ICANN & IANA Update

Dubai, United Arab Emirates
October 2008

Kim Davies
Manager, Root Zone Services
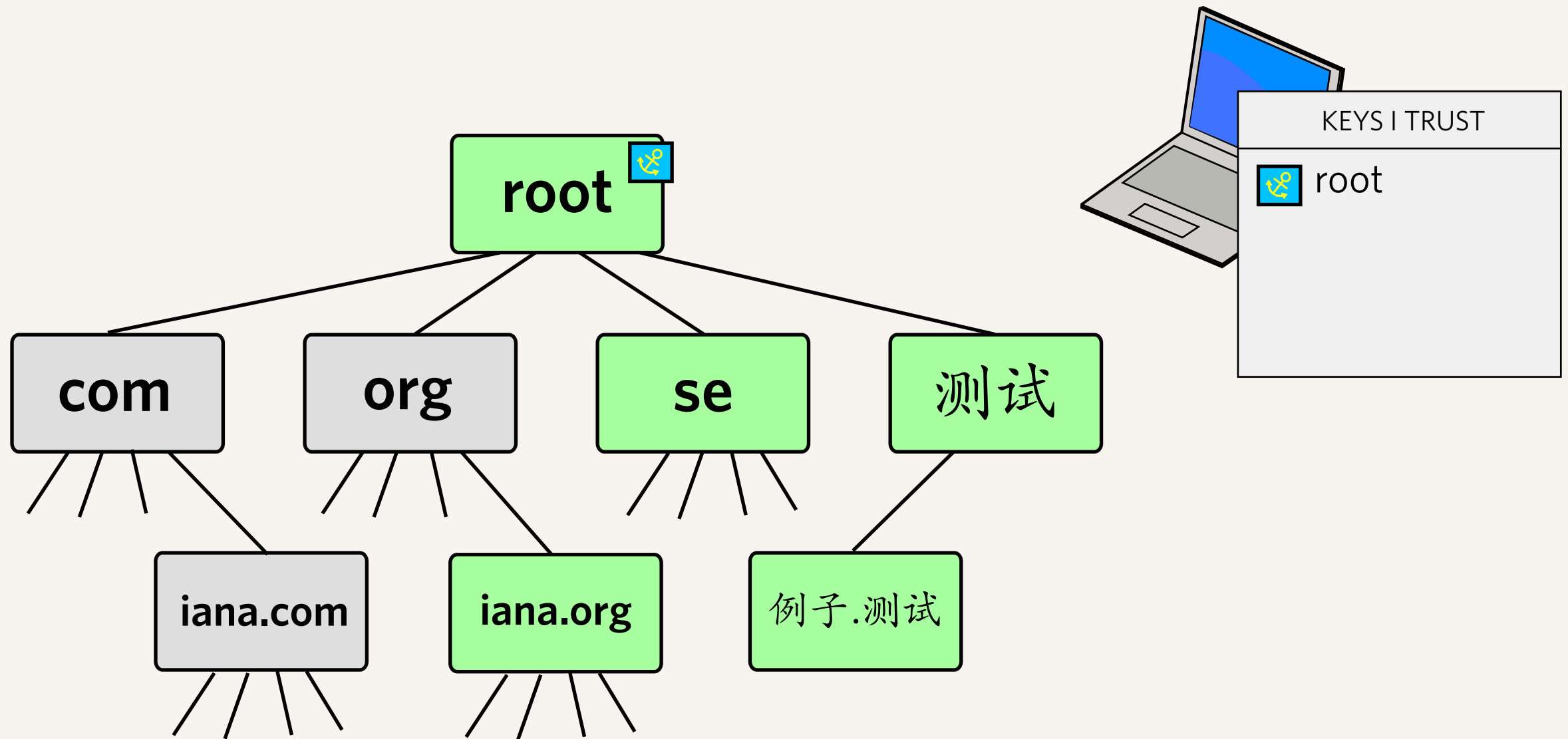
ICANN

