

# Interim Trust Anchor Repository

Mexico City, Mexico

March 2009

Kim Davies

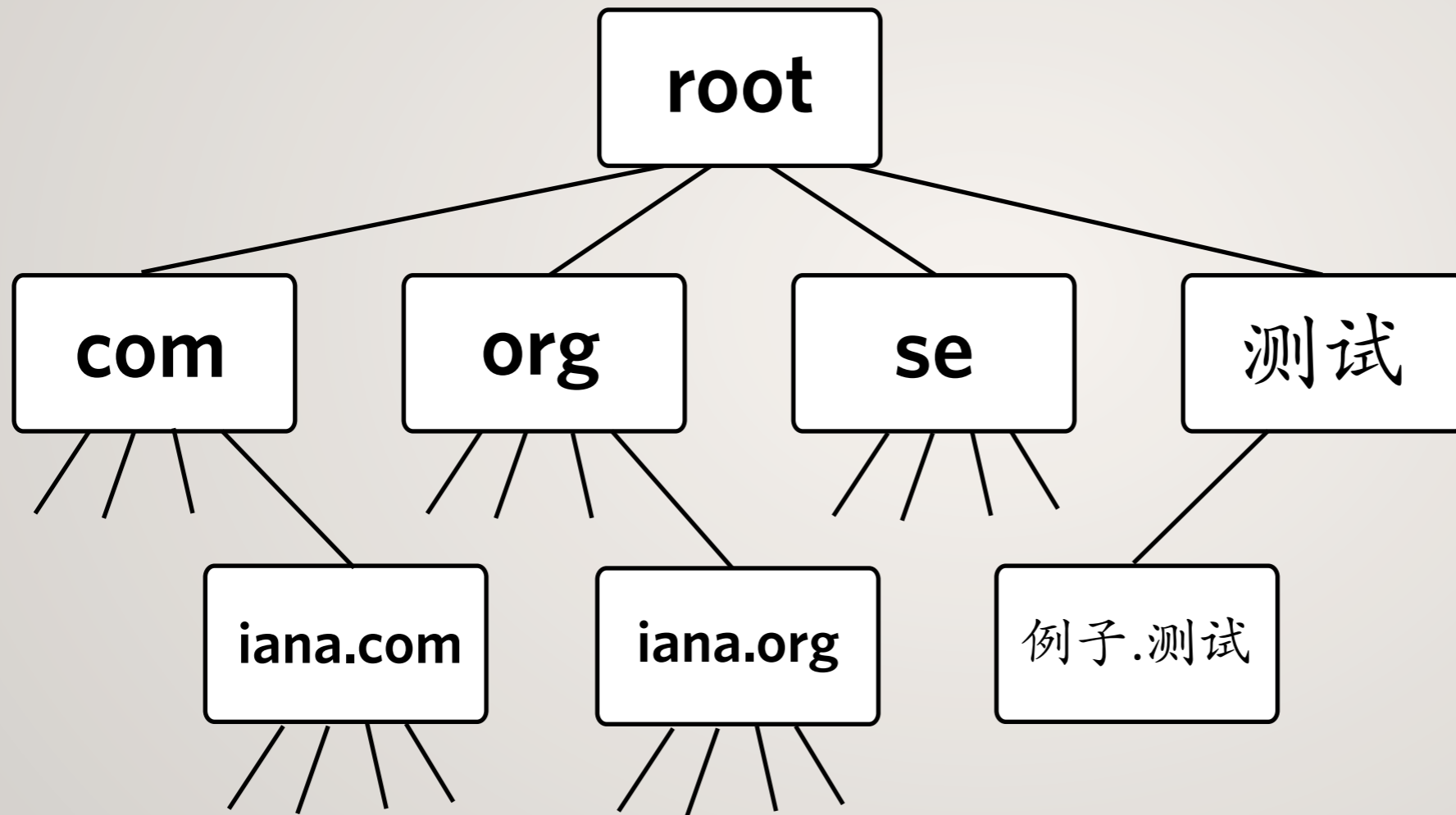
Manager, Root Zone Services

