“Representation and Verification of Domain-Based Application Service Identity in Certificates Used with Transport Layer Security”
(draft-saintandre-tls-server-id-check-08)

IETF 78, Maastricht
Peter Saint-Andre & Jeff Hodges
Problem Statement

• Many client-server technologies use X.509v3 certificates with TLS (HTTP, IMAP, LDAP, SIP, SMTP, XMPP, syslog, etc.)

• Client needs to verify identity of the server to which it connects

• Each application protocol defines slightly different rules for identity verification
Goals

• Define best practices for authentication of a server in client-server applications

• Provide guidance to:
  • Certificate issuers
  • Application client developers

• Might also be helpful to server developers, operators, etc.
Scope

• Define rules for representation (certificate issuance) and verification (client handling)
• FQDN-based application services only (not clients, not IP addresses, etc.)
• TLS only (not IPsec, DTLS, etc.)
• PKIX (X.509v3) only (not OpenPGP, etc.)
Terminology

• Re-use terms from X.500, X.501, X.509, RFC 5280, RFC 4514, RFC 4519, RFC 4985

• Define a number of terms: application service, source domain vs. target domain, presented identifier vs. reference identifier

• Also discuss subject naming
Issuance Rules

• Encourage dNSName in subjectAltName

• If appropriate, use SRVName or uniformResourceIdentifier

• Discourage FQDN in CN (but not prohibited yet)
Verification Rules

• Reference identifier comes directly from user or config (not automated resolution)

• Accept on first match found between presented identifier and reference identifier

• Check wildcard “*” only as left-most label

• Check CN only if no FQDN in SAN
Next Steps

• Version -08 in IETF Last Call now
• Feedback needs to be incorporated
• Authors are meeting this week to coordinate regarding changes to the spec
• Version -09 to be submitted very soon
• Please provide feedback!