DNS Root Zone DNSSEC Operations -

Ed Lewis| FIRST-TC Auckland, NZ | February 21, 2016
edward.lewis@icann.org

My Motivation

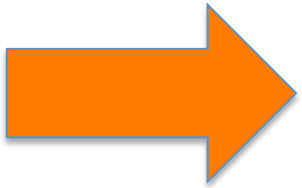
- ICANN is tasked with changing a crucial configuration parameter of DNS security
  - We need to develop a plan (working on it)
  - We don't have a fixed date for the change
- In preparation for the task
  - We are engaging with various groups who might be impacted by the work and/or might help us improve upon our planning work

Agenda

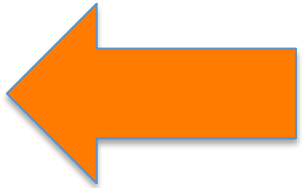
- Background on Domain Name System (DNS) and DNS Security Extensions (DNSSEC)
- Internet Corporation for Assigned Names and Numbers (ICANN) role in DNSSEC
- The process of DNSSEC Validation
- Managing Trust Anchors - Impact of a Key Roll

For Engineers Who Don't Like Protocols

What is the IPv4 address for www.nic.tld.?

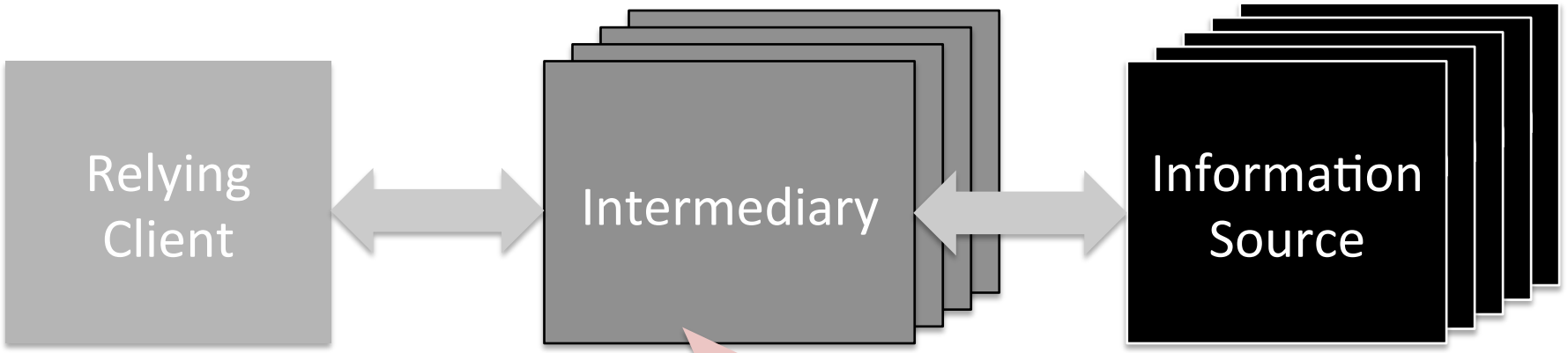


The IPv4 address for www.nic.tld. is W.X.Y.Z



Why is there DNSSEC?

- DNS is not "client-server"
  - No end-to-end session to protect

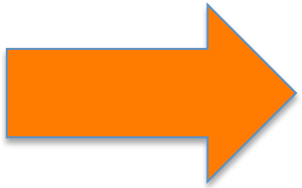


DNSSEC Design Approach

- Digital Signatures
  - A cryptographically encrypted checksum is sent alongside the data
  - A system of public keys is used to verify

DNSSEC for Those Who Don't Like Protocols

What is the IPv4 address for www.nic.tld.?



