# DNS for IoT Security

Yazid Akanho and Paul Muchene

Webinar to ITU-D Workshop on IoT and IPv6

01 June 2022

# Agenda

- IoT and the DNS: Opportunities, Risks and Challenges
- DNSSEC in a Nutshell
- How DNSSEC can protect IoT

# Ask Questions

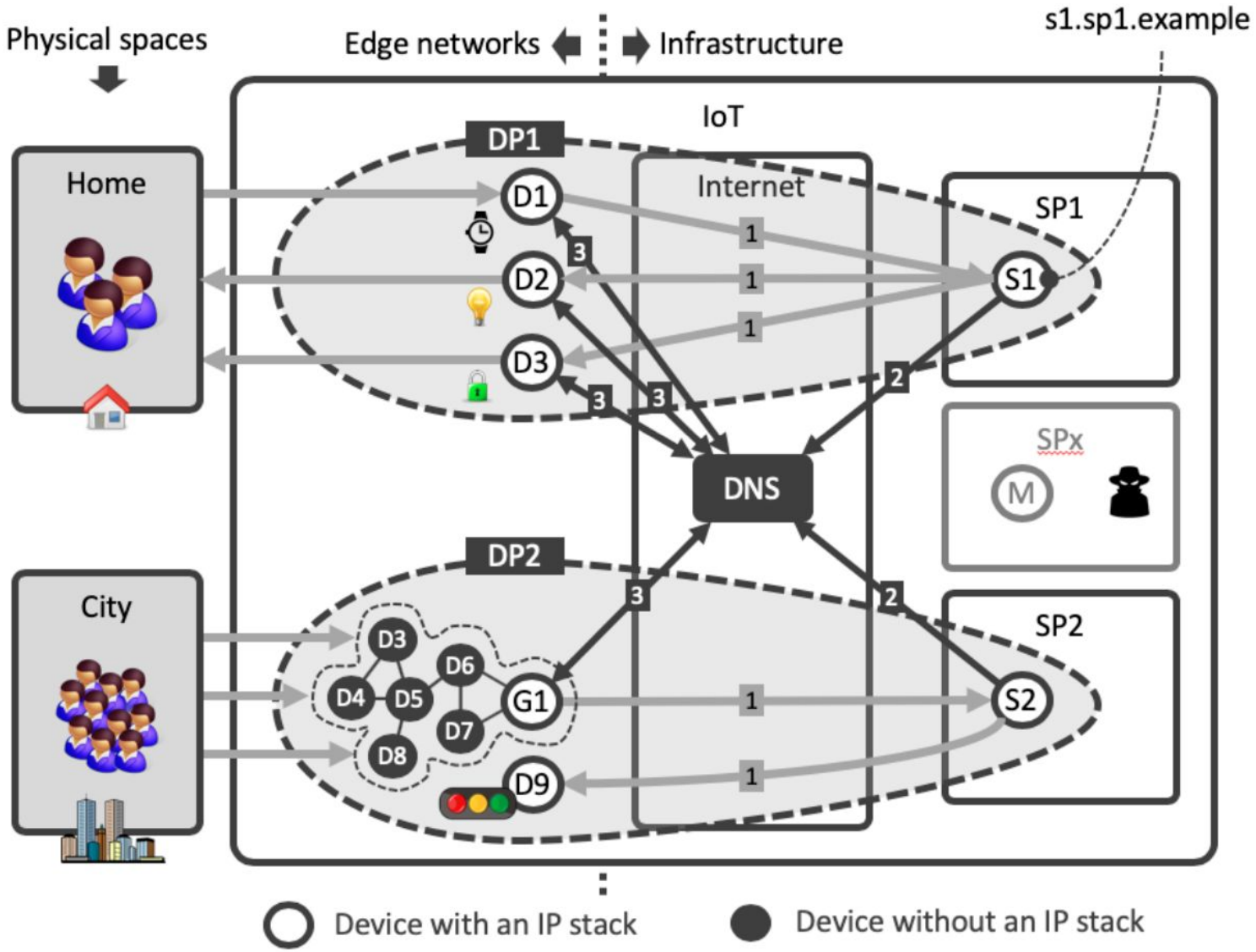
**Questions & Feedback**

# IoT: Opportunities, Risks and Challenges

# IoT and the DNS

- The Internet of Things (IoT) through billions of connected devices promises to enhance and ease our day-to-day lives by seamlessly and automatically interacting with our physical actions and environment.
- Introduce new security, availability and transparency requirements that isn't apparent with traditional connected devices e.g. smart phones
- The DNS as a pervasive, global infrastructure can partly fulfill some of these requirements
- IoT is both a value to further increase the value of the DNS and a risk that can potentially reduce the value of the DNS

# Example IoT Deployment using DNS



# IoT is a Risk to DNS

**IoT's scale is a serious threat to the stability of the DNS:**

- IoT devices could stress the DNS in ways never seen before. Programming errors could lead to a situation where too many devices make simultaneous DNS requests - Case: Tunein App software bug (2012)

Image Source: izoologic.com

# IoT is a Risk to DNS: Botnets

- IoT botnets can be assembled and run on a wider range of devices numbering in the millions
- Increased size and complexity of IoT botnets targeting the DNS (e.g. Mirai at IoT scale)
- Increase DDoS amplification through open DNS resolvers
  - One 2018 report estimated ~3 million open recursors in 2018
  - Some IoT devices can also act as Open DNS resolvers
  - So if Mirai had several hundred thousand bots directing DDoS attacks via open recursors, what would it look like if there were several billion bots?
- IoT botnets can also be leveraged to spread malware - Hajime botnet exploited vulnerability to infect GPON routers
- Problem compounded by the fact that IoTs are difficult to fix and patch quickly at scale and infections of IoT devices can stay undetected much longer

