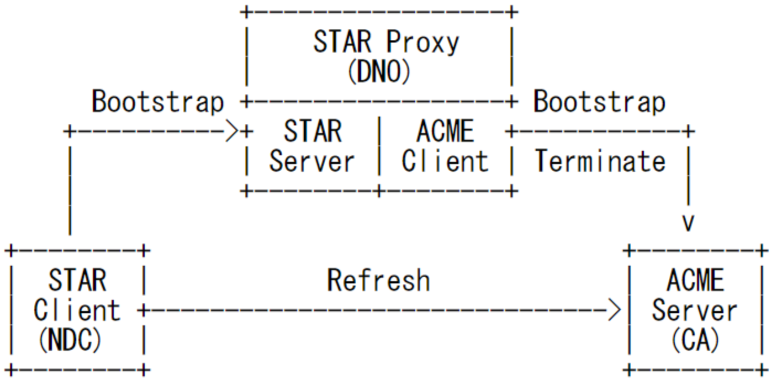
HTTPS in Local Network featuring STAR

W3C HTTPS in Local Network Community Group

Tatsuya Igarashi (tatsuya.igarashi@sony.com)

STAR

- Use of Short-Term, Automatically-Renewed (STAR) Certificates to Delegate
  - draft-ietf-acme-star-00
  - Abstract This memo proposes an ACME extension to enable the issuance of short- term and automatically renewed certificates. This allows a domain name owner to delegate the use of certificates to another party, while retaining the capability to cancel this delegation at any time with no need to rely on certificate revocation mechanisms.



```
                    +------------------+
                    |    STAR Proxy    |
                    |      (DNO)       |
       Bootstrap    +------------------+ Bootstrap
    +-------------->+  STAR  |  ACME   +-----------+
    |               | Server | Client  | Terminate |
    |               +--------+---------+           |
    |                                              v
+--------+                                    +--------+
|  STAR  |              Refresh               |  ACME  |
| Client +----------------------------------->| Server |
| (NDC)  |                                    |  (CA)  |
+--------+                                    +--------+
```

