Welcome

DANISH BOF
IETF111
Tuesday July 27
12:00 PDT
not-in-SFO

Agenda / Todo

- Note Well
- The story so far
- Current state of the Chartering
- Open MIC
- AOB

Note Well

This is a reminder of IETF policies in effect on various topics such as patents or code of conduct. It is only meant to point you in the right direction. Exceptions may apply. The IETF's patent policy and the definition of an IETF "contribution" and "participation" are set forth in BCP 79; please read it carefully.

As a reminder:

- By participating in the IETF, you agree to follow IETF processes and policies.
- If you are aware that any IETF contribution is covered by patents or patent applications that are owned or controlled by you or your sponsor, you must disclose that fact, or not participate in the discussion.
- As a participant in or attendee to any IETF activity you acknowledge that written, audio, video, and photographic records of meetings may be made public.
- Personal information that you provide to IETF will be handled in accordance with the IETF Privacy Statement.
- As a participant or attendee, you agree to work respectfully with other participants; please contact the ombudsteam (https://www.ietf.org/contact/ombudsteam/) if you have questions or concerns about this.

Definitive information is in the documents listed below and other IETF BCPs. For advice, please talk to WG chairs or ADs:

- BCP 9 (Internet Standards Process)
- BCP 25 (Working Group processes)
- BCP 25 (Anti-Harassment Procedures)
- BCP 54 (Code of Conduct)
- BCP 78 (Copyright)
- BCP 79 (Patents, Participation)
- https://www.ietf.org/privacy-policy/(Privacy Policy)

Administrivia

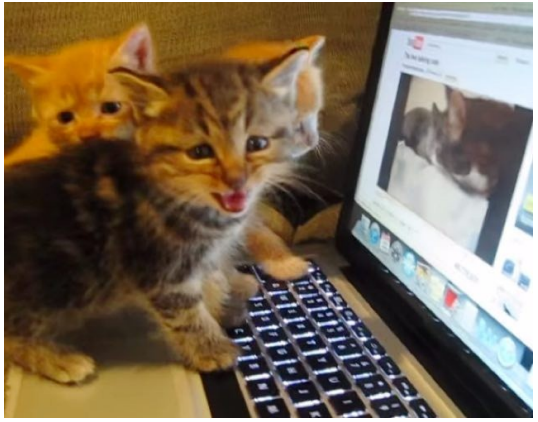
- CodIMD for notes:
  - https://codimd.ietf.org/notes-ietf-111-danish
- Meetecho will do blue sheets
- Jabber is at: danish@jabber.ietf.org
  - Please prefix with “mic:” if you want it relayed
-

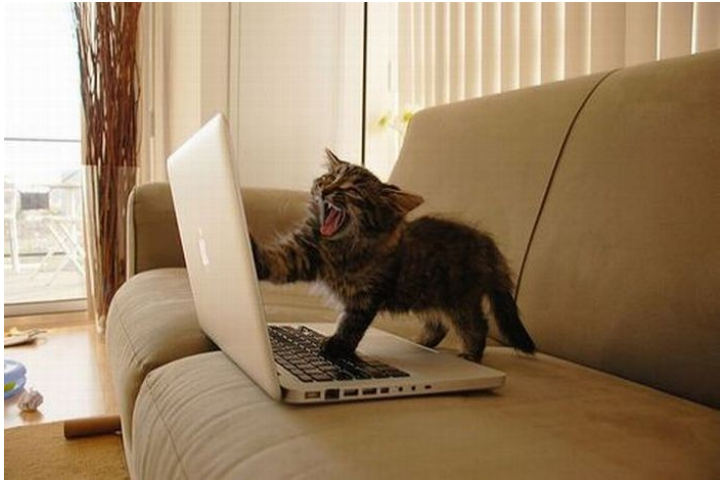
The story so far

- A non-WG forming BOF occured at IETF110
- The problem statement was presented, and it seemed to be well understood.
  - Lack of disagreement and confusion was almost a concern
- A charter was written in April/May, and trimmed down in June

The story so far

- The revised charter did not get a lot of agreement or disagrement, it was hard to tell apathy from silent support





Charter (1)

Objective

The DANE AutheNtication for Iot Service Hardening (DANISH) WG seeks to

extend DANE to encompass TLS client authentication using certificates or Raw Public Keys (RPK).

Charter (2) Problem Statement

The process of establishing trust in public-key-authenticated identity typically involves the use of a Public Key Infrastructure (PKI), and a shared PKI root of trust between the parties exchanging public keys. A Certification Authority (CA) is one example of a root of trust for a PKI, which can be then used for establishing trust in certified public keys.

The DNS namespace, together with DNSSEC, forms the most widely-recognized namespace and authenticated lookup mechanism on the Internet.

DANE builds on this authenticated lookup mechanism to enable public key-based TLS authentication which is resilient to impersonation, but only for TLS server identities.

However, DANE did not define authentication for TLS client identities.

Charter (3) Problem Statement [2]

In response to the challenges related to ambiguity between identically named identities issued by different CAs, application owners frequently choose to onboard IoT device's client identities to a single private PKI with a limited CA set that is specific to that vertical.

This creates a silo effect where different parts of large deployment can not communicate. For instance the heating/cooling system of a building wishing to turn lights off to reduce room temperatures can not authenticate to the lighting control system.

Charter(4): Scope of Work

DANISH will specify the TLS client authentication use case and an architecture describing the primary components and interaction patterns.

DANISH will establish usage conventions for DANE DNS records to represent client identities for TLS connections.

DANISH will coordinate with the TLS working group to define any required TLS protocol updates required to support client authentication using DANE.

Future work may include using client identifiers for other tasks including object security, or authenticating to other protocol services.

The DANISH working group will take care to ensure a potential path for interoperability, enabling these potential future directions.

Discussion

?

Next slide is deliverables

Deliverables

- DANISH architecture document (9 months)
-
- DANE for device certificates (current draft) (6 months)
-
- DANE for TLS client authentication (current draft) (6 months)

Next Steps