

Bootstrapping DNSSEC

Methods, Implementations, Open Issues

ICANN 77 – DNSSEC Workshop
June 12, 2023

Peter Thomassen
peter.thomassen@securesystems.de



Problem Statement

— — —

Securing a delegation = Ry creates DS record with child's DNSSEC parameters.

Problems:

- 1. How does the Registry get these parameters?**
 - Largely the same problem as “DS Automation” in general
- 2. How are those parameters authenticated?**
 - NB: for key *rollovers*, existing chain of trust can be used. Not here!
- 3. When this happens automatically, are there any risks?**

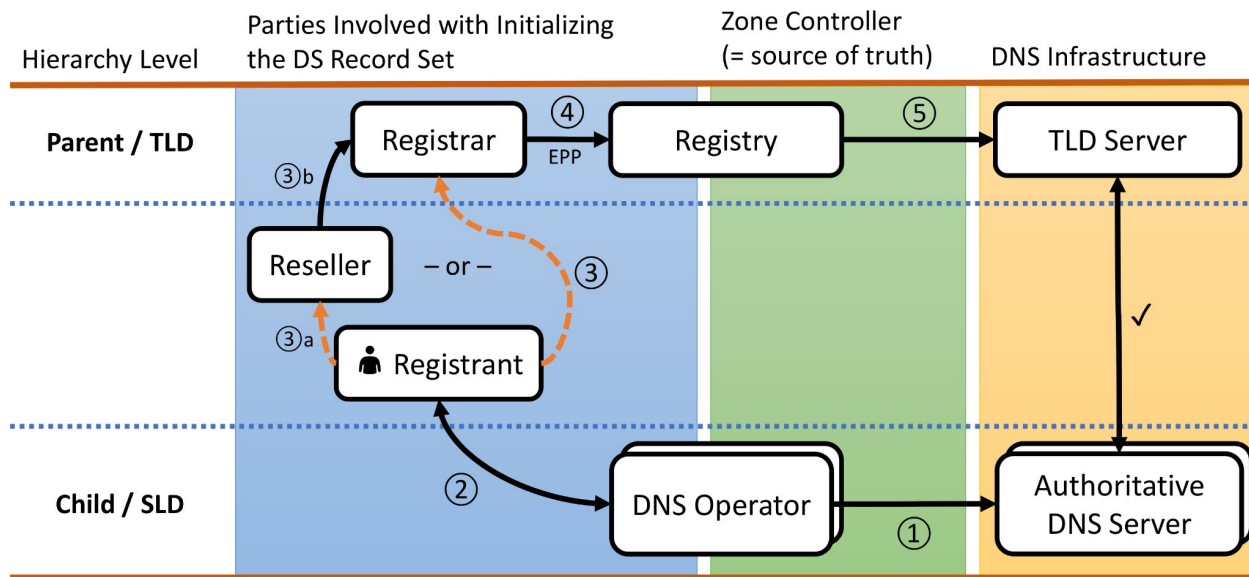
Approaches to DNSSEC Bootstrapping

— — —

1. manual submission

- Generally supported, but cumbersome

Approaches: Manual Submission



- Slow
- Error-prone
- Out of band
- Not properly authenticated

- Involves the Child DNS Operator (origin) and Parent Registry (recipient)
 - ... typically with the Registrar as the messenger
 - ... typically facilitated through the Registrant

Approaches to DNSSEC Bootstrapping

— — —

1. **manual submission**
 - Generally supported, but cumbersome
2. **trust on first use (TOFU):** query DNSKEY, compute DS, and hope for the best
 - Used by notable Registrar in Germany

Approaches to DNSSEC Bootstrapping

— — —

1. **manual submission**
 - Generally supported, but cumbersome
2. **trust on first use (TOFU)**: query DNSKEY, compute DS, and hope for the best
 - Used by notable Registrar in Germany
3. Several attempts on **REST interfaces** or REST-DNS hybrids, driven by CIRA
 - ICANN [53](#), [54](#) (2015), [draft-ietf-regext-dnsoperator-to-rrr-protocol](#) (2018)
 - No known deployments

“Need to redesign around the DNS Operator”

