DNSSEC for the Root Zone

IETF'76 Hiroshima
November 2009

Jakob Schlyter

Richard Lamb, ICANN Matt Larson, VeriSign

This design is the result of a cooperation between ICANN & VeriSign with support from the U.S. DoC NTIA

Design Requirements Keywords

Transparency

Processes and procedures should be as open as possible for the Internet community to trust the signed root

Audited

Processes and procedures should be audited against industry standards, e.g. ISO/IEC 27002:2005

High Security

Root system should meet all NIST SP 800-53 technical security controls required by a HIGH IMPACT system

Roles and Responsibilities

ICANN

IANA Functions Operator

- Manages the Key Signing Key (KSK)
- Accepts DS records from TLD operators
- Verifies and processes request
- Sends update requests to DoC for authorization and to VeriSign for implementation

DoC NTIA

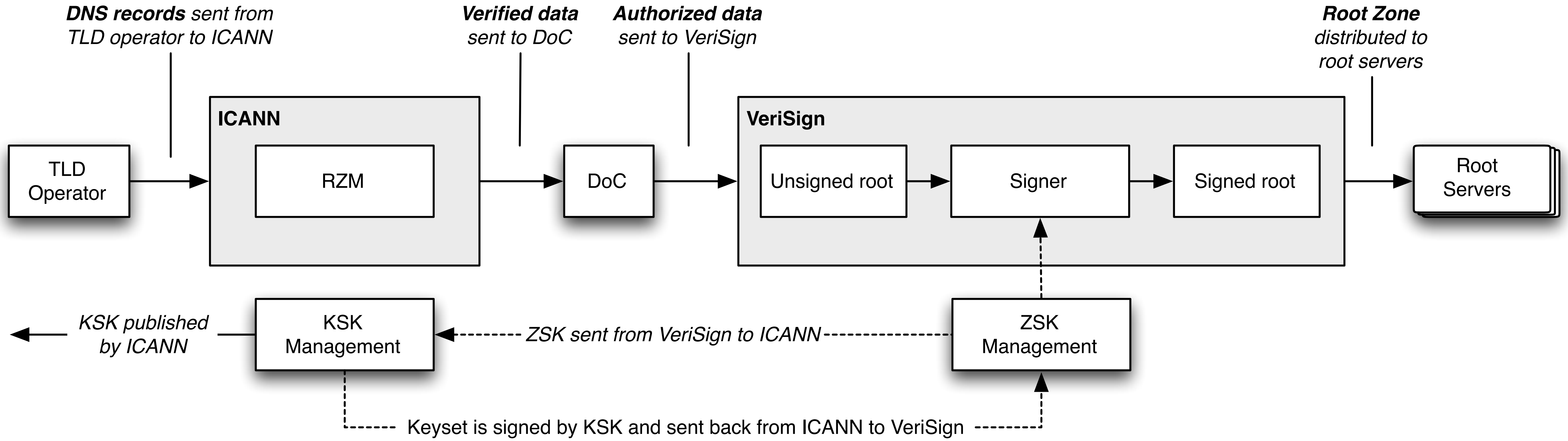
U.S. Department of Commerce
National Telecommunications and Information Administration

- Authorizes changes to the root zone
  - DS records
  - Key Signing Keys
  - DNSSEC update requests follow the same process as other changes
- Checks that ICANN has followed their agreed upon verification/processing policies and procedures

