Interim Trust Anchor Repository

Paris, France
June 2008

Kim Davies
Internet Assigned Numbers Authority

ICANN
Internet Corporation for
Assigned Names & Numbers

‣ Whereas, in the interests of aiding DNSSEC deployment, the ICANN board believes that DNSSEC trust anchors for Top Level Domains should be made available conveniently to the DNS community.

‣ It is **hereby resolved** that the Board instructs IANA staff, as an interim measure, to create and maintain a Registry of DNSSEC trust anchors for Top-Level Domains until such time as the root zone is DNSSEC signed.

30 April 2008

What is the ITAR?

‣ 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

‣ ICANN Board voted to implement in April 2008, based on community requests
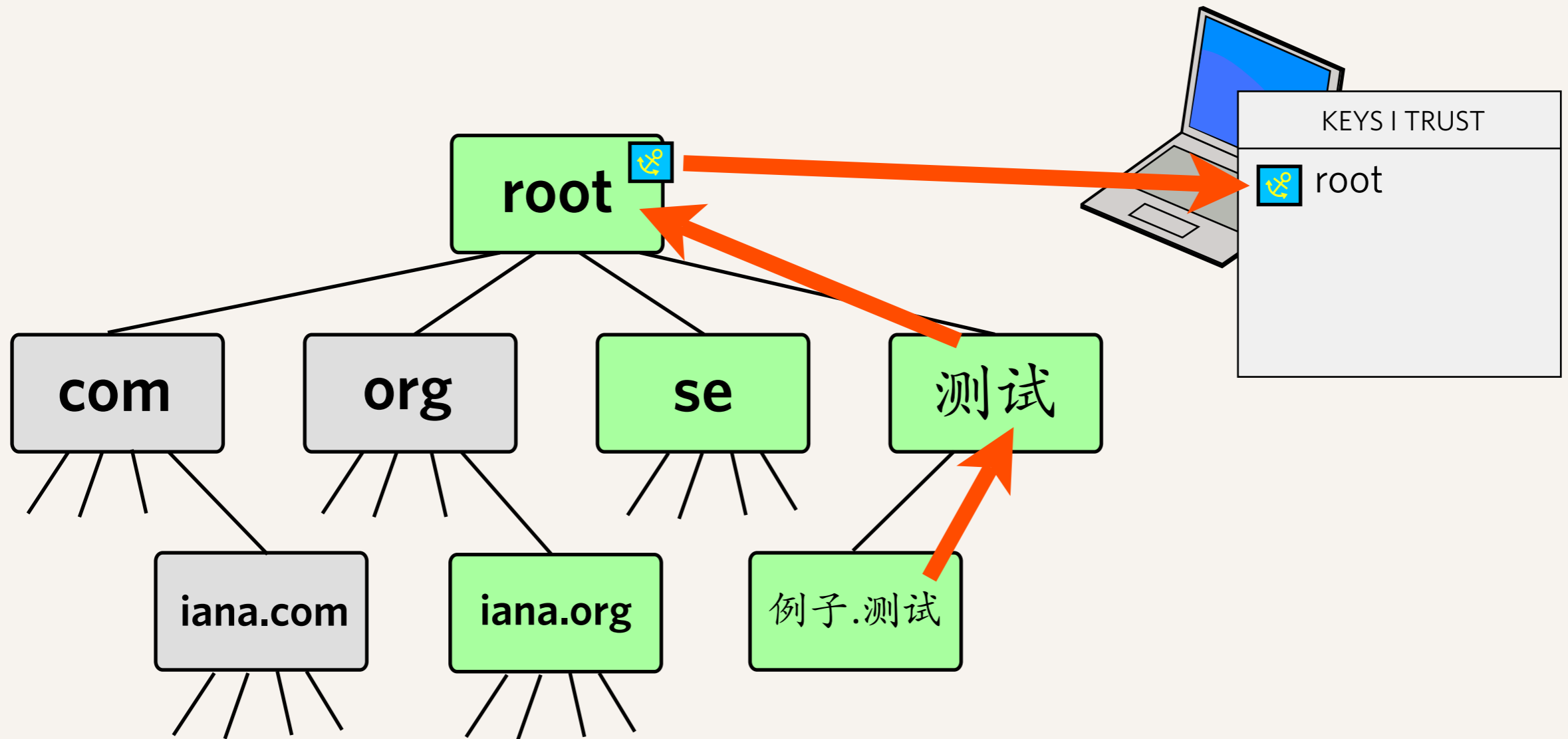
If the root was signed
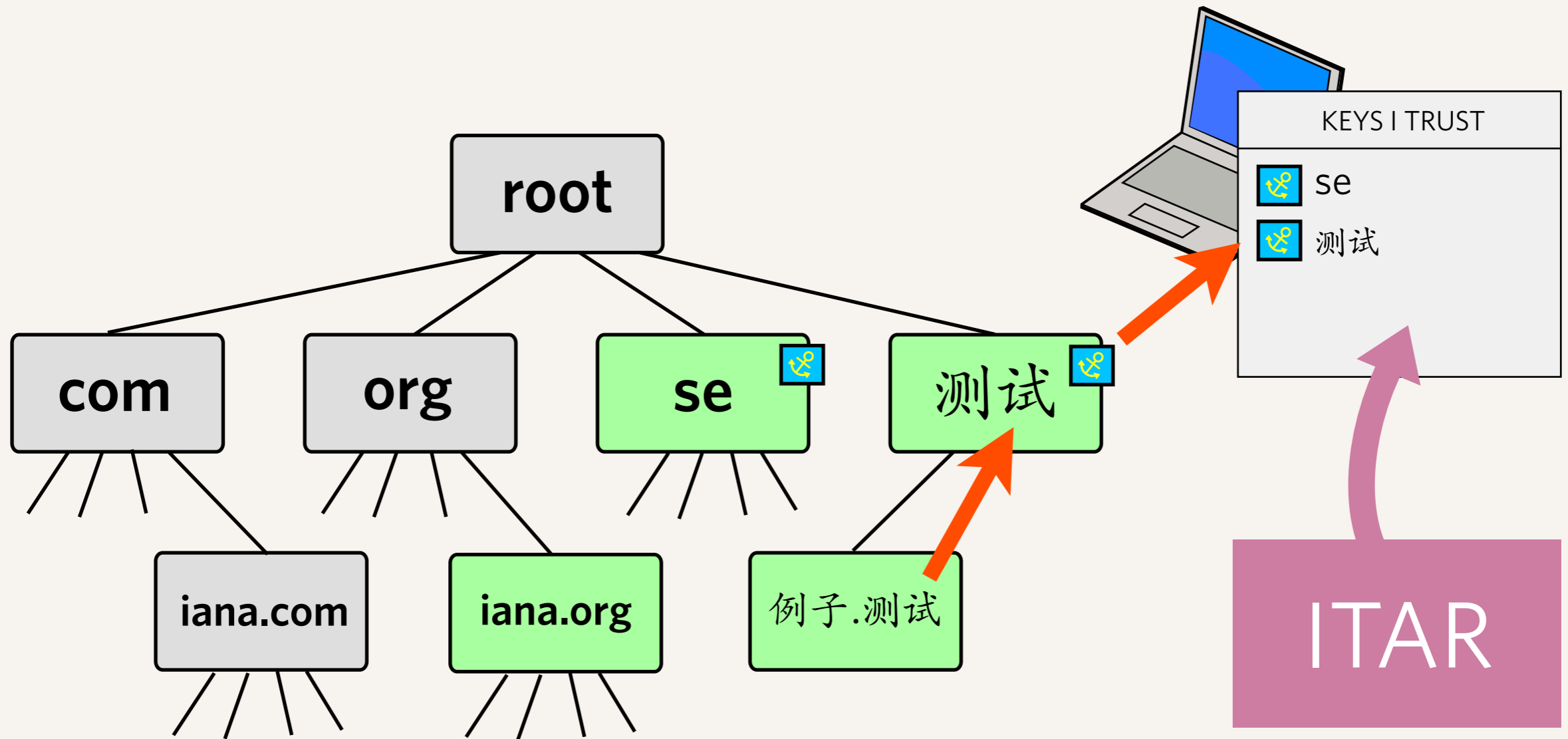
It isn't so there are multiple trust apexes

Proposed registry details

‣ Supports different types of DNSSEC signing

   ‣ DS hashes either SHA-1 or SHA-256

   ‣ DNSKEYs in any algorithm (agnostic implementation)

‣ Published in number of formats

   ‣ List on website; XML structured format; Master file format

   ‣ Should work with major software implementations

   ‣ 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

Removal Model

‣ Identical to acceptance model, without the technical test

‣ List of revoked trust anchors will be provided

Exit Strategy

‣ ITAR will be decommissioned within x days of the DNS root being signed.

Limitations

‣ The ITAR will only operate for top-level domains

  ‣ i.e. the keying information that would otherwise go in the root.

  ‣ IANA will not accept anchors for descendants of top-level domains

    ‣ Even if the relevant TLD is not signed

Why are we doing this?

‣ There is interest in having the DNS root zone signed with DNSSEC

‣ There are many unanswered questions that inhibit deployment

   ‣ "Layer 9" issues — political, etc.

‣ IANA has had an operational testbed for some time signing the root zone

   ‣ Aim is to be operationally ready once policy is set

‣ ITAR will assist early-adopters utilise the technology until root signing is solved

Thanks!

kim.davies@icann.org