terim Trust Anchor Repository and Up

sterdam, Netherlands

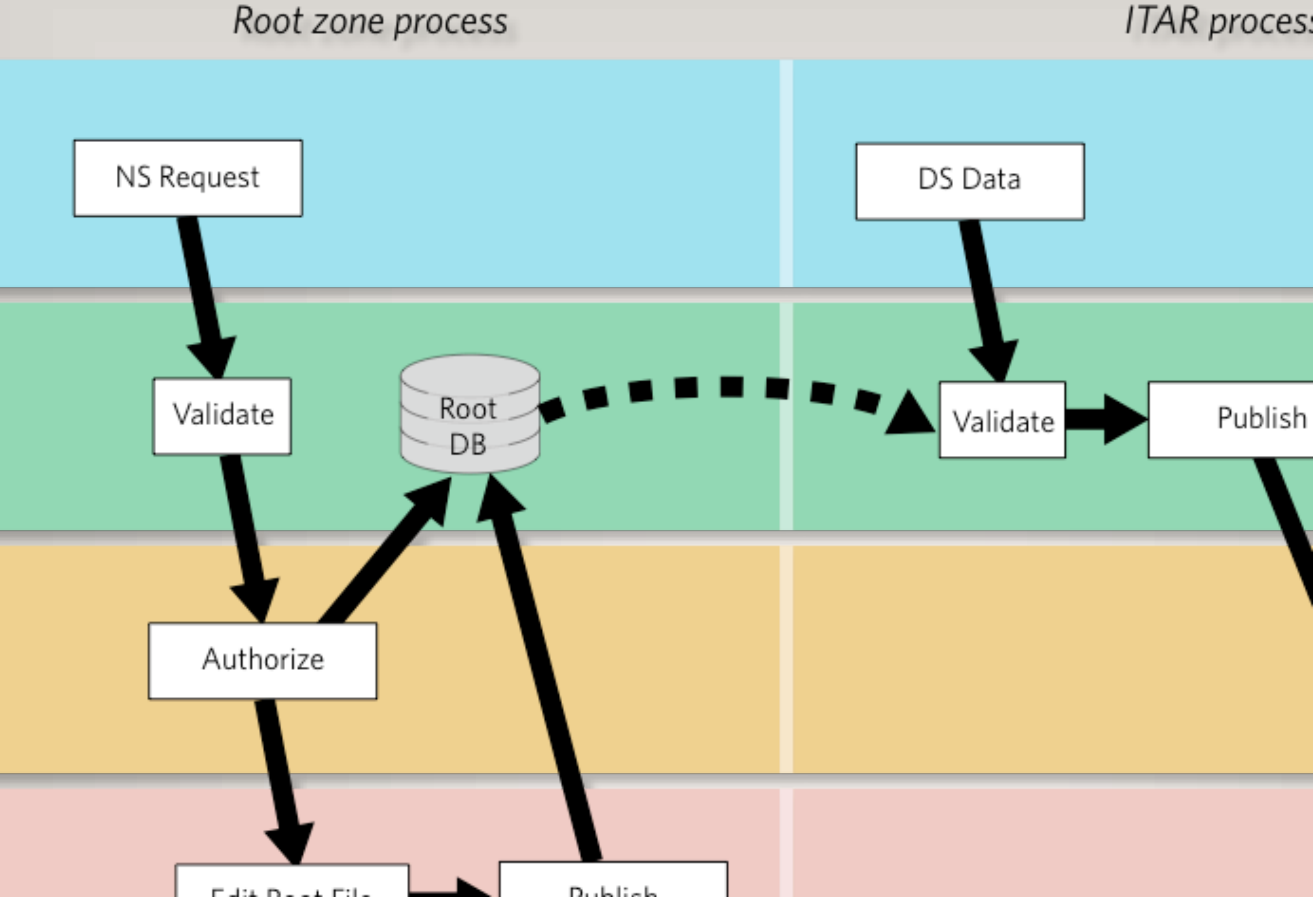
y 2009

terim Trust Anchor Repository

A mechanism to publish keys of top-level do currently implement DNSSEC

f the root zone is DNSSEC signed, such a r unnecessary

- Therefore this is a stopgap measure
- Current plan is to decommission when the roo