# IoT Challenges

- Developing a DNS library for IoT devices that makes the DNS's security functions (e.g., DNSSEC validation and DoH/DoT) available. Libraries and tools should also take into account the constrained hardware and software environments that run on IoTs.

- Training IoT and DNS professionals  to help DNS players such as registrars and registrants understand the implications of providing services for domain names that act as a backend for IoT devices rather than as a means for making content available to humans and to help IoT device manufacturers understand how to use the DNS and how to configure resolvers

# IoT Challenges (Continued)

- Developing a shared system that enables different DNS operators to automatically and continuously share information on IoT botnets , allowing them to more quickly respond to rapidly growing botnets and the DDoS attacks they generate e.g. DDOS Open Threat and Signaling WG (DOTS)

- Developing a system that enables DNS operators to measure how the IoT uses the DNS , to better understand how IoT risks evolve — for instance to develop new domain name policy or for incident response purposes.

# DNSSEC in a Nutshell

# What Is DNSSEC?

**DNSSEC** stands for **Domain Name System (DNS) Security Extensions.**


- DNSSEC is a protocol being deployed since 2000s to secure the DNS.
- DNSSEC adds security to the DNS by incorporating public key cryptography into the DNS hierarchy.
- DNSSEC is the result of over two decade of community-based, open standards development.
- Complementary to other technologies like SSL that secure the delivery of the content in increasing the security of online services.
- RFCs 4033, 4034, 4035 and 5155

# DNSSEC in summary


- To achieve Authenticity and Integrity of DNS data.
- Allows two major functionalities:
  - domain name **registrants** to cryptographically **SIGN** their DNS data.
  - **DNS operators** to **VALIDATE** all DNS data passing through DNS resolvers.
- Provide assurances to users that the DNS data they are seeing is **valid and true**.
- Helps prevent DNS threats and abuses.