Internet Corporation for
Assigned Names & Numbers

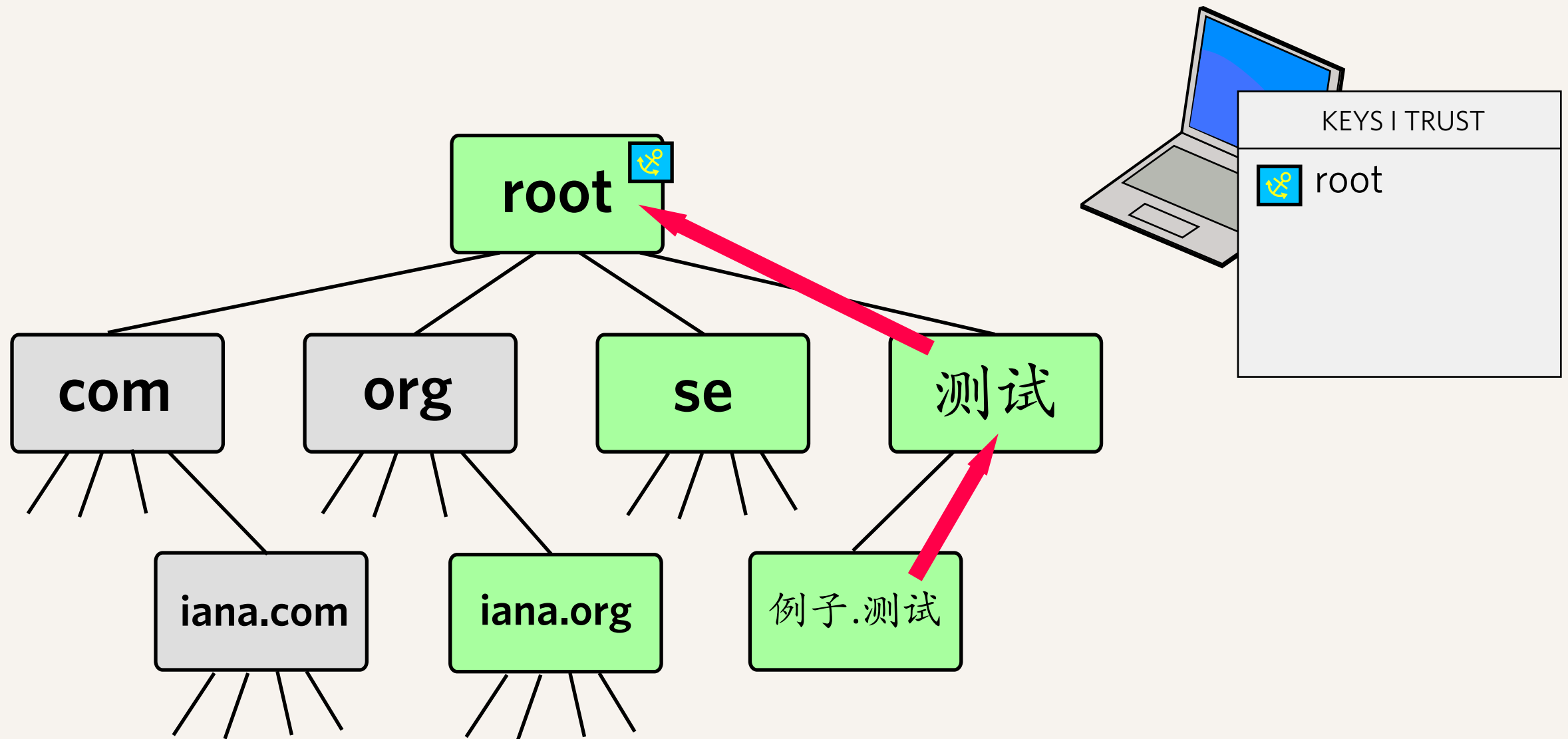# Interim Trust Anchor Repository

Interim Trust Anchor Repository

‣ A mechanism to publish keys of top-level domains that currently implement DNSSEC

