting for the creation of new DS RRs in its parent zone.

Fast changes may break the chain of trust. The part of DNS tree having this zone as apex can become unverifiable, but the break of the chain of trust is necessary if the administrator wants to prevent the compromised key from being used (to spoof DNS data).

Parent and child zones sharing an automated rollover mechanism, should have an out-of-band way to re-establish a consistent state at the delegation point (DS and DNSKEY RRs). This allows to avoid that a malicious party uses the compromised key to roll the zone keys.

6. Security consideration

The automated key rollover process in DNSSEC allows automated renewal of any kind of DNS key (ZSK or KSK). It is essential that parent side and child side can do mutual authentication. Moreover, integrity of the material exchanged between the parent and child zone must be provided to ensure the right DS are created.

As in any application using public key cryptography, in DNSSEC a key may be compromised. What to do in such a case can be describe in the zone local policy and can violate some requirements described in this draft. The emergency rollover can break the chain of trust in order to protect the zone against the use of the compromised key.

7. Acknowledgments

The authors want to thank members of IDsA project for their contribution to this document.

8 Normative References

[1] Gudmundsson, O., "Delegation Signer (DS) Resource Record (RR)", RFC 3658, December 2003.

[2] Kolkman, O., Schlyter, J. and E. Lewis, "Domain Name System KEY (DNSKEY) Resource Record (RR) Secure Entry Point (SEP) Flag", RFC 3757, May 2004.

[3] Kolkman, O., "DNSSEC Operational Practices", draft-ietf-dnsop-dnssec-operational-practice-01 (work in progress), May 2004.

[4] Eastlake, D., "Domain Name System Security Extensions", RFC 2535, March 1999.

[5] Arends, R., Austein, R., Larson, M., Massey, D. and S. Rose, "Resource Records for the DNS Security Extensions", draft-ietf-dnsext-dnssec-records-11 (work in progress), October 2004.

[6] Arends, R., Austein, R., Larson, M., Massey, D. and S. Rose, "DNS Security Introduction and Requirements", draft-ietf-dnsext-dnssec-intro-13 (work in progress), October 2004.

[7] Arends, R., Austein, R., Larson, M., Massey, D. and S. Rose, "Protocol Modifications for the DNS Security Extensions", draft-ietf-dnsext-dnssec-protocol-09 (work in progress), October

2004.

Authors' Addresses

Gilles Guette
IRISA / INRIA
Campus de Beaulieu
35042 Rennes CEDEX
FR

EMail: gilles.guette@irisa.fr
URI: http://www.irisa.fr

Olivier Courtay
Thomson R&D
1, avenue Belle Fontaine
35510 Cesson S?vign? CEDEX
FR

EMail: olivier.courtay@thomson.net

Appendix A. Documents details and changes

This section is to be removed by the RFC editor if and when the document is published.

Section about NS RR rollover has been removed

Remarks from Samuel Weiler and Rip Loomis added

Clarification about in-band rollover and in emergency section

Section 3, details about recursive cache servers added

Intellectual Property Statement

Full Copyright Statement

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.