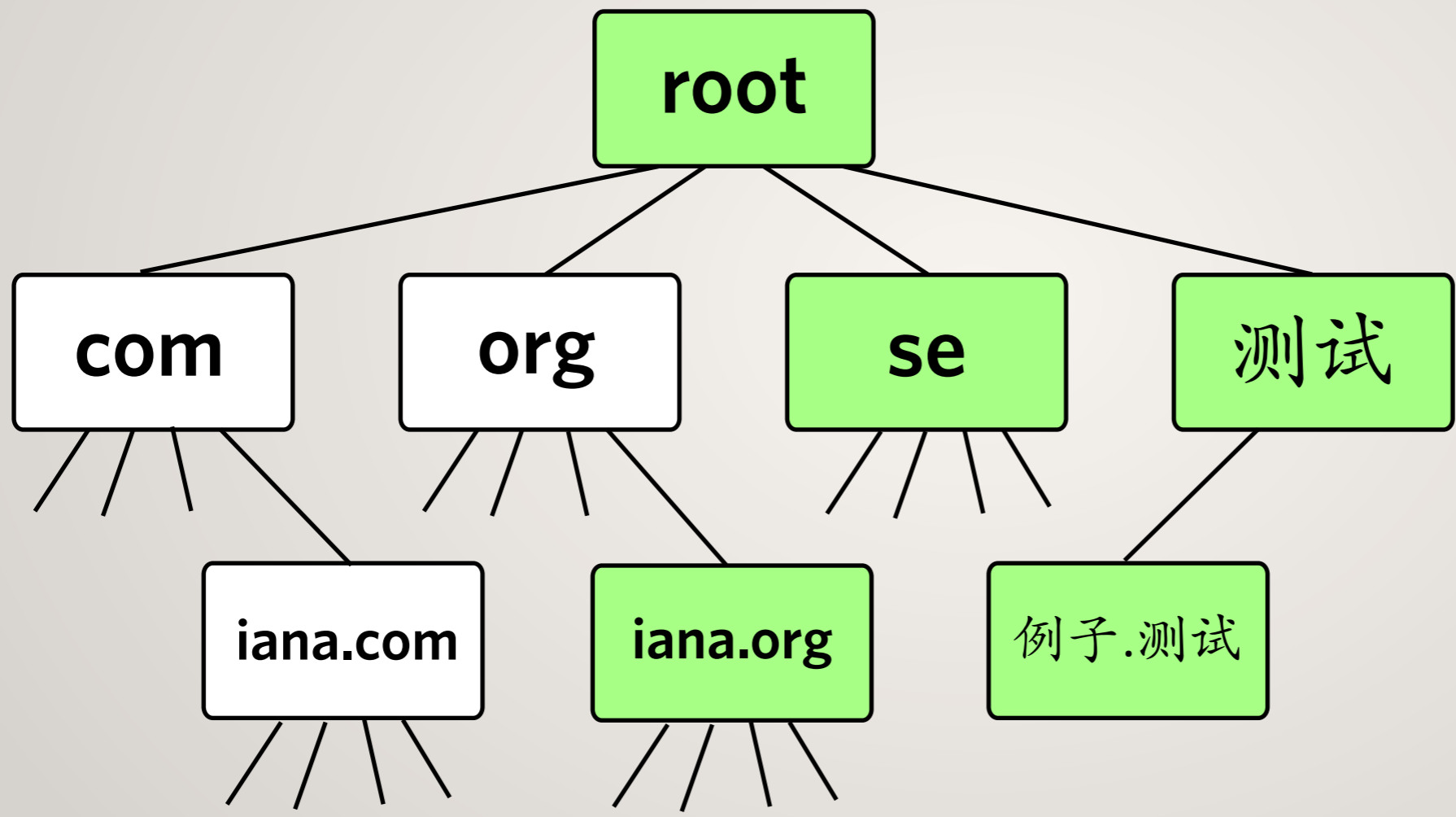


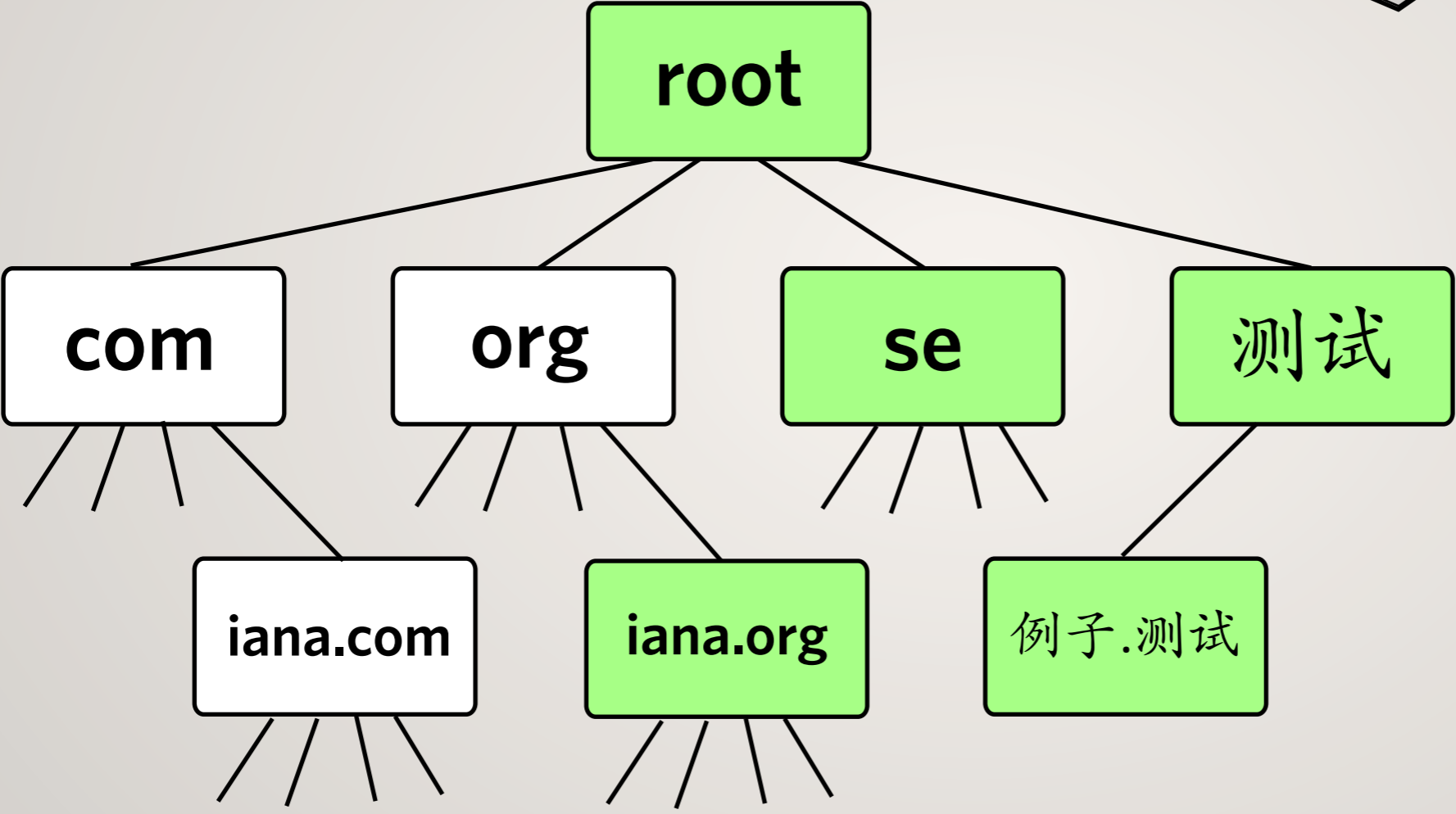
Internet Corporation for  
Assigned Names & Numbers