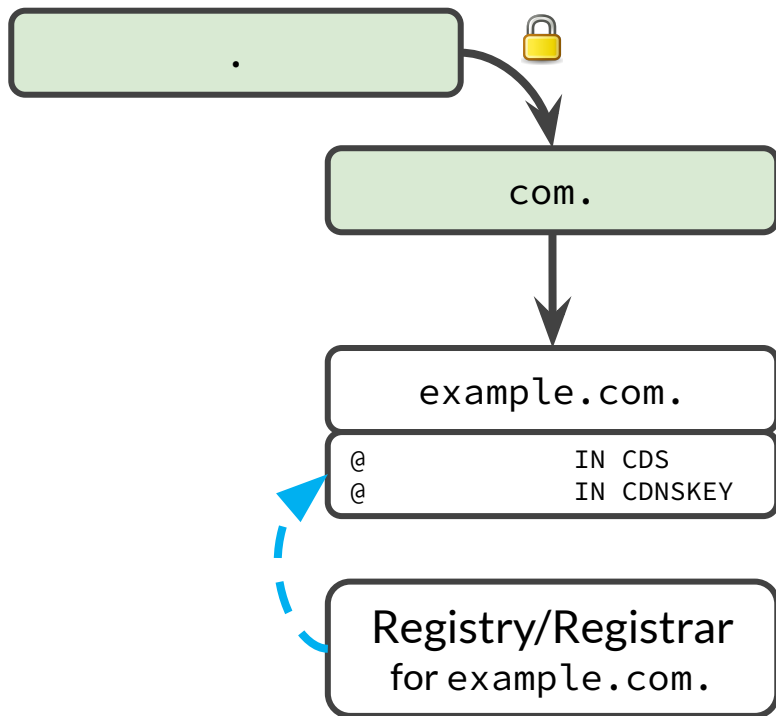
— Jacques Latour, Tech Day at ICANN 53

Approaches to DNSSEC Bootstrapping

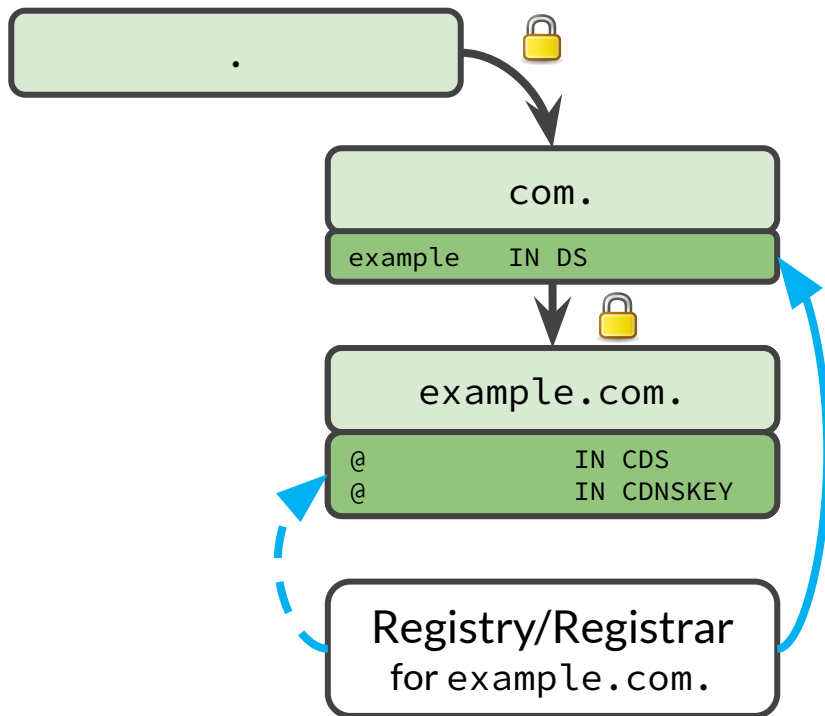
— — —

1. **manual submission**
 - Generally supported, but cumbersome
2. **trust on first use (TOFU)**: query DNSKEY, compute DS, and hope for the best
 - Used by notable Registrar in Germany
3. Several attempts on **REST interfaces** or REST-DNS hybrids, driven by CIRA
 - ICANN [53](#), [54](#) (2015), [draft-ietf-regext-dnsoperator-to-rrr-protocol](#) (2018)
 - No known deployments
4. CDS/CDNSKEY from **insecure child** (RFC 8078)
 - Requires stateful monitoring
 - Used by **.ch/.cr/.cz/.fo/.li/.nu/.se/.sk/.alt.za/.edu.za** (parent) and various DNS operators (child)

