draft-dthakore-tls-authz

Draft-03

IETF 86, Orlando

Quick Recap

- **Proposal**? Allow for the exchange of DTCP certificates as authorization data in the TLS Handshake
  - Use extensions defined in RFC4680 and RFC5878
- **DTCP Certs**? Used for link protection of audio visual content; already deployed in Smart TV's, game consoles, blu-ray players etc.
  - HTML5 support on these devices becoming a reality
  - # of "apps" on these devices exploding
- **Benefit**? reusing the deployed certs will enable and encourage use of HTTPS for services (instead of non-standard mechanisms)!

Updates Since IETF85

- Two updates (-02 and -03) since Atlanta
  - Latest I-D: http://tools.ietf.org/html/draft-dthakore-tls-authz-03

- Latest version addresses comments and suggestions from: Mark B., Nikos M., et. al. (thanks)

Major Changes

1. DTCP Authz Structure

- Explanation on the use of nonce (by client, by server)
  - Nonce vs running hash
- Signature covers nonce when DTCP/X.509 certs sent
- See: draft-dthakore-tls-authz-03#section-3.2

2. Example Handshake

- Added a sample handshake that shows client authorization
- See: draft-dthakore-tls-authz-03#section-3.5

Related Info: Sample Implementation

- Extension implemented in OpenSSL 1.0.2 dev
  - Patches submitted to Openssl
- Adding support in Qt (QtWebKit)
  - Contributing back to Qt Base
- Will be on bitbucket.org shortly, contact me
  - d.thakore@cablelabs.com

Next Steps

- Any other Feedback?
- Ready for Last Call?