

Individual
Internet-Draft
Expires: April 20, 2004

G. Guette
IRISA/INRIA Rennes
O. Courtay
ENST-Bretagne
October 20, 2003

Requirements for Automated Key Rollover in DNSsec
draft-guette-dnsop-key-rollover-requirements-00

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of [Section 10 of RFC2026](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/1id-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on March 30, 2004.

Copyright Notice

Copyright (C) The Internet Society (2003). All Rights Reserved.

Abstract

This internet-draft describes problems that appear during an automated rollover and gives the requirements for the design of automated solutions rollover process. It essentially concerned key rollover, but rollover of other Resource Records present at delegation point (NS RR) is also discussed.

1. Introduction

The DNS security extensions (DNSsec) [1] uses public-key cryptography and digital signatures. It stores needed keys in KEY Resource Records (RRs). Because old keys and frequently used keys are vulnerable, they must be changed periodically. In DNSsec this is the case for Zone Signing Keys (ZSKs) and Key Signing Keys (KSKs) [2] [4]. Automation of key rollover process is necessary for large zones because inside a large zone, there are too many changes to handle for a single administrator.

Let us consider for example a zone with one million child zones among which only 10% of secured child zones (that is, 100,000 child zones). If the child zones change their keys once a year on average, that implies 300 changes per day for the parent zone. All these changes are hard to manage manually.

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

This document describes the requirements for the design of automated solutions for key rollover process.

2. The Key Rollover Process

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

In ZSK rollover, all changes are local to the zone that changes its key, there is no need to contact other zones (e.g. parent zone) to propagate the performed changes.

In KSK rollover, the right DS RR MUST be created and stored in the parent zone, so the child zone MUST contact its parent zone and notify it about the KSK changes.

Manual key rollover exists and works [3] but in this draft we describe a way to automate the key rollover process.

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

- An algorithm that changes keys
- Communication between parent and child zone

One example of manual key rollover is:

Child zone creates a new KSK, waiting for a certain time, DS is created in parent zone, child zone deletes old key.

In manual rollover, communications are managed by administrators and

security of these communications is out of scope of DNSsec.

Automatic key rollover should define a secure communication between parent and child zone. In this draft we concentrate our efforts on defining interactions between entities present in key rollover process that are not explicitly defined in manual key rollover method.

3. Basic Requirements

The main constraint to respect during a key rollover is that the chain of trust **MUST** be preserved. Every RR **MUST** be verifiable at any time, every message exchanged during rollover **MUST** be authenticated and data integrity **MUST** be guaranteed even if some RRs are retrieved from recursive name server (cache).

Two entities are present during a KSK rollover: child zone and parent zone. These zones are generally managed by different administrators. These administrators **MUST** agree on some parameters like doing automatic rollover, maximum delay between notification of changes into child zone and resigning of the parent zone, etc.

4. Messages authentication

Every exchanged message **MUST** be authenticated and the authentication tool **MUST** be a DNSsec tool such as TSIG [5], SIG(0) [6] or DNSsec request with verifiable SIG records.

Some errors could occur during transmission between child zone and parent zone. Key rollover solution **MUST** be fault tolerant, i.e. at any time the rollover **MUST** be in a consistent state and all RRs must be verifiable, even if an error occurs.

5. Transmission method and information exchanged

Once the changes related to a KSK are made in a child zone, this zone **MUST** notify its parent zone in order to create the new DS RR and store this DS RR in parent zone file.

Whatever the transmission methods used, the parent zone **MUST** receive the child KSKs for which the child wants that associated DS RRs exist in the parent zone.

6. Local separation entities

Secret keys are generally stored in a secure off-line area [7]. The name server has no on-line access to these keys. The key rollover solution **SHOULD** not assume that the server has on-line access to

these keys. We have distinguished three entities concerned by the local key rollover process inside a zone: the name server, the zone file manager and the secret key manager.

Any automatic rollover solution MUST take into account the possible separation of these three entities and must support partial administrator intervention as manipulation of private key.

For example, we can imagine that all entities are handled by automated process but signing action with the private keys is done by human administrator (he retrieves zone file from a repository and put back the signed zone file on well-known location).

7. Emergency Rollover

Inside a zone, a key might be compromised and this key MUST be changed as fast as possible. The fast changes could 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 we want that no one can use the compromised key to spoof DNS data.

Parent zone behavior after an emergency rollover in one of its child zone is an open discussion.

Must we define:

- an EMERGENCY flag, when a child zone does an emergency KSK change, it uses the EMERGENCY flag to notify its parents that the chain of trust is broken and will stay broken until right DS creation and a parent zone resigning.
- a maximum time delay after next parent zone resigning, we ensure that after this delay the parent zone is resigned and the right DS is created.
- or no pre-defined behavior

8. Other Resource Record concerned by automatic rollover

NS records are also present at delegation point, so when the child zone changes some NS records, the corresponding records at delegation point in parent zone MUST be updated. NS record are concerned by rollover and this rollover could be automated too. In this case, when the child zone notifies its parent zone that some NS records have been changed, the parent zone MUST verify that NS records are present in child zone file before doing any changes in its own zone file. Otherwise the DNS child name server could not be

reached.

9. Security consideration

This document describes requirements to design an automated key rollover in DNSsec based on DNSsec security. In the same way the, as plain DNSsec, the automatic key rollover contains no mechanism protecting against denial of service (DoS) resistant. The security level obtain after an automatic key rollover, is the security level provided by DNSsec.

10. Acknowledgments

The authors want to acknowledge Mohsen Souissi, Bernard Cousin, Bertrand Leonard and members of IDSA project for their contribution to this document.

Normative references

- [1] Eastlake, D., "Domain Name System Security Extensions", [RFC 2535](#), March 1999.
- [2] Gudmundsson, O., "Delegation Signer Resource Record", [draft-ietf-dnsext-delegation-signer-15](#) (work in progress), June 2003.
- [3] Kolkman, O. and Gieben, R., "DNSSEC key operations", [draft-ietf-dnsext-operational-practices](#) (work in progress), June 2003.
- [4] Kolkman, O. and Schlyter, J., "KEY RR Secure Entry Point Flag" [draft-ietf-dnsext-keyrr-key-signing-flag-10](#) (work in progress), September 2003.
- [5] Vixie, P., Gudmundsson, O., Eastlake, D., and Wellington, B., "Secret Key Transaction Authentication for DNS (TSIG)", [RFC 2845](#), May 2000.
- [6] Eastlake, D., "DNS Request and Transaction Signatures (SIG(0)s)", [RFC 2931](#), September 2000.
- [7] Eastlake, D., "DNS Security Operational Considerations", [RFC 2541](#), March 1999.

Author's Addresses

Gilles Guette
IRISA/INRIA Rennes
Campus Universitaire de Beaulieu
35042 Rennes France
Phone : (33) 02 99 84 71 32
Fax : (33) 02 99 84 25 29
E-mail : gguette@irisa.fr

Olivier Courtay
ENST-Bretagne
2, rue de la châtaigneraie
35512 Cesson Cévigé CEDEX France
Phone : (33) 02 99 84 71 31
Fax : (33) 02 99 84 25 29
olivier.courtay@enst-bretagne.fr

Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on the IETF's procedures with respect to rights in standards-track and standards-related documentation can be found in [BCP-11](#). Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementors or users of this specification can be obtained from the IETF Secretariat.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to practice this standard. Please address the information to the IETF Executive Director.

Full Copyright Statement

Copyright (C) The Internet Society (2003). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assignees.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION

HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF
MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.