DANE

Jakob Schlyter – jakob@kirei.se – Kirei AB

Workshop „E-Mail-Sicherheit: Was Provider beitragen können“

kirei

Jakob Schlyter

kirei

Kirei AB

kirei

DNSSEC since 1999

kirei

DNSSEC for .SE in 2007

kirei

Root DNSSEC in 2010

kirei

Swedish e-Id Scheme

SOU 2010:104

kirei

RFC 6698

kirei

DANE

kirei

Why DANE?

kirei

Constrained trust

kirei

Keep PKI on a leash

kirei

Why?

In theory PKI is simple

kirei

Issuance

kirei

Revocation

kirei

Validation

kirei

In practice, PKI is complex

kirei

Identity proofing via insecure channels

kirei

No name constraints

kirei

Relaxed revocation checks

Limit trust in PKI using DNSSEC

kirei

Limit the amount of damage that a CA can do

kirei

Bridge trust using DNSSEC

kirei

Validate identity without the legacy PKI

kirei

If DNS is used for identity proofing …

kirei

… and DNSSEC provides

data origin authentication,

why involve another

3rd party?

kirei

How DANE?

kirei

TLSA

Provides bindings of keys to
domains that are asserted by DNS

kirei

CA Lock

- TLSA enumerates acceptable CA certs
- Only accept certificates under a specific CA
- Optionally used together with classic PKIX

Protects against CA malpractice

kirei

Certificate Lock

- TLSA enumerates acceptable certificates for end entities (servers)
- Only accept specific certificates
- Optionally used together with classic PKIX