‣ If the root zone is DNSSEC signed, such a repository is unnecessary

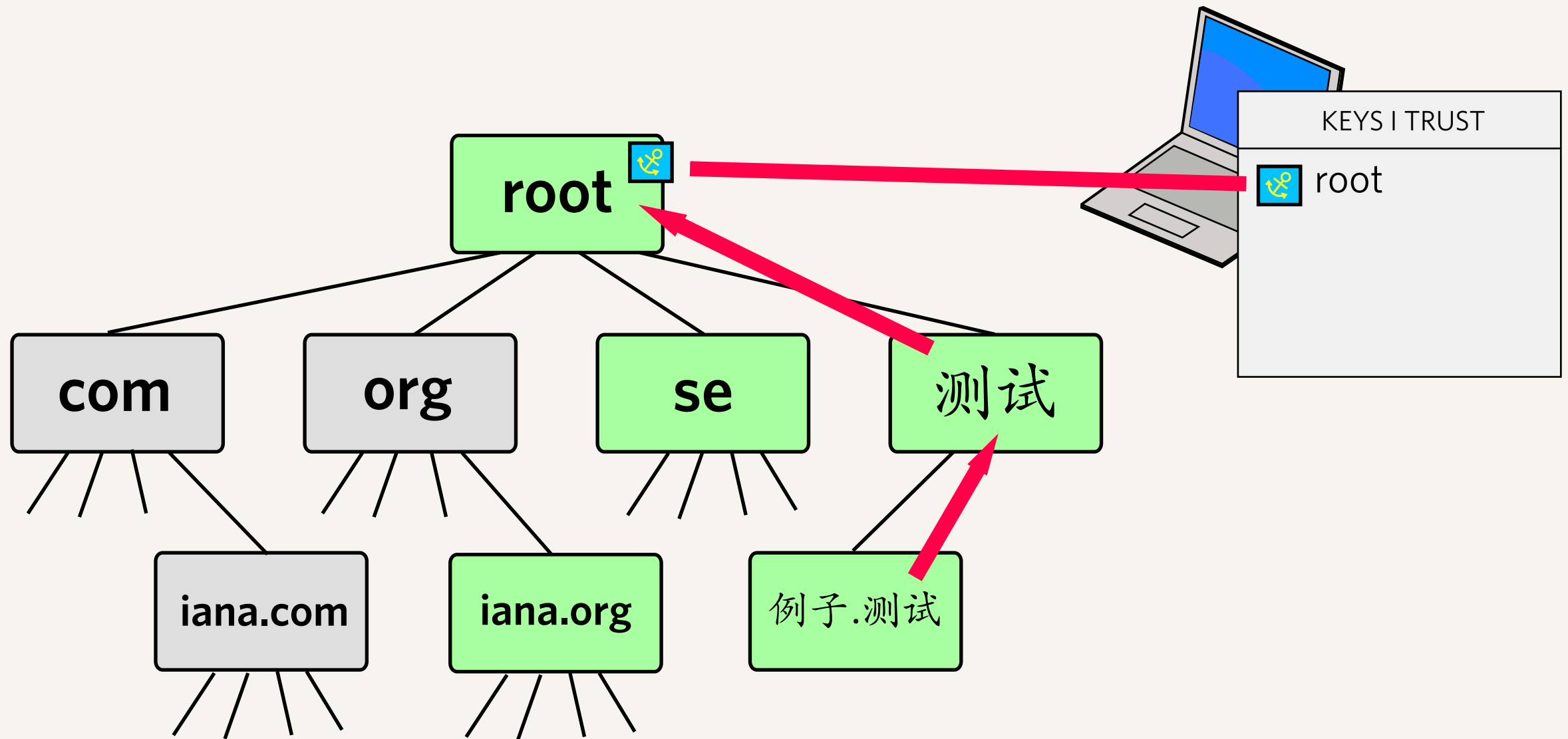 ‣ Therefore this is a stopgap measure

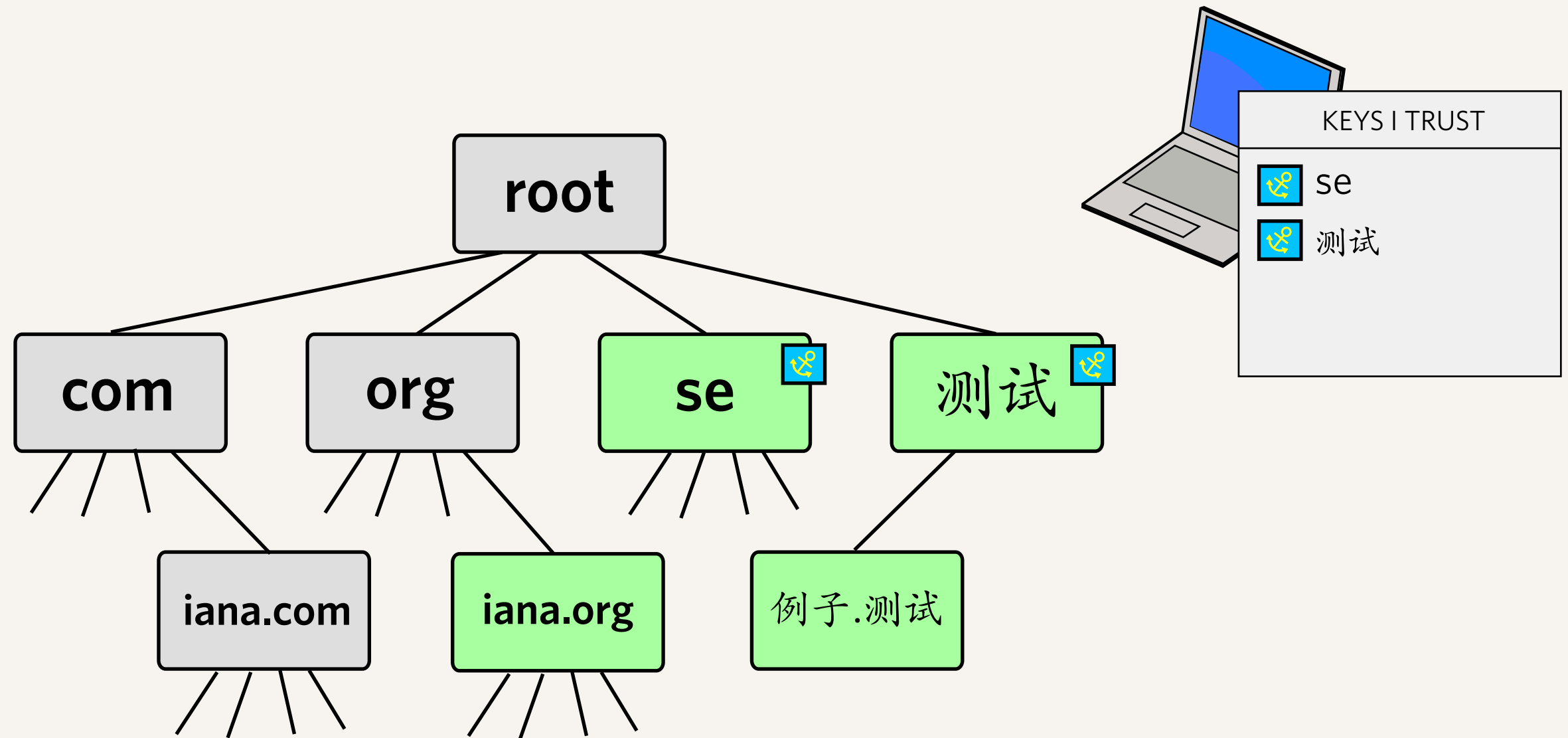 ‣ Should be decommissioned when the root is signed

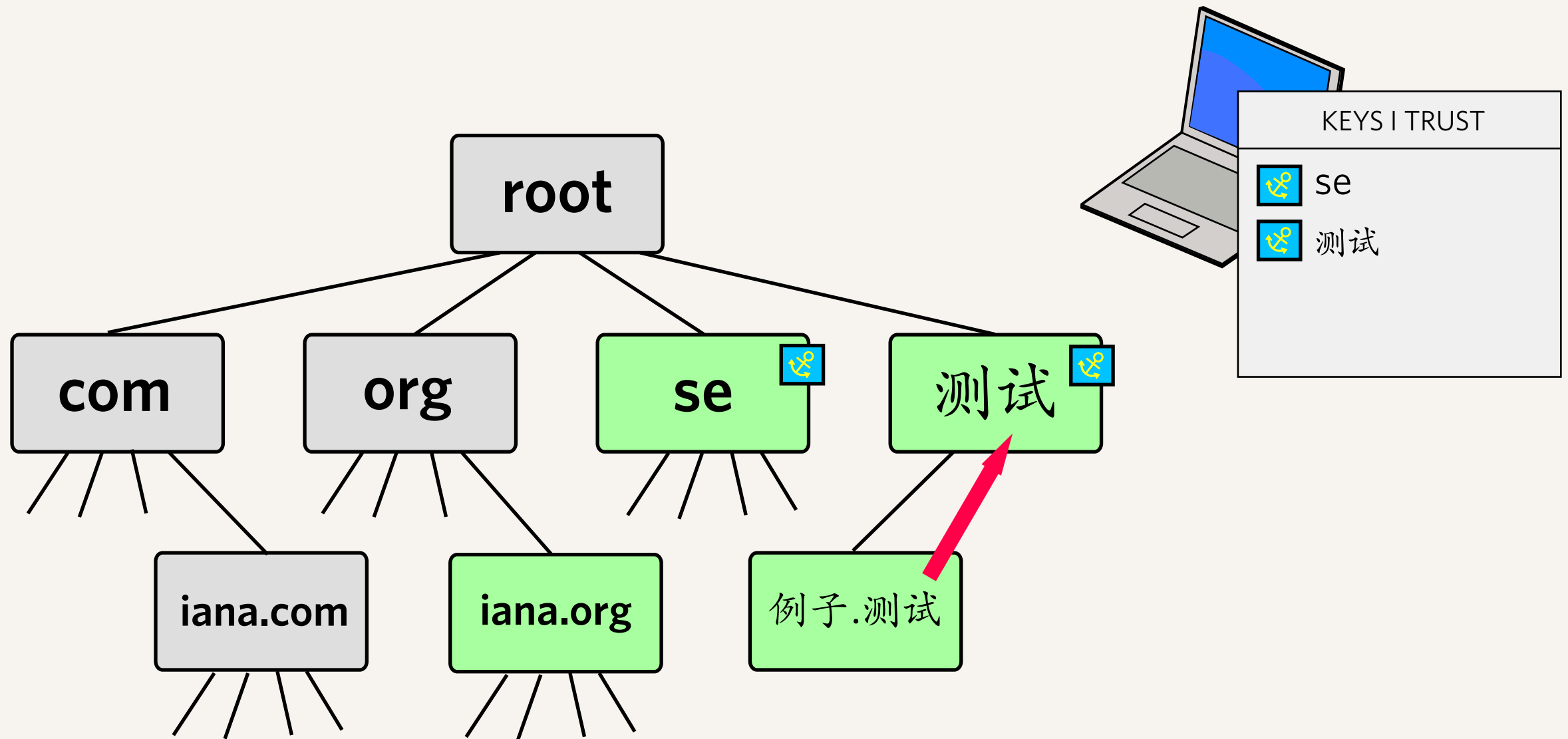If the root was signed
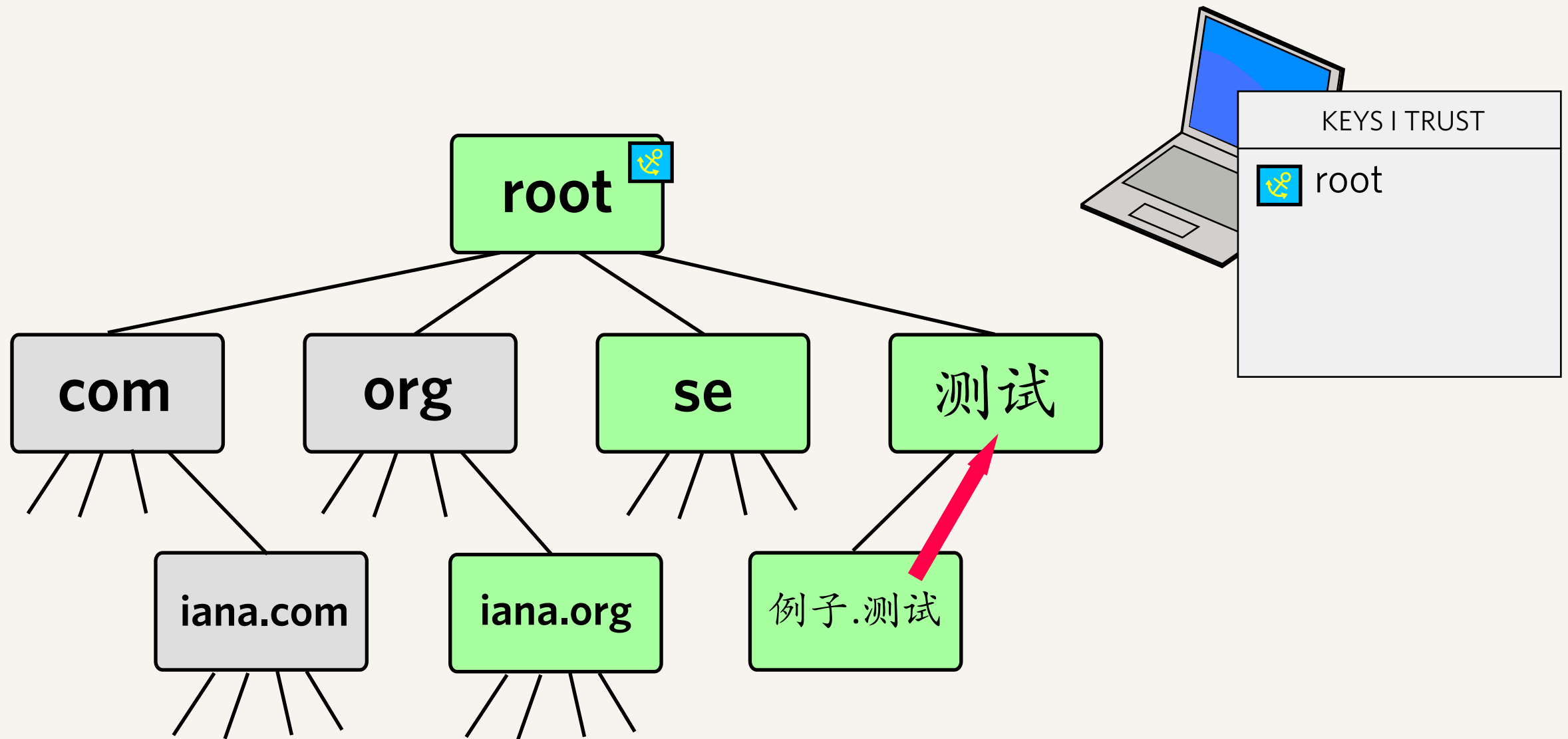
If the root was signed