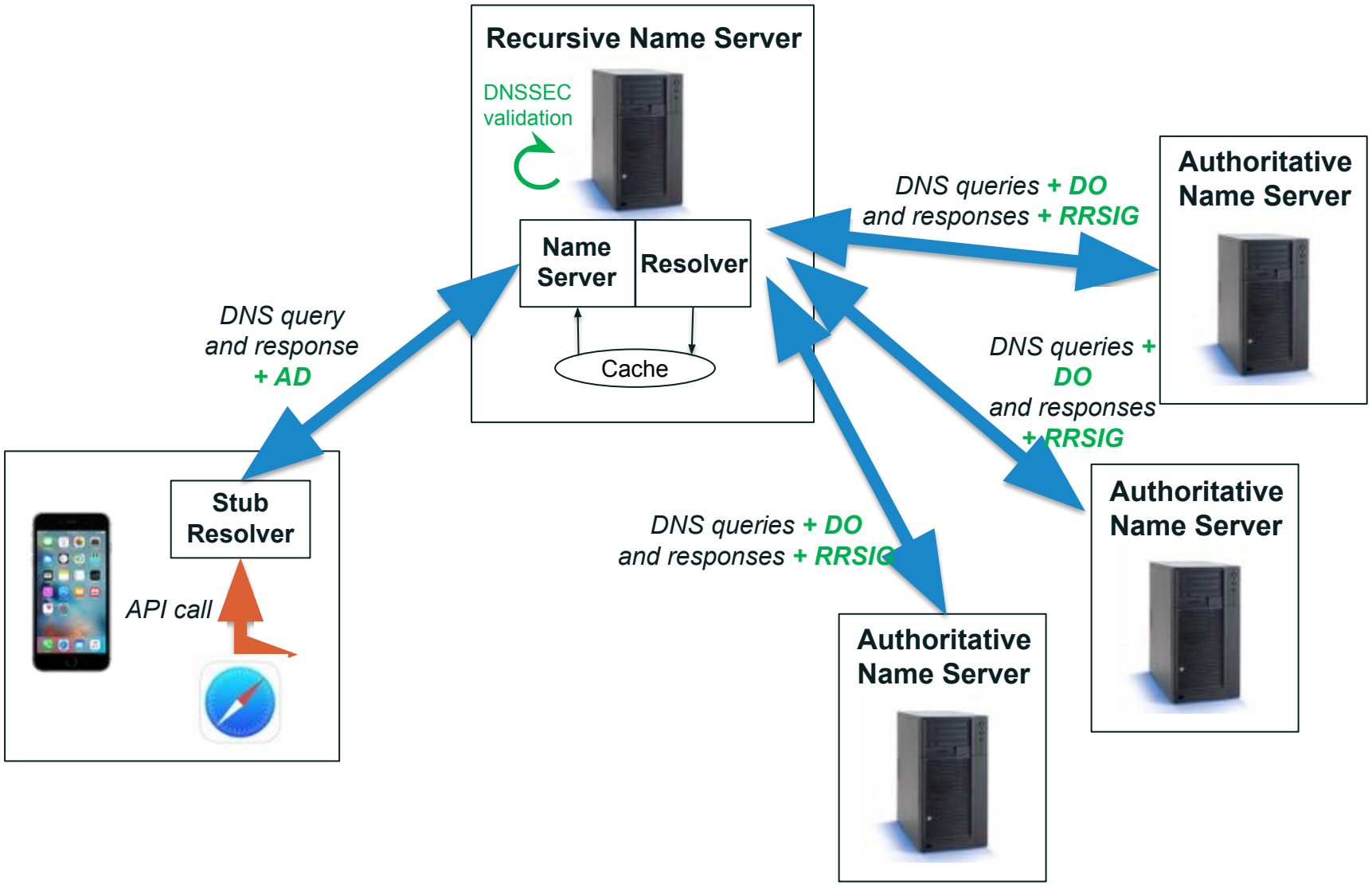
# What DNSSEC Does Vs what it doesn't do

- DNSSEC uses public-key cryptography and digital signatures to provide:
  - **Data Origin Authenticity :** "Did this response really come from the *example.com* zone?"
  - **Data Integrity:** "Did an attacker (e.g., a man in the middle) modify the data in this response since the data was originally signed?"
- DNSSEC offers **protection against spoofing** of DNS data
- DNSSEC **does not provide** any confidentiality for DNS data:
  - no encryption
  - Man in the middle-attack
- DNSSEC **does not address** attacks against DNS software: DDoS; BCP38

