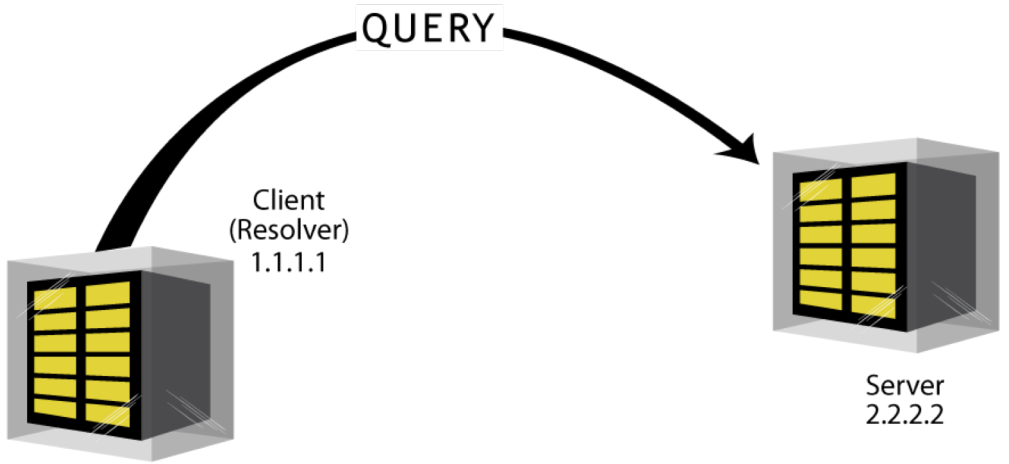
Increasing DNS Security with DNSSEC

Matt Larson
VP of Research, Office of the CTO, ICANN

22 October 2018

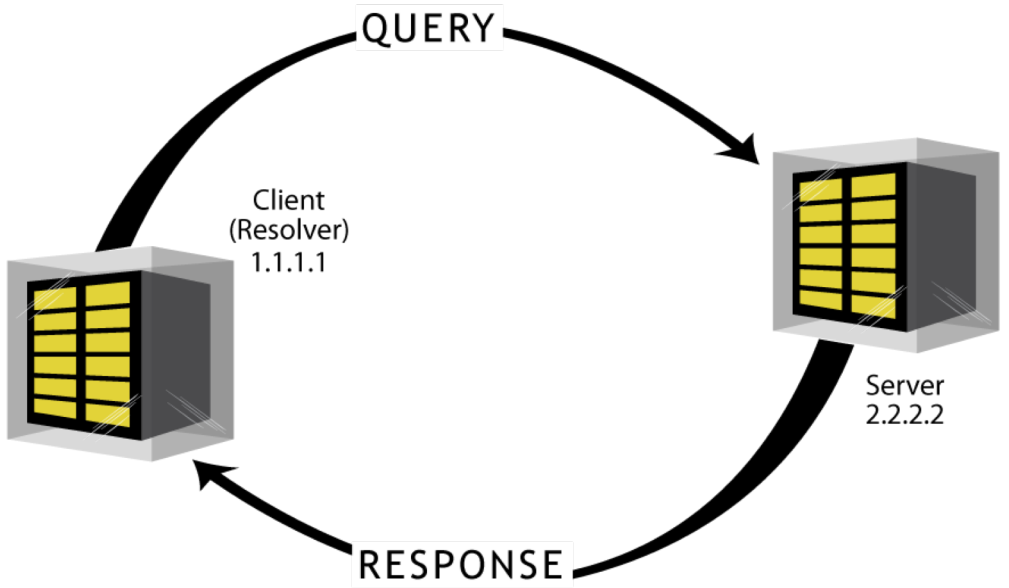
DNS and Lack of Security

- One packet for a DNS query, one packet for a DNS response