Addresses the problem with fraudulently issued certificates

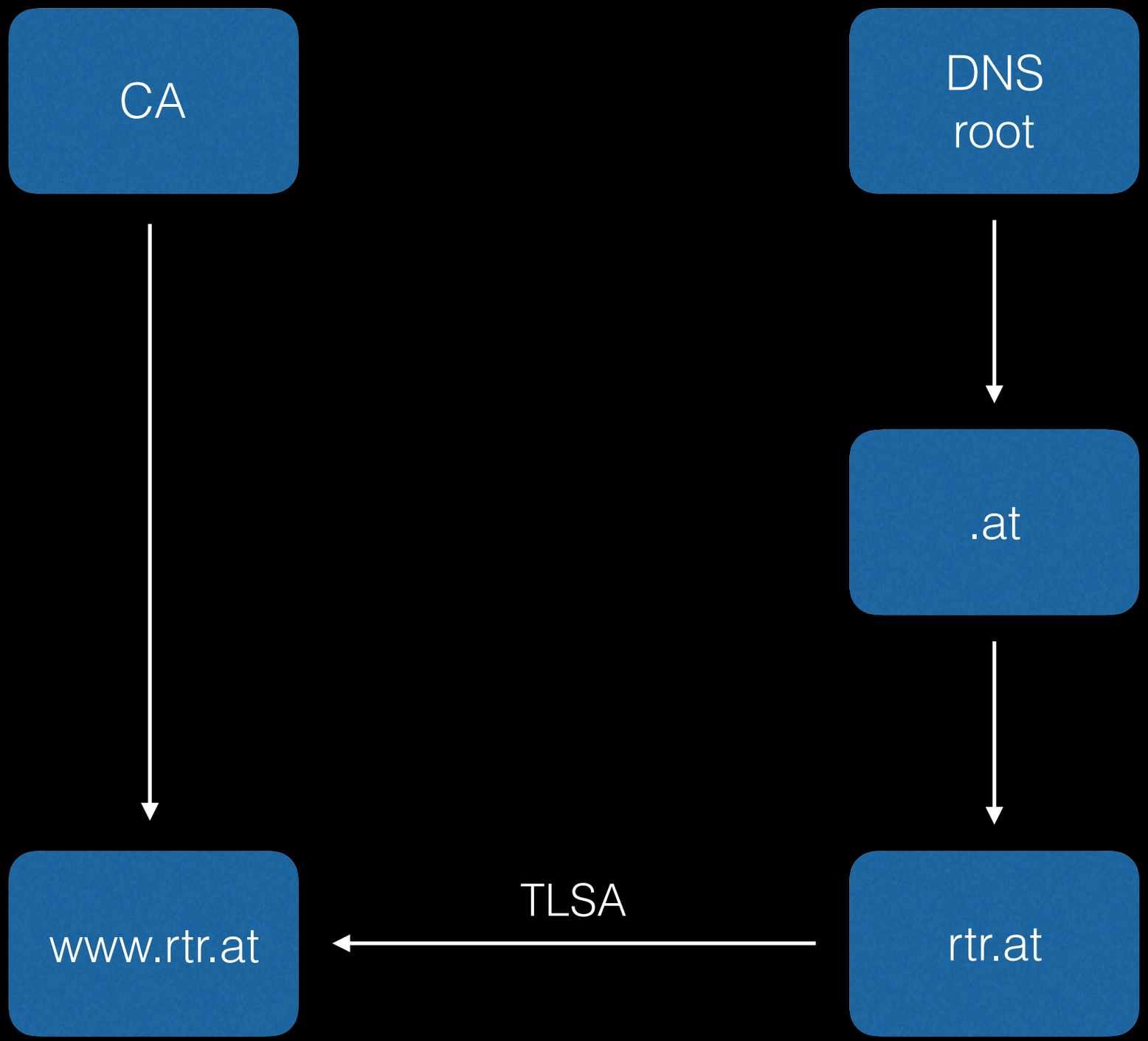
kirei

Self-signed Certificates

- Self-signed key pair certified by the user, or by a private CA

Enables TLS without depending on existing PKI infrastructure

kirei



kirei

	PKI	DANE
Authentication	DNS for identity proofing	DNSSEC when used
Revocation	OSCP / CRL / CT	DNSSEC
Validation	PKIX	PKIX & DNSSEC

kirei

DANE for Mail Transport Security

kirei

How does SMTP authentication & encryption work today?

kirei

Not

kirei

Or rather…

kirei

Opportunistic

kirei

No widespread deployment of universal trusted certificates

No endpoint validation

Depending on trust in DNS and routing

RFC 7672

SMTP Security via Opportunistic DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS)

kirei

Example: SMTP with DANE

kirei

kirei.se

kirei

MX for kirei.se ?

kirei

spg.kirei.se

kirei

TLSA for _25._tcp.spg.kirei.se ?

TLSA 3 1 1

Hash of the public key from the X.509 certificate for spg.kirei.se

kirei

#win

kirei

Multiple implementations

Postfix by Wietse Venema

kirei

Halon SMTP platform

kirei

Inbound

kirei

Publish TLSA records in a signed DNS zone

kirei

Outbound

kirei

DNSSEC validation at mail egress

kirei

Validate TLSA for outbound connections

kirei

DANE for
End-to-end Mail Security

kirei

PGP mostly used by the technical community

kirei

S/MIME supported
by not widely deployed

kirei

Why?

S/MIME requires certificates

kirei

DANE for OpenPGP

kirei

DANE for S/MIME

kirei

Signed email

kirei

Encrypted email

kirei

Subjects are
email addresses

kirei

jakob@kirei.se

kirei

SHA2-256("jakob") [0:28]

kirei

5205c624938881 49cb6953d0a542

kirei

5205c624938881 49cb6953d0a542
._smimecert.kirei.se.

kirei

SMIMEA 3 0 0

Full certificate for jakob@kirei.se

kirei

Work in progress

kirei

Local part processing

jakob@kirei.se

≠

Jakob@kirei.se

kirei

mariahilfer-straße@rtr.at

≠

mariahilfer-strasse@rtr.at

kirei

jakob@kirei.se

kirei