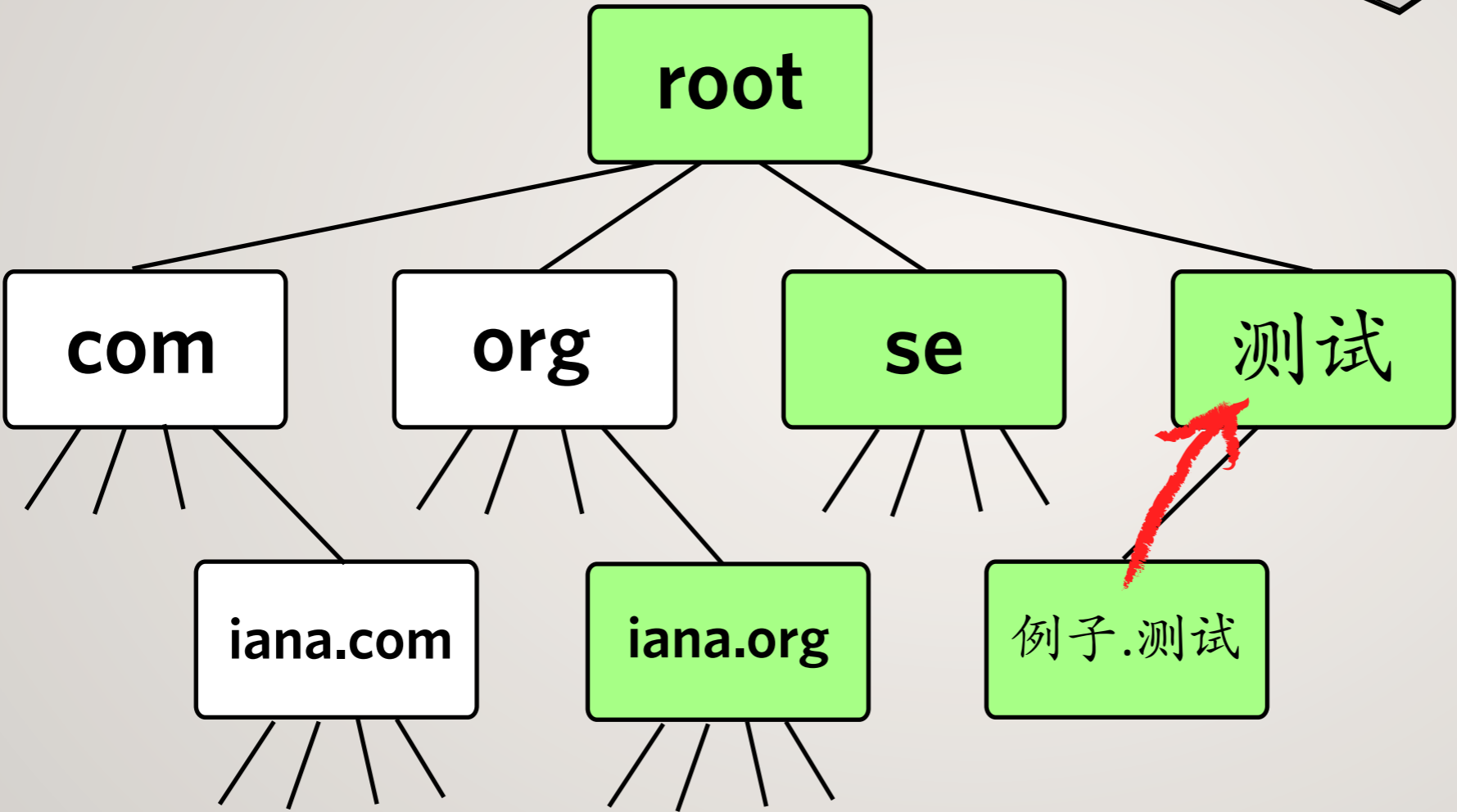
# Interim Trust Anchor Repository

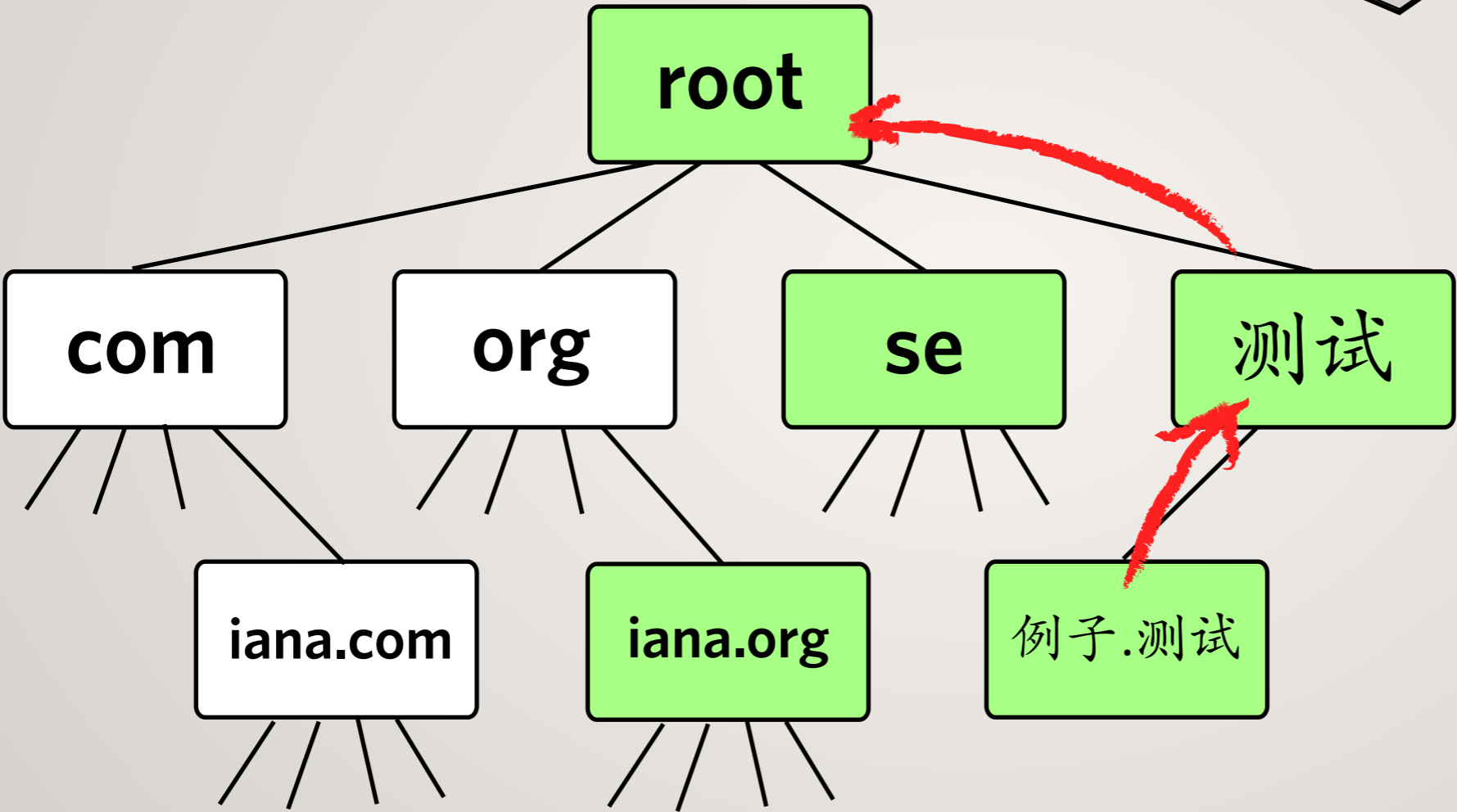
- ▶ A mechanism to publish keys of top-level domains that currently implement DNSSEC
- ▶ If the root zone is DNSSEC signed, such a repository is unnecessary
  - ▶ Therefore this is a stopgap measure
  - ▶ Should be decommissioned when the root is signed






