

SIP and DNS-sec based TLS setup (DANE)

random thoughts by oej@edvina.net
Olle E. Johansson

V 3.14 - 2014-02-27

IETF 89, London, March 2014

Today's question

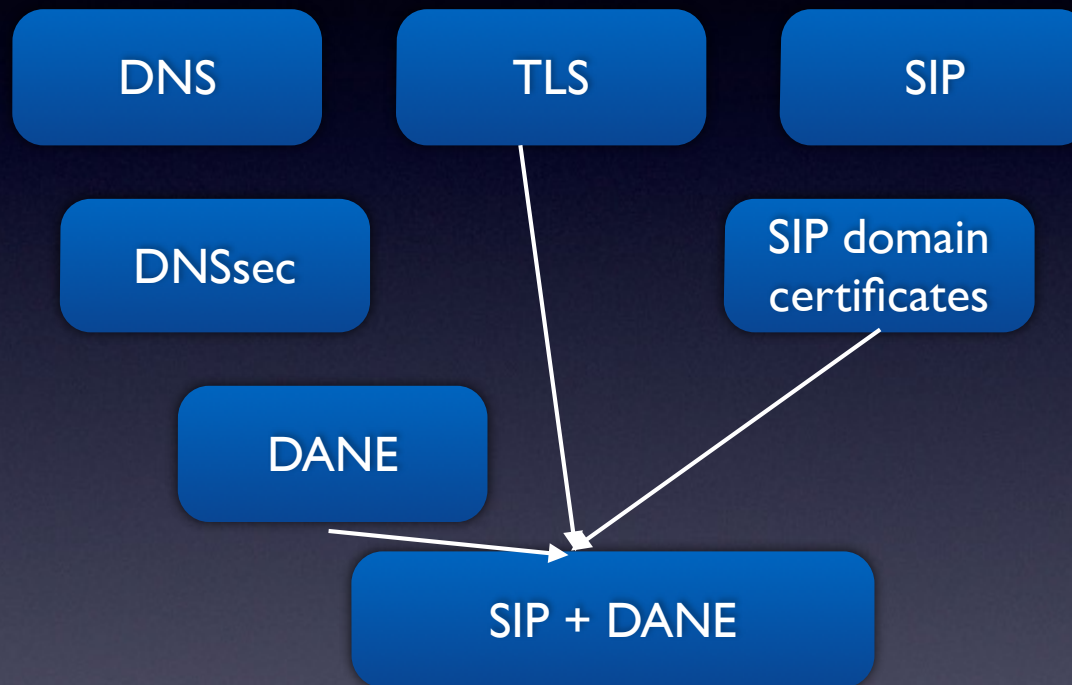
- Do we want to add this work to our charter?

SIP & TLS

- SIP uri target domain is verified against SubjectAltName uri records
- if no SAN uri records, SAN DNS records
- If no SAN records, CN
 - *But no CN check if there are SAN records!*