VeriSign

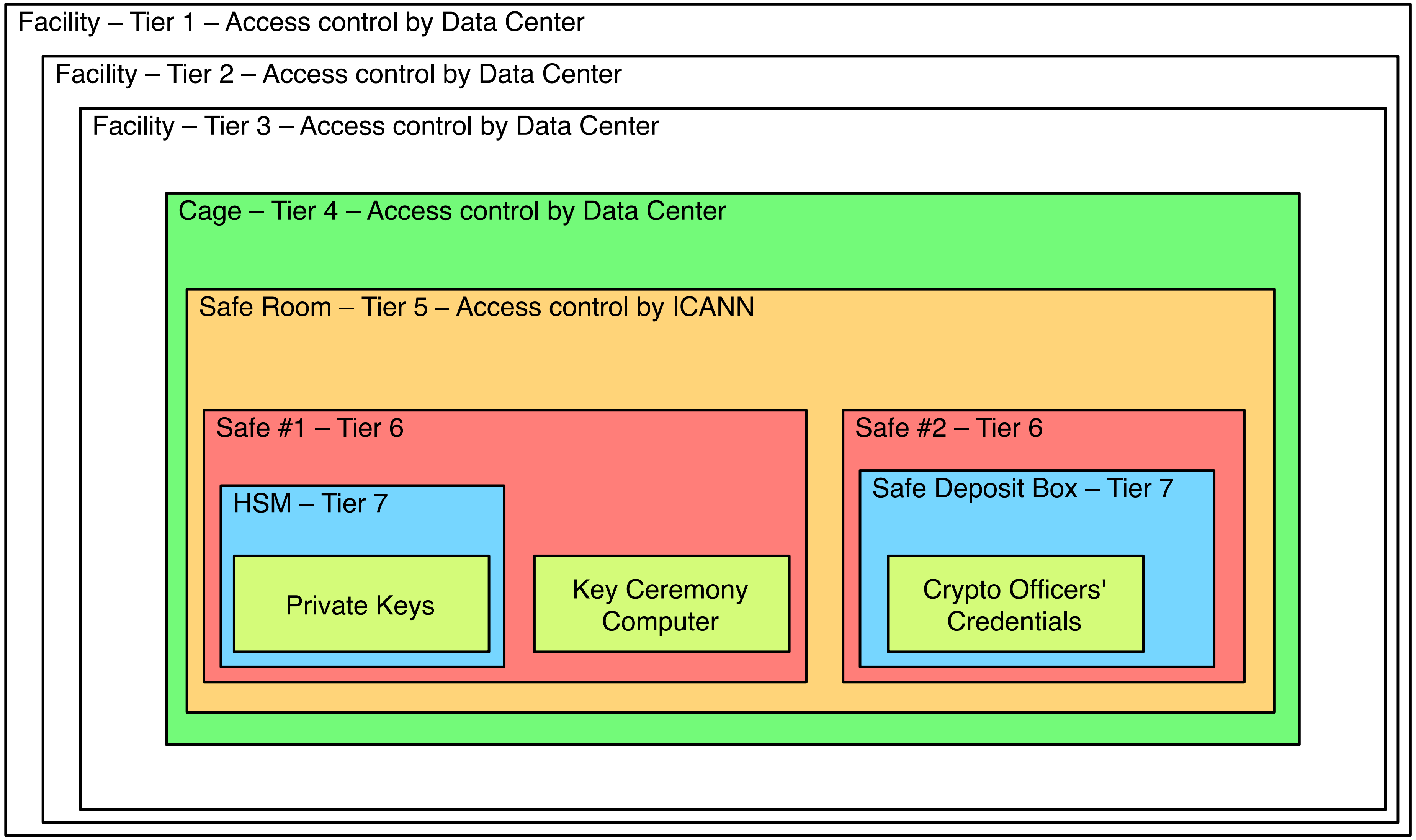
Root Zone Maintainer

- Manages the Zone Signing Key (ZSK)
- Incorporates NTIA-authorized changes
- Signs the root zone with the ZSK
- Distributes the signed zone to the root server operators


DNS records *sent from TLD operator to ICANN*
Verified data *sent to DoC*
Authorized data *sent to VeriSign*
Root Zone *distributed to root servers*
TLD Operator
ICANN
RZM
DoC
VeriSign
Unsigned root
Signer
Signed root
Root Servers
KSK published by ICANN
KSK Management
ZSK sent from VeriSign to ICANN
ZSK Management
Keyset is signed by KSK and sent back from ICANN to VeriSign

Proposed Approach to Protecting the KSK

Physical Security


Facility – Tier 1 – Access control by Data Center
Facility – Tier 2 – Access control by Data Center
Facility – Tier 3 – Access control by Data Center
Cage – Tier 4 – Access control by Data Center
Safe Room – Tier 5 – Access control by ICANN
Safe #1 – Tier 6
HSM – Tier 7
Private Keys
Key Ceremony Computer
Safe #2 – Tier 6
Safe Deposit Box – Tier 7
Crypto Officers' Credentials