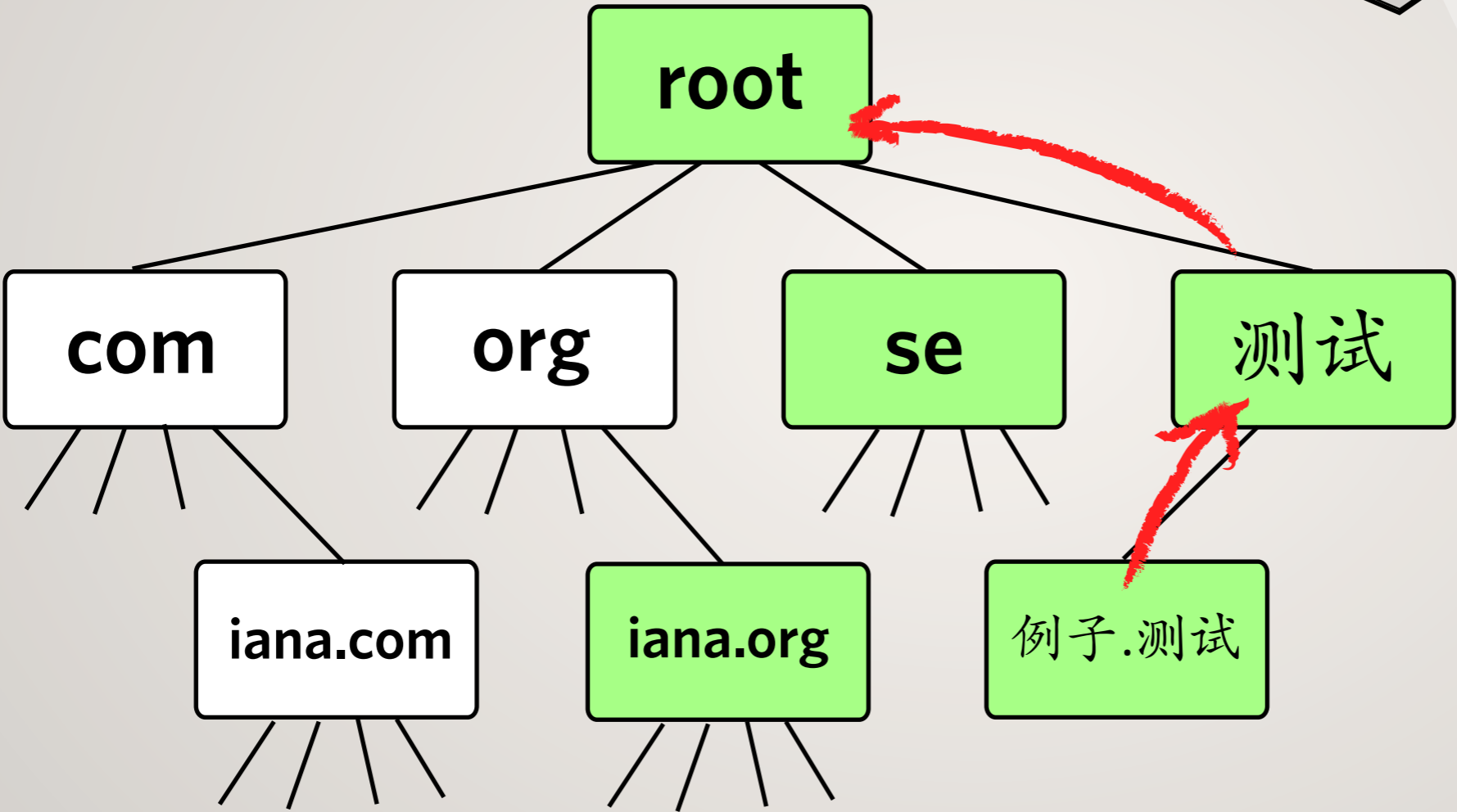




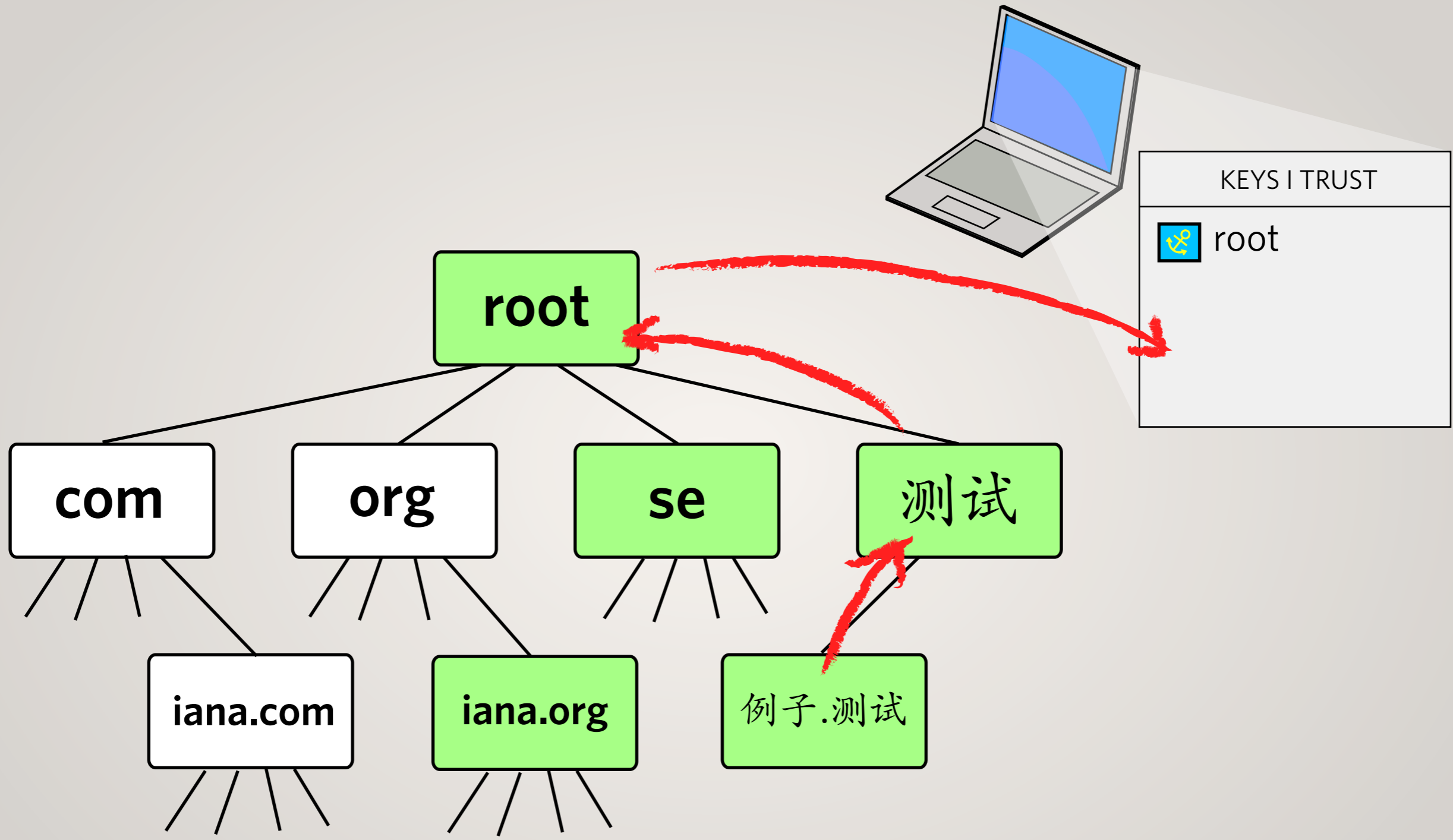


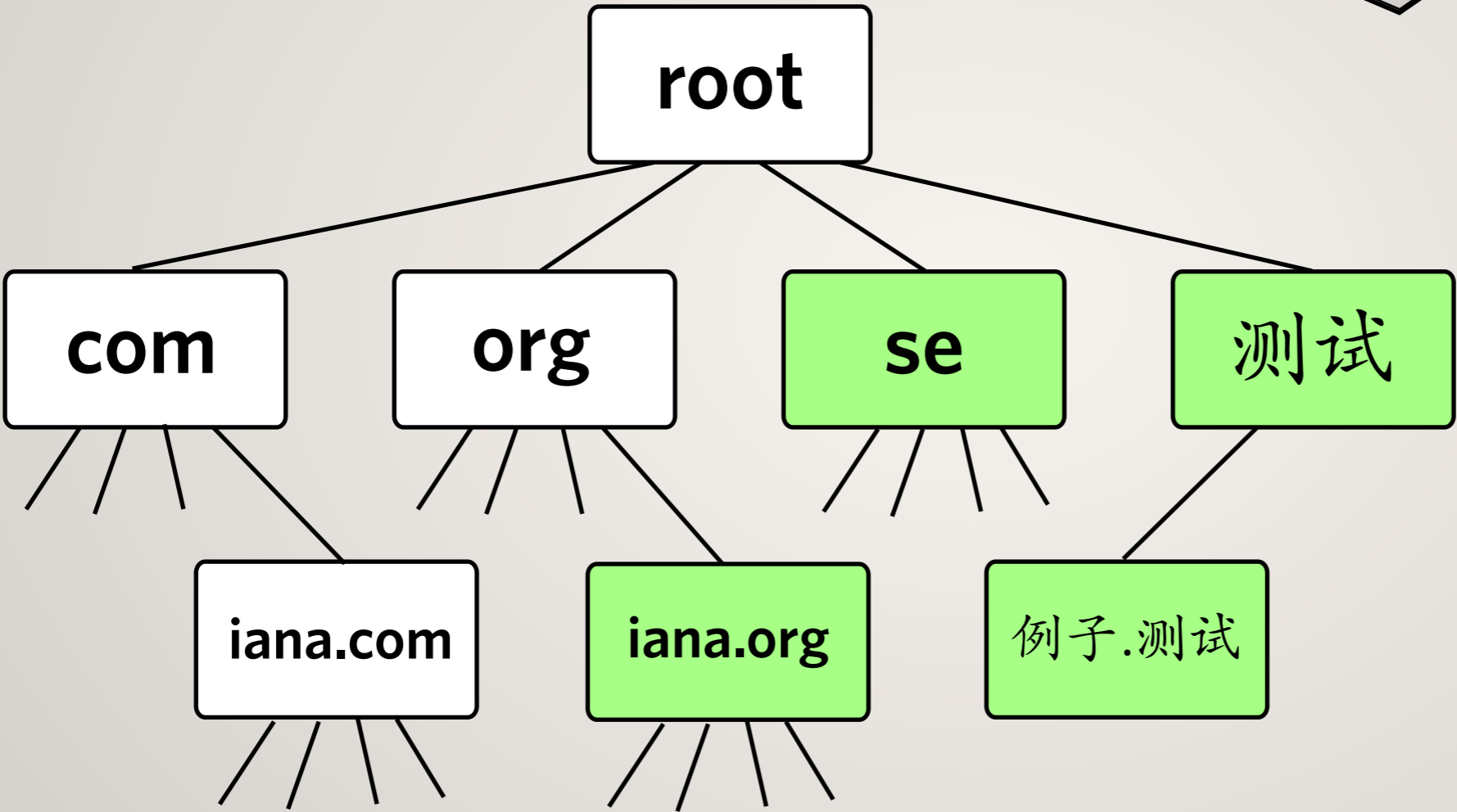


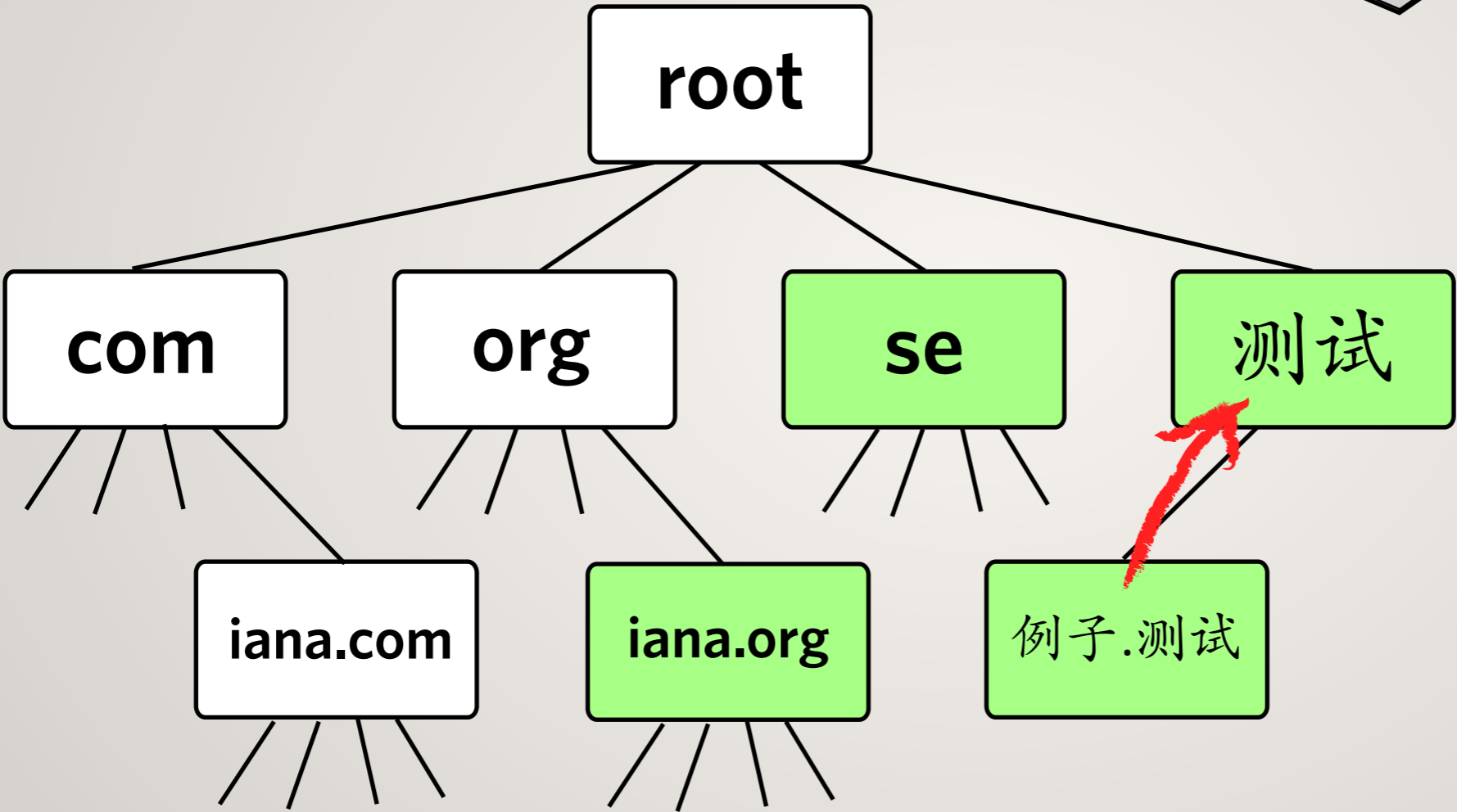
KEYS I TRUST	
	root

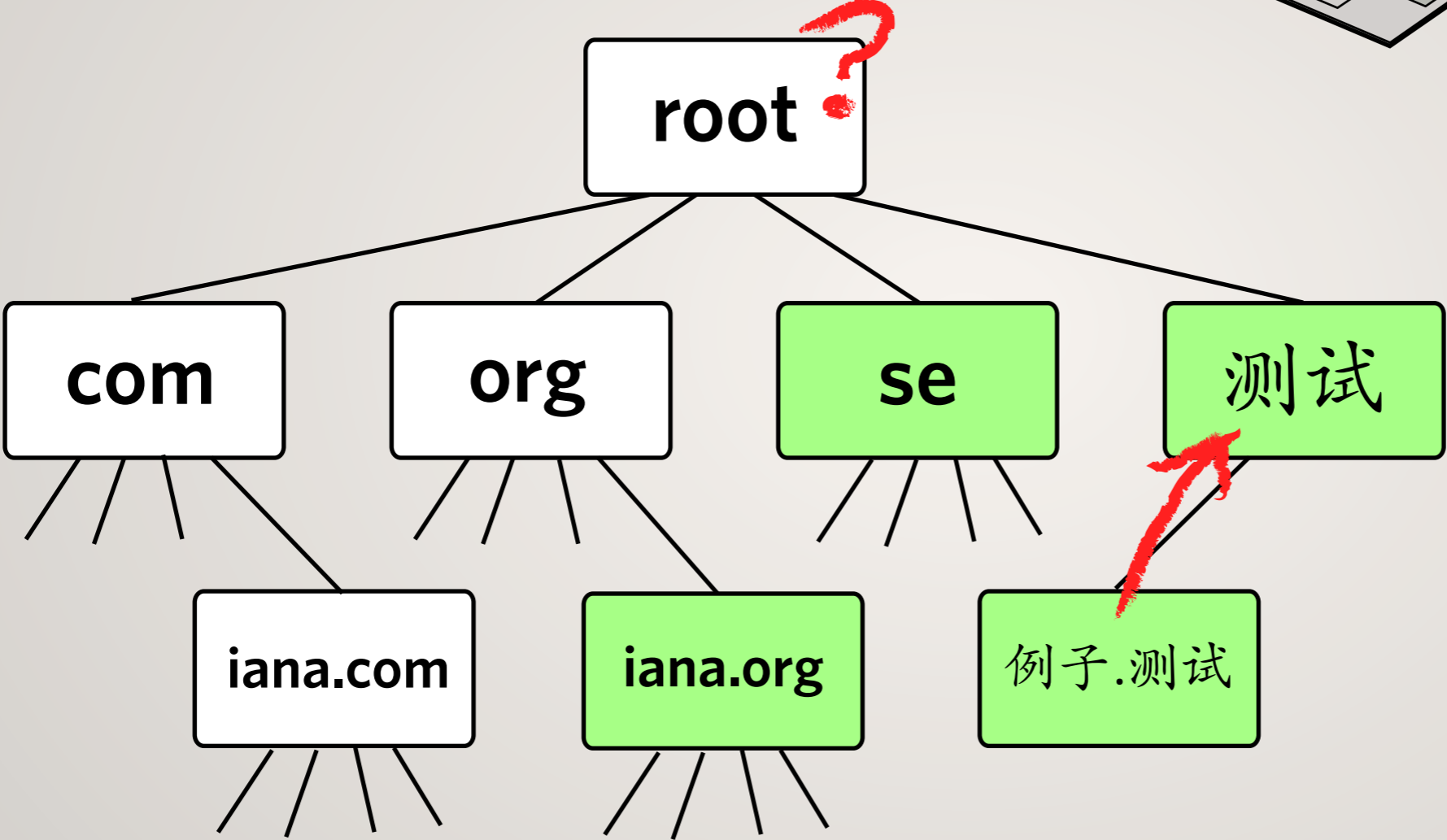


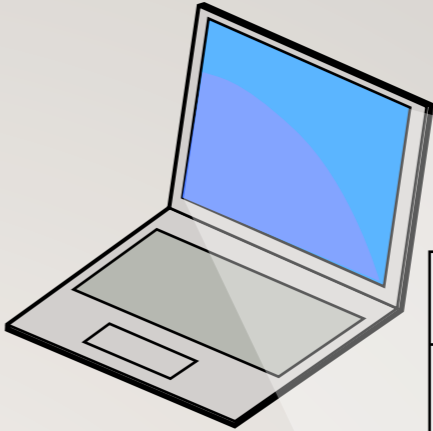




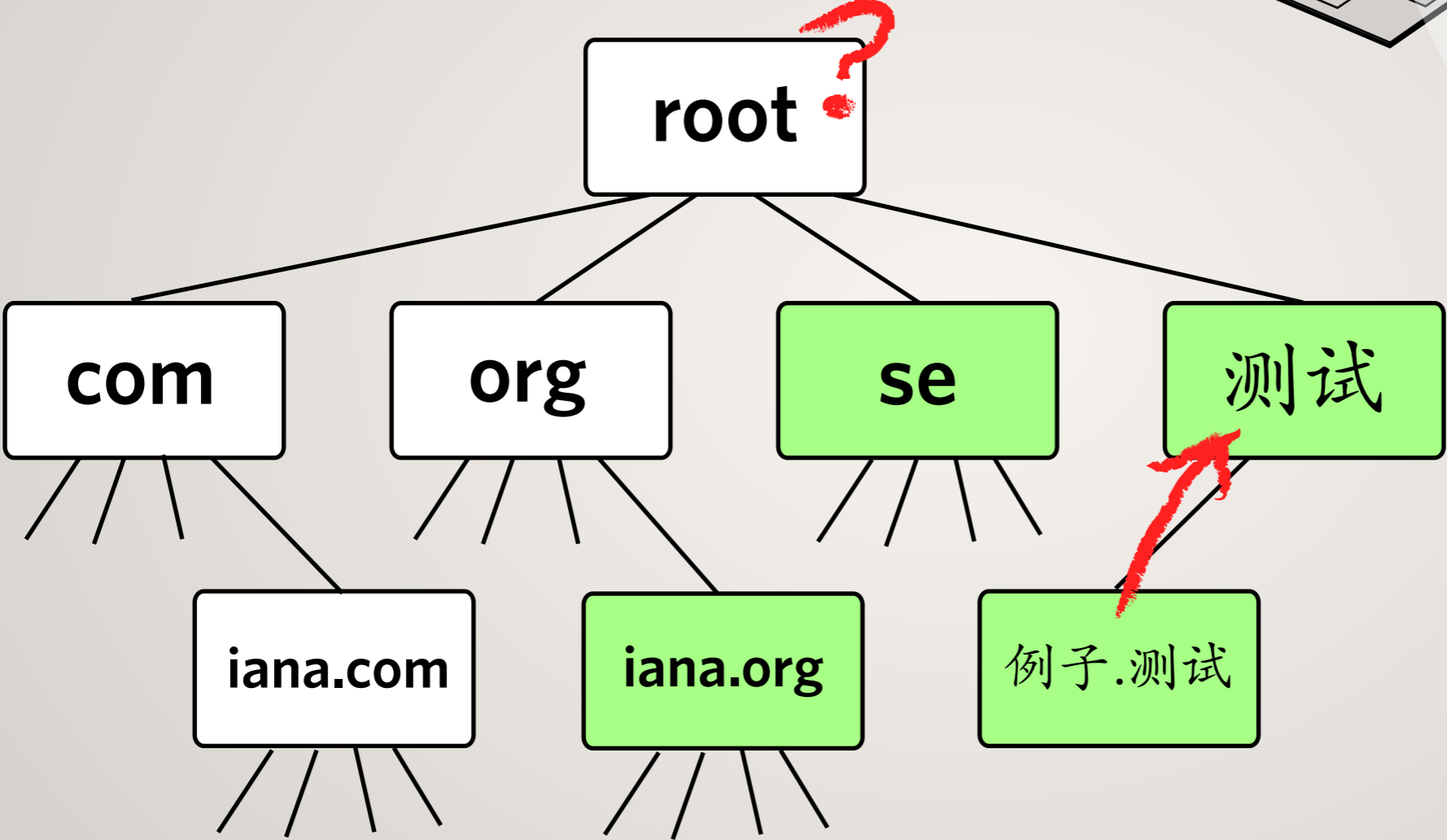