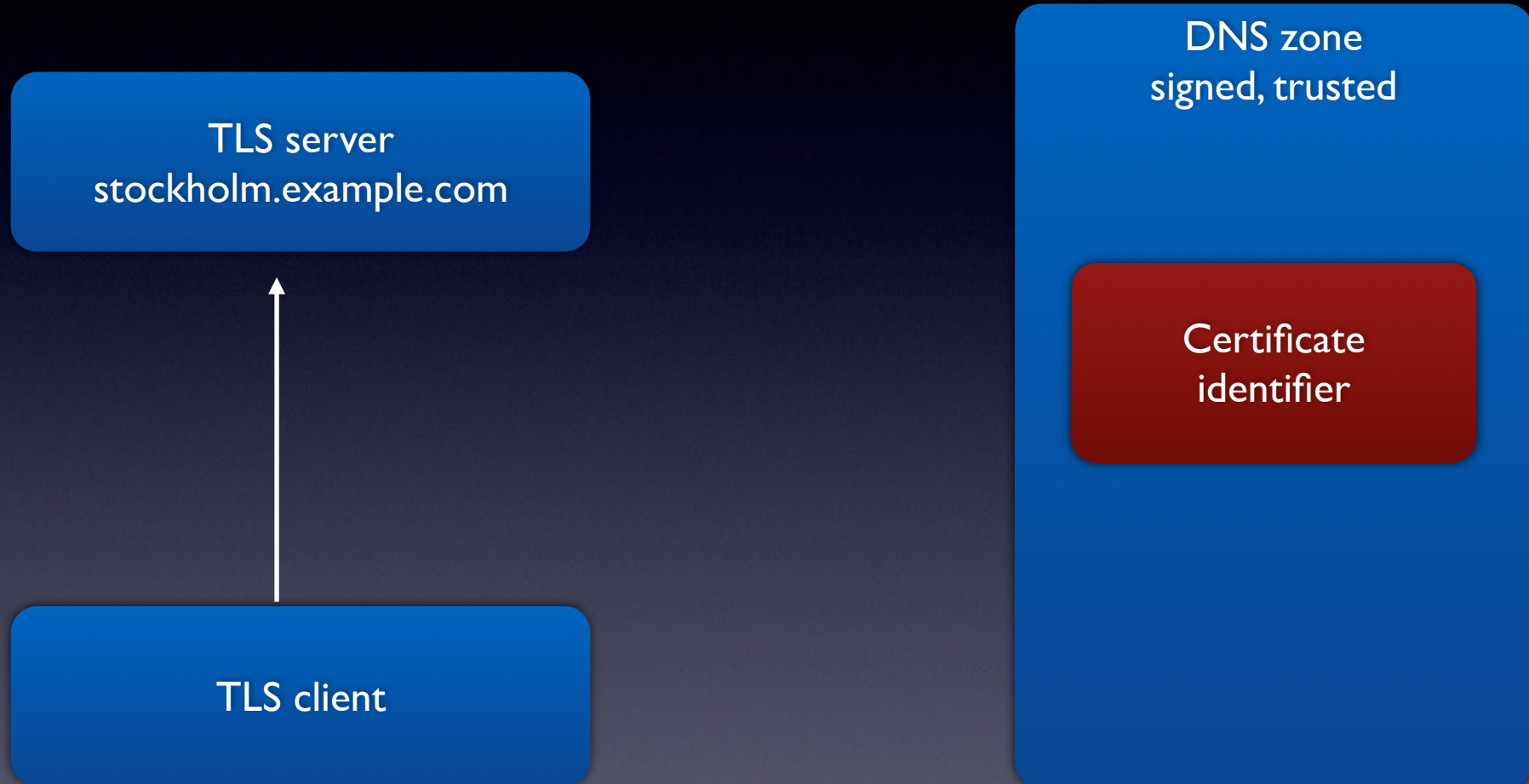
RFC 5922

Dependencies



*To trust DANE
you need to trust DNSsec*

Dane simplified



Questions



Is the certificate signer (CA) the right one?

Do I trust this certificate?

Am I talking with the right server?

DANE simplified



Dane summary

- Can publish constraints
 - This CA is the only one accepted
 - This certificate is the only one accepted
- Can publish root of private CA
 - This CA cert is the one used to sign my server certificates
- Can publish certificates

In all cases, a full cert or the public key can be published - or fingerprints of these.