DNS and Lack of Security

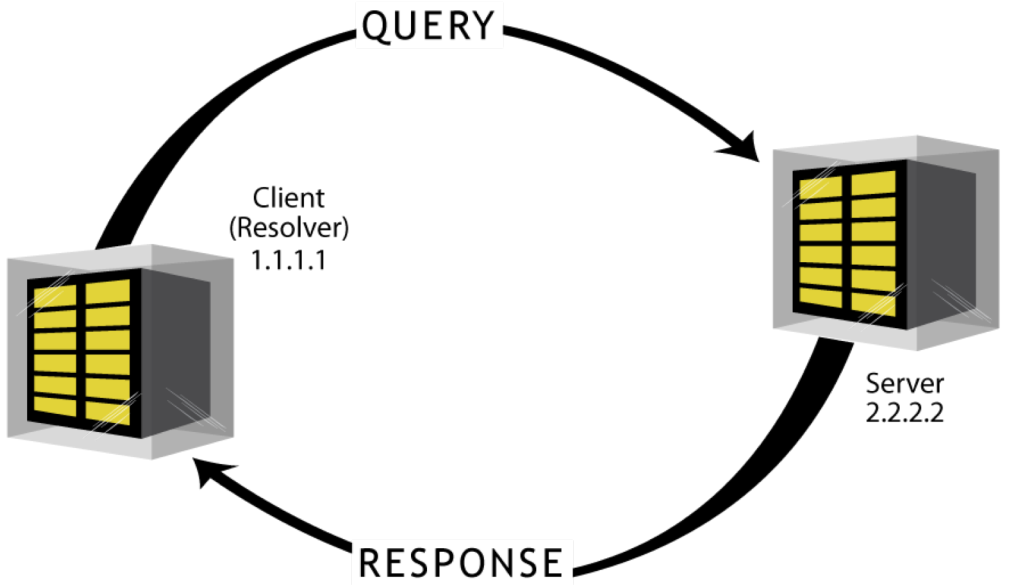
- One packet for a DNS query, one packet for a DNS response



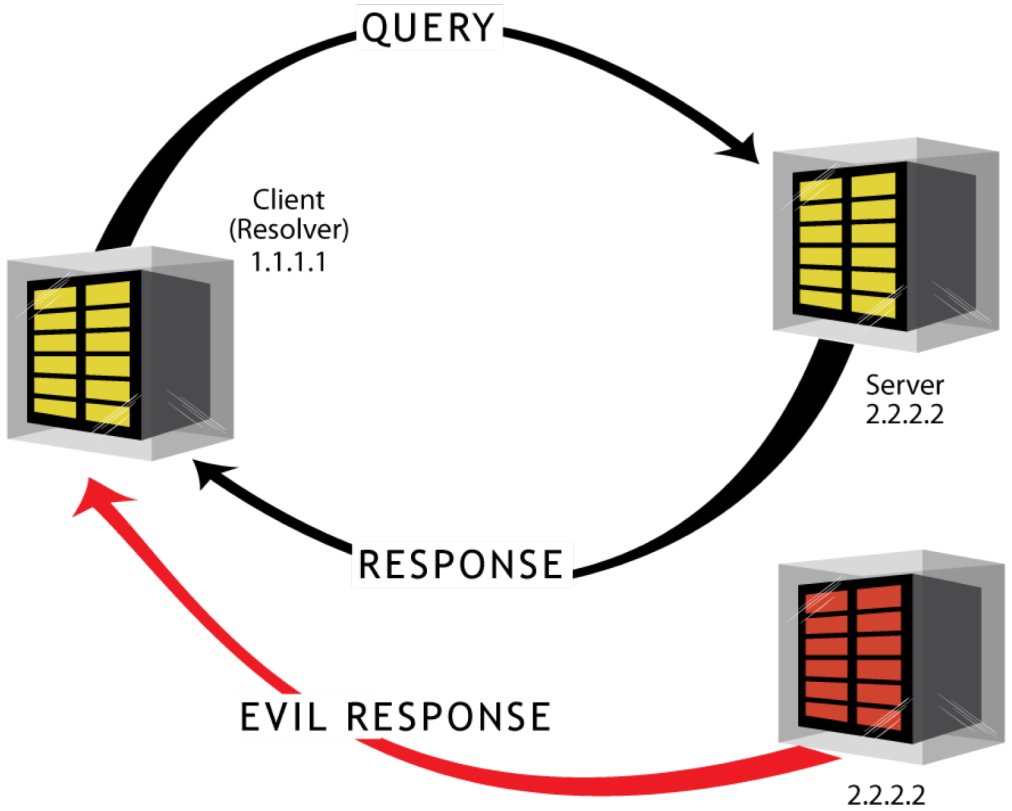
Who are you *really?*

- Client has to trust the source address of the server
- But source addresses can be faked or “spoofed”

