SONY

Publicly Trusted Cert. and Local Network Discovery

HTTPS in Local Network CG@W3C_TPAC2018

Tatsuya Igarashi

R&D Center
Sony Corporation

Copyright 2018 Sony Corporation

Background

1. W3C people has discussed on **HTTPS in local network**
   - TPAC 2014 breakout: startSession("WoT devices") [1]
   - TPAC 2015 breakout: Secure communication with local network devices [2]
   - TPAC 2016 breakout: HTTPS Migration in Local Network [3]
   - TPAC 2017 breakout: HTTPS in Local Network [4]
   - TPAC 2018 (this time) F2F meeting of W3C HTTPS in Local Network Community Group [5]
2. There are some solutions to use **Publicly trusted cert.** for local servers
   - PLEX and Digi Cert: How to Use Secure Server Connections [6]
   - Let's Encrypt: Let's Encrypt for intranet websites? [7]
3. W3C Pepole has discussed on **Local network discovery**
   - Web and TV Interest Group: Home Network TF [8]
   - Devices & Sensors Working Group (aka DAP) : Web Intents Addendum - Local Services W3C Editor's Draft 16 October 2018 [9]
   - Devices & Sensors Working Group (aka DAP): Network Service Discovery W3C Working Group Note 12 January 2017 [10]
   - Second Screen Community Group: Open Screen Protocol [11]

The presentation describes the issues of using Public trusted cert for local servers, and explore a solution of integrating **Publicly trusted cert.** with **Local network discovery**.

Copyright 2018 Sony Corporation

Why Publicly Trusted Cert. is needed for local network?

1. It is not easy for consumers to install private Cert. of their server devices to their client devices, e.g. smartphone, tablet, PC.
   - It is very risky for consumers to install private certs. of devices on public local network, e.g. Cafe, Hotel, Library, Airport, Station, etc.

2. It is messy for users to manage security of many devices from different vendors.
   - This is not the case only about consumer devices but also IOT devices such in office and factory

3. It is costly for small companies to manage private PKI.
   - Also, companies would like to allow employees to use their BYOD devices in a intra-net without forcing a special client software.

Copyright 2018 Sony Corporation

What are the issues ?

1. Scalability and Privacy of DNS and CT servers
   - The scalability does matter if a huge of IoT devices have publicly trusted cert.
   - There is also a privacy issue on information disclosure about private devices and local network.

2. Binding Local network domain to publicly trusted cert.
   - A PLEX solution which registers a device to public DNS has the issue of scalability and Privacy. Also, PLEX solution works only if a device is engaged in a specific service, since a service has to know the URL of device in a secure manor.
   - IETF has been discussed a proxy solution from local network discovery, i.e. mDNS to public DNS[12]. However it does work only for managed network.

Copyright 2018 Sony Corporation

What are the solutions ?

1. About the scalability and privacy issue,
   - IETF is discussing on Short-Term, Automatically-Renewed (STAR) Certificates in ACME[13], however it will take time and then the approval by CAB Forum is needed.
   - Alternatively, the issue can be addressed by the Technically Constrained Subordinate CA Certificate defined by the CAB Forum baseline guideline[14]. And the remaining issue is if all the major browsers support it.

2. About the binding issue,
   - The extension to Local Network Discovery can address the issue. For example, mDNS provides a common name to be used as an global origin which can be verified by publicly trusted cert. for a HTTPS connection. Note that a friendly name of mDNS would be mainly used for device selection.
   - IETF could define such extension, however W3C should initiate the discussion because it is required for W3C to define the Local Network Discovery API to show a global origin of device and get user content to access it. Also, the secure origin issue is very related to W3C web security standards such as Mixed Content[15] and Secure Contexts [16].

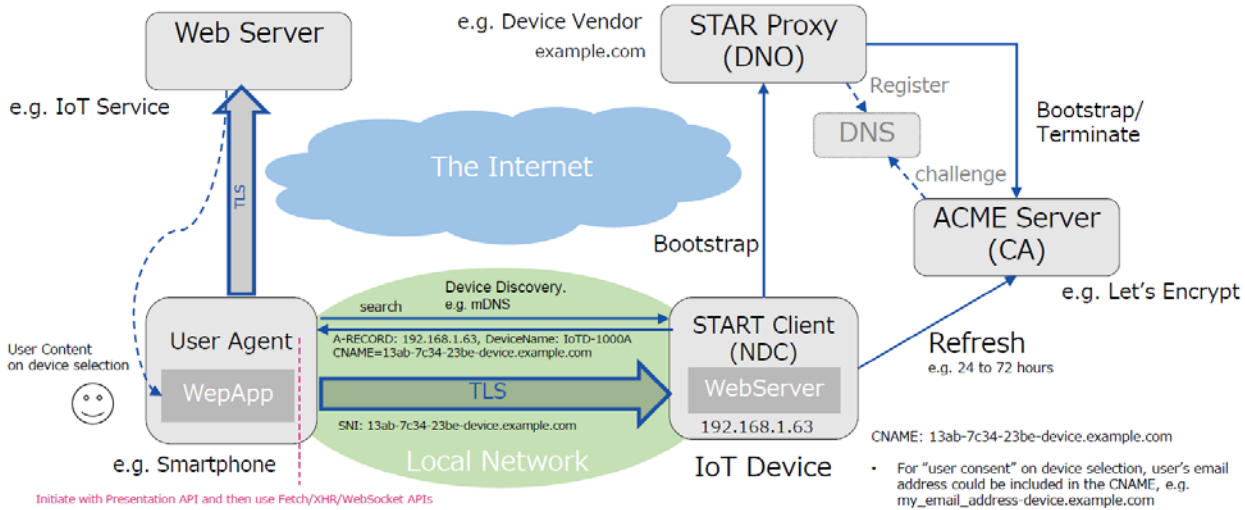
Copyright 2018 Sony Corporation

Strawman of Local Network Discovery API

- The presentation at the break-out session of TPAC 2017
  - https://www.w3.org/wiki/File:TPAC2017_httpslocal-3_HTTPS_in_LocalNetwork_featuring_STAR.pdf

HTTPS in local network featuring STAR

- IoT device is configured to get a short-term server cert. via STAR Proxy and refresh the server cert. with ACME server
- On TLS handshake with IoT device, Use Agent verifies the server cert. with CNAME in Device Discovery
- For User Content, User Agent shows green colored DeviceName and CNAME by checking with "pre-flight".



 Copyright 2018 Sony Corporation

SONY

SONY is a registered trademark of Sony Corporation.
Names of Sony products and services are the registered trademarks and/or trademarks of Sony Corporation or its Group companies.
Other company names and product names are registered trademarks and/or trademarks of the respective companies.