Root zone process
ITAR process
NS Request
DS Data
Validate
Root DB
Validate
Publish
Authorize
Edit Root File
Publish

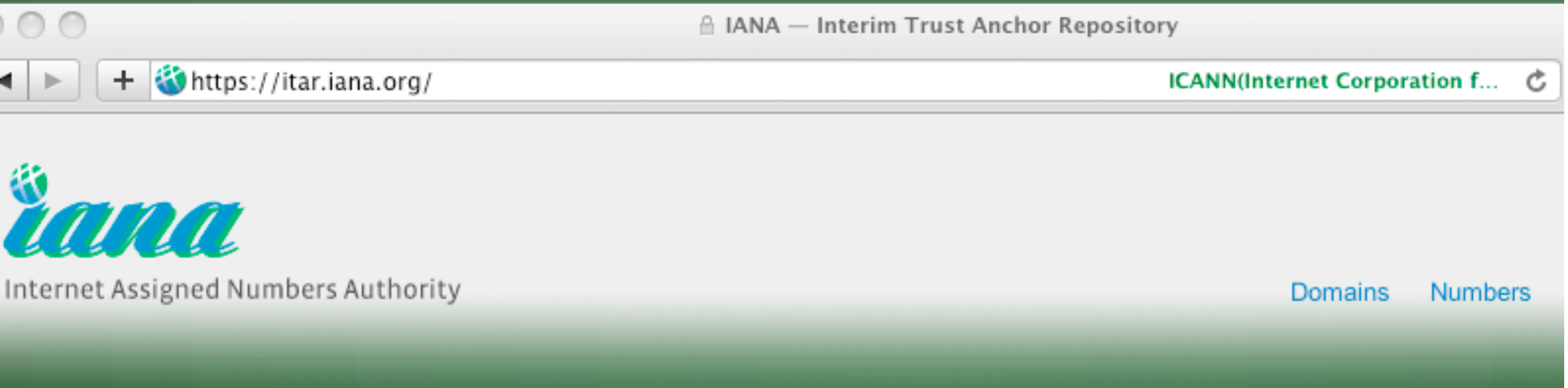
enefits

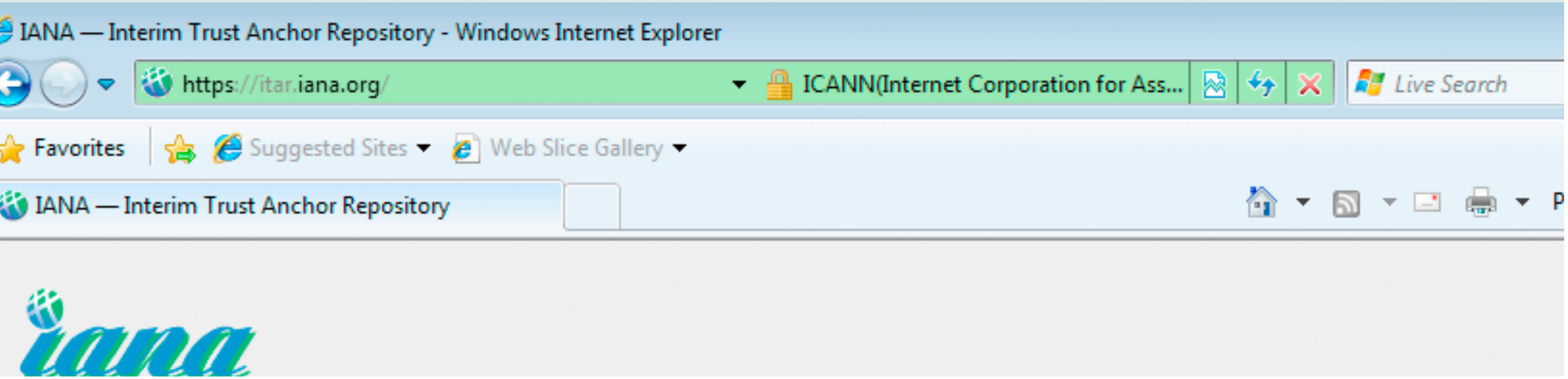
Fully meets a set of recommendations provic RIPE