Who are you *really?*



Who are you *really?*



Cyber Threat: DNS Cache Poisoning

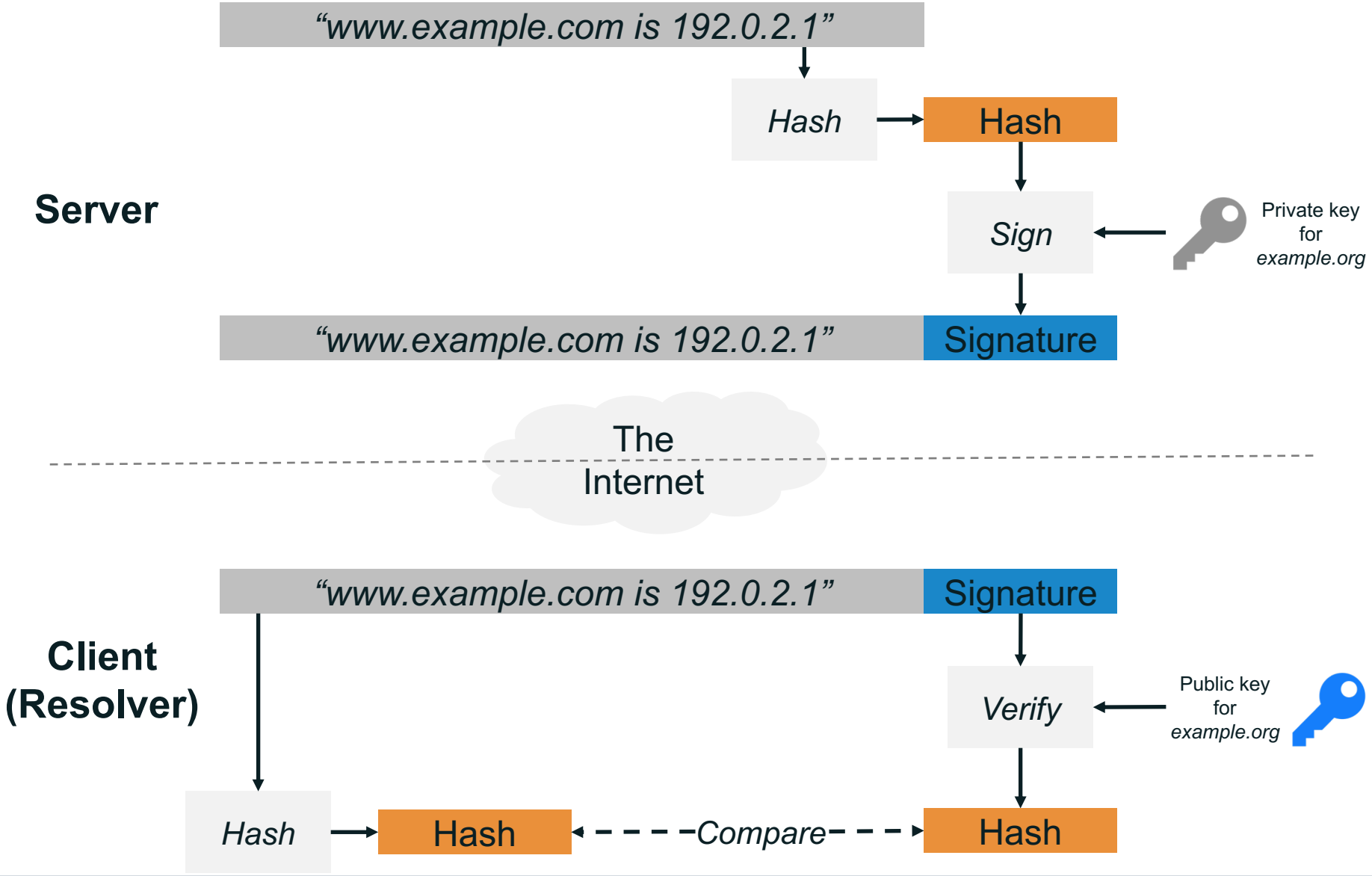
- DNS response spoofing can lead to *cache poisoning*
- The bad guys can insert bogus information into your recursive resolver's cache
- Modern resolvers are resistant to naïve cache poisoning attempts
- Need something better than resolver paranoia for a long-term fix
- That something better is DNSSEC, the DNS Security Extensions

