How to use DNSSEC to keep PKI on a leash

Jakob Schlyter

ICANN'46 DNSSEC Workshop

kirei

¿ Jakob Schlyter ?

- DNSSEC since 1999
  - .SE and other ccTLDs
  - Root DNSSEC Design Team
- IETF contributor – SSHFP, DANE

kirei

Why does PKI have to be kept on a leash?

kirei

kirei

Problem #1

- Any universally trusted (e.g., WebTrust™) PKIX Certification Authority can issue a certificate for any host on the Internet.
  - X.509 name constraints are not in wide use.
  - CA malpractice hard to mitigate.
  - Attacks happening today. Perhaps even here.

kirei

Problem #2

- The current CA model effectively puts a tax on enabling secure communications.
  - Domain validation certificates costs approximately $12 per host.
  - Extended validation costs considerably more.

kirei

Goal

- Enable path restrictions
  - Limit the amount of damage that a single Certification Authority can do.
- DNSSEC for identity validation
  - Certification validation without legacy PKI

kirei

If DNS is used for identity proofing …

kirei

… and DNSSEC provides data origin authentication,

kirei

why involve a 3rd party?

kirei

Is this a new idea?

kirei

CERT

RFC 2538 – 1999

"Alternatively, if certificates are retrieved from a secure DNS zone with DNS security checking enabled and are verified by DNS security, the key within the retrieved certificate MAY be trusted without verifying the certificate chain if this conforms with the user's security policy."

kirei

draft-schlyter-pkix-dns-02

2002

PKIX WG – "We are not amused"

kirei

DANE

DNS-based Authentication of Named Entities

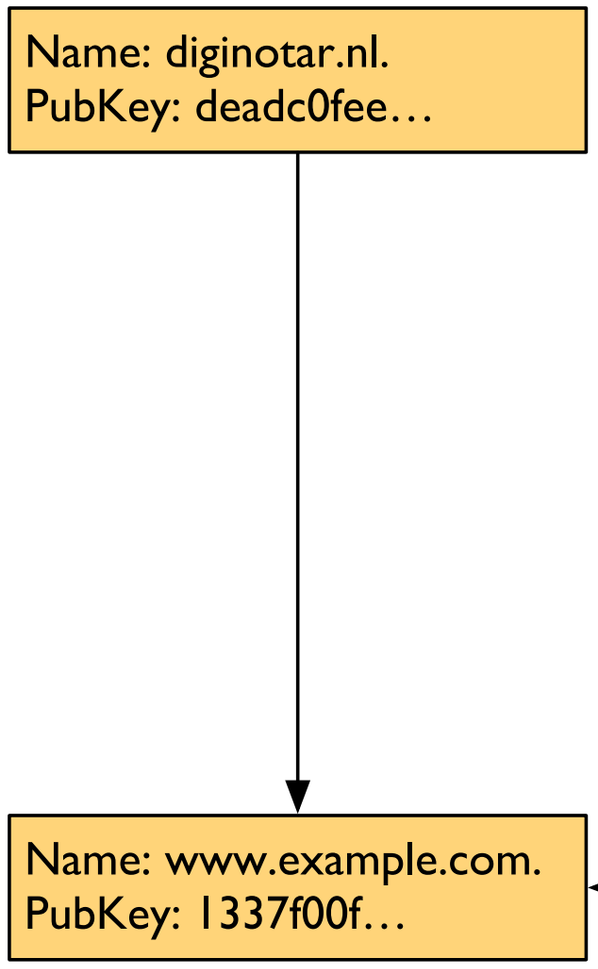
kirei

RFC 6698

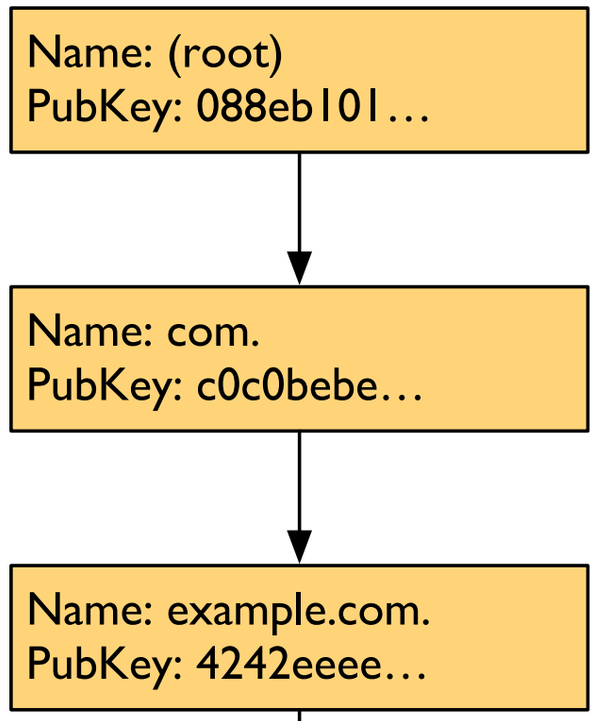
Provides bindings of keys to
domains that are asserted by DNS

kirei

PKIX Hierarchy



DNSSEC Hierarchy



kirei

CA Lock

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

✓ Protects against CA malpractice,
e.g., fraudulently issued certificates.

kirei

Certificate Lock

- TLSA enumerates acceptable EE certificates
  - Only accept specific certificates
  - Optionally used together with classic PKIX

✓ Addresses the problem with fraudulently issued certificates.

kirei

Self-signed Certificates

- Possible with or without a private CA

✓ Enables TLS without depending on existing PKI infrastructure.

kirei

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

kirei

Got rough consensus.
Got running code?

kirei

Implementations

- DANE Utilities
  - https://github.com/pieterlexis/**swede**
  - http://people.redhat.com/pwouters/**hash-slinger**/
- Postfix with DANE
  - https://github.com/vdukhovni/postfix
- Generic OpenSSL with DANE
  - Work in progress

kirei

Challenges & Future Work

kirei

Last Mile Security

- Is DNSSEC validation in the endpoint realistic?
- Can we get DNSSEC data to someone behind filtering infrastructure?
  - Is tunneled DNS a viable solution?

kirei

DANE for S/MIME

draft-ietf-dane-smime-01

- Binding an email address to a domain name
- Use TLSA-like mechanisms to validate certificate

kirei

jakob@kirei.se

kirei