The IPv4 address for www.nic.tld. is W.X.Y.Z

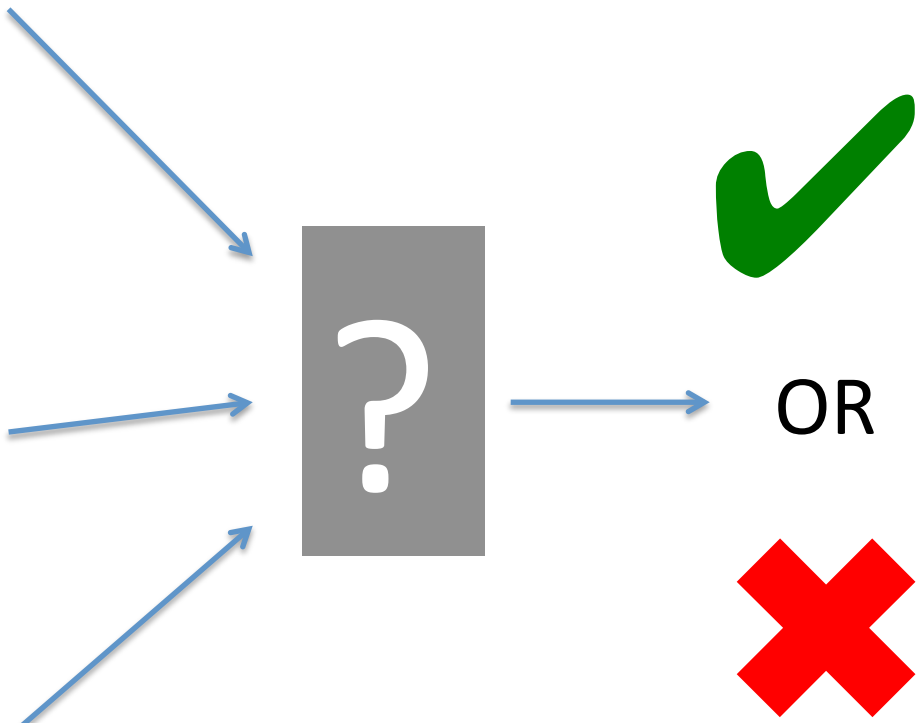
Digital signature by nic.tld covering answer