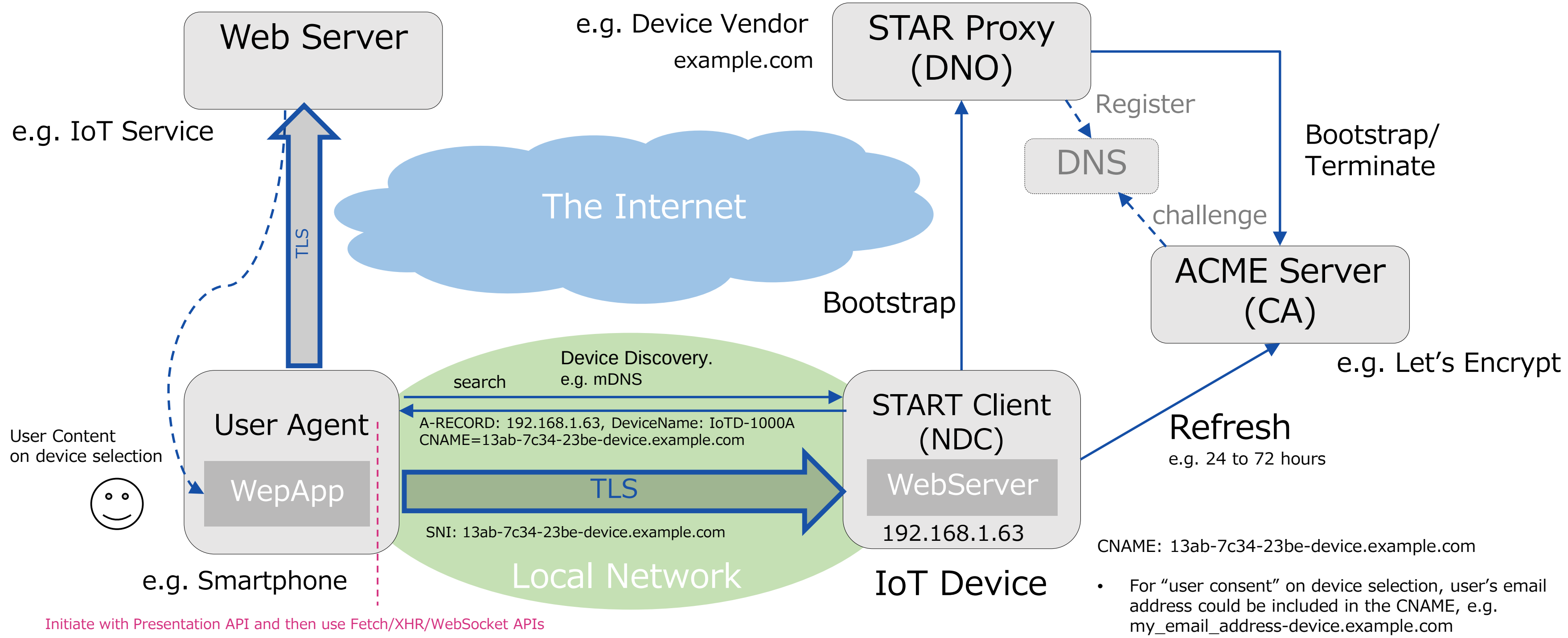
e.g. CDN Edge Server

Terminology

DNO Domain Name Owner, the owner of a domain that needs to be delegated.
NDC Name Delegation Consumer, the entity to which the domain name is delegated for a limited time. This is often a CDN (in fact, readers may note the similarity of the two acronyms).
CDN Content Delivery Network, a widely distributed network that serves the domain's web content to a wide audience at high performance.
STAR Short-Term, Automatically Renewed X.509 certificates.
ACME The IETF Automated Certificate Management Environment, a certificate management protocol.
CA A Certificate Authority that implements the ACME protocol.

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”.



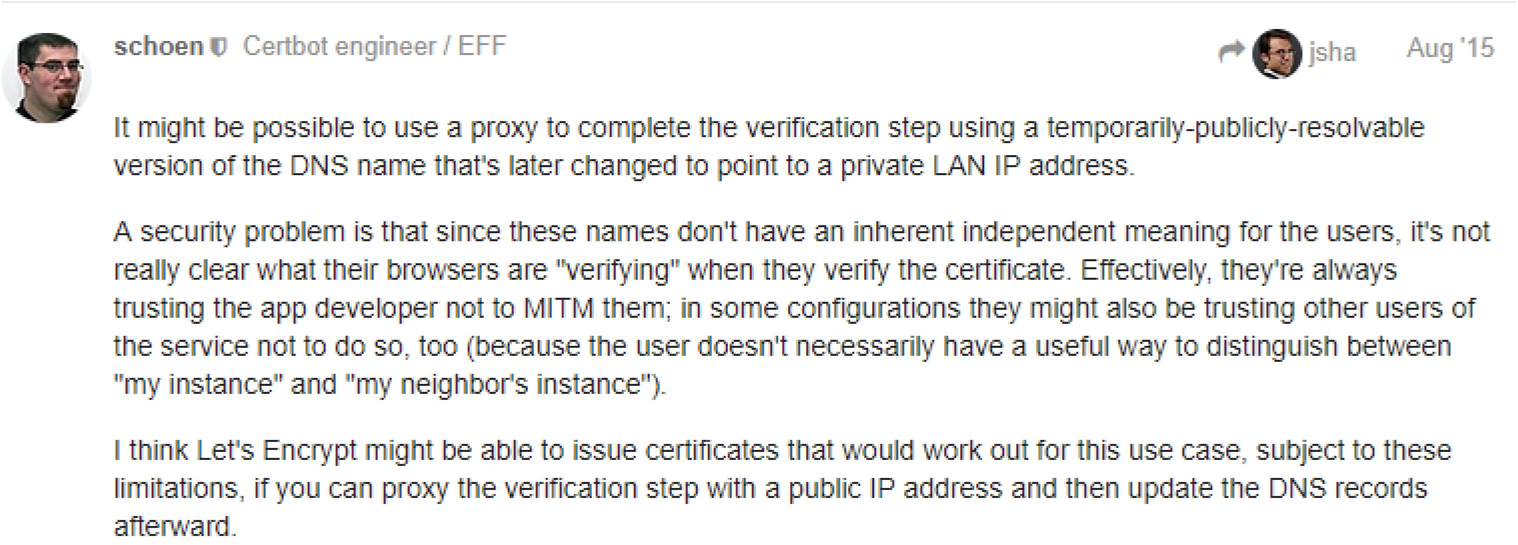
- For “user consent” on device selection, user’s email address could be included in the CNAME, e.g. my_email_address-device.example.com

Initiate with Presentation API and then use Fetch/XHR/WebSocket APIs

Proxy was discussed in the community of Let’s Encrypt [1]

Mr. Scheon> The Security Problem is how browsers are “verifying” when they verify the certificates and the user has no useful way to distinguish between “my instance” and “my neighbor’s instance”.

Igarashi’s comment> To mitigate the security risk, I wonder browsers can verify CNAME in device discovery with a user content on device selection


schoen Certbot engineer / EFF

jsha Aug '15

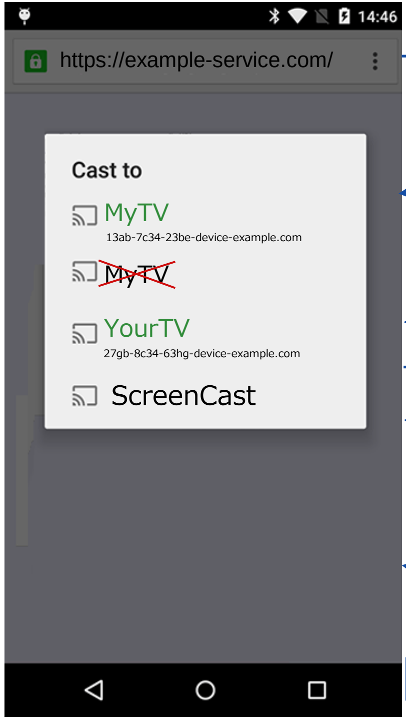
It might be possible to use a proxy to complete the verification step using a temporarily-publicly-resolvable version of the DNS name that's later changed to point to a private LAN IP address.