TLSA selector and matching

Selector

- 0 - Full certificate included in TLSA
- 1 - Public key included in TLSA

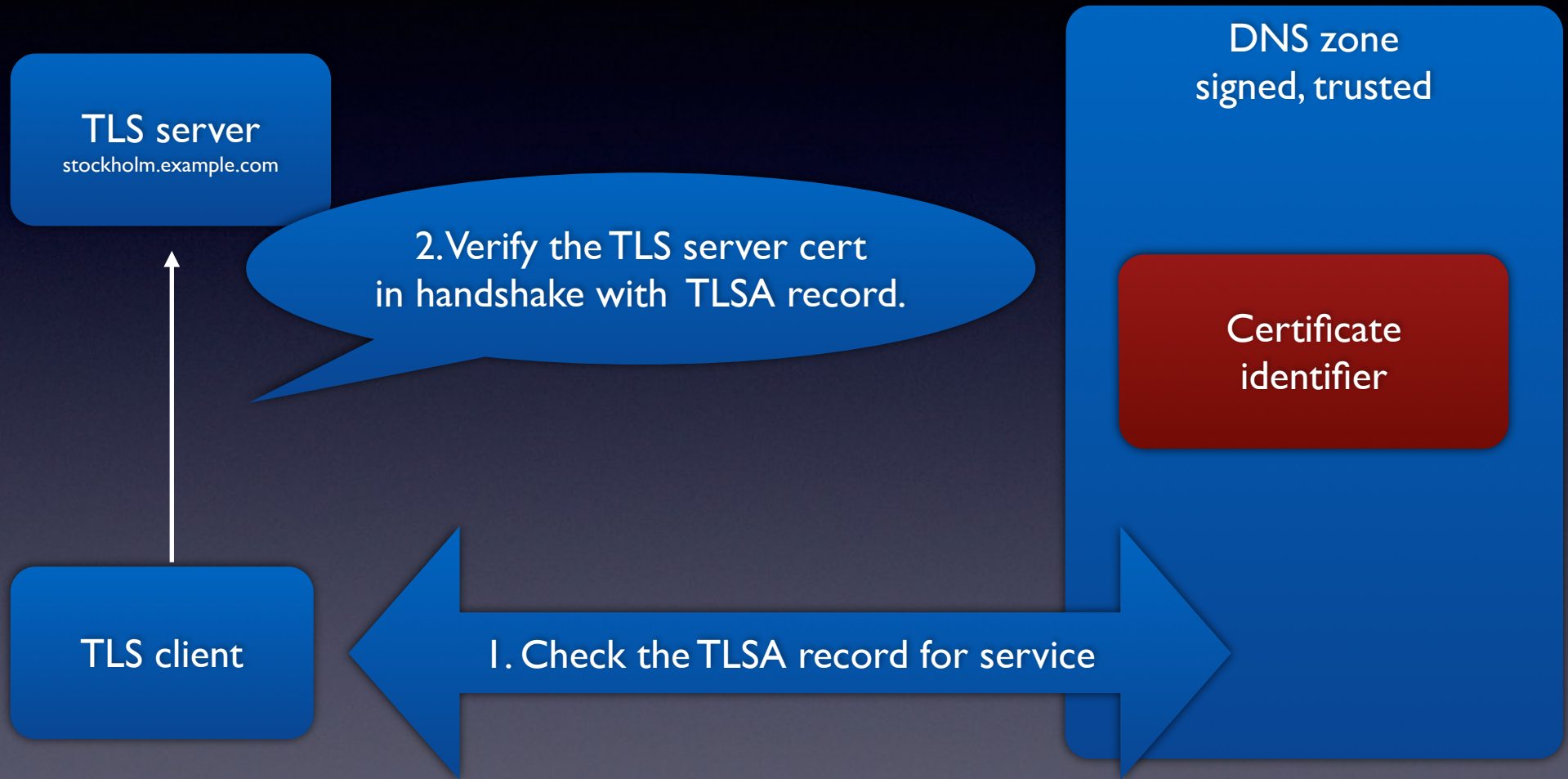
Matching

- 0 = Exact match
- 1 = the data is SHA-256 hash of content
- 2 = the data is SHA-512 hash of content

TLSA records

- Usage 0: CA constraint. Certificate or public key of CA
- Usage 1: Certificate constraint. Certificate or public key of cert signed by CA.
- Usage 2. Certificate or public key of cert serving as trust anchor for the cert given by the server ("private CA")
- Usage 3: A certificate or public key that matches the cert given by the server (No PKIX check)

DANE simplified



The DANE promise

- If you trust the DNS (using DNSsec) then we can use that instead of the certificate store to check server identity and authorisation.

