










# DNSEXT Working Group

A decorative graphic element consisting of a horizontal blue gradient bar that starts with a solid blue on the left and fades to white on the right. A black crosshair is positioned at the left end of the bar, with a vertical line extending upwards and a horizontal line extending to the left.

# Agenda DNSEXT

- |   |        |
|---|--------|
|  Administrivia   | 5 min  |
| <ul style="list-style-type: none"><li> appointing scribes (<a href="mailto:dnsext@jabber.xmpp.org">dnsext@jabber.xmpp.org</a>)</li><li> blue sheet</li><li> agenda bashing</li><li> ISSUE tracker</li></ul> |        |
|  Working group Document status   | 5 min  |
|  Call for Interop report volunteers   | 5 min  |
|  Wild card clarify<br>draft-ietf-dnsext-wcard-clarify-02.txt   | 10 min |
|  DNSSEC-bis session  | 90 min |

# ISSUE Tracking

*“Oh no... he had a workflow course”*

## 🐼 Purpose:

- 🐼 Keeping track
- 🐼 Helps distinguishing “work” from “discussion”
- 🐼 Helps to keep an overview of open and closed issues

## 🐼 Most important:

- 🐼 Clearly describing the issue and proposing text.

## 🐼 Tools:

- 🐼 Form to describe the issue precisely and uniformly
- 🐼 Issue tracker

# Issue Tracking

---

The form:

To be found in the monthly posting

The tracker:

<https://roundup.machshav.com/dnsex/>

or

The tool of preference of the doc editor

## WG (Highly) Active

---

- 🐛 draft-ietf-dnsext-dnssec-intro-06
- 🐛 draft-ietf-dnsext-dnssec-protocol-03
- 🐛 draft-ietf-dnsext-dnssec-records-05
- 🐛 draft-ietf-dnsext-wildcard-clarify-02

# WG Final stages

---

- 🦉 draft-ietf-dnsext-mdns-24
  - 🦉 Needs WGLC summary
- 🦉 draft-ietf-dnsext-tkey-renewal-mode
- 🦉 draft-ietf-dnsext-case-insensitive
  - 🦉 Both have WGLC completed, summary needs to be posted. After final review on ID nits the docs can go to IESG.

# WG stalled

- 🦋 draft-ietf-dnsext-rfc2536bis-dsa-4
  - 🦋 stalled
- 🦋 draft-ietf-dnsext-rfc2539bis-dhk-4
  - 🦋 stalled
- 🦋 draft-ietf-dnsext-ecc-key-4
  - 🦋 stalled

All waiting for 2535bis.

# Docs @ IESG

- 🦉 draft-ietf-dnsex-axfr-clarify-05
  - 🦉 Waiting for AD writeup
- 🦉 draft-ietf-dnsex-delegation-signer
  - 🦉 In the RFC queue
- 🦉 draft-ietf-dnsex-dnssec-2535typecode-change-
  - 🦉 Needs IANA considerations fixed then to RFC queue
- 🦉 draft-ietf-dnsex-keyrr-key-signing-flag-11
  - 🦉 Needs IANA considerations fixed then to RFC queue



# More Docs @ IESG

- 🐛 draft-ietf-dnsextd-dnssec-opt-in-05
  - 🐛 WG needs to provide boilerplate indicating non-standards track status. (Stalled, 2535bis first)
- 🐛 draft-ietf-dnsextd-dhcid-rr-07
  - 🐛 Waiting for DHC WG
- 🐛 draft-ietf-dnsextd-dns-threats-4
  - 🐛 AD Evaluation
- 🐛 draft-dnsextd-opcode-discover
  - 🐛 Waiting for editorial changes.

# RFC since IETF57

- 🐉 draft-ietf-dnsext-unknown-rrs
  - 🐉 RFC3597
- 🐉 draft-ietf-dnsext-rfc1886bis
  - 🐉 RFC3596
- 🐉 draft-ietf-dnsext-gss-tsig
  - 🐉 RFC3645
- 🐉 draft-ietf-dnsext-ad-is-secure
  - 🐉 RFC3655

# RIP since IETF57

- 🦋 draft-ietf-dnsext-dnssec-roadmap
  - 🦋 RIP
- 🦋 draft-ietf-dnsext-ipv6-name-auto-reg
  - 🦋 RIP
- 🦋 draft-ietf-dnsext-rfc2782bis-2
  - 🦋 MIA

