

Domain Name System (DNS) Security Key Rollover

Donald E. Eastlake 3rd, Mark Andrews

Status of This Document

This draft, file name [draft-ietf-dnssec-rollover-00.txt](#), is intended to become a Proposed Standard RFC. Distribution of this document is unlimited. Comments should be sent to the DNS security mailing list <dns-security@tis.com> or to the authors.

This document is an Internet-Draft. 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. Internet-Drafts may be updated, replaced, or obsoleted by other documents at any time. It is not appropriate to use Internet-Drafts as reference material or to cite them other than as a ``working draft'' or ``work in progress.''

To view the entire list of current Internet-Drafts, please check the "1id-abstracts.txt" listing contained in the Internet-Drafts Shadow Directories on ftp.is.co.za (Africa), ftp.nordu.net (Northern Europe), ftp.nis.garr.it (Southern Europe), munnari.oz.au (Pacific Rim), ftp.ietf.org (US East Coast), or ftp.isi.edu (US West Coast).

Abstract

Practical deployment of Domain Name System (DNS) security with good cryptologic practice will involve large volumes of key rollover traffic. A standard format and protocol for such messages is specified.

INTERNET-DRAFT

October 1998

DNSSEC Key Rollover

Table of Contents

Status of This Document.....	1
Abstract.....	1
Table of Contents.....	2
1 . Introduction.....	3
2 . Key Rollover Scenarios.....	3
3 . Rollover Operation.....	4
3.1 Rollover to Parent.....	4
3.2 Rollover to Children.....	5
4 . Rollover NOTIFY.....	6
5 . Security Considerations.....	7
References.....	8
Authors Address.....	8
Expiration and File Name.....	9

INTERNET-DRAFT

October 1998

DNSSEC Key Rollover

1. Introduction

The Domain Name System (DNS) [RFC 1034, [RFC 1035](#)] is the global hierarchical replicated distributed database system for Internet addressing, mail proxy, and other information. The DNS has been extended to include digital signatures and cryptographic keys as described in [[draft-ietf-dnssec-secext2-*](#)].

The principle security service provided for DNS data is data origin authentication. The owner of each zone signs the data in that zone with a private key known only to the zone owner. Anyone that knows the corresponding public key can then authenticate that zone data is from the zone owner. To avoid having to preconfigure resolvers with all zone's public keys, keys are stored in the DNS with each zone's key signed by its parent (if the parent is secure).

To obtain high levels of security, keys must be periodically changed, or "rolled over". The longer a private key is used, the more likely it is to be compromised due to cryptanalysis, accident, or treachery [[draft-ietf-dnssec-secops-*](#).txt].

In a widely deployed DNS security system, the volume of update traffic will be large. Just consider the .com zone. If only 10% of its children are secure and change their keys only once a year, you are talking about hundreds of thousands of new child public keys that must be securely sent to the .com manager to sign and return with their new parent signature. And when .com rolls over its private key, it will need to send hundreds of thousands of new signatures on the existing child public keys to the child zones.

The key words "MUST", "REQUIRED", "SHOULD", "RECOMMENDED", and "MAY"

in this document are to be interpreted as described in [RFC 2119](#).

2. Key Rollover Scenarios

Although DNSSEC provides for the storage of other keys in the DNS for a variety of purposes, DNSSEC zone keys are included solely for the purpose of being retrieved to authenticate DNSSEC signatures. Thus, when a zone key is being rolled over, the old public key should be left in the zone, along with the addition of the new public key, for as long as it will reasonably be needed to authenticate old signatures that have been cached or are held by applications. If DNSSEC were universally deployed and all DNS server's clocks were synchronized and zone transfers were instantaneous etc., it might be possible to avoid ever having duplicate old/new KEY RRsets but they will be necessary in practical cases. Security aware DNS servers decrease the TTL of secure RRs served as the expiration of their authenticating SIG(s) approaches but some dithered fudge must

D. Eastlake 3rd, M. Andrews

[Page 3]

INTERNET-DRAFT

October 1998

DNSSEC Key Rollover

generally be left due to clock skew and to avoid massive load on large zones due to the signatures on their entire contents expiring simultaneously.