DPS
DNSSEC Policy & Practice Statement

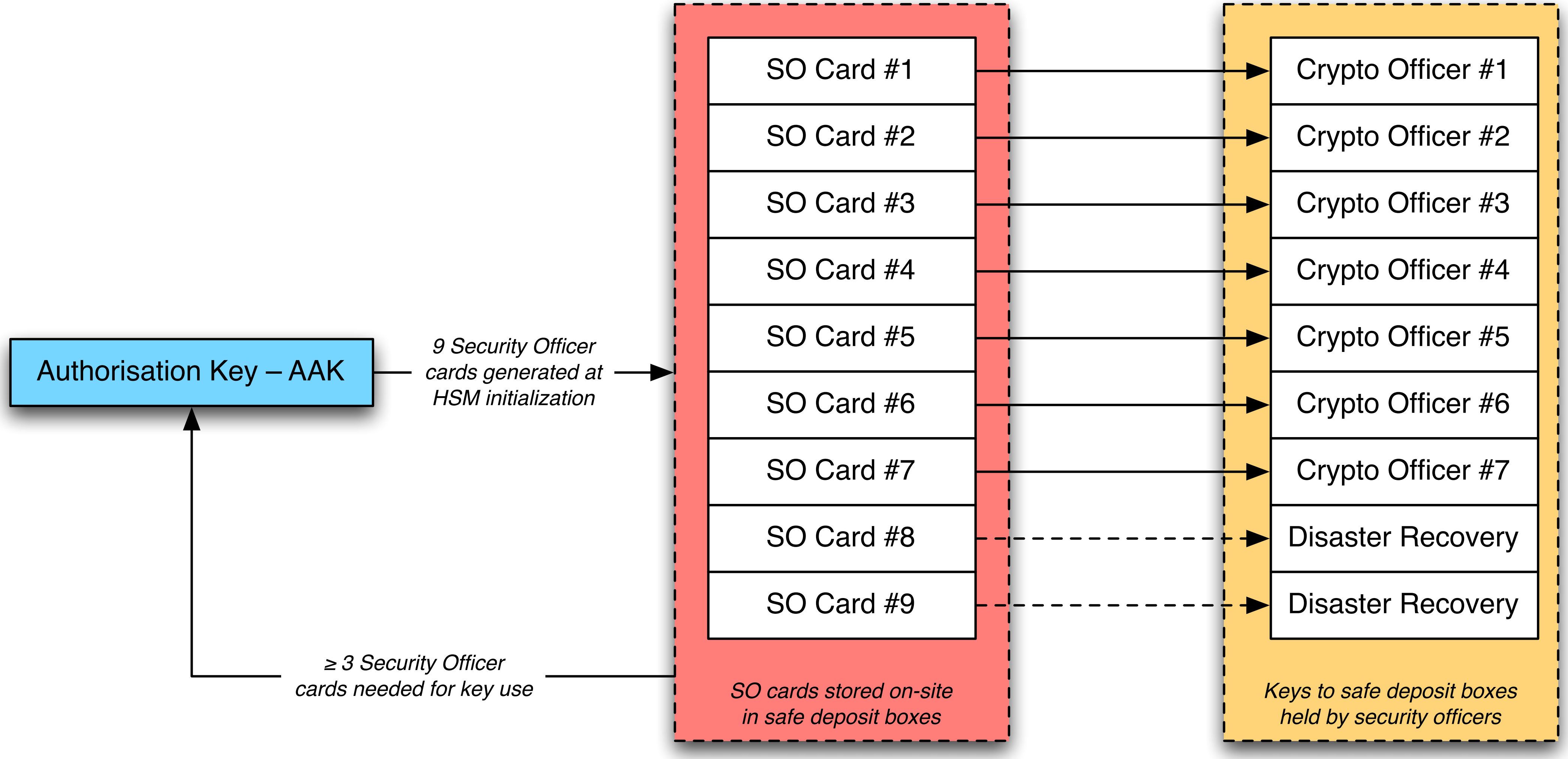
- States the practices and provisions that are employed in root zone signing and zone distribution services
  - Issuing, managing, changing and distributing DNS keys in accordance with the specific requirements of the U.S. DoC NTIA
- Comparable to a certification practice statement (CPS) from an X.509 certification authority (CA)