Approaches: CDS/CDNSKEY from Insecure Child



Approaches: CDS/CDNSKEY from Insecure Child

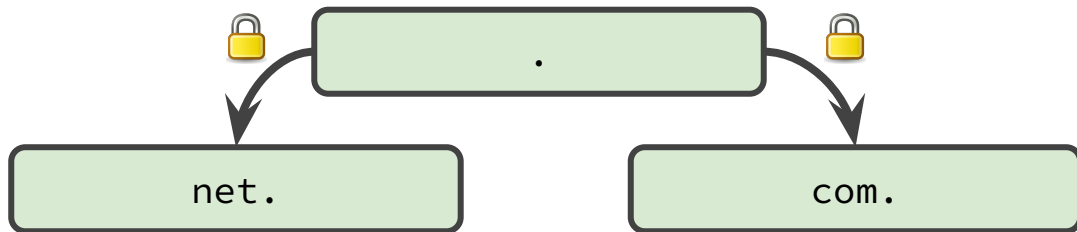


Approaches to DNSSEC Bootstrapping

— — —

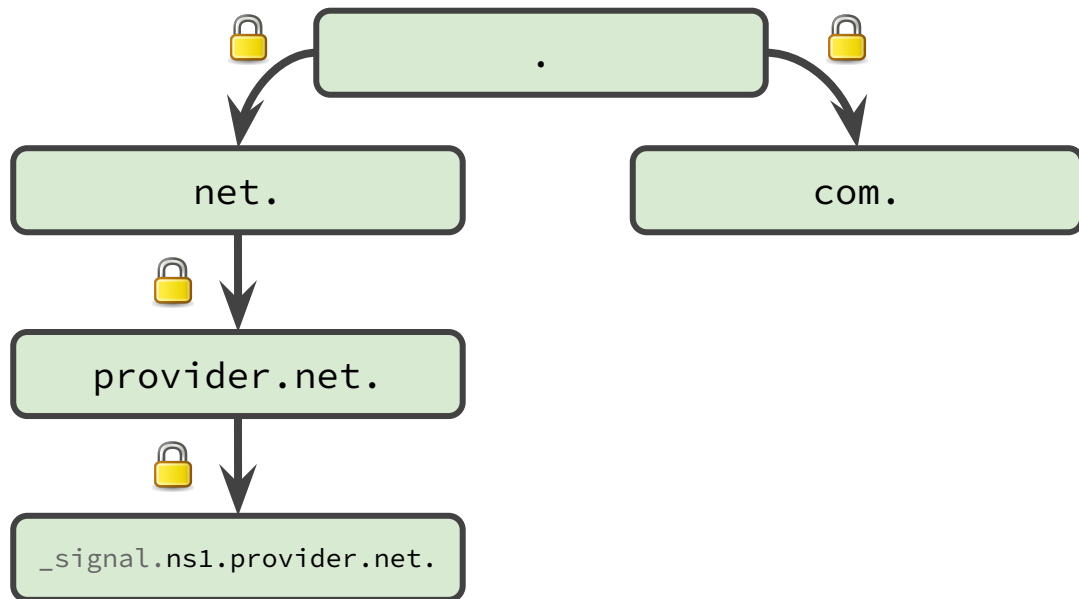
1. **manual submission**
 - Generally supported, but cumbersome
2. **trust on first use (TOFU):** query DNSKEY, compute DS, and hope for the best
 - Used by notable Registrar in Germany
3. Several attempts on **REST interfaces** or REST-DNS hybrids, driven by CIRA
 - ICANN [53](#), [54](#) (2015), [draft-ietf-regext-dnsoperator-to-rrr-protocol](#) (2018)
 - No known deployments
4. CDS/CDNSKEY from **insecure child** (RFC 8078)
 - Requires stateful monitoring
 - Used by [.ch/.cr/.cz/.fo/.li/.nu/.se/.sk/.alt.za/.edu.za](#) (parent) and various DNS operators (child)
5. **CDS/CDNSKEY with authentication** by child operator ([IETF DNSOP draft](#))
 - Used by [.ch/.li](#) (parent) and **Cloudflare/deSEC/Glauca HexDNS** (child)
 - Implementations exist for PowerDNS Auth and Knot DNS (upstream PRs coming up)