The DNS Security Extensions (DNSSEC)

- All DNS data is cryptographically signed to generate a *digital signature*
- Authoritative name servers return the data queried for plus that data's digital signature
- Recursive resolvers validate the signature to confirm the authenticity of the data

- DNS *zones* have public/private key pairs
- What's a zone?
  - A zone is a DNS administrative grouping
  - All DNS data within a zone is managed by the same entity

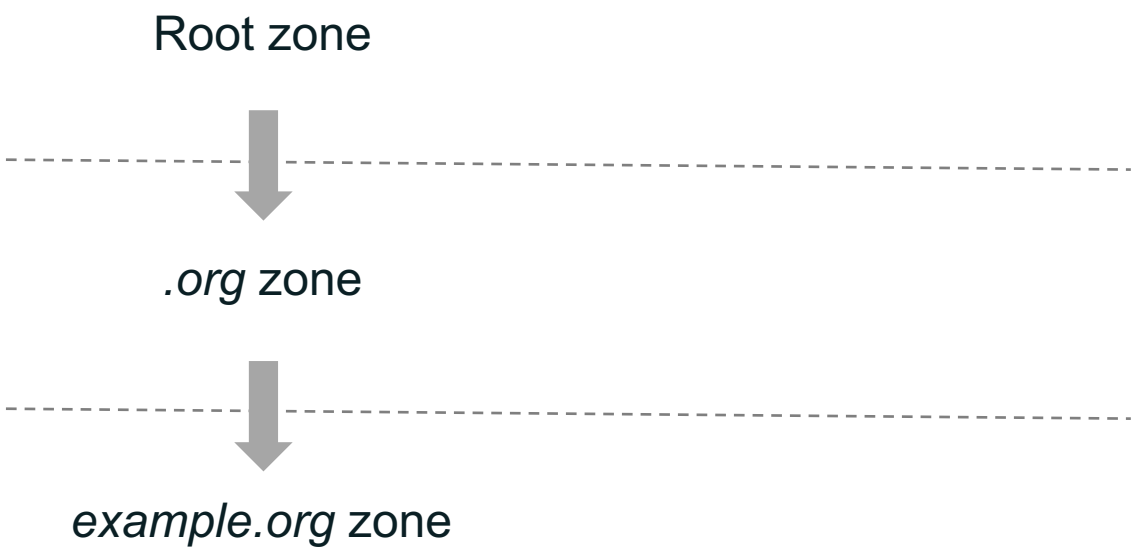
Public Key Cryptography and DNSSEC



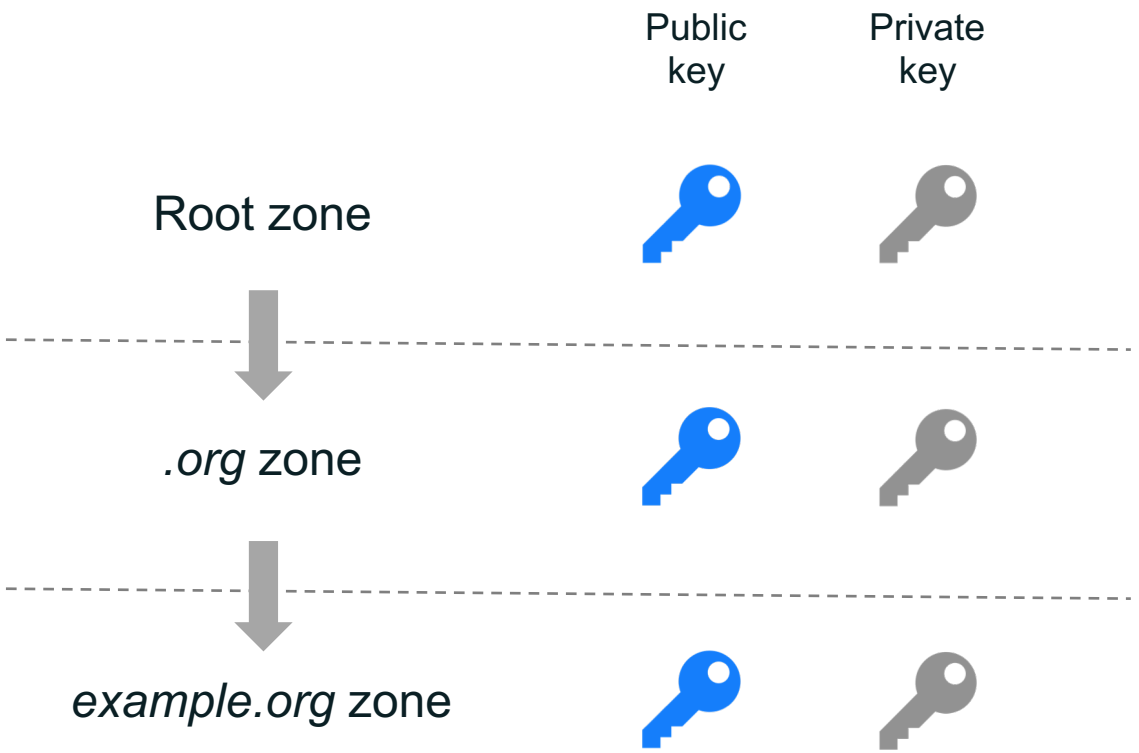
The DNS Security Extensions (DNSSEC)

- How do you trust a zone's public key?
- A zone's *parent zone* vouches for its public key
  - E.g., *.org* is the parent zone of the *example.org* zone
  - The root zone is the parent of the *.org* zone