Assume a zone with a secure parent and secure children wishes to role over its KEY RRset. This RRset would probably be one KEY RR per crypto algorithm used to secure the zone, but for this scenario, we will simply assume it is one KEY RR. The old KEY RR and two SIG RRs will exist at the apex of the zone and these RRs may also exist at the leaf node for this zone in its parent. The contents of the zone and the zone KEY RRs of its secure children will have SIGs under the old key.

The zone owner needs to communicate with its parent to obtain a new parental signature covering both the old and new KEY RRs and covering just the new KEY RR. It would probably want to obtain these in advance so that it can install them at the right time along with its new SIG RRs covering the content of the zone. Finally, it needs to give new SIG RRs to its children that cover their KEY RRs if it has these, or signal its children to ask for such SIG RRs.

[3.](#) Rollover Operation

Rollover operations use a DNS request syntactically identical to the UPDATE request [[RFC 2136](#)] except that the operation is ROLLOVER which is equal to TBD. Considerations for such request to the parent and children of a zone are given in the subsections.

[This draft does not currently consider cross-certification key rollover.]

[3.1](#) Rollover to Parent

A zone rolling over its KEY RRset sends a ROLLOVER command to the parent. The Zone should be specified as the parent zone and no Prerequisites are included. The Update section has the KEY RRset on which the parent signature is requested along with the requesting zone's SIG(s) under its old KEY(s) as RRs to be added to the parent zone. The inception and expiration times in this SIG are the requested inception and expiration times for the parent SIG.

If the ROLLOVER command is erroneous or violates parental policy, an Error response is returned.

If the ROLLOVER command is OK and the parent can sign online, its response may include the new parent SIG(s) in the Update section.

This response MUST be sent to the originator of the request.

If the parent can not sign online, it should return a response with an empty Update section and queue the SIG(s) calculation request. This response MUST be sent to the originator of the request.

Regardless of whether the server has sent the new signatures above, it MUST, once it has calculated the new SIG(s), send a ROLLOVER to the child zone using the DNS port (53) and the server selection algorithm defined in [RFC 2136, Section 4](#). This ROLLOVER request contains the KEY RRset that triggered it and the new SIG(s). This downward ROLLOVER request is distinguished from those in [Section 3.2](#) below in that the Zone section is the parental zone.

The reason for sending the ROLLOVER request regardless of whether the

new SIG RR(s) were sent in the original response is to provide an indication to the operators of the zone in the event someone is trying to hijack the zone.

Although the parent zone need not hold or serve the child's key, the ROLLOVER command MUST NOT actually update the parent zone. A later UPDATE command can be used to actually put the new KEY into the parent zone if desired and supported by parent policy.

This document does not cover the question of parental policy on key rollovers. Parents may have restrictions on how far into the future they will sign KEY RRsets, what algorithms or key lengths they will support, might require payment for the service, etc. The signing of a future KEY by a parent is, to some extent a granting to the controller of the child private key of future authoritative existence even if the child zone ownership should change. The only effective way of invalidating such future signed child public keys would be for the parent to roll over its key(s), which might be an expensive operation.

[3.2](#) Rollover to Children

When a zone is going to rollover its key(s), it needs to re-sign the zone keys of any secure children under its new key(s).

If the parent holds the KEY RRset for the child (whether or not it actually serves it from the parent zone), it can simply do a ROLLOVER request to to child specifying the child as the Zone in the request and the new SIG(KEY)s to be added in the Update section. The inception and expiration times in the SIG(s) indicate the time during which the parent will be utilizing the new parent key. It is up to the child when and how it adds the new parental SIG(s). The ROLLOVER request may optionally indicate the deletion of old parental SIG(s)

but SHOULD only do so if the corresponding key is being withdrawn by the parent in advance of the expiration time in the old SIG(s). It is up to the child when and how it deletes the old parental SIG(s). Even if the expiration of the old SIG(s) equals the inception time of the new SIG(s), the child should serve both signatures for a fudge time to account for clock skew.

A ROLLOVER request is used instead of an UPDATE because servers may wish to support ROLLOVER via special techniques, such as notification to the operator, even when they have not implemented UPDATE. With adequate advance notice, even manual cut and paste editing of the master file and restarting of a DNS server process could work.

If the parent does not retain knowledge of the child KEY RRset, then the parent simply notifies the child via a ROLLOVER NOTIFY (see [Section 4](#) below) that the parent KEY(s) have changed. The child then proceeds to do an upward ROLLOVER request to obtain the new parental SIG(s). (This requires that a different method, such as TSIG, be used to secure such ROLLOVER requests since we are assuming the parent does not have authoritative knowledge of the child public key. See [Section 5](#) below.)