Approaches: CDS/CDNSKEY with Authentication



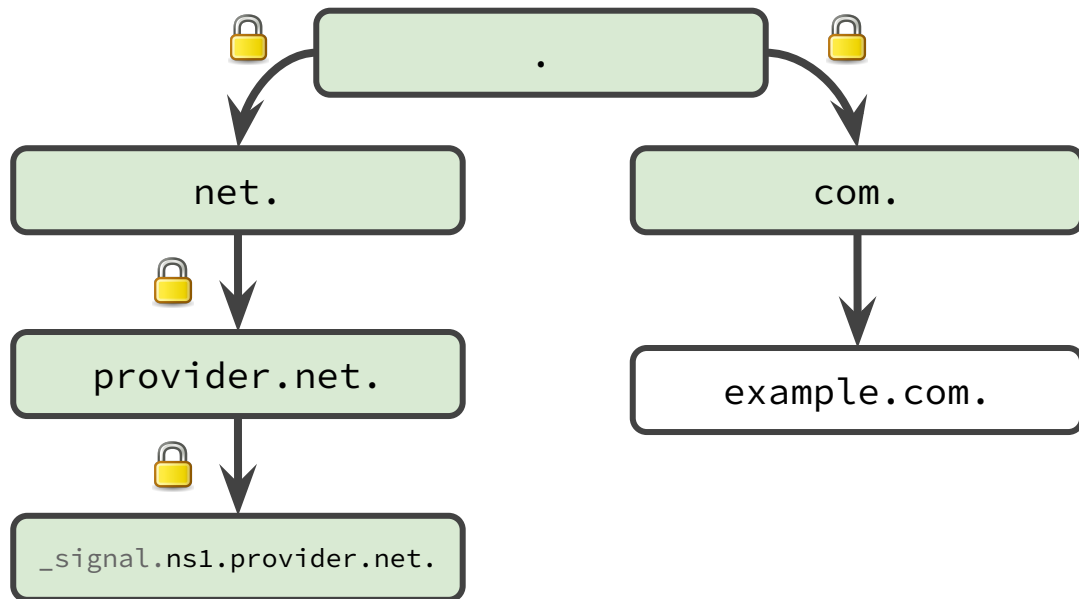
Approaches: CDS/CDNSKEY with Authentication

