DNSSEC Deployment Update

Joe Waldron, Verisign

ICANN, Dakar
October 2011

VERISIGN

DNSSEC ROLLOUT STATUS

- Approximately ¼ of the TLDs are now signed
- Root - http://stats.research.icann.org/dns/tld_report/ Status as of October 14, 2011

Total TLDs	310
Signed TLDs	80
(gTLDs)	11
(ccTLDs)	56
(IANA IDN Testbed)	13
TLDs with Trust Anchor in Root	69

- Many leverage the DURZ approach

VERISIGN

83%

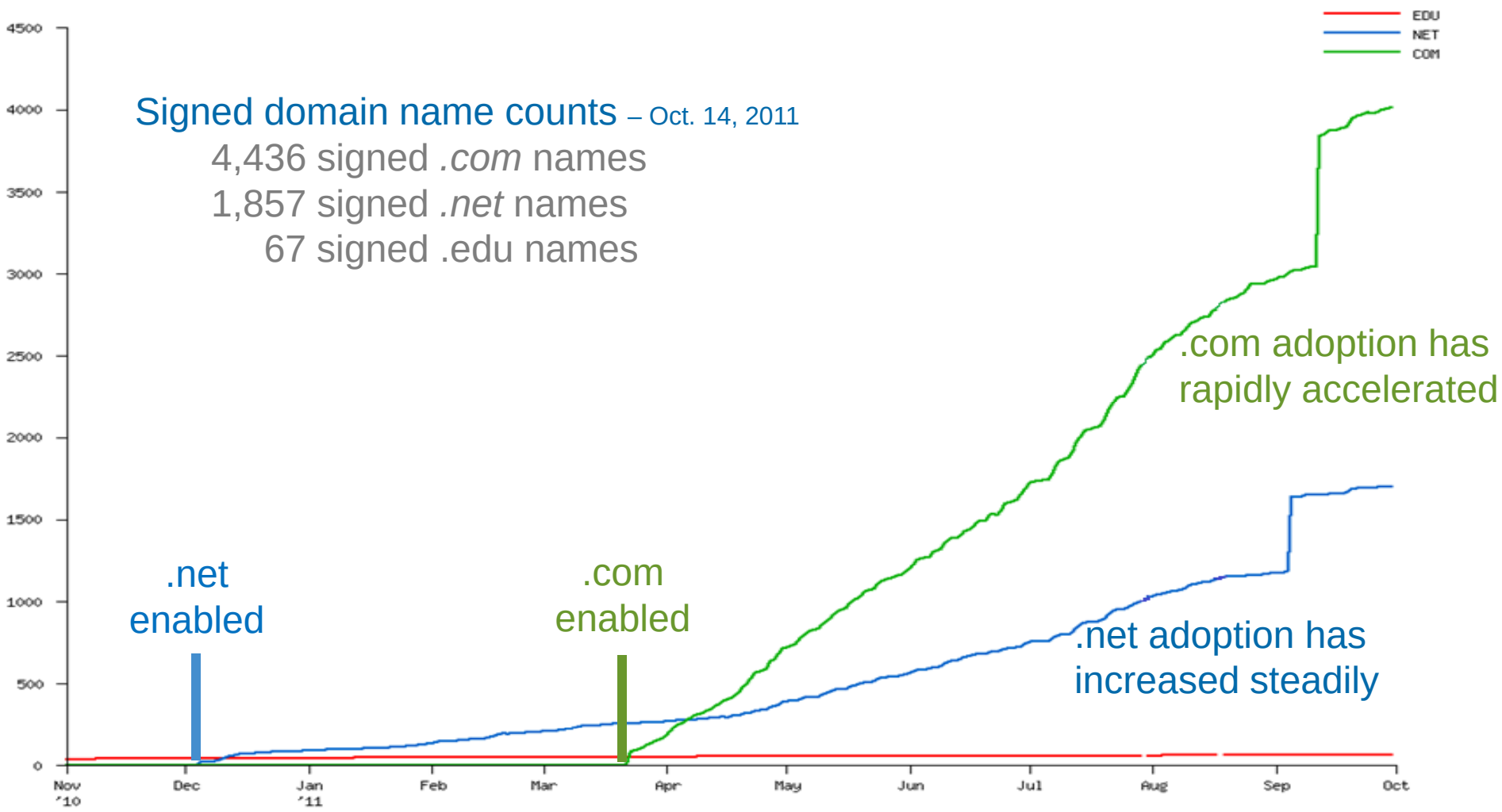
of registered domains are in signed TLDs.

