DANE Best Current Practice

draft-dukhovni-dane-ops-01

Viktor Dukhovni
&
Wes Hardaker

IETF 87, Berlin
July 2013

General DANE Guidelines (Type Independent)

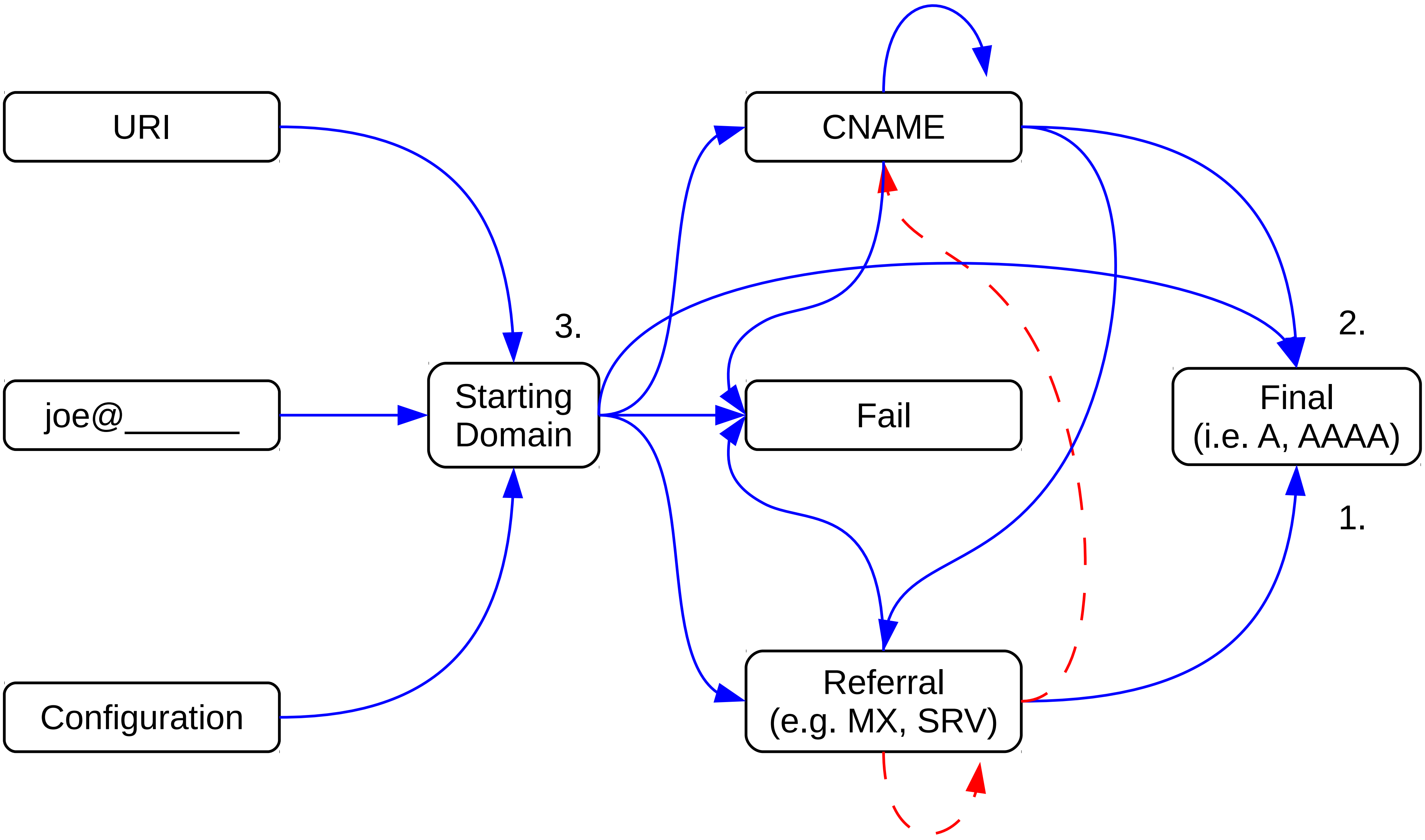
Large DNS payload issues

- Issues with large UDP packets:
  - UDP fragments can not always be delivered
  - Provides a greater opportunity for amplification attacks
  - Doubling of TLSA RR size during X.509 key rollover
    - (and may not have been anticipated in initial testing)
- Conclusion:
  - Hashes are best (use “TLSA * * [12]”)
  - Avoid publishing certificates directly (avoid “TLSA * 0 0”)
  - Keys are better, but still big (try to avoid “TLSA * 1 0”)
    - Test “TLSA * 1 0” RRs, thoroughly!
    - 2048-bit RSA key is 256 bytes, so 2 keys exceed 512 bytes
  - Be sure to enable DNS over TCP everywhere