If the root was signed

If the root was signed

It isn't so there are multiple trust apexes

It isn't so there are multiple trust apexes
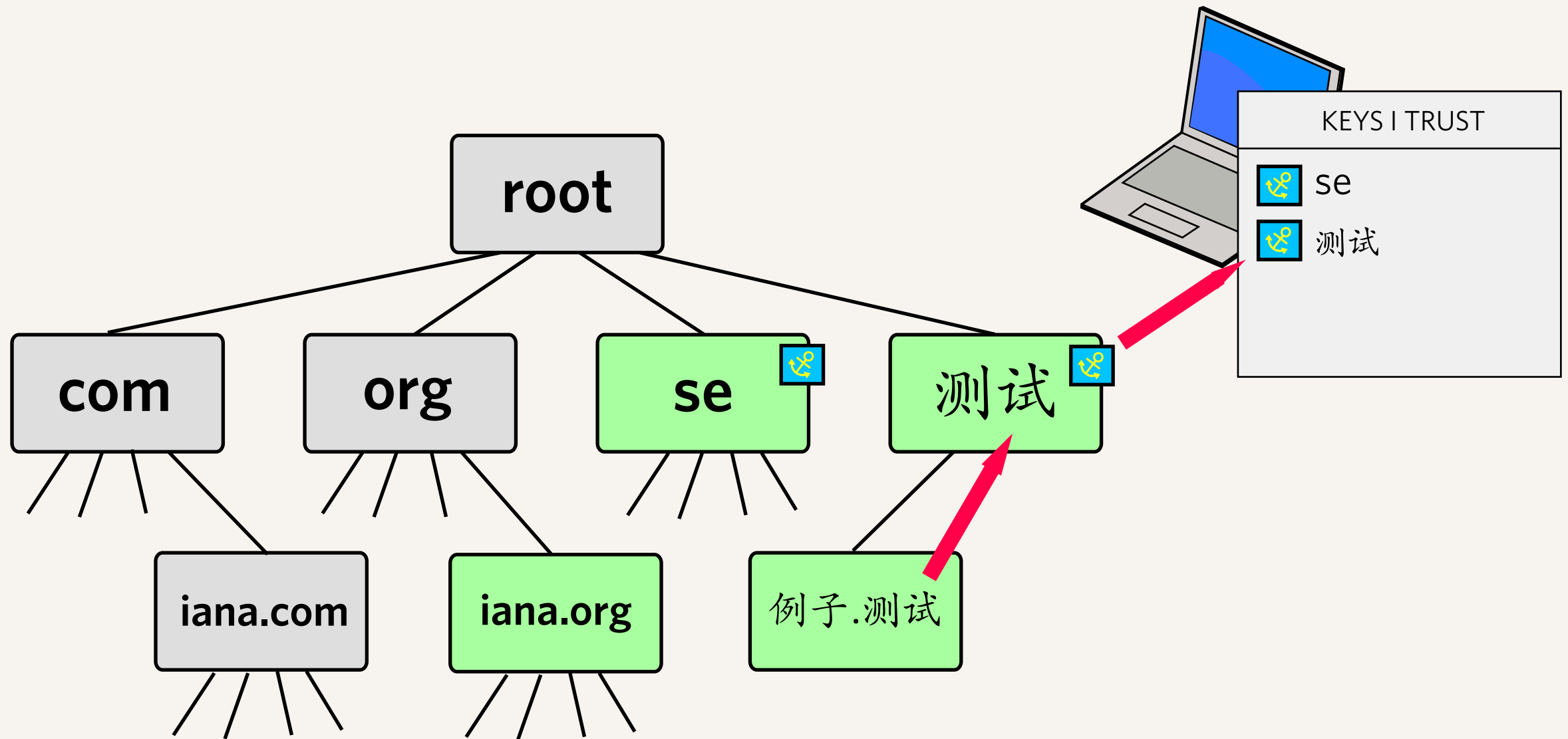
It isn't so there are multiple trust apexes
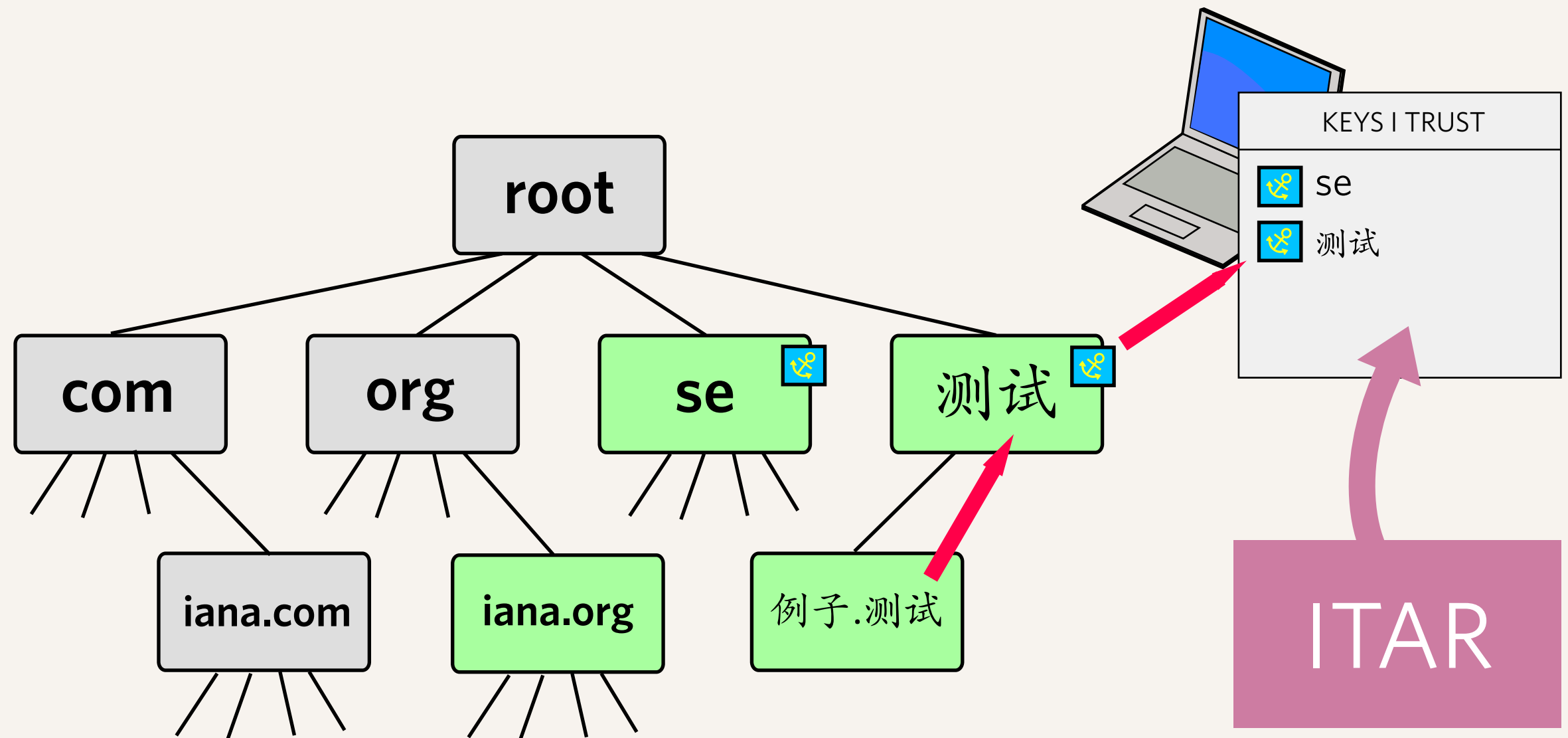
It isn't so there are multiple trust apexes

RIPE Recommendations

1. Different "flavours" of TAs should be supported

2. Implementation neutral, supports common name servers

3. Verify key material is consistent and formatted correctly; Should have secure channel for authenticating requests

4. Process needed to revoke trust anchor, notify users of revocation.

5. Clear declaration of what "support" is available

6. Published exit strategy

7. Keys only published with consent of TLD operator

Supported Keying Material

‣ DNSSEC Key Algorithm

  ‣ RSA/SHA-1 (type 5, see RFC 3110)

‣ DS Record Digest Types

  ‣ SHA-1 (type 1, see RFC 4034)

  ‣ SHA-256 (type 2, see RFC 4509)

Publishing formats

‣ Publication formats

  ‣ List on website

  ‣ XML structured format

  ‣ Master file format

‣ Should work with major software implementations

‣ Formats are plain text and readable so implementors can modify to suit

‣ Implementors should <u>not</u> be putting special ITAR provisions in code — this is meant to go away when the root is signed!

Acceptance Model

‣ TLD operator can submit DS key data via web form

  ‣ DS record validated against DNSKEY data in the DNS

    ‣ Must match before the DS key is made active in the registry.

    ‣ DNSKEY does not need to be in the DNS at time of submission (to allow for pre-deployment), but needs to validate prior to publication.

  ‣ Administrative and Technical contacts for the domain must consent to the listing

Revocation Model

‣ Identical to acceptance model, without the technical test

‣ Optionally a reason can be provided

   ‣ Free text field, URL to an announcement or similar could be used

‣ List of revoked trust anchors will be provided separate to the active trust anchors

iana
Internet Assigned Numbers Authority

Interim Trust Anchor Repository

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.

This repository is maintained using the same trust relationships used to manage the DNS root zone delegations by IANA.