Source: zook_domain_analysis_q22011

Issues Encountered During Deployment

- *.edu* zone
  - None reported
- *.net* zone
  - Bug in some versions of the BIND name server affected DNSSEC validation in certain circumstances
    - Resolution failures after DS for *.net* added to root zone
    - Name servers required restart
    - Verisign reported issue to BIND developers
    - Was publicized before *.com* signing
    - Apparent low impact (one report)
- *.com* zone
  - None reported

DNSSEC Adoption



Source: http://scoreboard.verisignlabs.com/count-trace.png

Verisign Tools for Registrars

A variety of tools for registrars to support their DNSSEC programs:

Registrar Engineering

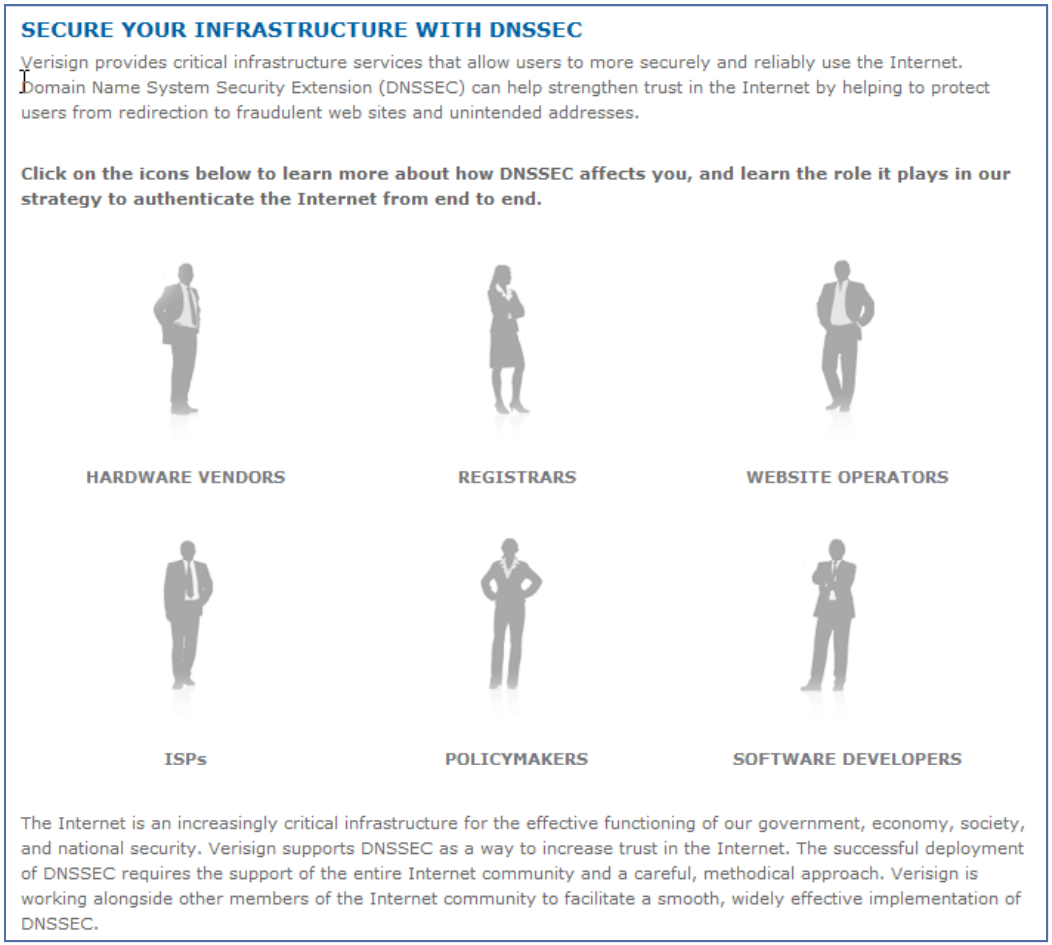
- Educational and technical webinars
- EPP Software Developer Kit
- DNSSEC Tool Guide
- Verisign's Downloadable Toolkit
- DNSSEC Transfer white paper
- Operational Testing & Evaluation environment (OT&E)

Business Support

- Educational webinars
- SME videos
- DNSSEC Data Sheets
- 3rd party research studies
- Verisign DNSSEC Signing Service
- DNSSEC Analyzer
- Interoperability Lab
- One on one Registrar sessions

DNSSEC RESOURCES

- Verisign DNSSEC Resource Center - verisign.com/dnssec
- Verisign Customer Center (VCC) – DNSSEC Forum for registrars



SECURE YOUR INFRASTRUCTURE WITH DNSSEC

Verisign provides critical infrastructure services that allow users to more securely and reliably use the Internet. Domain Name System Security Extension (DNSSEC) can help strengthen trust in the Internet by helping to protect users from redirection to fraudulent web sites and unintended addresses.

Click on the icons below to learn more about how DNSSEC affects you, and learn the role it plays in our strategy to authenticate the Internet from end to end.

