OCSP is dead. Long live...

TF-OpenSpace – Session 1, room yellow. 12 February 2014.

Lead by: Joost van Dijk (SURFnet)

Attendees: Joost, Brook, ...

Notes: Brook Schofield

Problem:

1. Certificate Transparency vs DANE for TCS (Brook)
2. What to do with DANE/Certificate Transparency/Pinning (Joost)

Joost provided info on how DANE works.

DANE requires DNSSec infrastructure.

Q: Browser Support?

A1: Generally no. DANE plugin (for Firefox) from the same team that wrote the DNSSec plugin.

A2: Chrome supports Certificate Transparency.

Q: DNSSec - who own the root certificate?

A: Generated via an open and auditable process.

Q: What do “we” want to do with DANE?

- if we can identify the use cases?

- eduroam? DANE - nl.eduroam.org -> uu.nl.eduroam.org

- RFC on use-cases ...

Securing the connection and define the routing is two different tasks.

The CA provides the “security” for the connection.

This is a possible use case for email? DKIM signatures are better.

http://datatracker.ietf.org/wg/dane/

http://www.certificate-transparency.org/comparison

http://tools.ietf.org/html/rfc6962

Chicken and Egg Problem

* Client to the resolver doesn’t do DNSSEC

* If the ISP

Pinning

* Always performed on the client

* Certificate rollover

http://googleonlinesecurity.blogspot.ch/2013/12/further-improving-digital-certificate.html

We need to find additional use cases ….

http://arstechnica.com/security/2013/12/french-agency-caught-minting-ssl-certificates-impersonating-google/

[**ACTION**] Ensure that any technical issues that should be reflected in the TCS tender are conveyed to Nicole ASAP.