# Call for interop reports

---

# Wildcard document

- 🐼 Number of issues
  - 🐼 Document contains language that potentially updates 1034
    - 🐼 Caching of QNAME=\*.example
    - 🐼 \*. <anydomain> where <anydomain> contains \* labels.
    - 🐼 \* CNAME and the search algorithm
    - 🐼 \* NS 'legality'
  - 🐼 Doc is more than clarification; it updates 1034
  - 🐼 Note: wcard-clarify is not a normative reference in 2535bis

# RFC2535bis

## DNSSEC

- 🦋 DNSSEC-bis editors report (Roy Arends)
- 🦋 Open issues list and open mike
  - 🦋 NSEC type code representation
  - 🦋 Caching and reuse of DNSSEC Rrsets
  - 🦋 Compression guidelines
  - 🦋 Protocol constraints on algorithm use
  - 🦋 RRSIG TTL use, follow corresponding RRset or RFC2181
- 🦋 Document status, next steps and schedule

# DNSSEC Editors Report

- ✉ Fix an omission: dnssec-editors mailinglist did not have a public archive.
  - ✉ Location on mailing list soon.
- ✉ Report by Roy Arends

# DNSSECBis drafts editors report

---

## 🐛 Current set:

- 🐛 draft-ietf-dnsext-dnssec-intro-07
- 🐛 draft-ietf-dnsext-dnssec-records-05
- 🐛 draft-ietf-dnsext-dnssec-protocol-03

## 🐛 Questions?

- 🐛 Email: [dnssec-editors@east.isi.edu](mailto:dnssec-editors@east.isi.edu)



# DNSSECbis Questions

## Recently Resolved:

- **Q6: Should resolvers cache known “BAD” data?**
  - protocol describes a method (4.1 rate limiting) to protect against DoS mentioned in threats (2.5 Denial of Service).
- **Q11: Allow DNSKEY at delegation points?**
  - protocol outlaws DNSKEY at delegation point. (2.1 Including DNSKEY RRs in a Zone)
- **Q16: server operation when query has DO = 0 and CD = 1.**
  - Original text made bits dependent. Since message bits are orthogonal, text has been removed.
- **Q17: Should the KEY RR typecode be retained for TKEY operations as well?**
  - KEY/SIG RR is retained for TKEY, typecode-change-05 addresses this.

# Open Questions

- ~~Q15: Should a security-aware stub resolver be allowed to set the CD bit?~~
- Q18: TTL values for RRSIG
- Q19: Suppression of duplicate RRs in a RRset
- Q20: expanding wildcards in authority section.
- Q21: Caching and Reuse of NSEC

# Hallway nits

- 🐛 Small fixes like typos, nits, wording, clarifications.
- 🐛 Implicit requirements (resolver/signer): need more explaining  
need to be made [more] explicit.