Browse   Master File Format   XML
                MD5 Checksum, PGP Signature   MD5 Checksum, PGP Signature

Maintenance

- Add a trust anchor
- Revoke a trust anchor

Historical

- Revoked keys
- Expired keys

Frequently Asked Questions

What is the ITAR for?
Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

http://itar/add/

iana

Internet Assigned Numbers Authority

Domains   Numbers   Protocols   About IANA

Add a Trust Anchor

Top-level domain operators who have used DNSSEC to sign their zones are invited to list their trust anchors in IANA's Interim Trust Anchor Repository. To successfully list a trust anchor, both the administrative and technical contacts for a domain must consent to the listing (as listed in IANA's root zone database). Matching DNSKEYs are also required to be in the secure domain's zone, however this does not need to be done straight away.

Applicant

Please provide the DNSSEC-signed domain to be listed in the repository. You may also provide and email address so that we may communicate to you the status of your request, as well as ask for any additional information.

Secured Domain

The interim trust anchor repository is limited to top-level domains such as "COM" and "SE".

Contact Email
(optional)

This email address will be informed of updates to this request.

Trust Anchor Details

The trust anchor itself is comprised of the attributes of a Delegation Signer (DS) key. These components are derived from the key that is used to sign the zone.

Key Tag

The key tag of the trust anchor to be listed.

Key Digest

The complete key digest of the trust anchor to be listed.

Key Digest

The complete key digest of the trust anchor to be listed.

Key Algorithm   RSA/SHA-1

The encryption algorithm used to compute the key.

Digest Type   SHA-1

The hash digest algorithm used to compute the trust anchor.

Listing Details

These periods are used to determine how and when the trust anchor is listed in the repository. Typically keys are only used for discrete periods of time, with multiple keys overlapping in validility. These times will help plan the listing of the keys in the repository. Dates can be entered in a number of formats, such as **YYYY-MM-DD** or **YYYY-MM-DD HH:MM:SS**.

Effectivity Period   From

Until

The period the key will be valid for.

Listing Period   From

Until

The period to list the key in the trust anchor repository.

Listing Password
(optional)

Protects this listing from revocation from those who do not know this password.

Review Form

Please review the material supplied above. Once you are happy with the supplied data submit the form and the details will be verified.

Submit — Submit these details for verification.

Cancel — Cancel the listing process.

iana
Internet Assigned Numbers Authority

Domains   Numbers   Protocols   About IANA

List of Trust Anchors

The following is a list of DNSSEC trust anchors supplied by top-level domain operators. These anchors have been authorised by the operators of these domains, as validated by IANA.

Domain	Trust Anchors
.テスト	🔑 **23512** 5 1 ed8b55b510fccc5c95ed5ff2c668320af00a33de 2008-10-27 06:04:58 → 2009-12-31 23:59:59
	🔑 **23512** 5 2 2e57aa1baabe0e56f5f79d7eb72ffae8442de6058eb2c7de604cc2eae9e887fc 2008-10-27 06:06:38 → 2009-12-31 23:59:59
.SE	🔑 **6166** 5 1 CE2B007F6D000B064B4A82E8840C19D3D09B8F8E 2008-09-22 00:00:00 → 2008-12-31 00:00:00

About
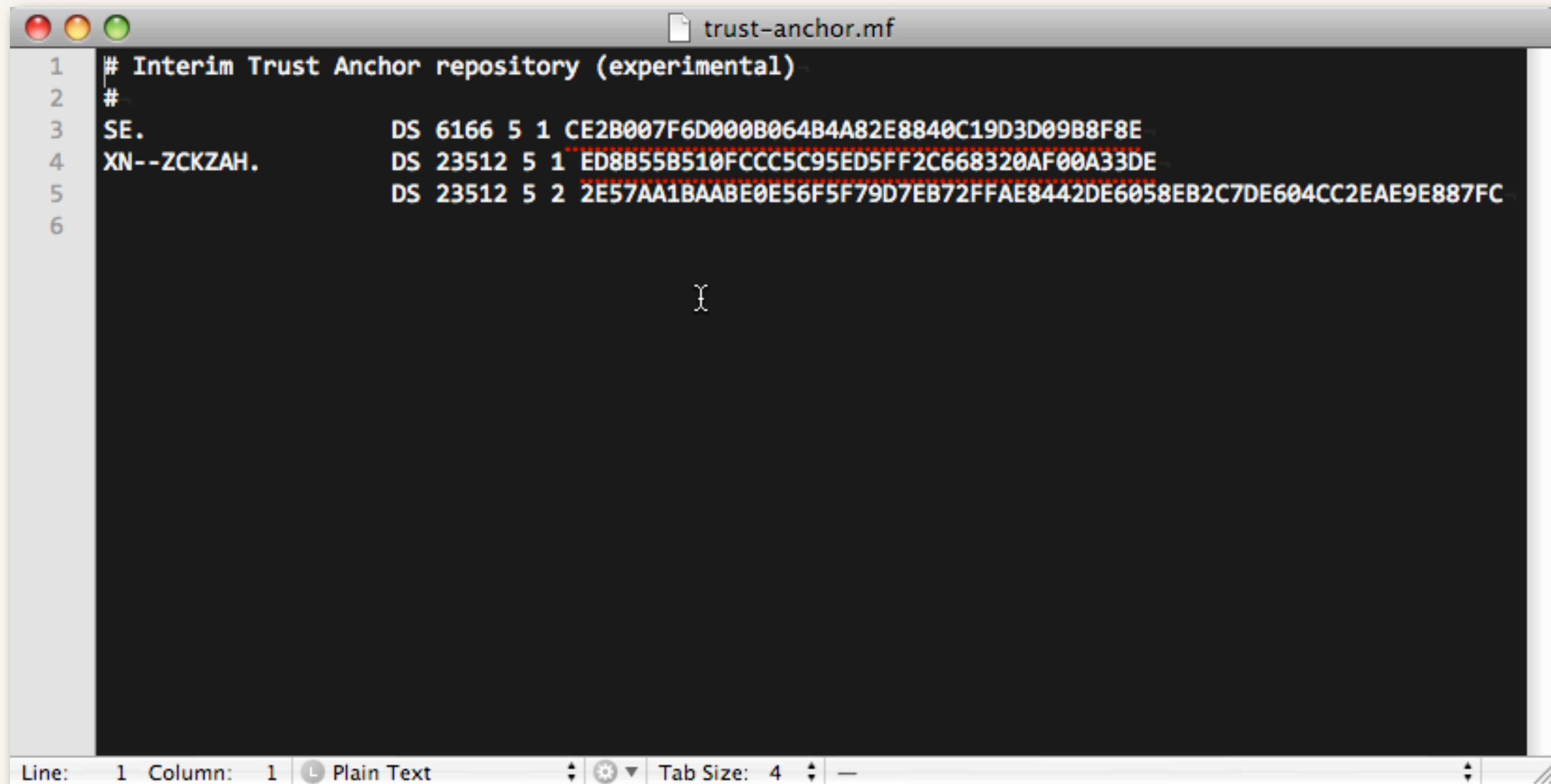Presentations
Performance
Reports
Projects
Site Map