— — —



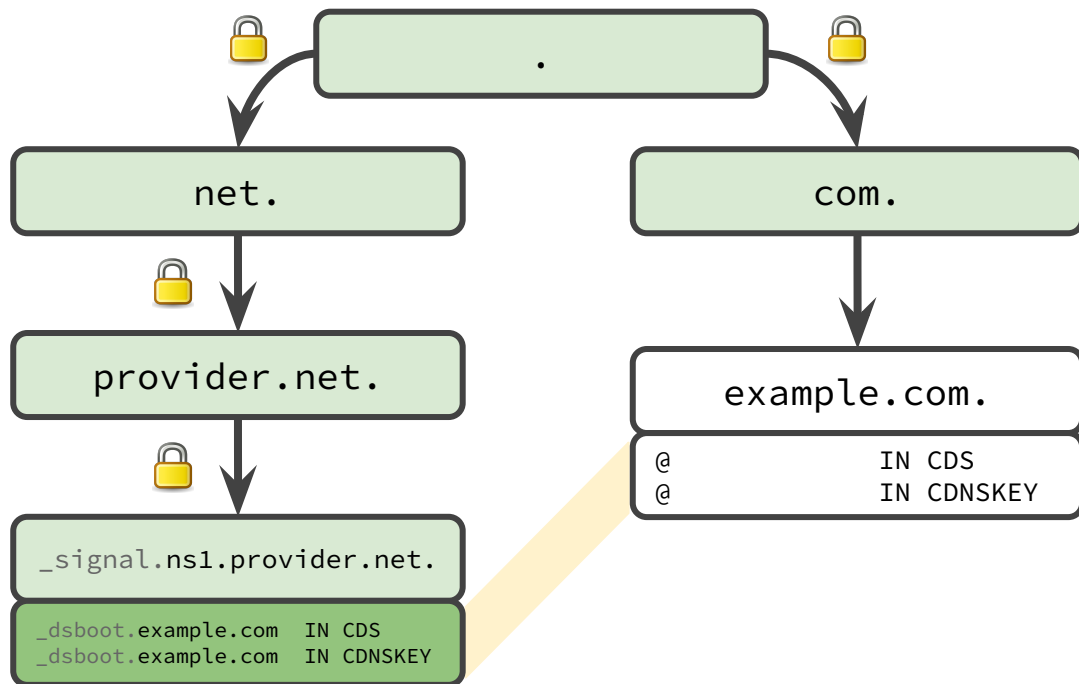
Approaches: CDS/CDNSKEY with Authentication