Community Trust

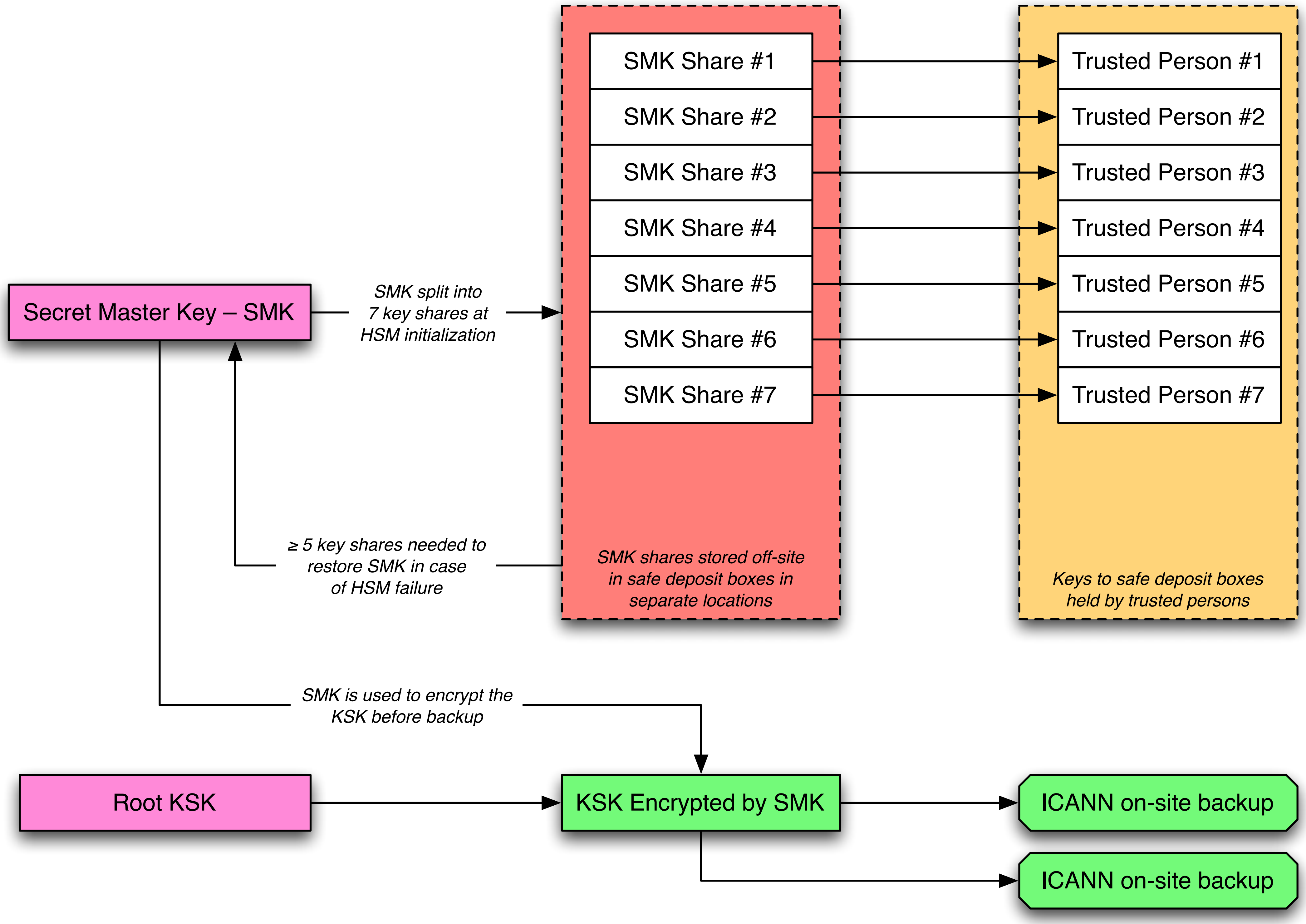
- Proposal that community representatives* have an active roll in management of the KSK
  - as Crypto Officers needed to activate the KSK
  - as Recovery Key Share Holders protecting shares of the symmetric key that encrypts the backup copy of the KSK