Crypto-checking a Signature

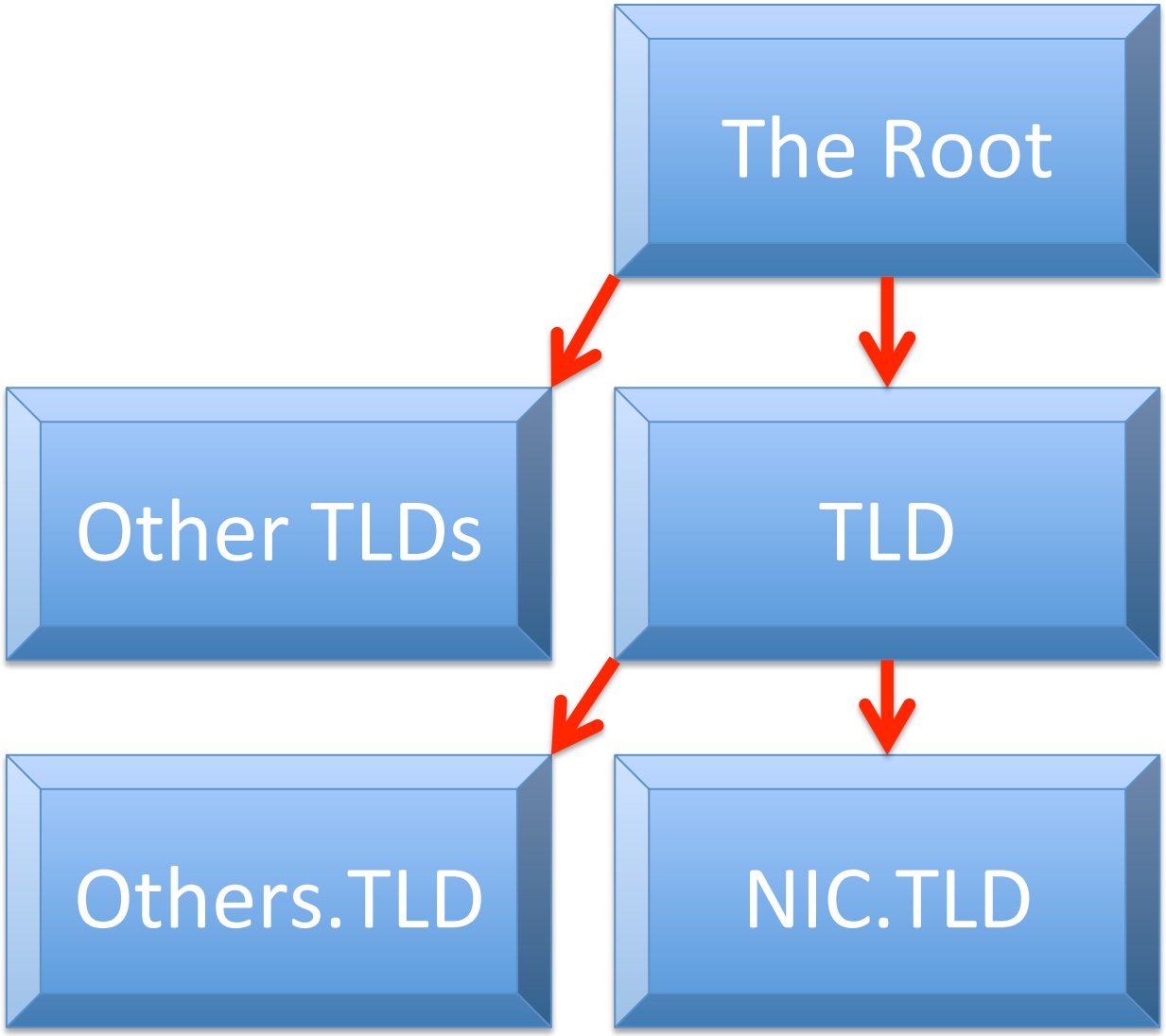
The IPv4 address for www.nic.tld. is W.X.Y.Z