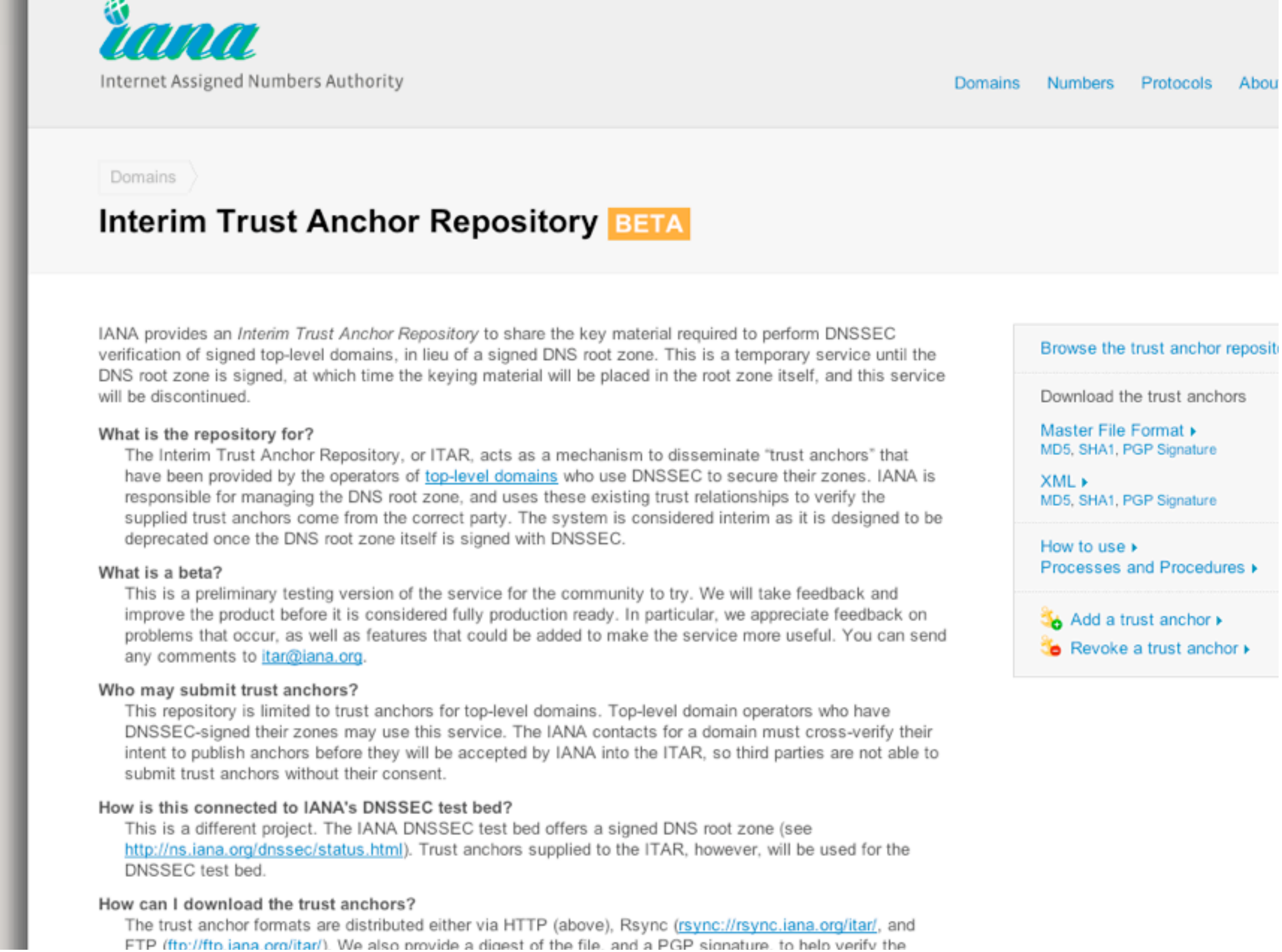
Simple to use for both top-level domain oper end users.

Works with different DNS software, different etc. Non proprietary.

