

INTERNET-DRAFT

Donald E. Eastlake 3rd
CyberCash, Inc.
March 1997

Expires: September 1997

The DNS Inverse Key Domain

--- --- ----- --- -----

Status of This Document

This draft, file name [draft-ietf-dnssec-in-key-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 the author.

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 learn the current status of any Internet-Draft, please check the lid-abstracts.txt listing contained in the Internet-Drafts Shadow Directories on ds.internic.net (East USA), ftp.isi.edu (West USA), nic.nordu.net (North Europe), ftp.nis.garr.it (South Europe), munnari.oz.au (Pacific Rim), or ftp.is.co.za (Africa).

INTERNET-DRAFT

The in-key.int Domain

March 1997

Abstract

Proposed Standard protocol extensions now exist to the Domain Name System (DNS) to authenticate the data in DNS and provide key distribution services ([RFC 2065](#)). This draft proposes a special in-key.int domain which would allow entities to be found from their keys if they have voluntarily registered them in that domain.

Table of Contents

| | |
|--|-------------------|
| Status of This Document..... | 1 |
| Abstract..... | 2 |
| Table of Contents..... | 2 |
| 1 . The Inverse Key Domain Domain..... | 3 |
| 2 . Inverse Key Domain Name Structure..... | 4 |
| 3 . Inverse Key Domain Administration..... | 5 |
| 4 . Inverse Key Domain Authentication..... | 6 |
| 5 . Security Considerations..... | 7 |
| References..... | 7 |
| Author's Address..... | 7 |
| Expiration and File Name..... | 7 |

INTERNET-DRAFT

The in-key.int Domain

March 1997

1. The Inverse Key Domain Domain

A special domain is defined, the in-key.int. domain, to permit inverse lookup by key. DNS servers for zones that include any updatable part of this domain have a special update policy and all servers and resolvers have a special authentication policy for this domain.

Normally the only RRs stored in this domain will be a KEY RR and an authenticating SIG with the SIG signer field pointing to the normal owner of the KEY. It is expected that an administrative restriction may be placed on the number of RRs stored under any particular owner name or that charges imposed (see [draft-eastlake-internet-payment-*.txt](#)) for additions to this domain by the as yet to be determined operator of the domain or of a zone within the domain.

Registration in the in-key.int. domain is voluntary. All servers that include key storage leaves of the in-key.int. domain MUST operate in mode A for those zones (see [draft-ietf-dnssec-update-04.txt](#) [approved as a Proposed Standard but not yet issued as an RFC]).

(Note: The structure of the IETF recommended top level domain names is currently being examined. If infrastructure domains such as ipv6.int are moved elsewhere, such as to the current infrastructure ".arpa" domain, then the in-key domain should move also, for example to in-key.arpa.)

[2.](#) Inverse Key Domain Name Structure

The owner name associated with a KEY RR in the in-key.int domain is

`<key-hash>.<key-footprint>.algorithm.in-key.int.`

key-hash is the hex representation of the SHA1 [SHA1] hash of the "public key" portion of the corresponding KEY RR (the portion of the RDATA after the algorithm octet) with label separating dots added every fourth hex digit.

key-footprint is the hex representation of the key footprint field of the KEY RR.

algorithm is the decimal number designating the public key algorithm from the "algorithm" octet portion of the corresponding key. Thus, at this time, algorithm will be either 1 or 254. Entries for algorithm 253 are prohibited.

For example, the RRs in this domain for a purported key with actual owner name example.tld could be as follows:

```
$ORIGIN xxxx.xxxx.xxxx.xxxx.xxxx.xxxx.xxxx.xxxx.xxxx.xxxx.1.in-key.int
```

```

IN KEY <flags> 0 1 (
45IkskceFGgiWCn/GxHhai6VAuHAoNUz4YoUMxFcby9k/yvedMfQgKzhH5er0Mu/vILz
80jEeC8aTr0+KKmCaY1tVfSCSqQYn6//11U6Nld= ;key
)
IN SIG KEY 1 3 ( ;type-cov=PTR, alg=1, labels=3
19991202030405 ;signature expiration
19951211100908 ;time signed
2143658709 ;key footprint
example.tld. ;signer
MxFcby9k/yvedMfQgKzhH5er0Mu/vILz45IkskceFGgiWCn/GxHhai6VAuHAoNUz4YoU
1tVfSCSqQYn6//11U6Nld80jEeC8aTr0+KKmCaY= ;signature
)

```

[3.](#) Inverse Key Domain Administration

The structure of the in-key domain names scatters keys within an algorithm by hash codes. Thus, while the domain has structure that can be used to split it into zones and avoid any zone within it from getting too large, this structure does not correspond in to communities that might wish to use or maintain the zone.

If only a small number of key holders wish to register there key here, this will probably not be a problem as a volunteer operator can likely be found and the entire inverse key domain can be run as one zone. If many registrants within this domain appear, some form of charging may be necessary and it may be necessary to split the domain into zones by algorithm and then key footprint. If huge numbers register, it may even be necessary to split it further based on the

highest SHA1 key hash derived label.

DNS dynamic update ([draft-ietf-dnsind-dynUPD-*.txt](#)) has been adopted as a Proposed Standard. Assuming the adoption of DNS charging ([draft-eastlake-internet-payment-*.txt](#)), the best way to populate the domain may be via dynamic updates for which a fee is charged by the maintainer(s) of the domain.

[4.](#) Inverse Key Domain Authentication

Retrievals and updates to this domain use special authentication policies as indicated below.

Retrievals from leaves of this domain are authenticated by validating the SIG against the KEY with the same owner name and checking that

this owner name correctly reflects the hash and key footprint of the key. Thus, for this type of validation only, the signer name is ignored and the SIG is NOT traced back to a known trusted key. In addition, entries in this domain are "eternal" in that the SIG time signed and signature expiration are ignored. Note that entries in this special domain, even when authenticated, give only a hint that the KEY stored there is or was valid for the signer name. A separate retrieval from the signer name must be done for confirmation that they key is currently valid.

Servers authenticate updates for this domain based on the requester's knowledge of the private key corresponding to a public key whose hash is encoded into the RR owner name as indicated by the update request SIG. No dynamic update key previously stored in the zone need be used.

5. Security Considerations

Storage of many keys in the in-key.int domain may lead to the discovery of duplicate keys due to bad random number generation or other causes. Someone seeking to enter a key and finding the same key their with a different signer could possibly exploit this to impersonate the other holder of the same key.

References

[RFC 2065] - Domain Name System Security Extensions, D. Eastlake, C. Kaufman, January 1997.

[draft-ietf-dnssec-update-04.txt](#) [approved as a Proposed Standard but not yet issued as an RFC].

[draft-eastlake-internet-payment-*.txt](#)

Author's Address

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

Telephone: +1 508-287-4877
 +1 508-371-7148 (fax)
 +1 703-620-4200 (main office, Reston, Virginia, USA)
email: dee@cybercash.com

Expiration and File Name

This draft expires September 1997.

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