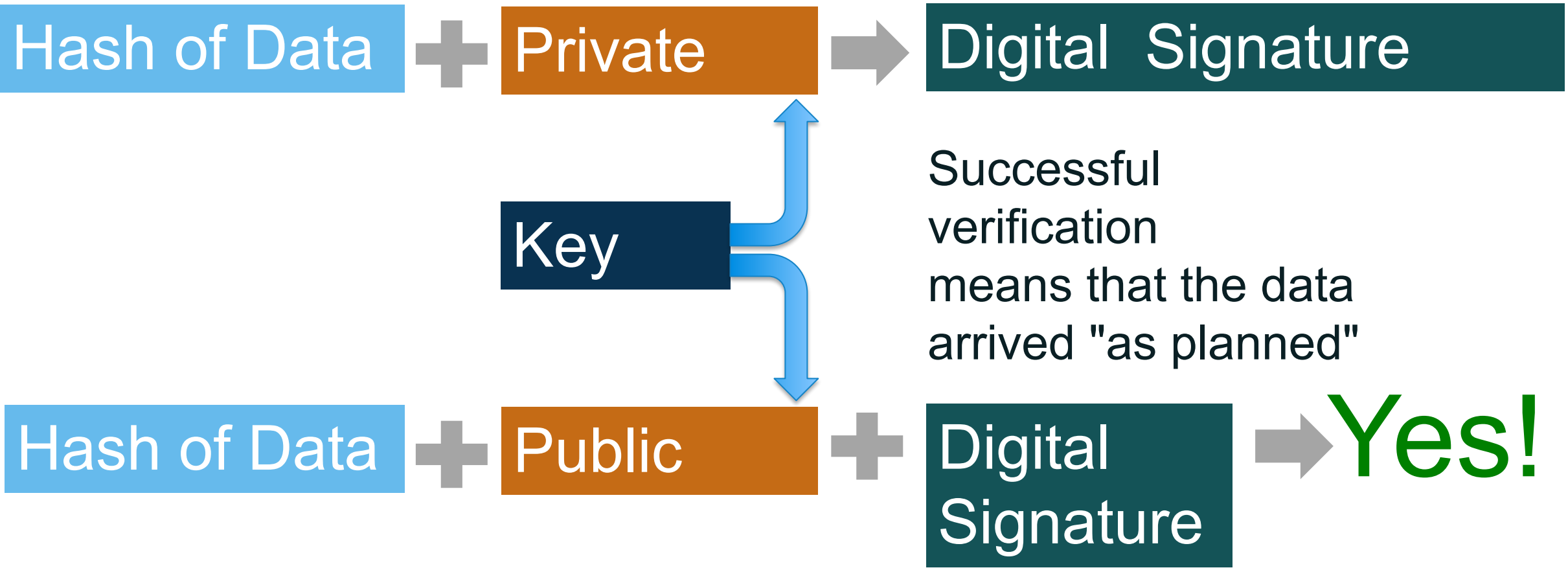
# DNSSEC Validation

- DNSSEC validation is the process of **checking the signatures** on DNSSEC data
- Validation can occur in applications, stub resolvers or recursive resolvers.
- Most validation today occurs in recursive resolvers.
- Trust Anchor: To perform DNSSEC validation, you have to trust somebody (some zone's key). **Root Zone KSK is the most important trust Anchor on the Internet. You can view root key signing ceremony on YouTube.**
- What happens when validation fails?
  - The recursive resolver protects the user by sending a "SERVFAIL" error response.