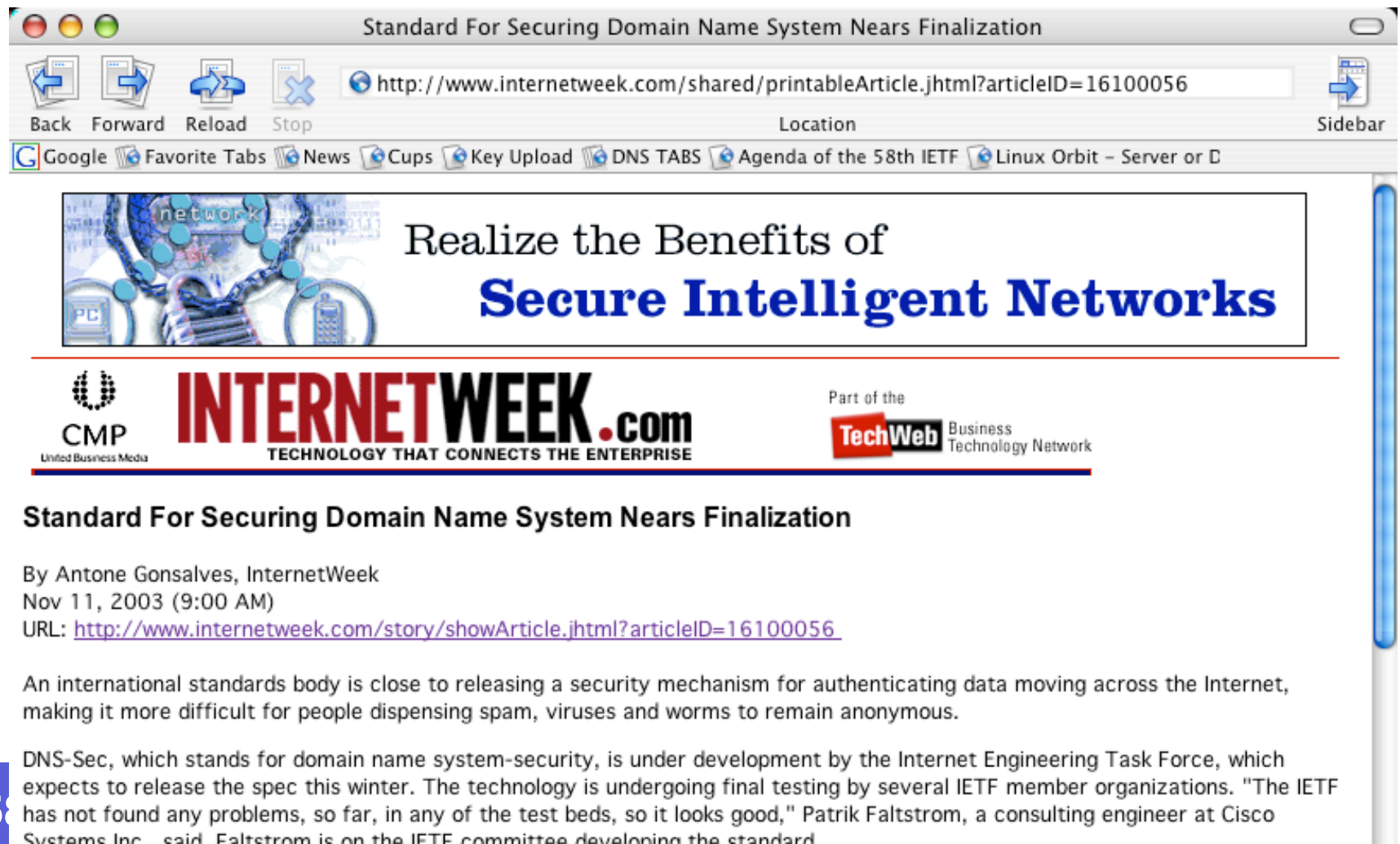
# DNSSEC

---

🐦 Open issues and open mike.

# Open ISSUES

## While nearing finalization...



Standard For Securing Domain Name System Nears Finalization

http://www.internetweek.com/shared/printableArticle.jhtml?articleID=16100056

Back Forward Reload Stop Location Sidebar

Google Favorite Tabs News Cups Key Upload DNS TABS Agenda of the 58th IETF Linux Orbit - Server or D

network

Realize the Benefits of  
**Secure Intelligent Networks**

**CMP**  
United Business Media

**INTERNETWEEK.com**  
TECHNOLOGY THAT CONNECTS THE ENTERPRISE

Part of the  
**TechWeb** Business  
Technology Network

### Standard For Securing Domain Name System Nears Finalization

By Antone Gonsalves, InternetWeek  
Nov 11, 2003 (9:00 AM)  
URL: <http://www.internetweek.com/story/showArticle.jhtml?articleID=16100056>

An international standards body is close to releasing a security mechanism for authenticating data moving across the Internet, making it more difficult for people dispensing spam, viruses and worms to remain anonymous.

DNS-Sec, which stands for domain name system-security, is under development by the Internet Engineering Task Force, which expects to release the spec this winter. The technology is undergoing final testing by several IETF member organizations. "The IETF has not found any problems, so far, in any of the test beds, so it looks good," Patrik Faltstrom, a consulting engineer at Cisco Systems Inc. said. Faltstrom is on the IETF committee developing the standard.

## Q15: Setting of CD bit

- 🐼 Should a security-aware stub resolver be allowed to set the CD bit?
- 🐼 No consensus:
  - 🐼 Protocol allows having the CD bit set, but explains why it isn't good for normal operation.
  - 🐼 Default to go with current text.

# Q18: RRsig TTL can violate RFC2181

- RFC2181 says
  - RRset must have the same TTL on all RR's.
- RRsig's at one name cover multiple RRsets that may have different TTL's
  - RRsig set is really a meta RRset
  - RRsig belongs with RR type it covers
- Consensus seems to be:
  - overwrite RFC2181 for RRsig.

# Q19: Suppression of duplications

---

## Options:

- SHOULD Signer suppress duplicate RR records before signing ?
  - SHOULD Verifier suppress duplicate RR records before verification ?
  - Force Hard Failure
- No consensus yet.