Digital signature by nic.tld covering answer

nic.tld KEY ZSK

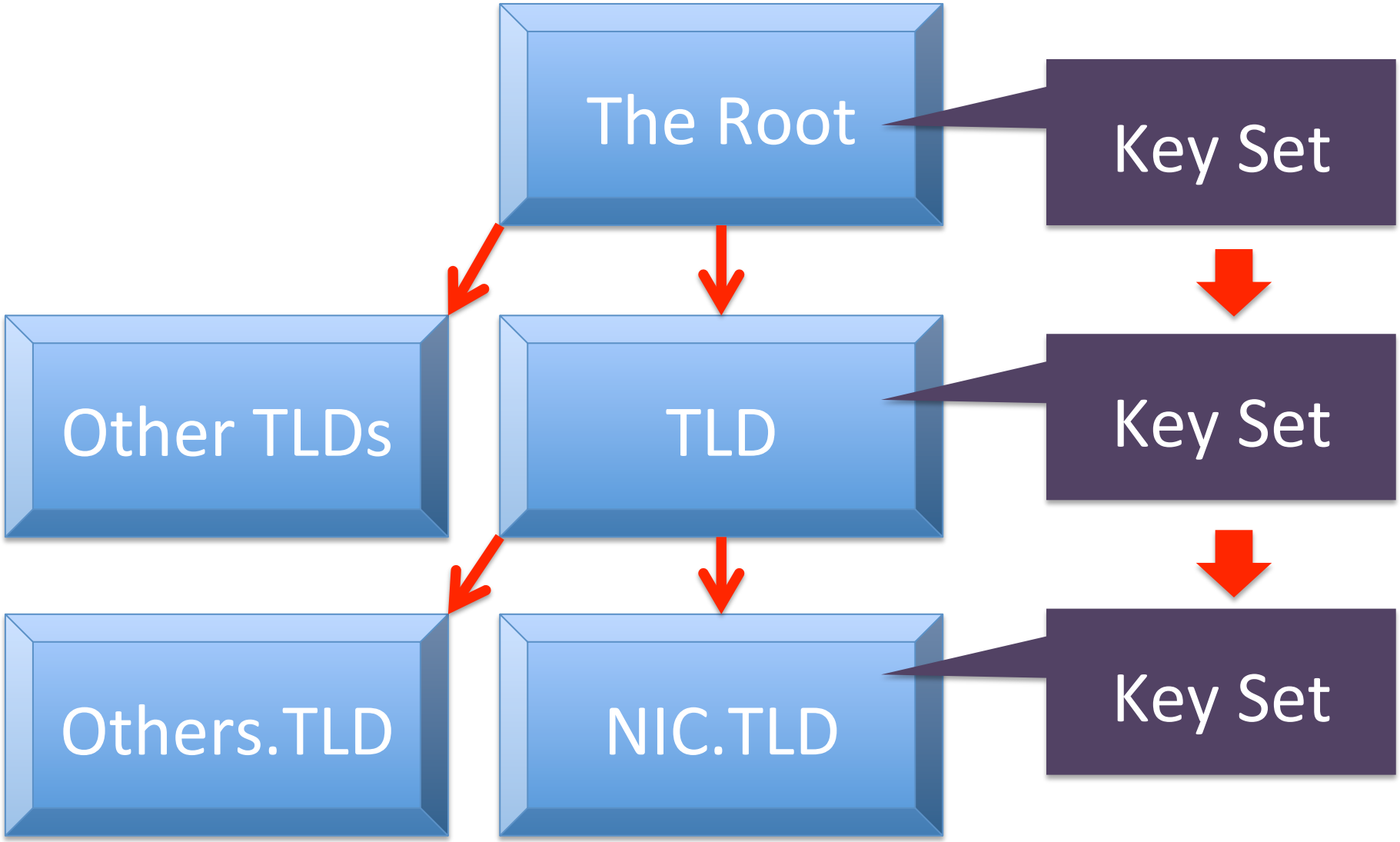


How this Works (DNS)