Back to SIP

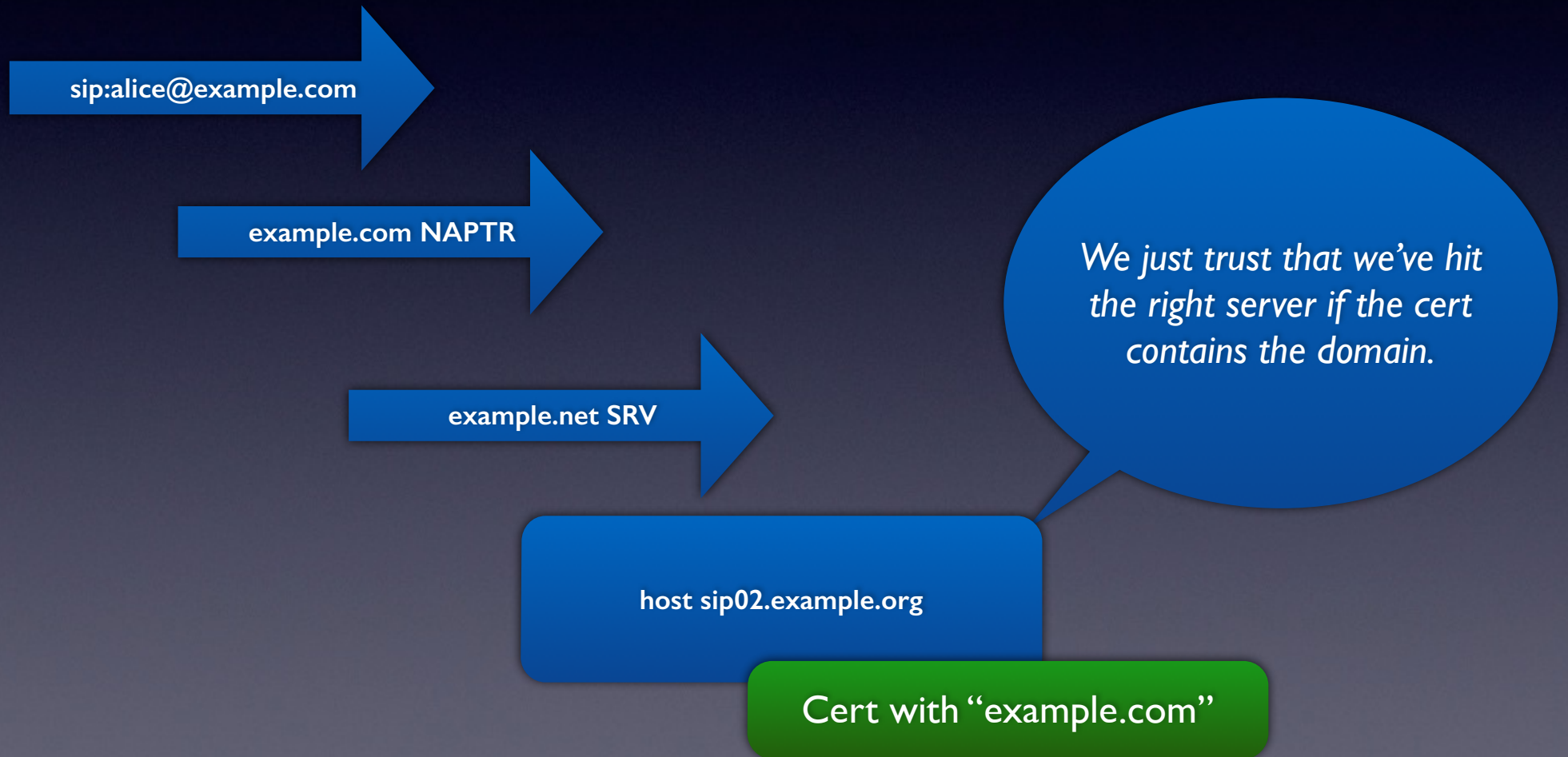
SIP DOMAIN CERTS

- Connect a SIP URI domain part with a certificate
- Mix server identification with domain authorisation
- Only domains in the certificates
- New certificate every time we add a domain or subdomain
- No wildcard certs