The NOTIFY technique MAY also be used by parents who retain knowledge of their children's KEY RRsets.

[4.](#) Rollover NOTIFY

A ROLLOVER NOTIFY informs a child zone that the parent zone wants it to resubmit its keys for resigning.

A ROLLOVER NOTIFY MUST be signed and if not signed a BADAUTH response generated.

A ROLLOVER NOTIFY is a NOTIFY request [[RFC 1996](#)] that has a QTYPE of SIG and the owner name of the child zone. The answer section is empty.

The ROLLOVER NOTIFY can be sent to any of the nameservers for the child using the nameserver selection algorithm defined in [RFC 2136, Section 4](#).

Nameservers for the child zone receiving a ROLLOVER NOTIFY query will forward the ROLLOVER NOTIFY in the same manner as an UPDATE is forwarded.

Unless the master server is configured to initiate an automatic ROLLOVER it MUST seek to inform its operators that a ROLLOVER NOTIFY request has been received. This could be done by a number of methods

including generating a log message, generating an email request to the child zone's SOA RNAME or any other method defined in the server's configuration for the zone. The default should be to send mail to the zone's SOA RNAME. Care should be taken to rate limit these message so prevent them being used to facilitate a denial of service attack.

Once the message has been sent (or suppressed) to the child zone's administrator the master server for the child zone is free to respond to the ROLLOVER NOTIFY request.

5. Security Considerations

The security of ROLLOVER or UPDATE requests is essential, otherwise false children could steal parental authorization or a false parent could cause a child to install an invalid signature on its zone key, etc.

A ROLLOVER request can be authentication by request SIG(s) under the old zone KEY(s) of the requestor [[draft-ietf-dnssec-secext2-*.txt](#)]. The response SHOULD have transaction SIG(s) under the old zone KEY(s) of the responder. (This public key security could be used to rollover a zone to the unsecured state but at that point it would generally not be possible to roll back without manual intervention.)

Alternatively, if there is a prior arrangement between a child and a parent, ROLLOVER requests and responses can be secured and authenticated using TSIG [[draft-ietf-dnssec-tsig-*.txt](#)]. (TSIG security could be used to rollover a zone to unsecured and to rollover an unsecured zone to the secured state.)

A server that implements online signing SHOULD have the ability to black list a zone and force manual processing or demand that a particular signature be used to generate the ROLLOVER request. This it to allow ROLLOVER to be used even after a private key has been compromised.

INTERNET-DRAFT

October 1998

DNSSEC Key Rollover

References

[RFC 1034] - P. Mockapetris, "Domain names - concepts and facilities", 11/01/1987.

[RFC 1035] - P. Mockapetris, "Domain names - implementation and specification", 11/01/1987.

[RFC 1996] - P. Vixie, "A Mechanism for Prompt Notification of Zone Changes (DNS NOTIFY)", August 1996.

[RFC 2136] - Dynamic Updates in the Domain Name System (DNS UPDATE). P. Vixie, Ed., S. Thomson, Y. Rekhter, J. Bound. April 1997.

[[draft-ietf-dnsind-tsig](#)-*[.txt](#)]

[[draft-ietf-dnssec-update2](#)-*[.txt](#)]

[[draft-ietf-dnssec-secext2](#)-*[.txt](#)]

[[draft-ietf-dnssec-secops](#)-*[.txt](#)]

Authors Address

Donald E. Eastlake 3rd
IBM
318 Acton Street
Carlisle, MA 01741 USA

Telephone: +1 978-287-4877
 +1 914-784-7913
FAX: +1 978-371-7148
EMail: dee3@us.ibm.com

Mark Andrews
Internet Software Consortium
1 Seymour Street
Dundas Valley, NSW 2117
AUSTRALIA

Telephone: +61-2-9871-4742
Email: marka@isc.org

D. Eastlake 3rd, M. Andrews

[Page 8]

INTERNET-DRAFT

October 1998

DNSSEC Key Rollover

Expiration and File Name

This draft expires in April 1999.

Its file name is [draft-ietf-dnssec-rollover-00.txt](#).

[D.](#) Eastlake 3rd, M. Andrews

[Page 9]