— — —

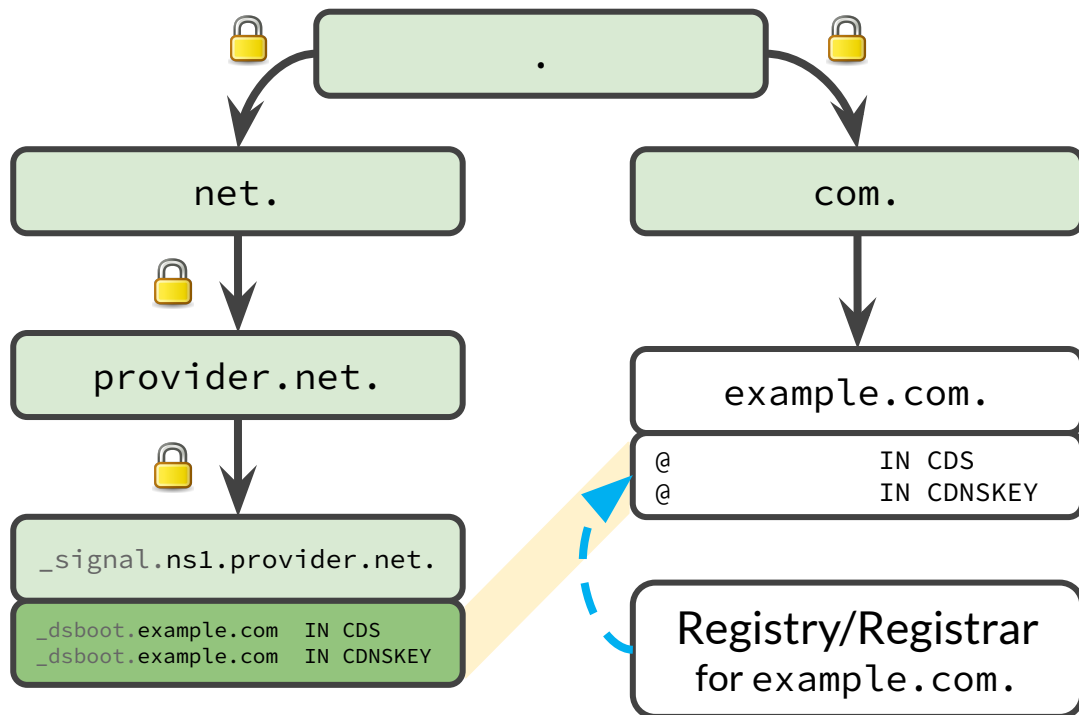


Approaches: CDS/CDNSKEY with Authentication

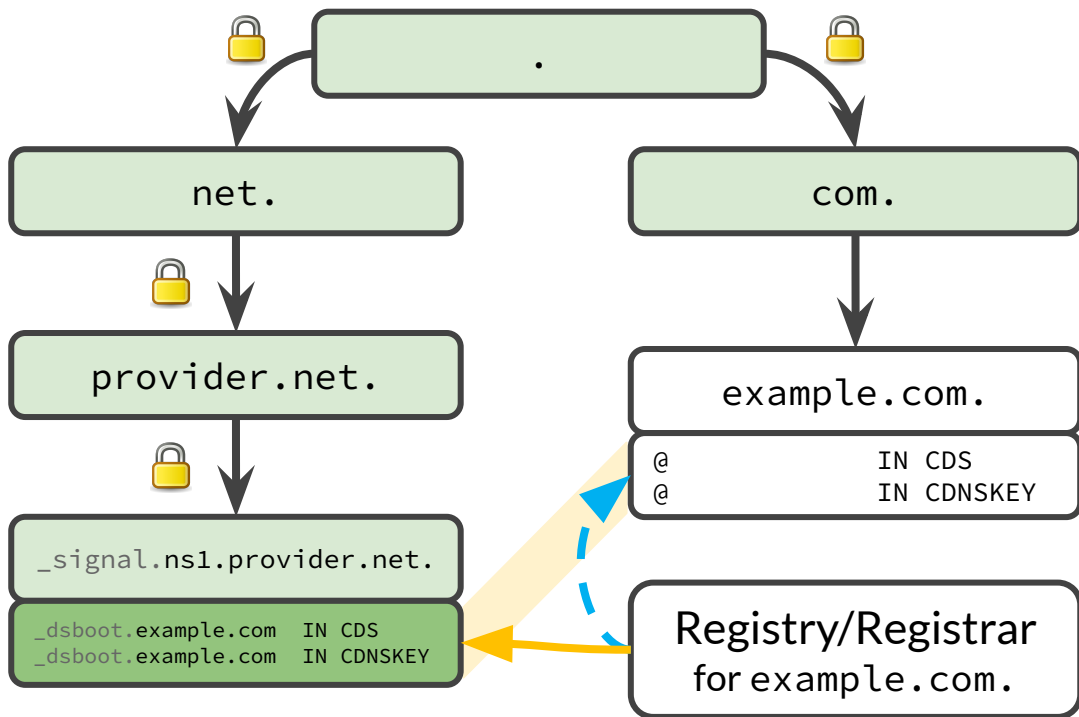
— — —



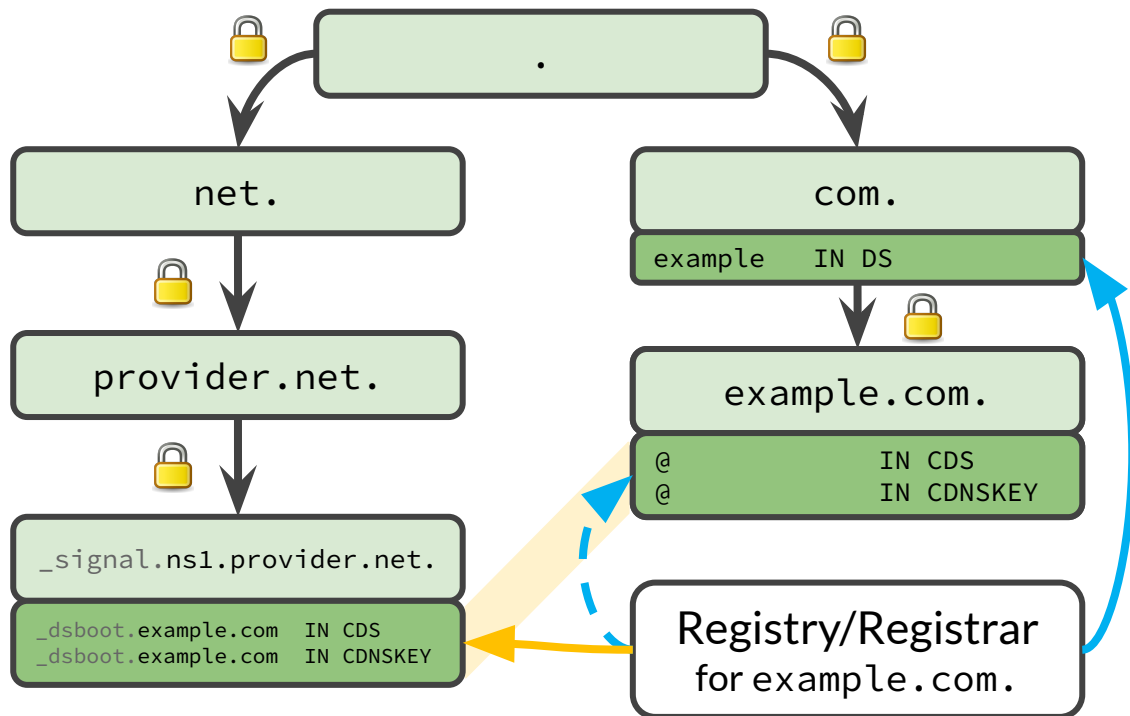
Approaches: CDS/CDNSKEY with Authentication