Almost fully automated


IANA — Interim Trust Anchor Repository
https://itar.iana.org/
ICANN(Internet Corporation f...
iana
Internet Assigned Numbers Authority
Domains
Numbers


IANA — Interim Trust Anchor Repository - Windows Internet Explorer
https://itar.iana.org/
ICANN(Internet Corporation for Ass...
Live Search
Favorites
Suggested Sites
Web Slice Gallery
IANA — Interim Trust Anchor Repository
P
iana



Interim Trust Anchor Repository BETA

IANA provides an *Interim Trust Anchor Repository* to share the key material required to perform DNSSEC verification of signed top-level domains, in lieu of a signed DNS root zone. This is a temporary service until the DNS root zone is signed, at which time the keying material will be placed in the root zone itself, and this service will be discontinued.

What is the repository for?

The Interim Trust Anchor Repository, or ITAR, acts as a mechanism to disseminate "trust anchors" that have been provided by the operators of top-level domains who use DNSSEC to secure their zones. IANA is responsible for managing the DNS root zone, and uses these existing trust relationships to verify the supplied trust anchors come from the correct party. The system is considered interim as it is designed to be deprecated once the DNS root zone itself is signed with DNSSEC.

What is a beta?

This is a preliminary testing version of the service for the community to try. We will take feedback and improve the product before it is considered fully production ready. In particular, we appreciate feedback on problems that occur, as well as features that could be added to make the service more useful. You can send any comments to itar@iana.org.

Who may submit trust anchors?

This repository is limited to trust anchors for top-level domains. Top-level domain operators who have DNSSEC-signed their zones may use this service. The IANA contacts for a domain must cross-verify their intent to publish anchors before they will be accepted by IANA into the ITAR, so third parties are not able to submit trust anchors without their consent.

How is this connected to IANA's DNSSEC test bed?

This is a different project. The IANA DNSSEC test bed offers a signed DNS root zone (see http://ns.iana.org/dnssec/status.html). Trust anchors supplied to the ITAR, however, will be used for the DNSSEC test bed.

How can I download the trust anchors?

The trust anchor formats are distributed either via HTTP (above), Rsync (rsync://rsync.iana.org/itar/, and FTP (ftp://ftp.iana.org/itar/). We also provide a digest of the file, and a PGP signature, to help verify the

xperiences

TLD managers are frequently approving trus
hat are wrong.

- They don’t get listed because we check for ma
  DNSKEY records
  - Except one, our bug: we didn’t compare algorith
    versus algorithm type of DNSKEY
- Suggests no-one is actually checking the dige
  “approving” during the review phase

equests from the community

- Ability to suppress NSEC3 records (done)
- Prohibit SHA1 digests
- Change to accepting DNSKEY records, not