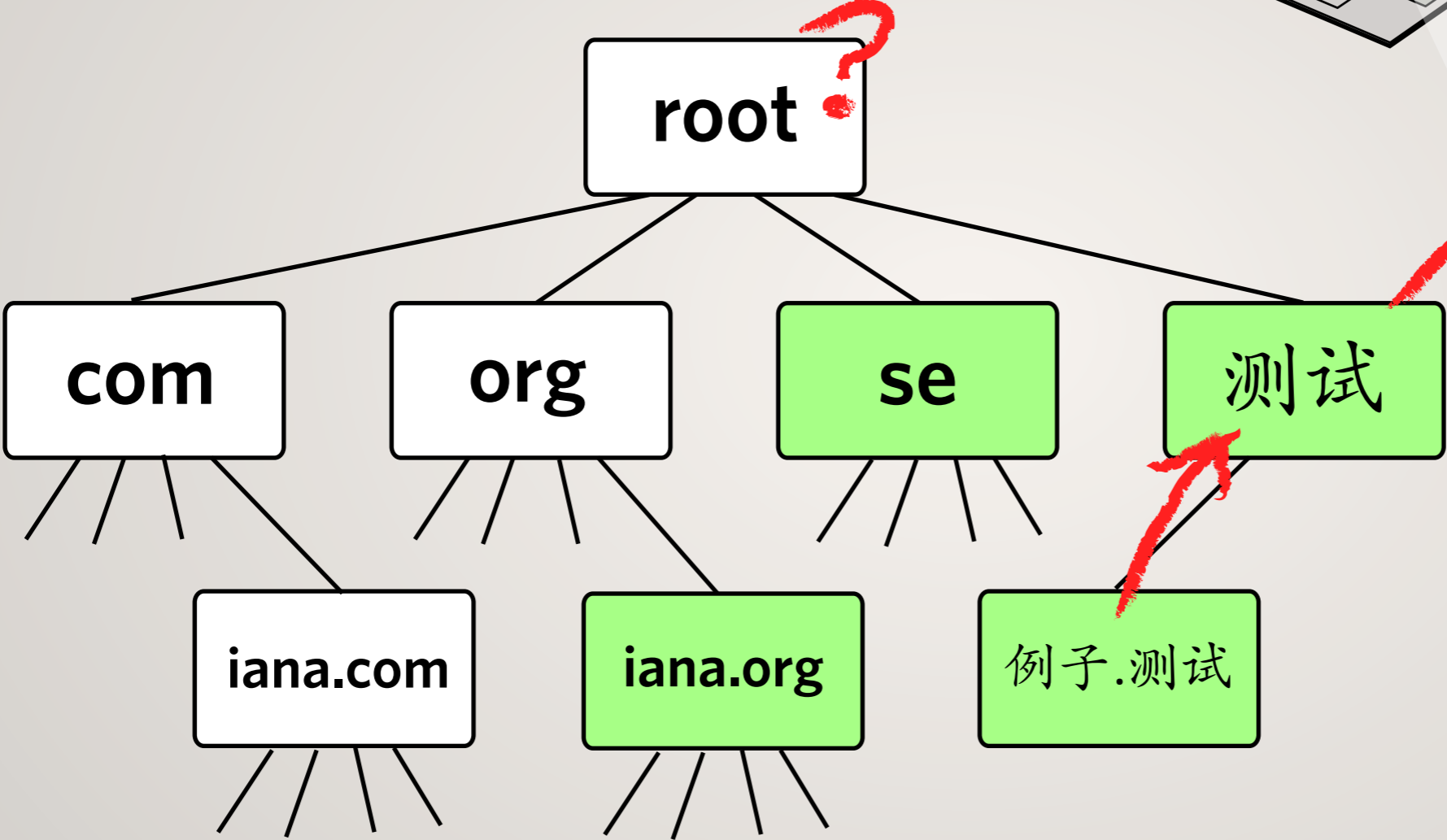


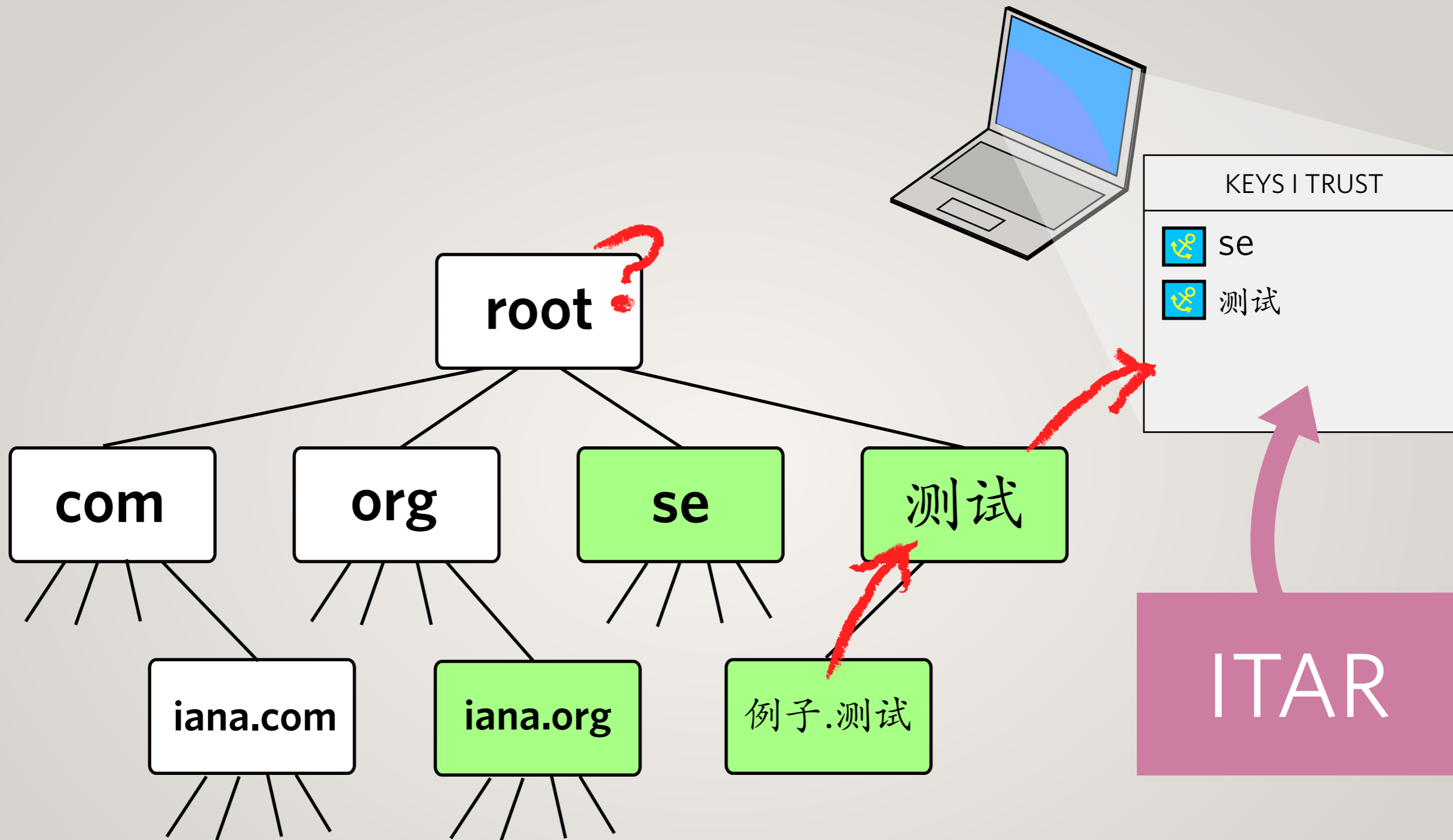
KEYS I TRUST	
	se
	测试





KEYS I TRUST	
	se
	测试








# Benefits

- ▶ Fully meets a set of recommendations provided by RIPE
- ▶ Simple to use for both top-level domain operators, and end users.
