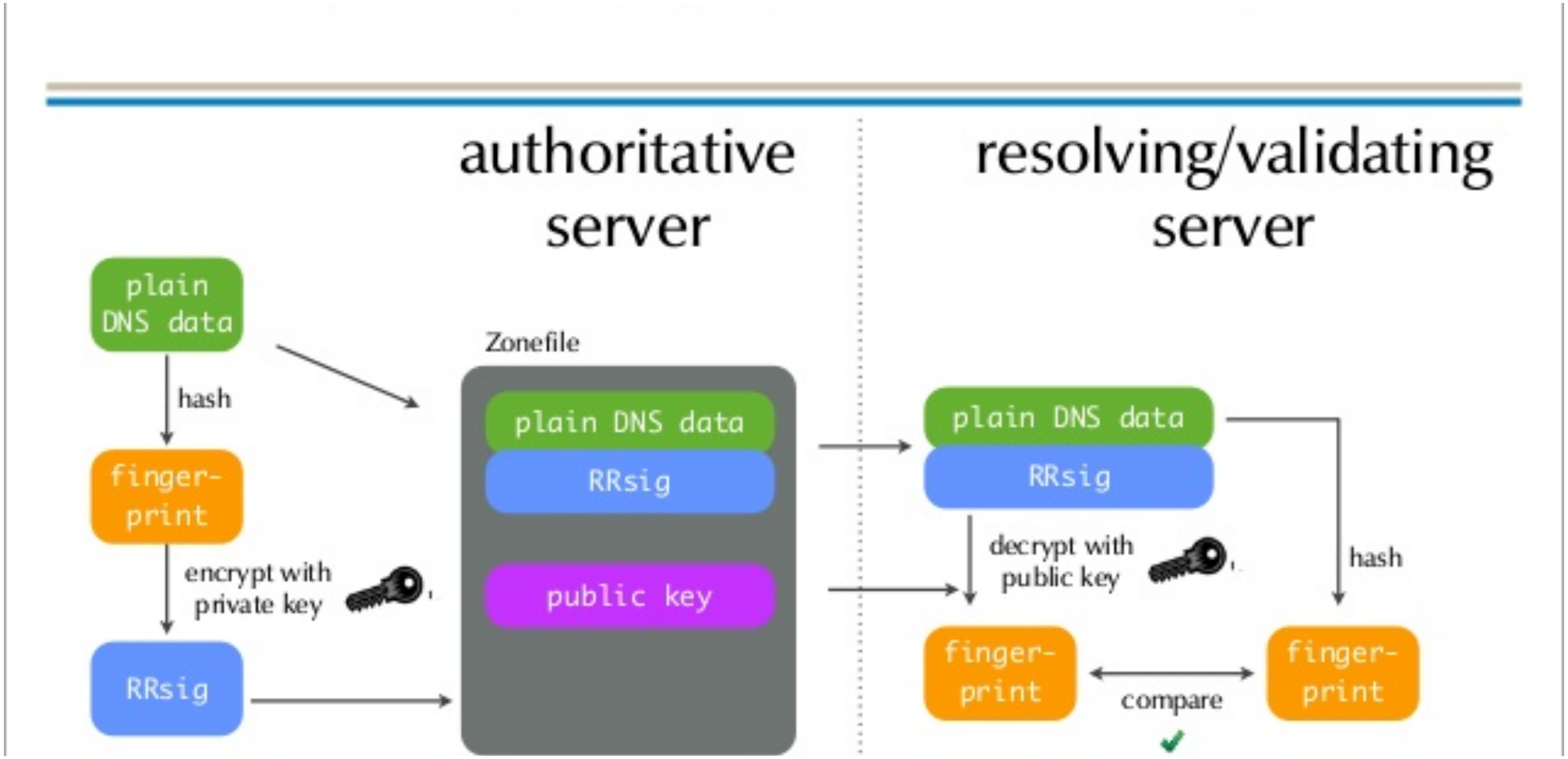
RP1 Monitoring DNSSec

Martin Leucht

Julien Nyczak

DNSSec Zone Signing



Intro

DNSSEC enabled zones need regular zone signing updates, since signatures have an expiry date (ZSK).

There are different (automated) mechanism required, when large amounts of DNSSec zones need to be maintained, such as

- Zone Signing Key Rollover (Double-Signature/Pre-Publish) for ZSK (KSK)
- Client push/publish DS to parent (CDS and CDNSKEY) RFC7344

→ Keys must be generated in advance

Intro

- If a key has expired and has not been rolled over, the **zone becomes unreachable**.
- Need to monitor key expiries within domains (think of 1000 zones) in order to prevent these problems
- Maybe other important DNSSec Parameter beside keys “monitorable”
- provide DNSSec parameter preferably local (e.g. SNMP Agent)
- Hence it will be easy to spot any zones that are not properly signed.

Research questions

- What are vital life signs for monitoring DNSSEC?
- How to construct a MIB for DNSSEC?
- How to conduct monitoring based on such a MIB?
- How do architectures for monitoring DNSSEC compare?

- How to proceed?

Constructing a MIB

- construct a SNMP MIB (Management Information Base) to gather signed zones data like the oldest signature in a zone, the signature on the SOA record, the SOA record itself…
- (optional SNMP Trap integration for passive monitoring)

Implementing the MIB

- write an SNMP agent (preferably in Python) which responds to inquiries like zone searching, and will answer with essential DNSSec zone data
- Make use of applications like Openddnssec for
- Data can be retrieved by SNMP based monitoring systems
- applicable alerts /escalations can be triggered by monitoring system