TLS Server Identity verification procedure for Email Servers (SMTP/IMAP/POP)

draft-melnikov-email-tls-certs-02.txt

Alexey Melnikov <alexey.melnikov@isode.com>

Changes since 01

- Clarified terminology for lazy readers (== people who don't want to read RFC 6125)

- Added "updates RFC 3207" (only for SMTP submission, MTA-to-MTA is currently out of scope)

What's next?

- Add more examples of certificates?
- Honestly, the document is done!

What is in X.509 certificate?

Subject Name/ subjectAltN	MUA Reqs.	CA Reqs.	ISP Reqs.	Comment
dnsName (DNS-ID)	MUST	MUST	SHOULD	In use
(SRV-ID)	MUST	MUST	SHOULD	Want to deploy
(URI-ID)	-	-	-	Not used
(CN-ID)	MAY	MAY	MAY	Widely used, but deprecated

Other points

- Wildcards are allowed (only the full leftmost component of FQDN can be "*") in DNS-ID and CN-ID

- No CNAME substitution of the original DNS server FQDN is allowed

- Secure DNS resolution (e.g. DNSSEC) is not prohibited, but not really described

Changes for SMTP/IMAP/POP

Protocol	What changed	
IMAP	DNS-ID SHOULD --> MUST, SRV-ID - new req., CN-ID - not allowed (?)	RFC 3501
POP	DNS-ID SHOULD --> MUST, SRV-ID - new req., CN-ID - not allowed (?)	RFC 2595
SMTP (Submission)	Was never properly specified before	RFC 3207
ManageSieve	DNS-ID, SRV-ID SHOULD --> MUST, DNS CNAME not mentioned	RFC 5804