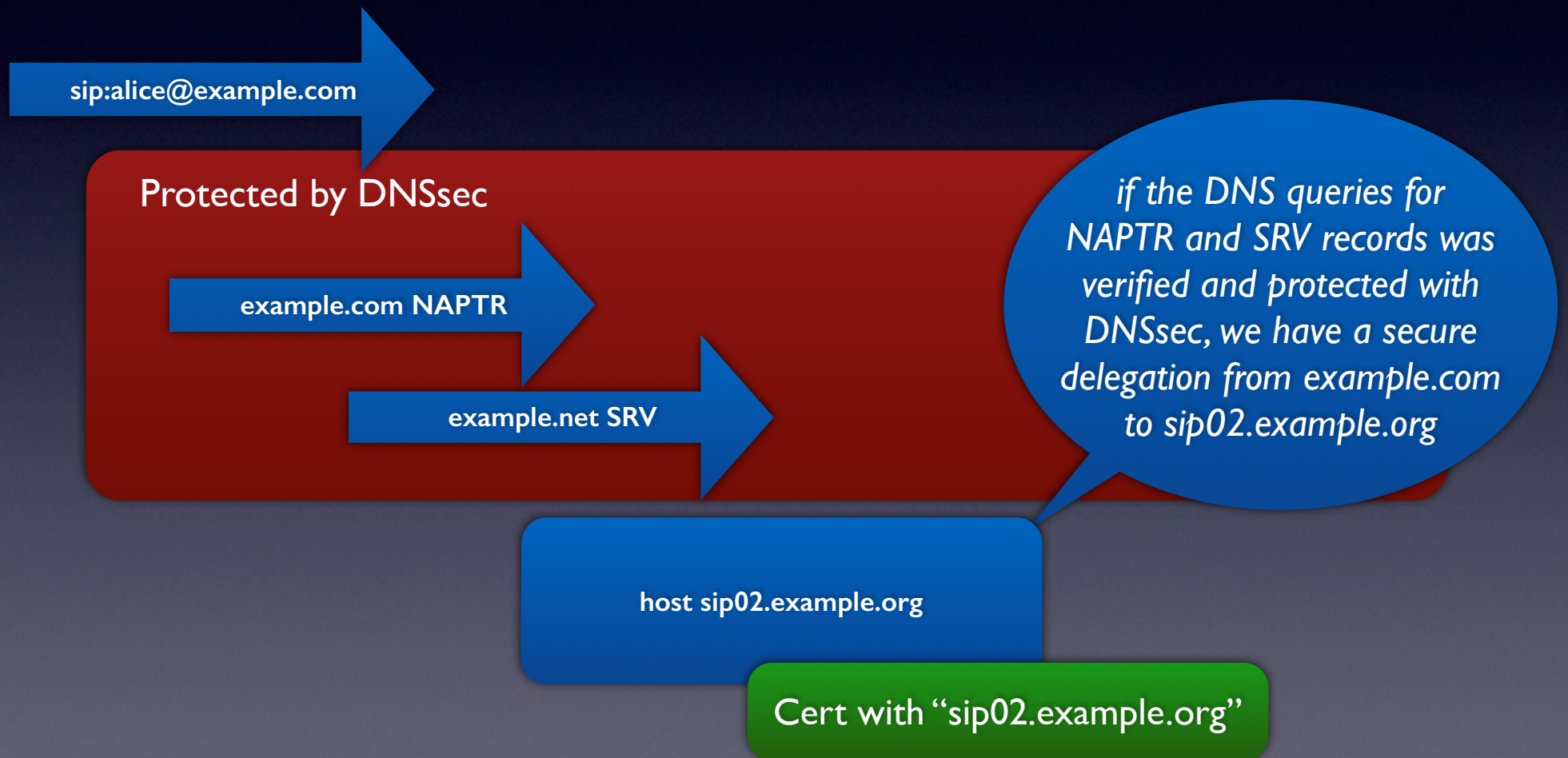
What about SNI

- Many certificates on one TLS server and IP.
- No support for DNS names
- ONLY host names.