- ▶ Works with different DNS software, different protocols, etc.  
Non proprietary.
- ▶ Almost fully automated
- ▶ Helps DNSSEC deployment



IANA — Interim Trust Anchor Repository

https://itar.iana.org/ ICANN(Internet Corporation for ... Google



Internet Assigned Numbers Authority

Domains Numbers Protocols About IANA

Domains

## 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](mailto: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 contents. During initial testing we are using a PGP key with ID [81D464F4](#).


[Browse the trust anchor repository](#)


Download the trust anchors

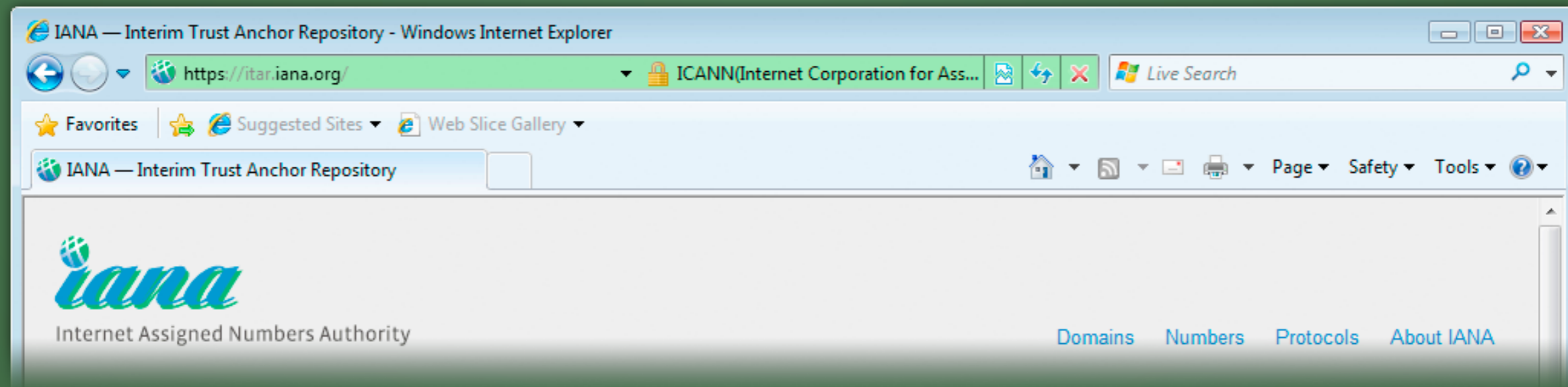
[Master File Format](#) ▶  
MD5, SHA1, PGP Signature

[XML](#) ▶  
MD5, SHA1, PGP Signature

[How to use](#) ▶  
[Processes and Procedures](#) ▶

 [Add a trust anchor](#) ▶

 [Revoke a trust anchor](#) ▶



[itar.iana.org](http://itar.iana.org)





Thanks!

[kim.davies@icann.org](mailto:kim.davies@icann.org)