Selector Matching Guidelines

- SHA256 vs SHA512:
  - SHA512 Optional for clients
  - No known security advantage to SHA512
  - Best current selector is SHA256
  - Servers should avoid publishing SHA512
  - Clients should support SHA512

Referral and CNAME Processing and TLSA Base Domain Preferences



CNAMEs

- The TLSA base domain should be the name sought in peer certificate
  - (when name checks are applicable).
- If a server has many aliases:
  - The server may need many certificates
  - SNI is needed to select the right one.
  - But SNI key management difficult in practice

CNAMEs

- Protocol design recommendation:
  - Start with primary server name
  - Chase CNAME RRs to obtain TLSA base domain
- If a protocol can't chase CNAMEs:
  - Operational guidance:
  - When server is a CNAME, also alias the TLSA RR

```
www.example.com.               IN CNAME www.example.net.
_443._tcp.www.example.com.     IN CNAME _443._tcp.www.example.net.
```

  - Avoids the need to mirror data from the server
    - (A and TLSA records)
  - Requires SNI at the server (unless using Type 3)

Type-Specific Guidelines

Type 3 Guidelines

- Usage 3 certificate is just an opaque public key container or reference
  - No external trust in the issuer for names, lifetimes, etc
  - No pre-configured trusted issuer needed
  - No expiration checks
    - (handled by the TLSA RRSIG expiration)
  - MUST ignore subject name checks
    - The TLSA base name = the name binding
    - Implementations hopefully won't check anyway

Type 3 Guidelines

- Least likely to fail validation of all certificate usages
  - provided DNS data correct
  - Best for KISS
- Operational Guidance:
  - DNS must be updated **before** the server key is updated
  - Servers SHOULD add matching subjectAltName DNS entries
    - For the base domains of all relevant TLSA RRs

Type 2 Guidelines

- Certificate usage 2 supports private-label TAs
- For Client Usage of TLSA 2 1 0:
  - Client may not have the TA certificate available
  - Current APIs make using a bare public key non-trivial
  - Same applies with usage 0 for protocols where clients don't distinguish between usages 0 and 2
- Recommendations:
  - **Server chain MUST include the certificate pointed at by the TLSA record**
  - Requires admin education
    - This is not current practice today

Type 0/1 Guidelines

- For some protocols, type 0/1 may not provide help
  - EG, STARTTLS man-in-the-middle attacks
  - These protocols SHOULD recommend against publishing and using 0/1
    - The SMTP draft will say “undefined behavior”
  - They MAY choose to map 0 → 2 and 1 → 3
    - If so, use the Type 2 and Type 3 guidelines

Interaction with Certificate Transparency

Certificate Transparency Interaction

- CT is designed to keep public CAs honest
- DANE is designed to bind certs to a DNS name
- CT says:
  - “TLS clients MUST reject certificates that do not have a valid SCT for the end-entity certificate.”
  - “(Note: This effectively excludes self-signed and DANE-based certificates until some mechanism to control spam for those certificates is found. The authors welcome suggestions.)”
- DANE says:
  - Don't do CA checks if type 3 or type 2 is in use

Certificate Transparency Interaction

- Advice for protocols and/or implementations:
  - Pick one
  - Don't do both

Certificate Transparency Interaction

What if you must do both?

- DANE Type 1/3:
  - Verification not subject to CT (there is no CA)
  - These bind the EE cert
  - Thus are immune to rogue or compromised CAs
- DANE Type 2 (Private-label CA):
  - Verification not subject to CT
- DANE Type 0 (Public PKIX CA):
  - CT still applies

What To Do With This Work?

- Accept as a WG document?
- BCP?
  - But some things were really “missing” from the original DANE spec
- Are there guidance items that are needed?
  - Algorithm rolling has been discussed as missing