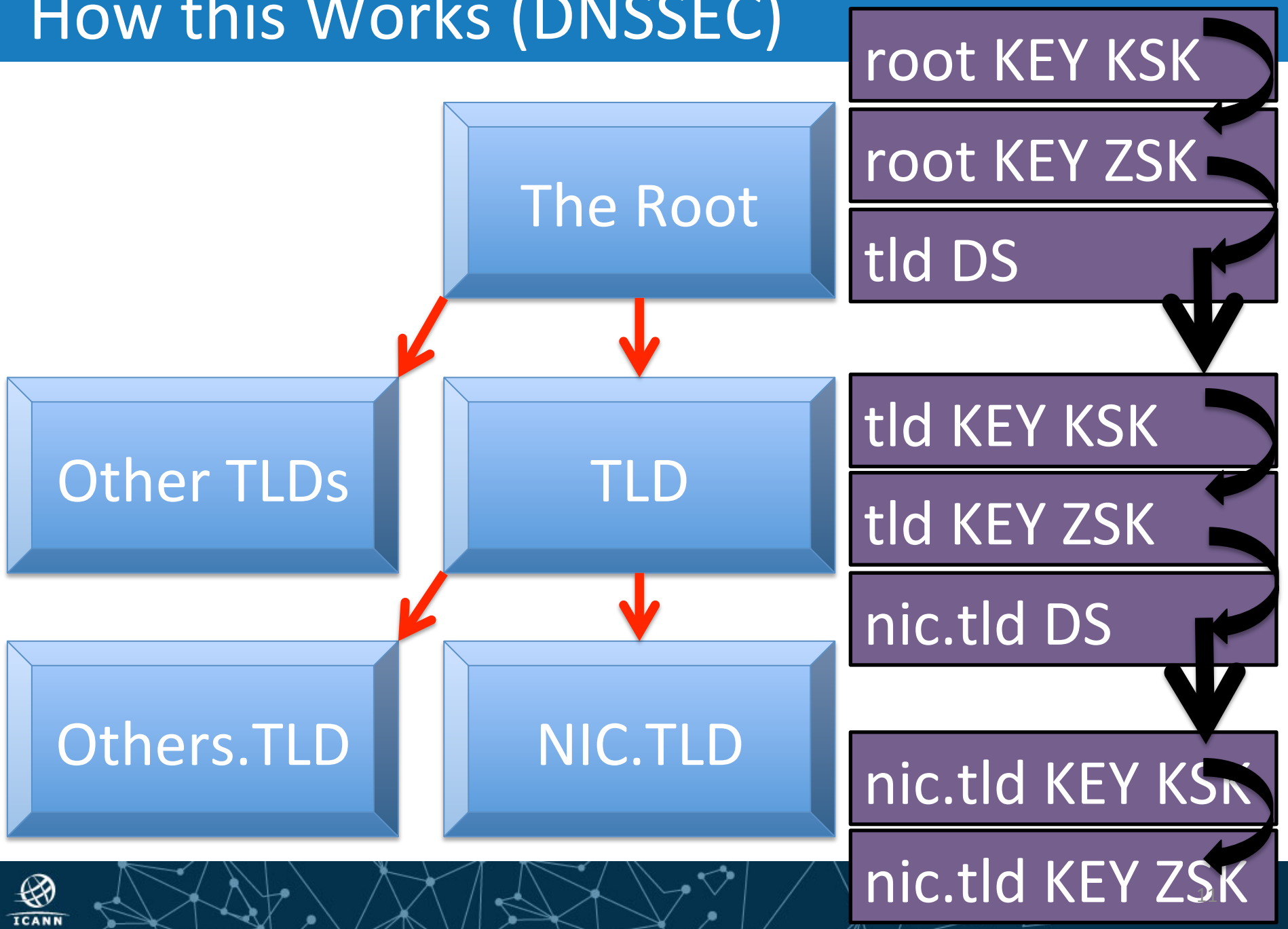


Top Level Domain

How this Works (Scaling)



How this Works (DNSSEC)



Roles of DNSSEC Keys

- KSK – key-signing key, signs internally managed keys
  - Internal refers to what an administrator manages
- ZSK – zone-signing key, signs other internally managed data

- DS – hash of external KSK "one layer down"
  - External refers to whom the administrator delegates authority

Chain of Trust in Operations

- The Internet's DNS system has a DNSSEC signed Root Zone
  - Since 2010
  - The KSK signs the ZSK, ZSK signs DS for TLDs
  - KSK and ZSK operators are separate organizations
- Trust is a matter for the consumers, not producers, to define
  - Goal is to reduce reliance to just one KSK (set)
  - If the consumer wants to "trust just one"

Root Zone KSK and ZSK Operators

- ICANN performs the management of the Root Zone KSK as part of fulfilling the IANA Functions Contract
  - That contract is managed by the US Department of Commerce's National Telecommunications and Information Administration (NTIA)

- Verisign performs the management of the Root Zone ZSK as part of their role as the Root Zone Maintainer

ICANN's role, in brief

- ICANN manages the KSK lifecycle
  - Create the KSK (has happened once)
  - Sign with the KSK (quarterly)
  - Protect the KSK (constantly)
  - Dispose of the KSK (hasn't happened yet)
  - and Publicize the KSK (constantly)

- Objective: operate in a manner to enable trust
  - SOC3/SysTrust, audited by third-party
  - (US) FIPS 140-2 level 4 cryptographic devices (HSM)