SIP



DANE Secure delegation



Not fully secure is insecure

- If the NAPTR was DNSsec protected but not the SRV, we have no secure delegation.
- If there's no DNSsec in either NAPTR nor SRV we're insecure too.
- The SIP Uri to TLS certificate matching in RFC 5922 applies in this case

If we have a secure delegation

- Check for TLSA record for the srv host name and port
 - `_5068._udp.sip02.example.org`
- If no TLSA record is found, then DANE doesn't apply - proceed according to RFC 5922
- If TLSA record exists, continue to the next slide

Our identifiers

- The SIP domain in the request URI
 - *Used in insecure delegation*
- The SRV FQDN from SRV lookup of the domain (protected with DNSsec)
 - *Used in secure delegation as well as with TLSA record verification*

Validation

- With TLSA usage 0 and 1, use these constraints then verify cert as before
- With TLSA usage 2 and 3, use the information to validate cert
 - *If either TLSA validation fails, connection should fail.*
 - *With usage 0 and 1, after TLSA validation normal PKIX validation happens.*

Sideways jumps

- When a NAPTR or SRV record points to a name in another domain, the client needs to make sure that the new domain is validated in DNSsec as well.
- If not, delegation is insecure

SIP Fallback logic

- If there's no secure delegation, use RFC 5922, if that fails go to next SRV server in the list
- When out of SRV servers, TLS connection has failed.

Compatibility with non-SRV clients

- Fallback to RFC 5922
- Since dane-srv-02 requires TLS SNI this will be sorted out by the server.
- SRV/DANE compatible UAs will require cert for SRV host name
- Non SRV/DANE UAs will require cert with SIP uri target domain

If no SNI support is available

- Cert with
 - *CommonName = hostname*
 - *SubjectAltName = SIP domain*

SIP connection reuse

- RFC 5923 use TLS cert content to add aliases to a connection.
- With DANE, the cert will include only the hostname
- SIP/DANE will have to add aliases as they are verified using DNSsec
- If a domain share a SRV hostname and the trust chain is verified between domain and SRV, the existing connection to the SRV host may be used for this domain too (and alias added to the alias table)

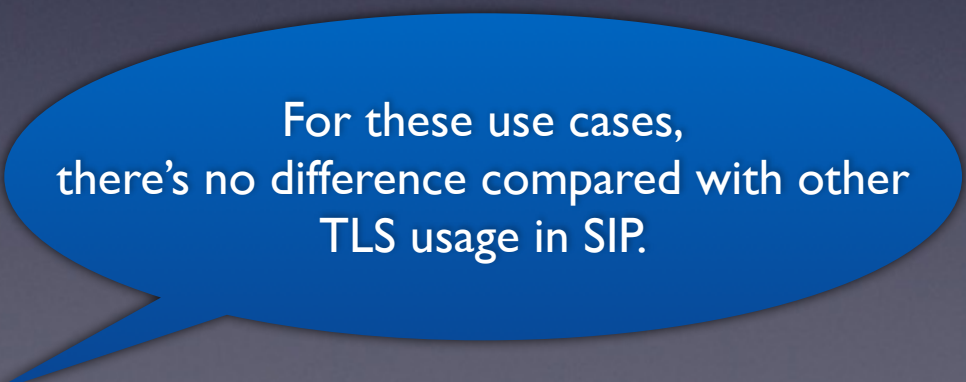
Verification of client certificates in RFC 5923

- Connection reuse requires a SIP server using RFC 5923 to request a client certificate
- Which DNS name do we use to look up TLSA records and verify the client?

Can this be done?

Not to worry about now

- SIP identity
- SIMPLE
- SIPS: uri's



For these use cases,
there's no difference compared with other
TLS usage in SIP.

Reading material

RFC 5922	SIP Domain Certificates
RFC 6698	DNS based authentication of named entities (DANE)
draft-ietf-dane-srv	DANE and SRV/MX records
draft-ietf-dane-smime	DANE and SMIME identities
draft-ogud-dane-vocabulary	DANE vocabulary for application usages
RFC 5923	Connection Reuse in SIP
draft-johansson-dispatch-dane-sip-01	The draft on SIP and DANE