# DNS resolution process with DNSSEC



# Digital Signatures - Verification



# Chain of Trust

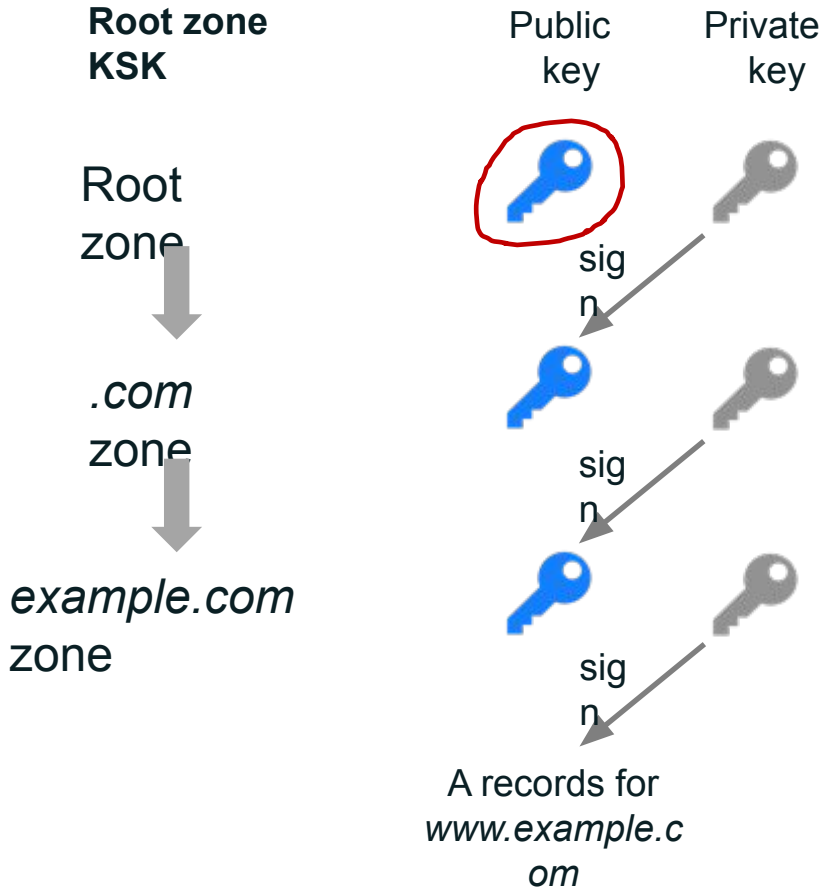
Finally, how do we trust DS record?

Well, we just sign DS record like we did with other RRsets, creating a corresponding RRSIG for the DS record in the parent.