Domains
Root Zone
.INT
.ARPA
IDN Repository

Protocols

Number Resources
Abuse Information

ICANN

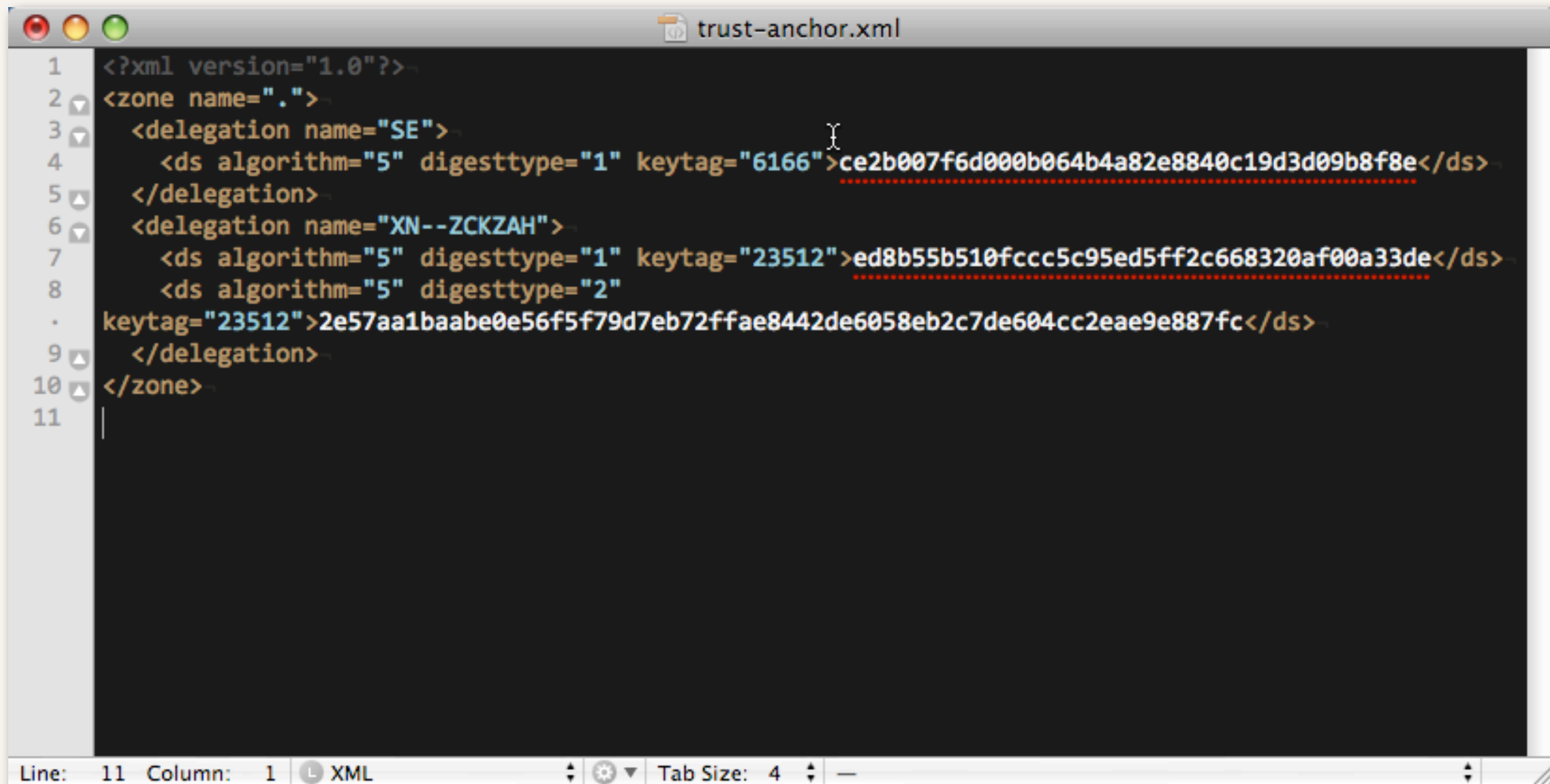IANA is operated by the
Internet Corporation for Assigned Names and Numbers

```
# Interim Trust Anchor repository (experimental)
#
SE.             DS 6166 5 1 CE2B007F6D000B064B4A82E8840C19D3D09B8F8E
XN--ZCKZAH.     DS 23512 5 1 ED8B55B510FCCC5C95ED5FF2C668320AF00A33DE
                DS 23512 5 2 2E57AA1BAABE0E56F5F79D7EB72FFAE8442DE6058EB2C7DE604CC2EAE9E887FC
```

Trust Anchors as master file

```xml
<?xml version="1.0"?>
<zone name=".">
  <delegation name="SE">
    <ds algorithm="5" digesttype="1" keytag="6166">ce2b007f6d000b064b4a82e8840c19d3d09b8f8e</ds>
  </delegation>
  <delegation name="XN--ZCKZAH">
    <ds algorithm="5" digesttype="1" keytag="23512">ed8b55b510fccc5c95ed5ff2c668320af00a33de</ds>
    <ds algorithm="5" digesttype="2"
keytag="23512">2e57aa1baabe0e56f5f79d7eb72ffae8442de6058eb2c7de604cc2eae9e887fc</ds>
  </delegation>
</zone>
```

Trust Anchors as XML

Availability

‣ Open to top-level domain operators this week

   ‣ Asked to play with it for a week or so, try revoking etc.

   ‣ System will then be reset to contain only valid records

   ‣ Implement any recommendations

‣ Public availability

Signed Root Zone

Signing the root zone

‣ ICANN's strategic plan is to be "operationally ready"

   ‣ Signed root test bed operating for over a year

   ‣ System is built with advise from current DNSSEC operators, and many other experts in both DNS and cryptography

   ‣ ICANN already signs 11 top-level domains operationally, and incrementally signing the last remaining zones under our control

Signing the root zone

‣ ICANN developed a proposal to sign the root zone which was submitted to US Government

‣ VeriSign followed up with a different proposal to sign the root zone

‣ The US Government has issued a "Notice of Inquiry" to seek views relating to signing the DNS root zone, which is open to comments until November 24.

