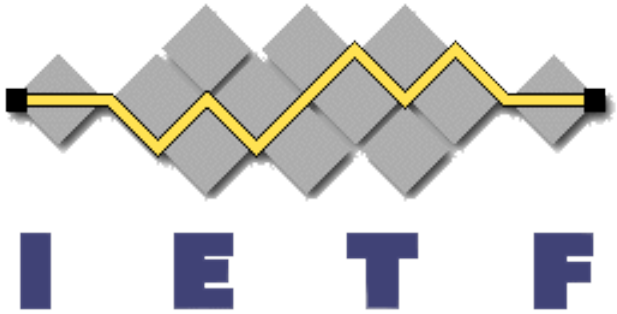


# Domain Certificates in SIP

Vijay K. Gurbani, Scott Lawrence, and Alan Jeffrey

draft-gurbani-sip-domain-certs-06

IETF-69, Chicago, Illinois

SIP WG

- Changes since IETF 68 (version -04):
  - Change in Abstract: document provides a profile of pkix-compliant certificates for domain authentication in SIP.
  - Extensive review from pkix WG around general RFC RFC 3280 guidelines and EKU usage.
  - Algorithmic description of finding and matching identities in subjectAltName to the server being authenticated.
  - The draft now provide behavioral guidelines for generic servers and clients.
  - The draft also provides behavioral guidelines for specific instances of a proxy, registrar, or redirect server and virtual servers.
  - URIs prefixed by “sip” in the certificate.
  - Removed all discussion of route pinning.

## ♣Feedback from PKIX WG:

- Regarding DNS names in CN:
  - Stephen Kent (pkix WG co-chair) ”PKIX standards made an exception for RFC 822 names in legacy certificates, but not for DNS names or URIs! There is a private extension, developed by Netscape for representing a DNS name in a certificate prior to the advent of SAN. I think it's rather late to be accommodating certificates that are not compliant with RFC 3280, a spec that is 5 years old.”
- Regarding FQDNs in certificate:
  - Authors and S. Kent: May be sufficient to have a domain identity (sip:example.net) instead of a host-specific identity (sip:proxyB.example.net).

- Feedback from pkix (continued):
  - id-kp-anyExtendedKeyUsage is a wildcard EKU.
  - Interaction of id-kp-sipDomain and id-kp-anyExtendedKeyUsage:
    - If certs are to be used ONLY for SIP: id-kp-sipDomain is REQUIRED. id-kp-anyExtendedKeyUsage MAY be present, but without the SIP EKU as well, the cert cannot be used for SIP validation.
    - A cert with ONLY id-kp-anyExtendedKeyUsage EKU MUST NOT be used for SIP domain validation, but can be used for any other application-specific use.
    - A cert with ONLY id-kp-sipDomain MUST be used for SIP domain validation ONLY, and not any other purpose.

- Next steps:
  - Authors believe that the work is nearly complete and contributes to the SIP charter item of “Guidelines for use of existing security mechanisms such as TLS, IPSec, and certificates.”
  - Adopt as working group agenda item?