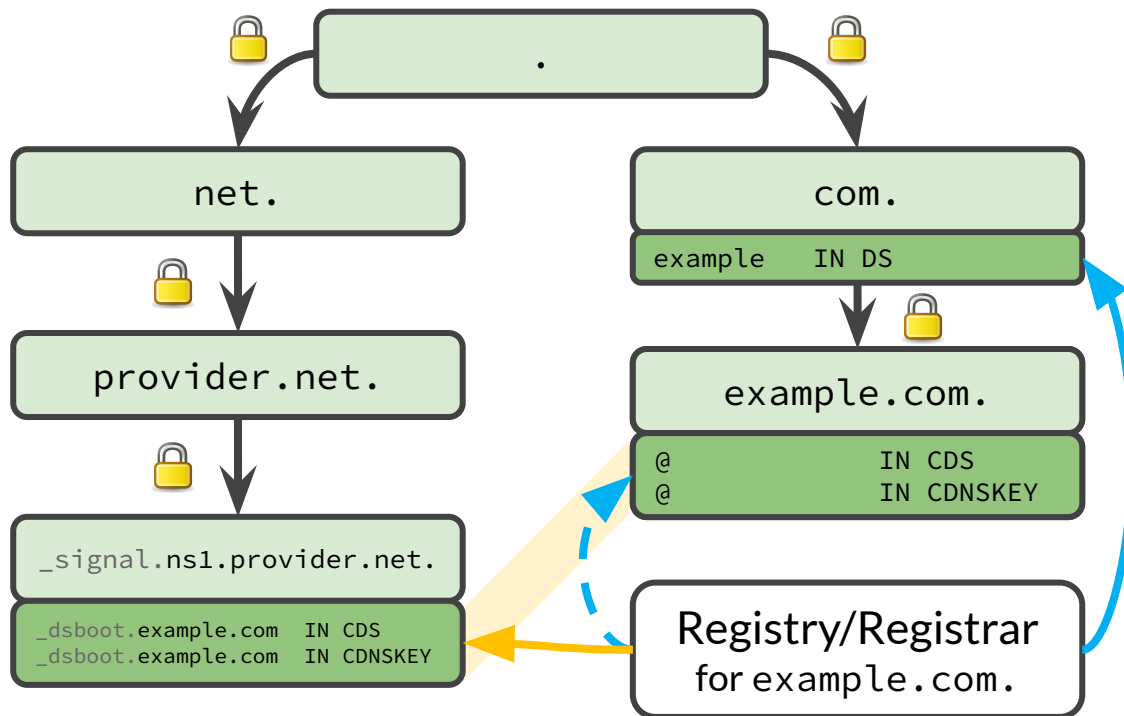
Approaches: CDS/CDNSKEY with Authentication