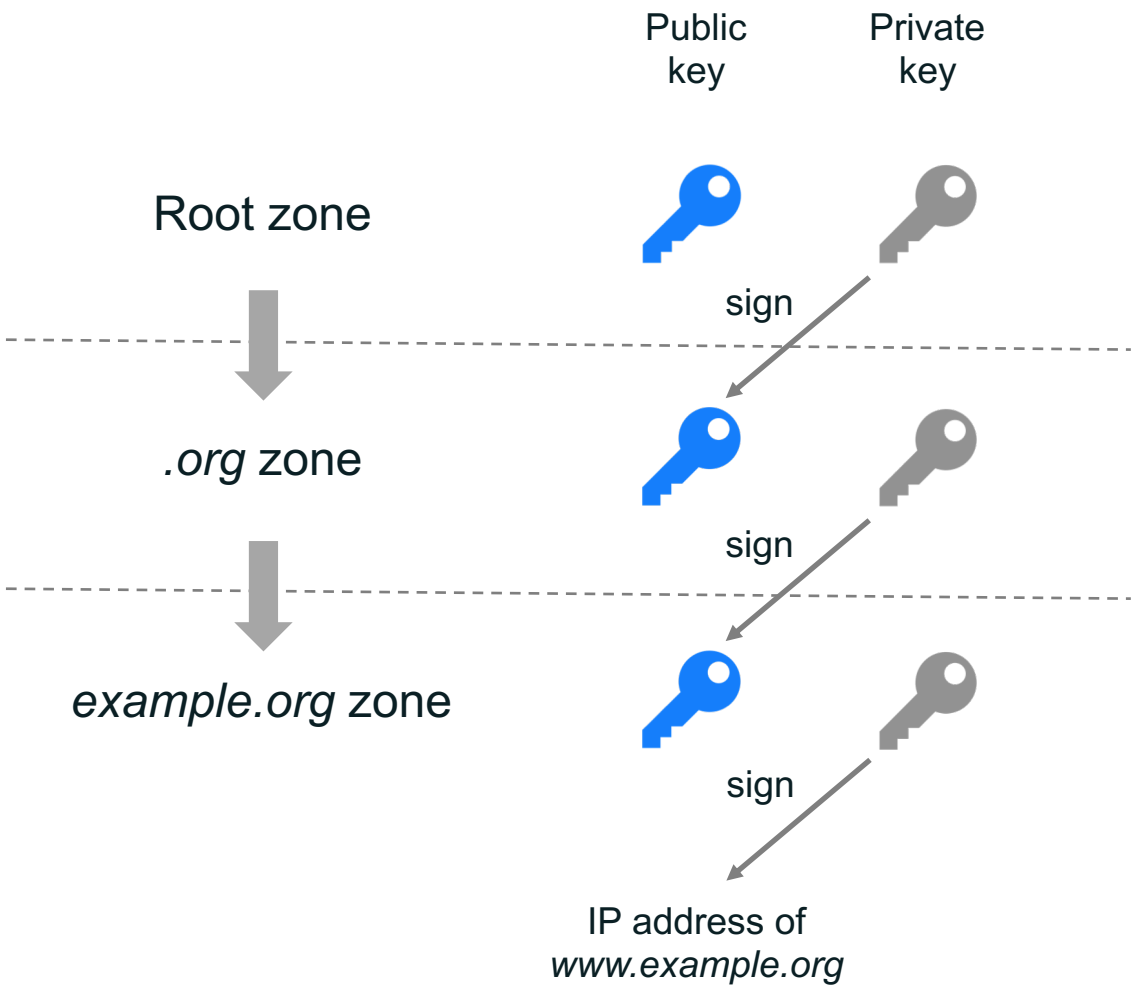
Hierarchy of Zones



Each Zone Has a Public/Private Key Pair



Chain of Trust



Oversimplification alert!
Each zone really has two keys:

1. Key-signing key (KSK)
2. Zone-signing key (ZSK)

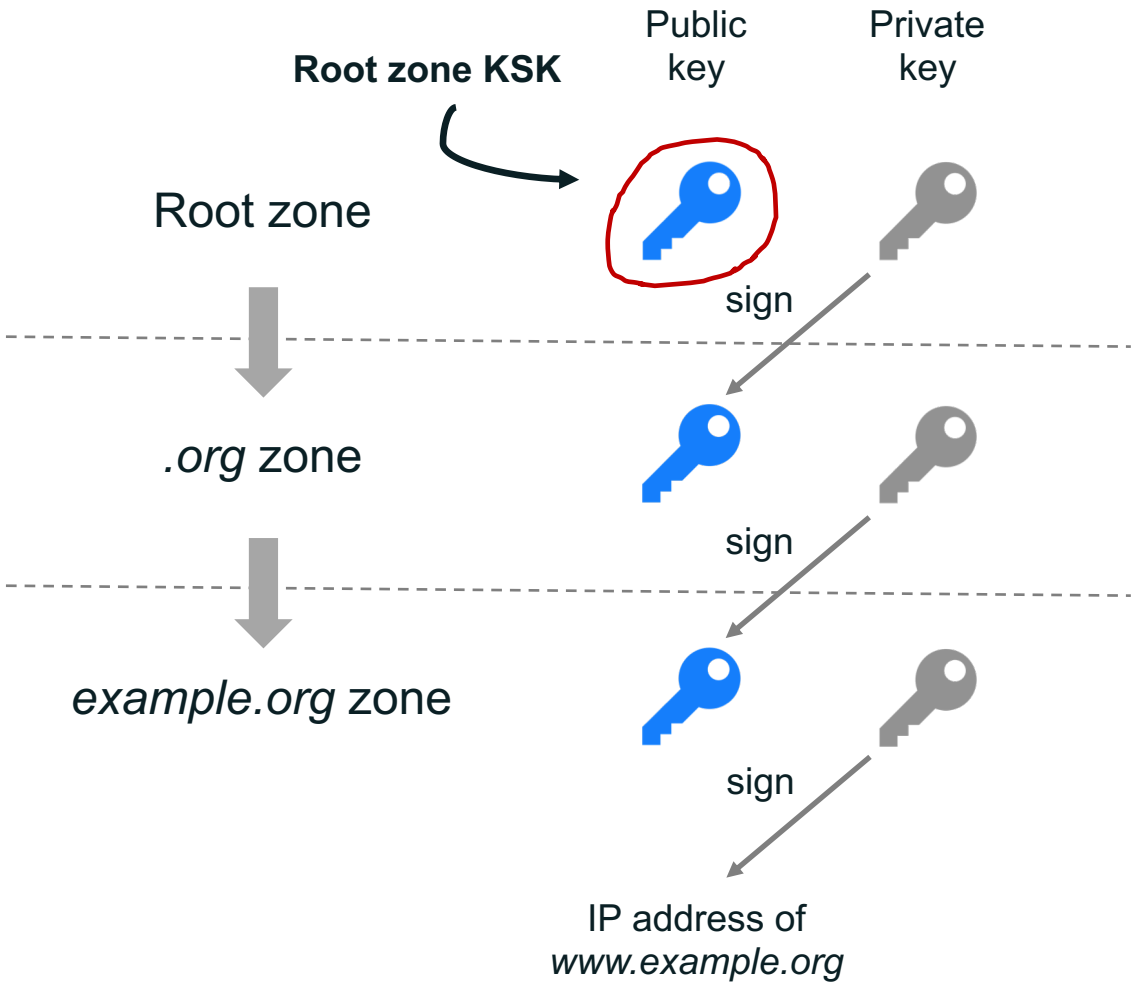
The KSK signs the ZSK, and the ZSK signs the rest of the zone.

And the ZSK in the parent zone doesn't sign the child zone's KSK. The parent zone's ZSK signs a Delegation Signer (DS) record for the child zone, which contains a cryptographic hash of the child zone's KSK.

Trust Anchors

- You have to trust someone
- A *trust anchor* is a public key that you trust implicitly
  - A human has to decide to trust it
  - Trust is not automatically discoverable

The Most Important Trust Anchor: Root Zone KSK



Root Zone KSK

- The most important cryptographic key in DNSSEC
- The start of almost every DNSSEC chain of trust
- Configured in many, many recursive resolvers
- Root zone KSK created when the DNS root zone first signed in 2010
- Managed very carefully by PTI/ICANN

Inside a Key Management Facility (KMF)

Key Ceremonies

Root Zone KSK Rollover

- Same root zone KSK used since 2010
- Initial guidance was to change or “roll” to a new root zone KSK “after five years”
- Why rollover?
  - No key should live forever
  - Want to roll under normal conditions, not an emergency
  - We said we would roll it
- There has been an ongoing multi-year project to roll the root zone KSK

Root Zone KSK Rollover

- The root KSK was rolled on 11 October 2018
  - Yes, last week. Really.
- The project to roll the KSK was the result of many years of planning and community consultation
- It went very smoothly
  - Anecdotal reports of minor problems
  - We are investigating two suspicious larger outages at ISPs in Ireland and Vermont, USA
- The project isn't over: the old root KSK will be revoked in January 2019

DNSSEC in the Future

- We need to keep investing in DNSSEC deployment
  - Sign more zones
  - Enable validation in more recursive resolvers
- Cache poisoning not believed to be a large issue today
  - Other easier attack mechanisms still work
- DNSSEC is our only long-term protection against cache poisoning
- The ability to trust information stored in the DNS can enable a whole new class of protocols and applications
  - But that's a story for another presentation

Engage with ICANN

Thank You and Questions

Visit us at **icann.org**
Email: email@icann.org

@icann

facebook.com/icannorg

youtube.com/icannnews

flickr.com/icann

linkedin/company/icann

slideshare/icannpresentations

soundcloud/icann