ICANN DNSSEC Update

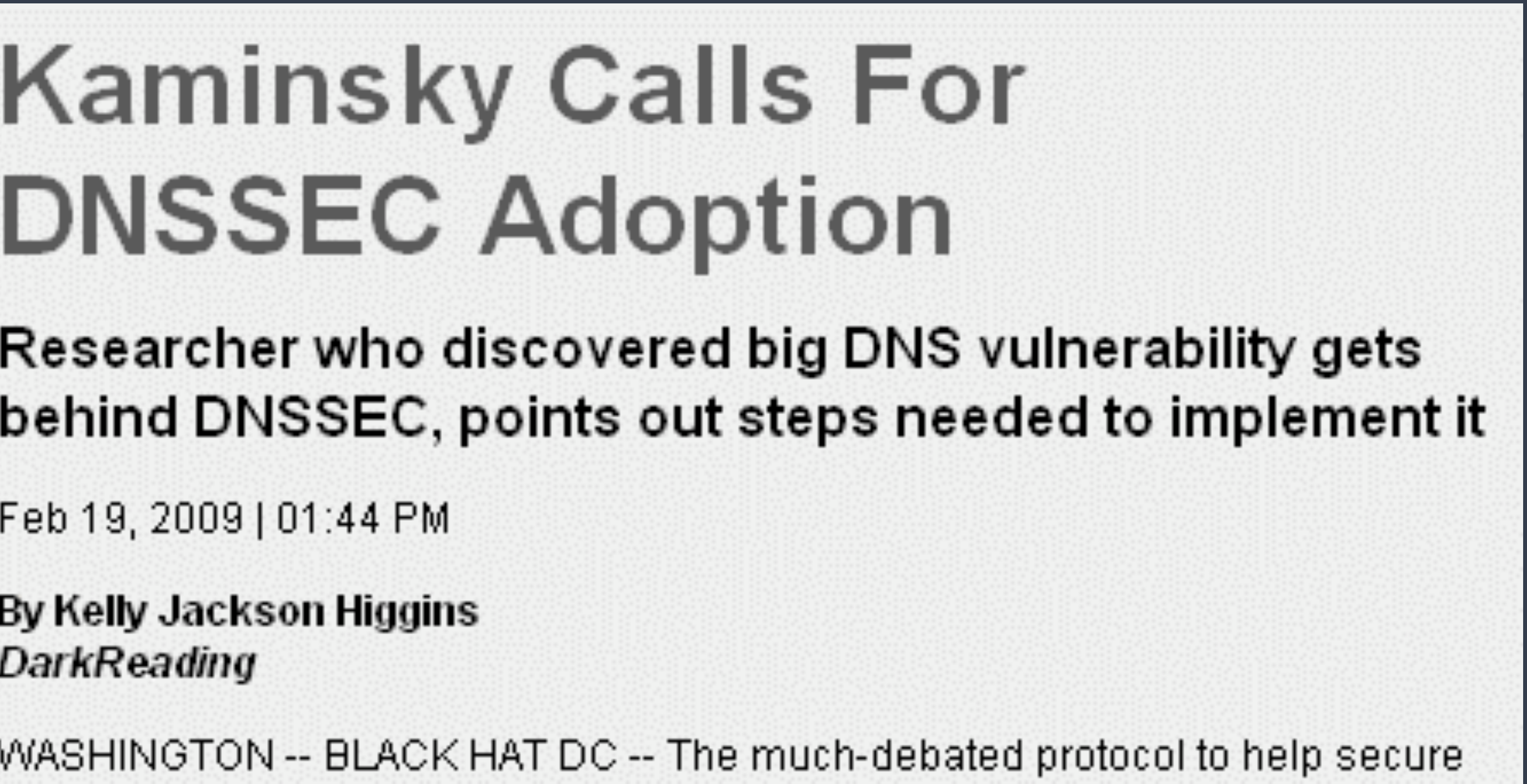
We have been asked by the community - uk, .n …, APNIC, ccNSO, RIPE and industry Google, ntel, Paypal… - to sign the root.

Revelations" from the outside regarding DNSSEC

I hear you can do cool things with DNSSEC

- Alternate/free source of trust for
- spam filtering (DKIM)
- free https:// certificates (SSL),

hy deploy DNSSEC?



Kaminsky Calls For DNSSEC Adoption

Researcher who discovered big DNS vulnerability gets behind DNSSEC, points out steps needed to implement it