Approaches: CDS/CDNSKEY with Authentication



Approaches: CDS/CDNSKEY with Authentication

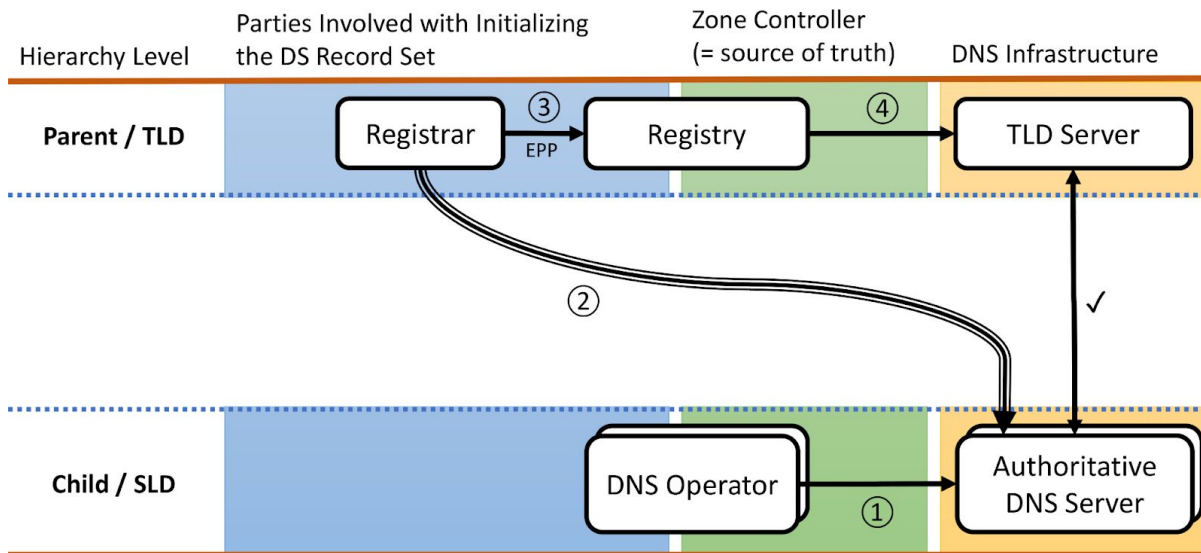


💡 Use an **established chain of trust** (left) to take a detour

- authenticated, immediate
- no active on-wire attacker

Automation Simplifies the Multi-Party Problem

- No manual dealing with cryptographic parameters
- Known timing
- Authenticated



Risks and Open Issues

— — —

- Operator might hamper provider change by turning on DNSSEC w/o consent
 - Inherent in all automation methods trying to avoid involving the Registrant
 - However: DNS Operator may not publish zone contents at will
 - CDS/CDNSKEY may only be published if ordered by customer (similar to MX)
 - When zone is signed, Registrant apparently wants DNSSEC (especially when signaled!)
 - Improper behavior of one business party best addressed contractually
 - RFC 8078 (CDS/CDNSKEY) defines special “delete” records; issue not otherwise raised in WG

Risks and Open Issues

— — —

- Operator might hamper provider change by turning on DNSSEC w/o consent
 - Inherent in all automation methods trying to avoid involving the Registrant
 - However: DNS Operator may not publish zone contents at will
 - CDS/CDNSKEY may only be published if ordered by customer (similar to MX)
 - When zone is signed, Registrant apparently wants DNSSEC (especially when signaled!)
 - Improper behavior of one business party best addressed contractually
 - RFC 8078 (CDS/CDNSKEY) defines special “delete” records; issue not otherwise raised in WG
- Loss of resolution in case of deployment of faulty DS record
 - Same for all DS deployment methods: parent responsible for performing acceptance checks

Risks and Open Issues

— — —

- Operator might hamper provider change by turning on DNSSEC w/o consent
 - Inherent in all automation methods trying to avoid involving the Registrant
 - However: DNS Operator may not publish zone contents at will
 - CDS/CDNSKEY may only be published if ordered by customer (similar to MX)
 - When zone is signed, Registrant apparently wants DNSSEC (especially when signaled!)
 - Improper behavior of one business party best addressed contractually
 - RFC 8078 (CDS/CDNSKEY) defines special “delete” records; issue not otherwise raised in WG
- Loss of resolution in case of deployment of faulty DS record
 - Same for all DS deployment methods: parent responsible for performing acceptance checks
- Timing considerations
 - Same as for DS automation: inefficiency/latency of scanning → see other presentations

Thank you!

Questions?