A security problem is that since these names don't have an inherent independent meaning for the users, it's not really clear what their browsers are "verifying" when they verify the certificate. Effectively, they're always trusting the app developer not to MITM them; in some configurations they might also be trusting other users of the service not to do so, too (because the user doesn't necessarily have a useful way to distinguish between "my instance" and "my neighbor's instance").

I think Let's Encrypt might be able to issue certificates that would work out for this use case, subject to these limitations, if you can proxy the verification step with a public IP address and then update the DNS records afterward.

[1] Certificates for hosts on private networks
https://community.letsencrypt.org/t/certificates-for-hosts-on-private-networks/174

Example of Device Selection



14:46

https://example-service.com/

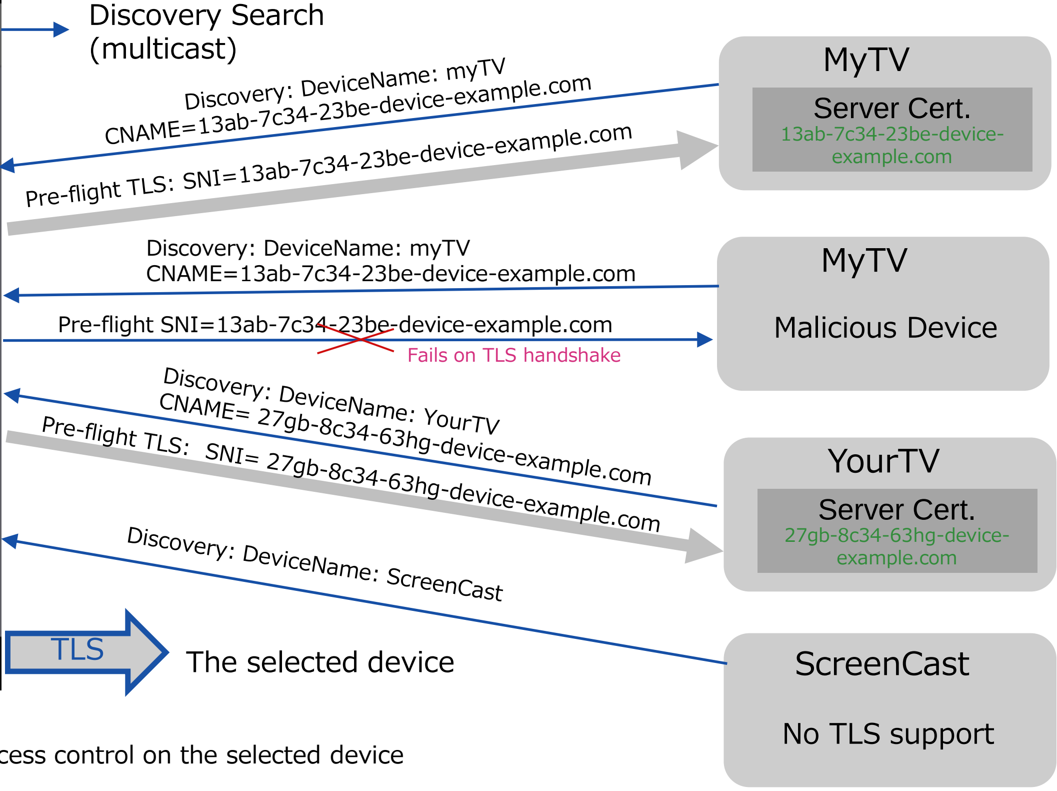
Cast to

MyTV
13ab-7c34-23be-device-example.com

~~MyTV~~

YourTV
27gb-8c34-63hg-device-example.com

ScreenCast



Discovery Search (multicast)

MyTV
Server Cert.
13ab-7c34-23be-device-example.com

Discovery: DeviceName: myTV
CNAME=13ab-7c34-23be-device-example.com

Pre-flight TLS: SNI=13ab-7c34-23be-device-example.com

MyTV
Malicious Device

Discovery: DeviceName: myTV
CNAME=13ab-7c34-23be-device-example.com

Pre-flight SNI=13ab-7c34-23be-device-example.com

Fails on TLS handshake

YourTV
Server Cert.
27gb-8c34-63hg-device-example.com

Discovery: DeviceName: YourTV
CNAME= 27gb-8c34-63hg-device-example.com

Pre-flight TLS: SNI= 27gb-8c34-63hg-device-example.com

ScreenCast
No TLS support

Discovery: DeviceName: ScreenCast

TLS

The selected device

Note:
Discovery information is faked by the malicious device or MITM attack

Note: PIN or Password could be used for access control on the selected device

SONY