*) drawn from members of entities such as ccNSO, GNSO, IAB, RIRs, ISOC

Crypto Officers



Key Backup


SMK Share #1
SMK Share #2
SMK Share #3
SMK Share #4
SMK Share #5
SMK Share #6
SMK Share #7
Trusted Person #1
Trusted Person #2
Trusted Person #3
Trusted Person #4
Trusted Person #5
Trusted Person #6
Trusted Person #7
Secret Master Key – SMK
SMK split into 7 key shares at HSM initialization
≥ 5 key shares needed to restore SMK in case of HSM failure
SMK shares stored off-site in safe deposit boxes in separate locations
Keys to safe deposit boxes held by trusted persons
SMK is used to encrypt the KSK before backup
Root KSK
KSK Encrypted by SMK
ICANN on-site backup
ICANN on-site backup

Auditing & Transparency

- Third-party auditors check that ICANN operates as described in the DPS
- Other external witness may also attend the key ceremonies

Proposed DNSSEC Protocol Parameters

Key Signing Key

- KSK is 2048-bit RSA
  - Rolled every 2-5 years
  - RFC 5011 for automatic key rollovers

- Propose using signatures based on SHA-256

Zone Signing Key

- ZSK is 1024-bit RSA
  - Rolled once a quarter (four times per year)
- Zone signed with NSEC
- Propose using signatures based on SHA-256