# Q20: expand wildcard in Authority section?

- Example B.7 has answer to a query that is answered by a wildcard match
- Does the wildcard NSEC record in authority section have owner name of
  - \*.w.example.com.
  - <QNAME>
- Suggested action:
  - unexpanded wildcard

# Q21: Caching and Reuse of NSEC

## 🐦 Current doc says:

- 🐦 Reuse only if Q-trinity is identical to old Q-trinity.

## 🐦 Suggested relaxation:

- 🐦 MAY reuse if QNAME and CLASS same but QTYPE is different
- 🐦 MAY reuse if ONAME is equal to QNAME

# Compression Guidelines

## 🐼 RFC2597 section 4:

- 🐼 Future specifications for new RR types that contain domain names within their RDATA MUST NOT allow the use of name compression for those names, and SHOULD explicitly state that the embedded domain names MUST NOT be compressed

## 🐼 Records says:

- 🐼 Server MUST NOT compress RDATA domain names in RRsig and NSEC
- 🐼 Resolver SHOULD decompress RDATA domain names in RRsig and NSEC

## 🐼 Suggested action:

# NSEC issue

- 🐦 Current NSEC/NXT definition
  - 🐦 allows types 1..127 (bit map)
  - 🐦 Representation of types 128..65535 undefined
- 🐦 WG seems to have consensus on fixing this
  - 🐦 Consensus on one and only one format!
  - 🐦 Backwards compatibility is not required
- 🐦 WG needs ID describing change

# NSEC road ahead

- 👤 Chairs have appointed document editor
  - 👤 Jakob Schlyter
- 👤 Shorten list of proposals to propose one format to namedroppers
  - 👤 Ask if there are prohibitive objections against any formats
  - 👤 Hum for each proposal that does not meet prohibitive objections
  - 👤 Loudest hum goes to list in the form of I-D.



# NSEC proposals

- 🐦 #0. Extend bitmap to all 64K types
  - 🐦 Simple compact, max size 8K
  - 🐦 Bad in the case of sparse/high type codes
  - 🐦 Easy to search
- 🐦 #1. List types present in sorted order
  - 🐦 Simple, linear growth, easy to search
  - 🐦 Can represent less than 32K types.

# NSEC proposals (cont)

🐼 #2. [DavidB] First 256 types in one byte each followed by sorted 16 bit type code list

- 🐼 `<length> <lower byte>+ <type codes>*`
  - 🐼 Optimizes the current and near term usage
  - 🐼 Simple to search,
  - 🐼 on average can represent few more types than #1

# NSEC proposals (cont)

- 🐼 #3 [MichaelG] Skip list of blocks
  - 🐼 Each block covers 256 type codes, corresponds to upper byte in type code.
    - 🐼 <block> <block>\*
      - ✓ [length] [block ID] [lower byte of type code]+
  - 🐼 Optimized for size
    - 🐼 if there are 128 or more types in a block, the list contains types **NOT** present.
  - 🐼 Max size is under 33K, can cover all types
    - 🐼 Smaller when lots of types present



## NSEC proposals (cont)

- 🐛 #4 [Mark A] Similar to #3 but uses bitmap in each block.
  - 🐛 Each block covers 256 type codes,
    - 🐛 corresponds to upper byte in type code.
  - 🐛 <block> <block>
    - 🐛 [block ID] [length] [bitmap 0..<top\_bit in block>]
  - 🐛 Covers all types, max size about 8.5K,
    - 🐛 relationship between number of types and size complicated.

# NSEC selection

- 🦋 #0 Expanded bitmap
- 🦋 #1 Sorted typecode list
- 🦋 #2 Sorted typecode with 1st 256 types optimization
- 🦋 #3 Skip list of blocks of typecodes
- 🦋 #4 Skip list of blocks of bitmaps

# Document status

- 🐛 Will reflect closed questions
- 🐛 Security considerations will get updated in new version
- 🐛 New versions RSN, with change list.
- 🐛 NSEC ID will delay us a little bit.
- 🐛 Goal: **WGLC before end of year.**

# Implementation Status

- 🐛 Chairs have got the following information (preliminary report)
  - 🐛 Authorative Servers
    - 🐛 Bind-9 and NSD will support soon
  - 🐛 Recursive Servers/Resolvers
    - 🐛 Bind-9 will support.
    - 🐛 IDSA project working on a new resolver ([www.idsa.prd.fr](http://www.idsa.prd.fr))
- 🐛 Chairs will issue a formal request for status to all implementations

# End of presentation

- 🐦 Did somebody already bring up those vikinghats?