Feb 19, 2009 | 01:44 PM

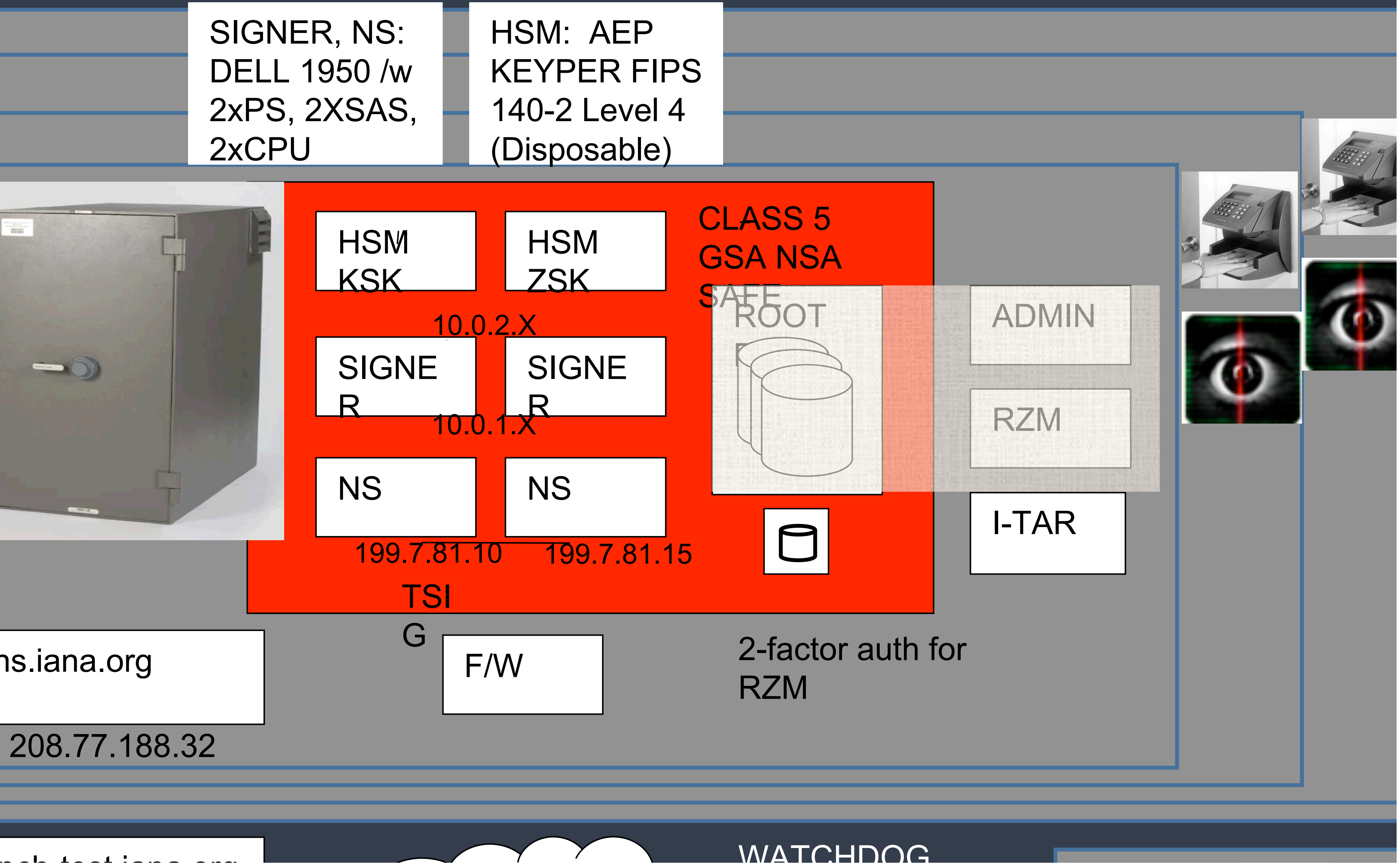
By Kelly Jackson Higgins
DarkReading

WASHINGTON -- BLACK HAT DC -- The much-debated protocol to help secure

need to make DNSSEC deployable today

testbed

xn-"test" (DS: .se, .br, .bg, .gov.)



SIGNER, NS: DELL 1950 /w 2xPS, 2XSAS, 2xCPU

HSM: AEP KEYPER FIPS 140-2 Level 4 (Disposable)

2-factor auth for RZM

Go Ahead – Test It!

Public caching recursive validating DNSSEC nam
149.20.64.22 (SFO). Thank you OARC / Duane!
66.165.162.24 (MIA)

See https://ns.iana.org/dnssec/status.html

Masters:

- 208.77.188.32 (ns.iana.org)
- **anycast** 204.61.216.37 (pch-test.iana.org) in Cairo, Johannesburg, Perth, Sydney, Dhaka, Jakarta, Hon Tokyo, Kuala Lumpur, Kathmandu, Auckland, Manil Paris, Frankfurt, Munich, Beirut, Amsterdam, Stockh Buenos Aries, Sao Paulo, Toronto, Puerto Rico, Bo

Opportunity

If deployed DNSSEC:

- Will be a critical tool in combating the nature of cyber crime allowing cross-organizational and trans-national auth

- Can be an integral part of any cyber s arsenal

- As a global security federation will be for cyber security innovation and inter

Symposium on Deploying a Signed Root: Issues and Solutions DNSSEC Coalition, June 11-12 DC

- *Key Distribution*
- *Key Rollover*
- *Trust and Transparency*
- *Impact on ISPs and Resolvers*
- *Contingency Plans*

Thanks!