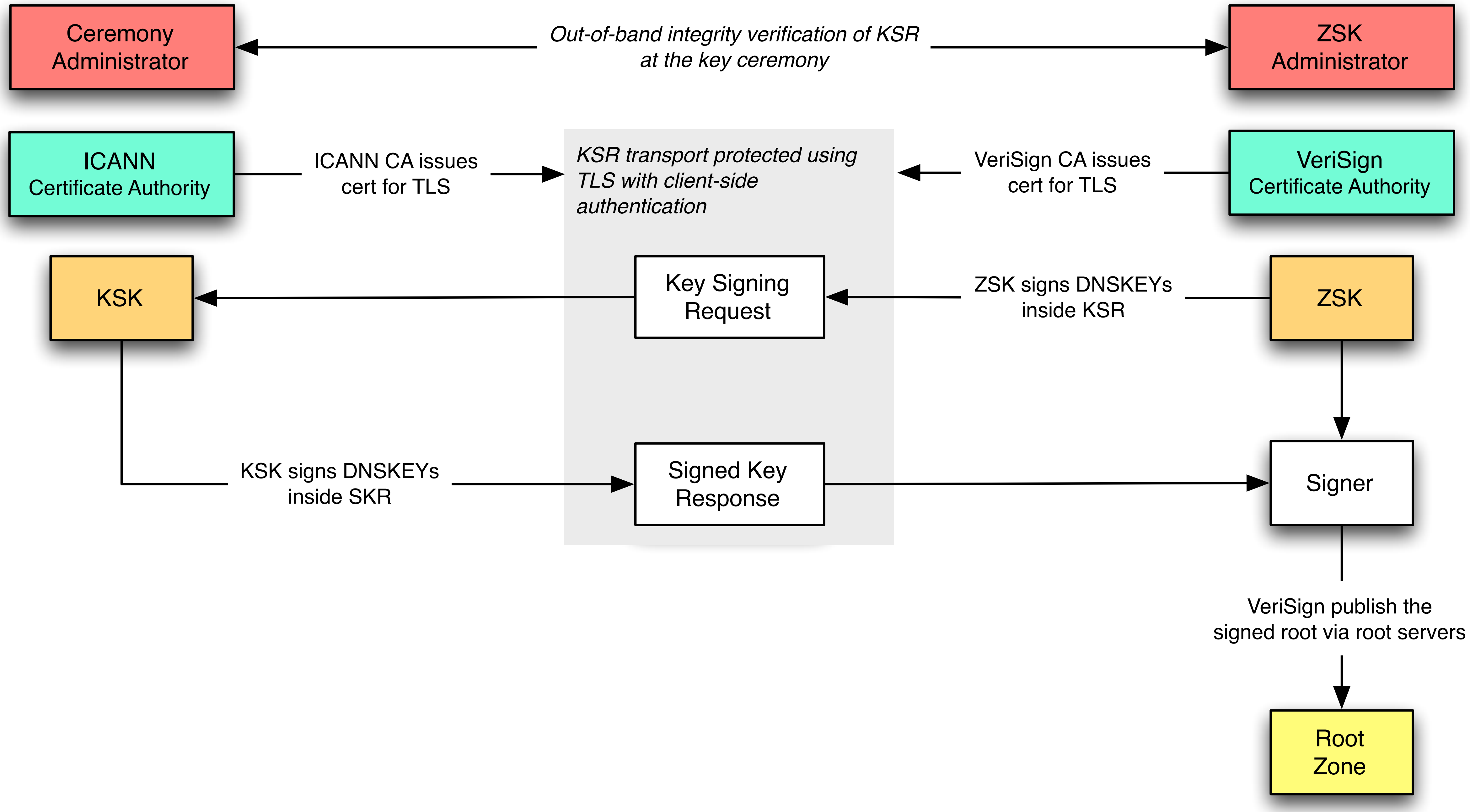
Signature Validity

- DNSKEY-covering RRSIG (by KSK) validity 15 days
  - new signatures published every 10 days
- Other RRSIG (by ZSK) validity 7 days
  - zone generated and resigned twice per day