HARDWARE VENDORS

REGISTRARS

WEBSITE OPERATORS

ISPs

POLICYMAKERS

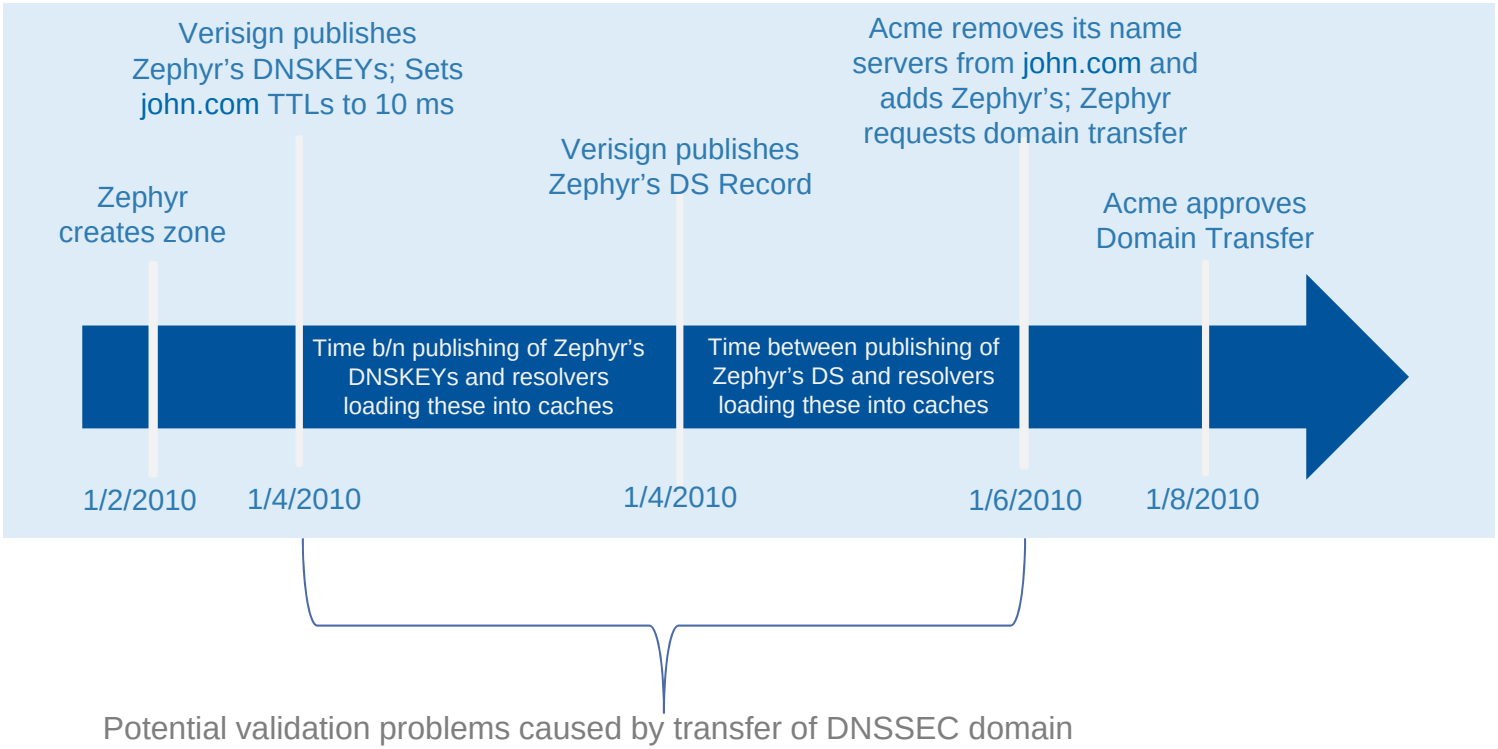
SOFTWARE DEVELOPERS

The Internet is an increasingly critical infrastructure for the effective functioning of our government, economy, society, and national security. Verisign supports DNSSEC as a way to increase trust in the Internet. The successful deployment of DNSSEC requires the support of the entire Internet community and a careful, methodical approach. Verisign is working alongside other members of the Internet community to facilitate a smooth, widely effective implementation of DNSSEC.

VERISIGN

Transfers

- Registrants expect their domains to resolve and validate via DNSSEC during domain transfers adding an additional layer of complexity
  - Delegation Signer (DS) resource records must be managed in the parent zone
  - The list of DNSKEY RRs must be coordinated between the old and new child zones



Source: http://www.verisigninc.com/assets/whitepaper-dnssec-transfers.pdf

DNSSEC Signing Service

Registrant

Register Domain
DNSSEC

Registrar
Web Site

Create
Unsigned
Zone

Unsigned
Zone
Master

Publish Unsigned Zone

Signed
Zone
Master

Publish
Signed
Zone

Public
DNS

Signed Zone
Update

Enable
Signing

Verisign DNSSEC
Signing Service

Questions?