  ‣ http://tinyurl.com/3v8akt

ACTION: Notice of Inquiry

SUMMARY: The Department of Commerce (Department) notes the increase in interest among government, technology experts and industry representatives regarding the deployment of Domain Name and Addressing System Security Extensions (DNSSEC) at the root zone level. The Department remains committed to preserving the security and stability of the DNS and is exploring the implementation of DNSSEC in the DNS hierarchy, including at the authoritative root zone level. Accordingly, the Department is issuing this notice to invite comments regarding DNSSEC implementation at the root zone.

DATES: Comments are due on November 24, 2008.

ADDRESSES: Written comments may be submitted by mail to Fiona Alexander, Associate Administrator, Office of International Affairs, National Telecommunications and Information Administration, U.S. Department of Commerce, 1401 Constitution Avenue, N.W., Room 4701, Washington, DC 20230. Written comments may also be sent by facsimile to (202) 482–1865 or electronically via electronic mail to DNSSEC@ntia.doc.gov. Comments will be posted on NTIA's website at http://

Internationalised Country Code Domains

The challenge

‣ Country-code top-level domains are limited to 2-letter ASCII codes listed in the ISO 3166-1 standard

  ‣ This is great — IANA does not make political decisions on country recognition, selecting country codes, etc.

‣ This is terribly inconvenient for populations who don't use Latin-based characters

‣ There is general recognition there should be internationalised country-codes available for these countries

The problems

‣ There is no equivalent of ISO 3166-1 in other scripts

‣ ICANN's formal Policy Development Process is likely to take several years

‣ Driven by demand, some communities are using plugins or alternate roots to patch in domains, which lack universal resolvability

The solution

‣ A "fast track" process for countries which are:

  ‣ Listed in the ISO 3166-1 standard

  ‣ Have a demonstrated need for a TLD in a non-Latin script, in a country's official language

  ‣ Have a non-contentious proposal for a country translation as a top-level domain, supported by government

‣ Apart from string selection, qualifications are the same as existing country-code domains as applied by IANA

How it is being rolled out

‣ A draft implementation plan has been released for discussion and comment

‣ ICANN has surveyed governments and existing ccTLD operators for their interest in the fast track

‣ http://tinyurl.com/6rcezx

‣ The ICANN Board would need to approve the final implementation to move forward

New Generic Top-Level Domains

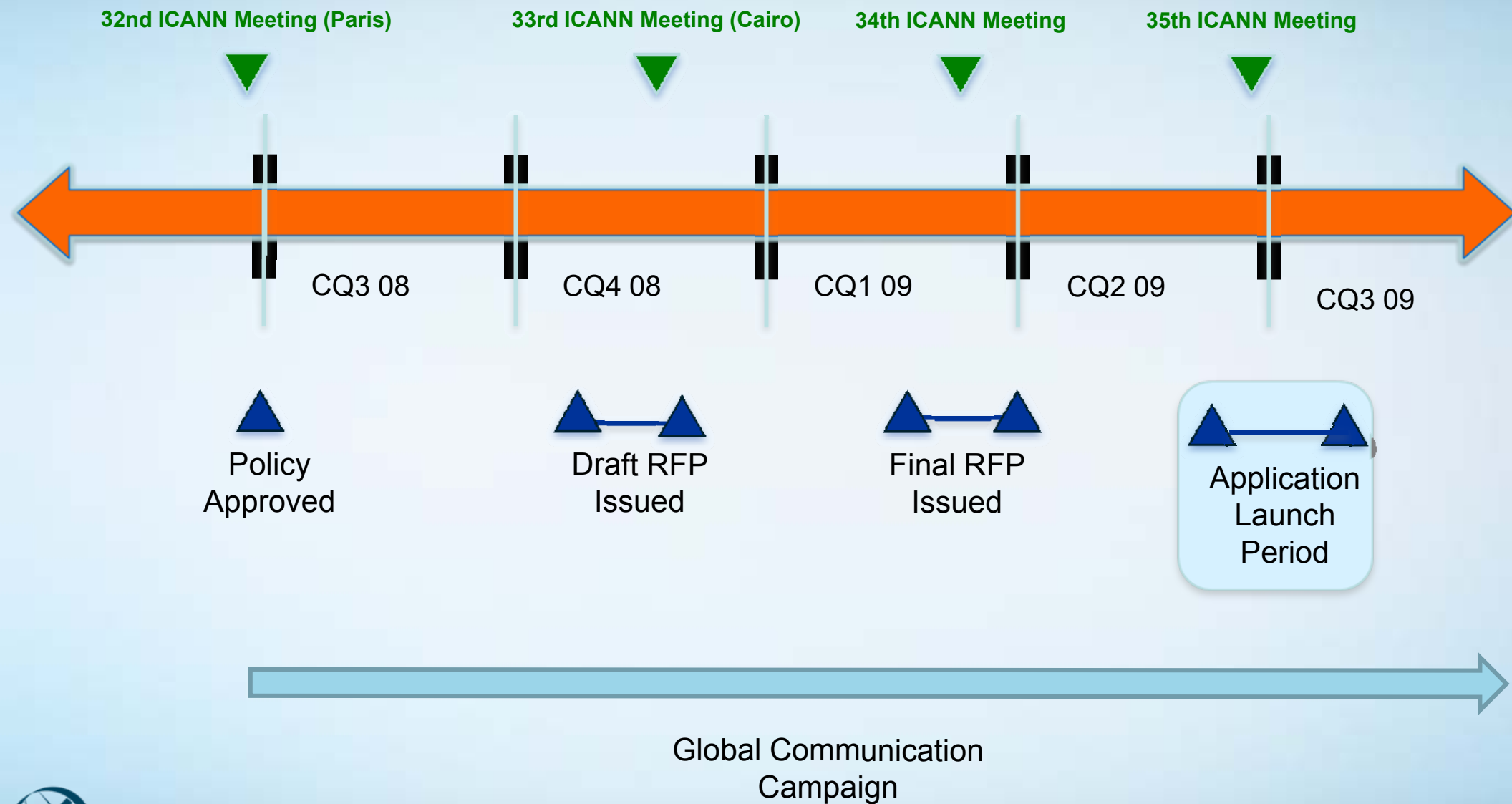# History

‣ ICANN has had two rounds of accepting applications for new GTLDs:

    ‣ 2000 — New Generic Top-Level Domains (resulting in .BIZ, .INFO, etc.)

    ‣ 2004 — New Sponsored Top-Level Domains (resulting in .TEL, .MOBI, etc.)

‣ Both have been one off events with their own rules for application.

The proposal

‣ Develop new qualifying criteria that will allow for perennial application periods

    ‣ The process can be repeated moving forward

‣ Make the rules and acceptance criteria clear from the beginning

Thanks!

kim.davies@icann.org