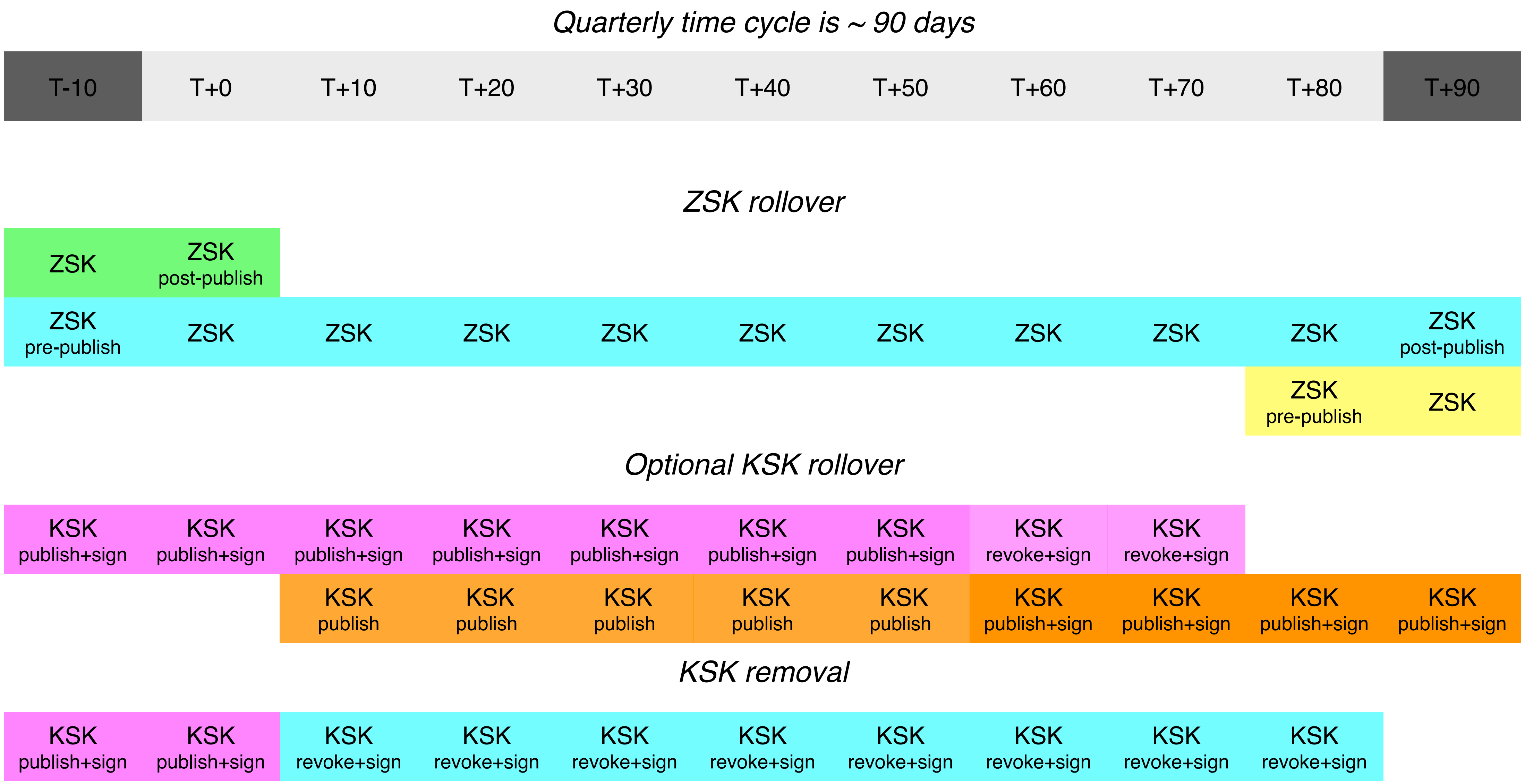
Key Ceremonies

- Key Generation
  - Generation of new KSK
  - Every 2-5 years
- Processing of ZSK Signing Request (KSR)
  - Signing ZSK for the next upcoming quarter
  - Every quarter

KSR Processing


Ceremony Administrator
Out-of-band integrity verification of KSR at the key ceremony
ZSK Administrator
ICANN Certificate Authority
ICANN CA issues cert for TLS
KSR transport protected using TLS with client-side authentication
VeriSign CA issues cert for TLS
VeriSign Certificate Authority
KSK
Key Signing Request
ZSK signs DNSKEYs inside KSR
ZSK
KSK signs DNSKEYs inside SKR
Signed Key Response
Signer
VeriSign publish the signed root via root servers
Root Zone

Key Schedule



Quarterly time cycle is ~ 90 days

T-10	T+0	T+10	T+20	T+30	T+40	T+50	T+60	T+70	T+80	T+90

ZSK rollover

T-10	T+0	T+10	T+20	T+30	T+40	T+50	T+60	T+70	T+80	T+90
ZSK	ZSK post-publish									
ZSK pre-publish	ZSK	ZSK	ZSK	ZSK	ZSK	ZSK	ZSK	ZSK	ZSK	ZSK post-publish
									ZSK pre-publish	ZSK

Optional KSK rollover

T-10	T+0	T+10	T+20	T+30	T+40	T+50	T+60	T+70	T+80	T+90
KSK publish+sign	KSK publish+sign	KSK publish+sign	KSK publish+sign	KSK publish+sign	KSK publish+sign	KSK publish+sign	KSK revoke+sign	KSK revoke+sign		
		KSK publish	KSK publish	KSK publish	KSK publish	KSK publish	KSK publish+sign	KSK publish+sign	KSK publish+sign	KSK publish+sign

KSK removal

T-10	T+0	T+10	T+20	T+30	T+40	T+50	T+60	T+70	T+80	T+90
KSK publish+sign	KSK publish+sign	KSK revoke+sign	KSK revoke+sign	KSK revoke+sign	KSK revoke+sign	KSK revoke+sign	KSK revoke+sign	KSK revoke+sign	KSK revoke+sign	

Root Trust Anchor

- Published on a web site by ICANN as
  - XML-wrapped and plain DS record
    - to facilitate automatic processing
  - PKCS #10 certificate signing request (CSR)
    - as self-signed public key
    - Allows third-party CAs to sign the KSK
    - ICANN will sign the CSR producing a CERT

Proposed Deployment

Goals

- Deploy a signed root zone
  - Transparent processes
  - Audited procedures
  - DNSSEC deployment
    - validators, registries, registrars, name server operators
- Communicate early and often!