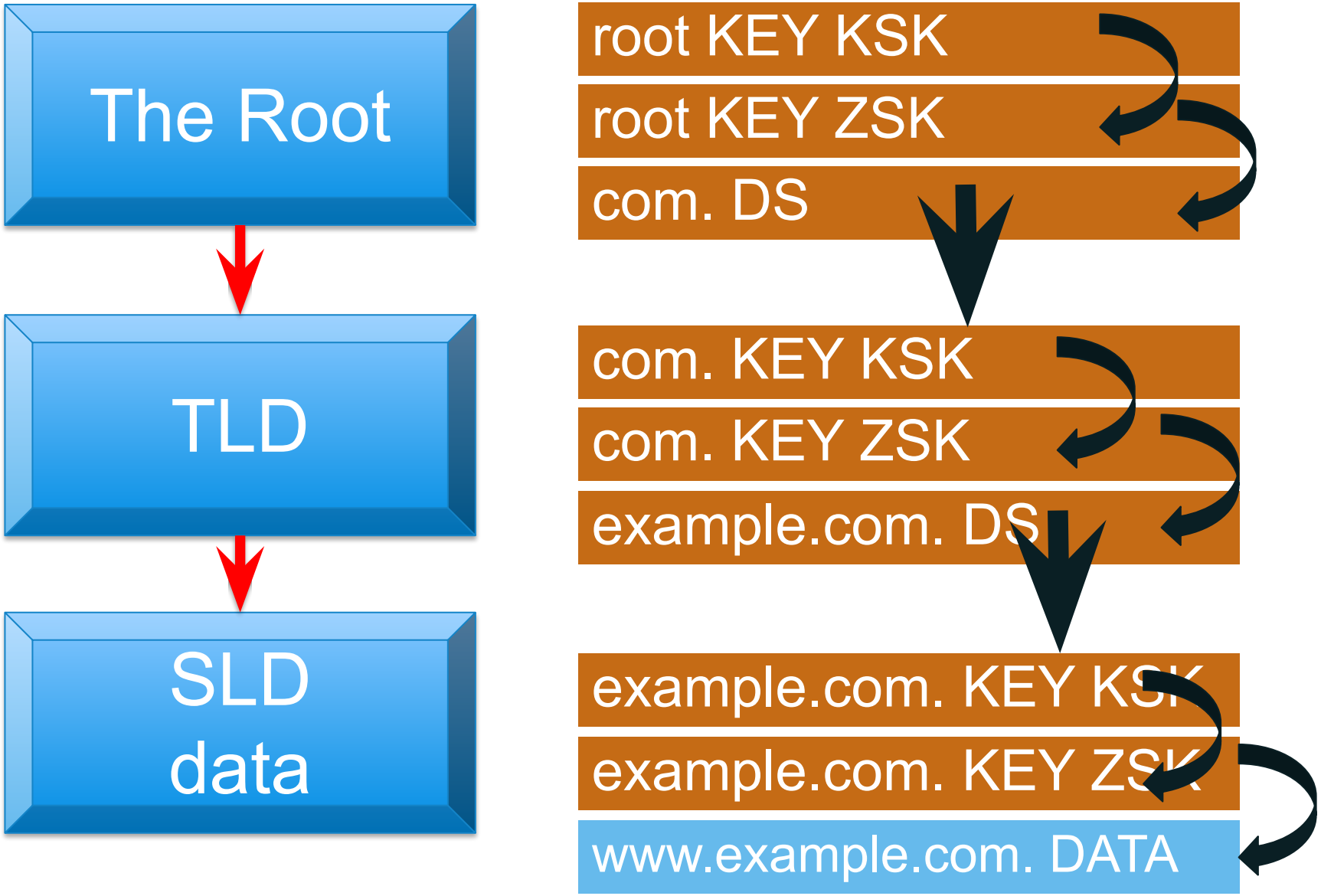
We repeat the validation process and get to the parents public KSK... And again must go to that parent's DS record to verify… on and on up to the DNS root.

Eventually, we get to the root and there's nothing up there (sadly no parent)… and so we must come with a solution to create a trust anchor for the root, a "one key to rule them all" (*sorry, can't resist quoting LOTR again*)… and here it comes a solution implemented since 2010 called:

The Root Signing Ceremony



# Signing Chain



# How DNSSEC can protect IoT

# Using DNSSEC to detect malicious redirects of IoT devices

- Manipulated DNS messages can redirect IoT devices to a malicious service, jeopardizing user privacy and security: attacker could conduct a Border Gateway Protocol (BGP) hijack to impersonate an authoritative DNS server or a resolver cache poisoning to return a wrong IP address to IoT devices. DNSSEC security mechanisms can protect the IoT devices and prevent such kind of attacks.

- IoT devices can also rely on DNS Authentication of Named Entities (DANE) to verify and confirm that the certificate associated with a specific entity is valid and really bounds to that entity (could be helpful for HTTPS communications). DANE builds on DNSSEC and requires DNSSEC validation to work.

# DoH and DoT to protect DNS messages

- DNS-over-HTTPS (DoH) and DNS-over-TLS (DoT) encrypt DNS messages between a DNS client and its resolver, thus hiding domain lookups and responses from on-path inspection and/or alteration.

- Advantage for IoT devices: reduce the possibility to observe DNS queries/responses contents, thus the possibility to collect information on the IoT system.

# References

- The DNS in IoT: Opportunities, Risks and Challenges: https://www.caida.org/catalog/papers/2020_dns_in_iot/dns_in_iot.pdf

- SAC 105: The DNS and the Internet of Things: Opportunities, Risks and Challenges: https://www.icann.org/en/system/files/files/sac-105-en.pdf

# Engage with ICANN – Thank You and Questions

One World, One Internet

Visit us at **icann.org**

@icann

facebook.com/icannorg

youtube.com/icannnews

flickr.com/icann

linkedin/company/icann

slideshare/icannpresentations

soundcloud/icann