Returning Focus to DNSSEC

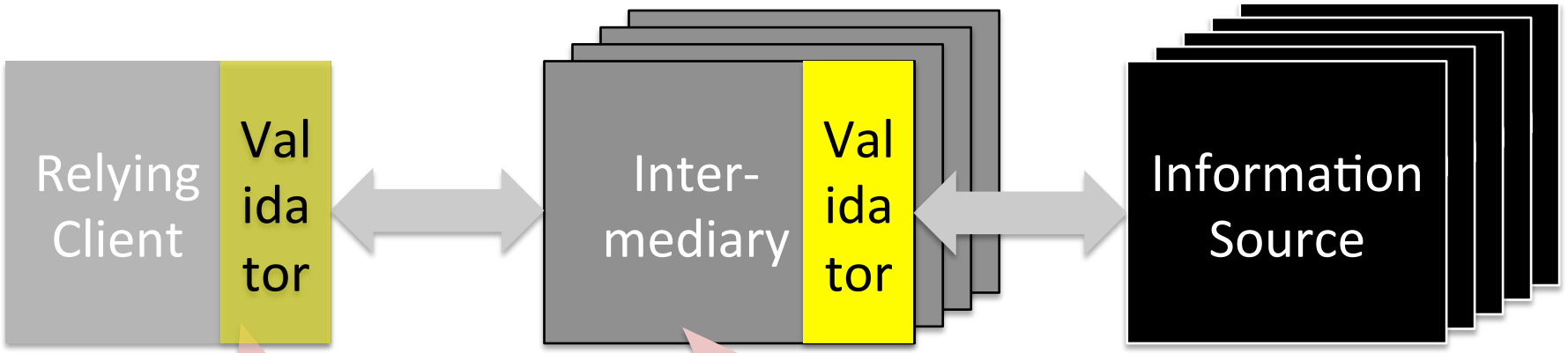
- Within DNSSEC there is
  - Signing the Data
    - Adding digital signatures
    - Cryptographic key lifetime management
    - This is not the subject of this talk
  - Validating the Data
    - Protecting the consumer of the answer
    - Assembling the chain of trust
    - Managing "who is trusted"

What is Validation?

- When a response is received
  - Check the digital signature, cryptographic and otherwise (time, authority, and so on)
  - Check all signatures "up the chain"
  - Once an answer is validated, it can be cached, used, forwarded
- What is needed
  - A trust anchor is needed, a "pinned" KSK

Where is Validation Done?

- DNS is not "client-server"
  - No end-to-end session to protect



- Might Validate

- Seeks and Aggregates Information
- Validates

Why and who does?

- Why validate?
  - Lessens the gullibility of the intermediary elements
  - Provides a trustable base for operations
- Why not?
  - Validation imposes some cost on operating
  - Validation could raise false alarms
- Have operators turned on validation?
  - Some have, a "significant minority"

Trust Anchor Management

- Function of the validation engine
  - Keys that are "pinned"
  - Root Zone KSK ought to be one of them
  - There may be other KSK sets
- There may also be "negative trust anchors"
  - Experience says some DNS operators botch KSK management

Getting the Root Zone KSK

- There are a few ways to get a copy of the Root Zone KSK
  - Via DNS
  - Via Web
  - Via Distributed Code
  - Via anything else – T-shirts, talks, asking someone

Getting the Root Zone KSK from DNS

- 'dig @i.root-servers.net . DNSKEY' and pull out the key with flags=257

- As an only method, this isn't very secure
  - Convenient but not secure

Automated Updates via DNS

- "Automated Secure Updates of DNSSEC Trust Anchors" (RFC 5011)
  - Describes a series of operational steps to have one trust anchor safely introduce the next
  - Lacks needed management hooks

- But if configurations are pushed by a configuration management tool, this approach won't work

Getting the Root Zone KSK from Web

- From https://www.iana.org/dnssec
  - https://data.iana.org/root-anchors/root-anchors.xml
  - OpenPGP signature and PKCS 7 signature
- Validate via appropriate public keys on that site
- In place since 2010
  - Examining ways to improve what's there (while maintaining backwards compatibility)

Future Considerations

- An open work item –
  - What's the best way to publicize a key to a wide audience?

- We are revisiting our approach to publication to enable trust to be built on the key

Root Zone KSK in Tool Distributions

- Software may come with a copy of the key embedded
  - Configuration file

- ICANN is working with software developers and distributors to make sure this is reliable

- Still, caution that embedded keys may be "stale" once keys are rolled

For more information

- Join the mailing list
  - https://mm.icann.org/mailman/listinfo/root-dnssec-announce
- Follow on Twitter
  - Hashtag: #KeyRollover
  - Follow @ICANNtech for the most up to date news