Issues

DO=1

- A significant proportion of DNS clients send queries with EDNS0 and DO=1
- Some (largely unquantified, but potentially significant) population of such clients are unable to receive large responses
- Serving signed responses might break those clients

Rollback

- If we sign the root, there will be some early validator deployment
- There is the potential for some clients to break, perhaps badly enough that we need to un-sign the root (e.g., see previous slide)
- Un-signing the root will break the DNS for validators

Proposal

Deploy Incrementally

- Serve a signed zone from just L-Root, initially
- Follow up with J-Root
- Then other root servers
  - M, I
  - D, K E,
  - B, H, C, G, F
- Last, A-Root

Deploy Incrementally

- The goal is to leave the client population with some root servers not offering large responses until the impact of those large responses is better understood
- Relies upon resolvers not always choosing a single server
  - Note we propose leaving A until last

DURZ

- “Deliberately Unvalidatable Root Zone”
- Sign RRSets with keys that are not published in the zone (but with matching keytag…)
- Publish keys in the zone which are not used, and which additionally contain advice for operators (see next slide)
- Swap in actual signing keys (which enables validation) at the end of the deployment process

DURZ

```
.       3600    IN     DNSKEY  256  3  5 (
                       AwEAAa++++++++++++++++++++++++++++++
                       ++THIS/KEY/AN/INVALID/KEY/AND/SHOULD
                       /NOT/BE/USED/CONTACT/ROOTSIGN/AT/ICA
                       NN/DOT/ORG/FOR/MORE/INFORMATION+++++
                       ++++++++++++++++++++++++++++++++++++
                       ++++++++++++++++++++++++++++++++++++
                       ++++++++++++++++++++++++++++++++++++
                       ++++++++++++++++++++++++++++++++++++
                       ++++++++++++++++++++++++++++++++++++
                       ++++++++++++++++++++++/=
                       ) ; Key ID = 6477
```

DURZ

- Deploy conservatively
  - It is the root zone, after all
- Prevent a community of validators from forming
  - This allows us to unsign the root zone during the deployment phase (if we have) to without collateral damage

Measurement

- For those root servers that are instrumented, full packet captures and subsequent analysis around signing events
- Ongoing dialogue with operator communities to assess real-world impact of changes

Testing

- A prerequisite for this proposal is a captive test of the deployment
  - Test widely-deployed resolvers, with validation enabled and disabled, against the DURZ
  - Test with clients behind broken networks that drop large responses

Communication

with non-technical audiences

- Reaching the non-technical and semi-technical audiences with press releases and other means.
- PR departments with people who know how to do this will be engaged.

Communication

with technical audiences

- Reaching the technical audiences via mailing lists and other means
  - IETF DNS lists (e.g. DNSOP)
  - non-IETF DNS lists (e.g. DNS-OARC)
  - General operator lists (e.g. NANOG)
  - …

Draft Timeline

- December 1, 2009
    - **Root zone signed**
        - Initially signed zone stays internal to ICANN and VeriSign
    - ICANN and VeriSign begin KSR processing
        - ZSK and KSK rolls
- January - July 2010
    - Incremental roll out of signed root
- July 1, 2010
    - KSK rolled and trust anchor published
    - **Signed root fully deployed**

Documentation

- NTIA Requirements
- High Level Technical Architecture
- Draft DPS for ICANN and VeriSign
  - http://www.ntia.doc.gov/dns/dnssec.html

Thoughts?

- Feedback on this proposal would be extremely welcome
  - Queue at the mic
  - Email to root-dnssec-feedback@verisignlabs.com

Root DNSSEC Design Team

Joe Abley
David Blacka
David Conrad
Richard Lamb
Matt Larson
Fredrik Ljunggren
David Knight
Tomofumi Okubo
Jakob Schlyter