HTTPS Migration in Local Network

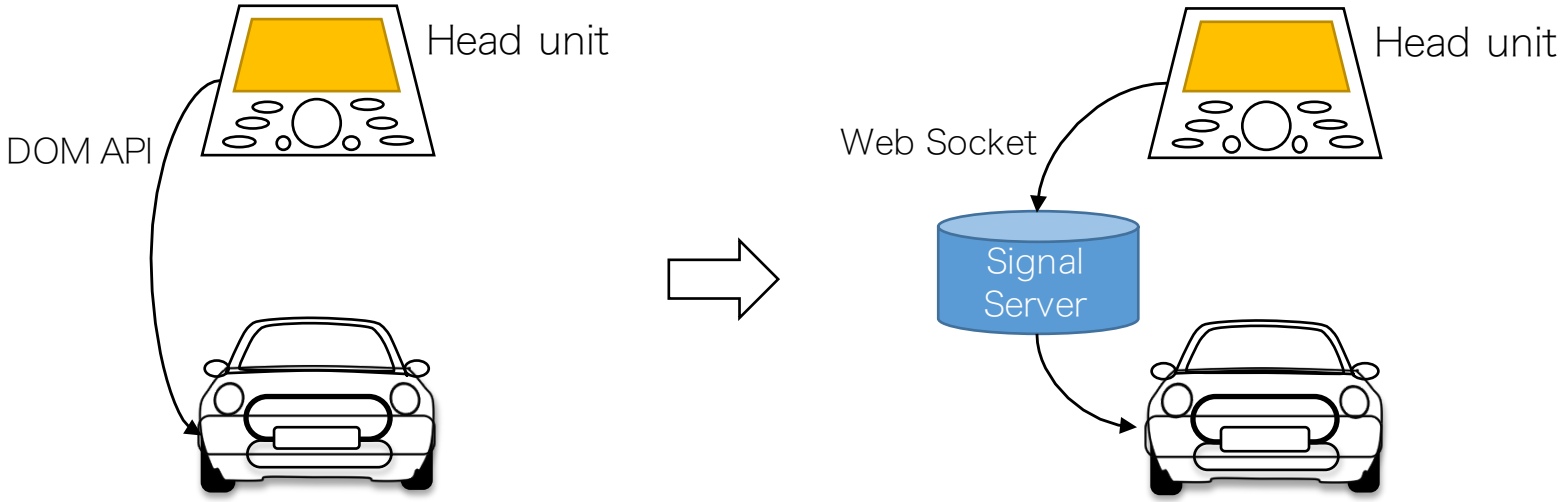
ju-hashimoto@kddilabs.jp

TPAC 2016 Lisbon

Related works

- startSession("WoT devices")
  - 2014
  - T. Igarashi, S. Homma, N. Sakamoto
  - https://www.w3.org/wiki/TPAC/2014/SessionIdeas#startSession.28.22WoT_devices.22.29
- Secure Communication with local network devices
  - 2015
  - M. Watson
  - https://www.w3.org/wiki/TPAC/2015/SessionIdeas#Secure_communication_with_local_network_devices

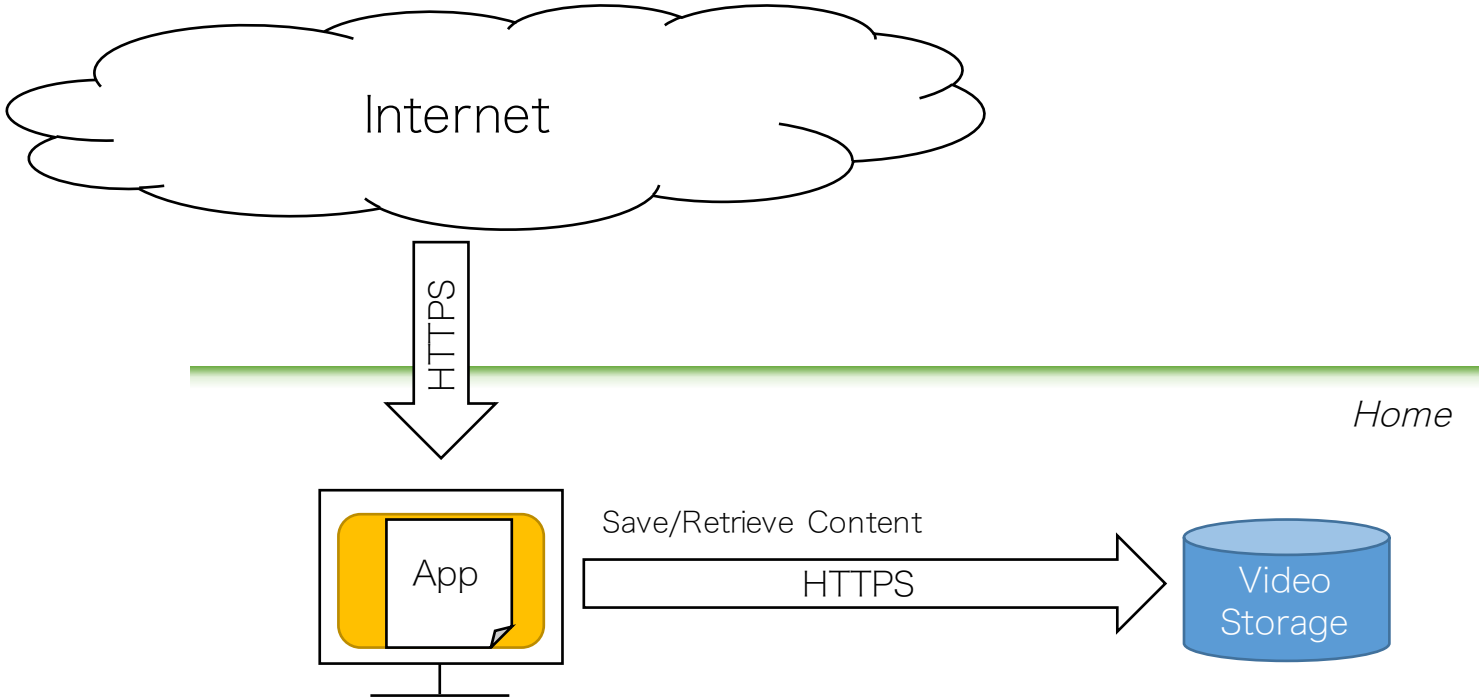
Use case: Vehicle API @Auto WG



Local server approach makes easy

- To implement access control
- To implement model specific function

Use case: Local Video Storage

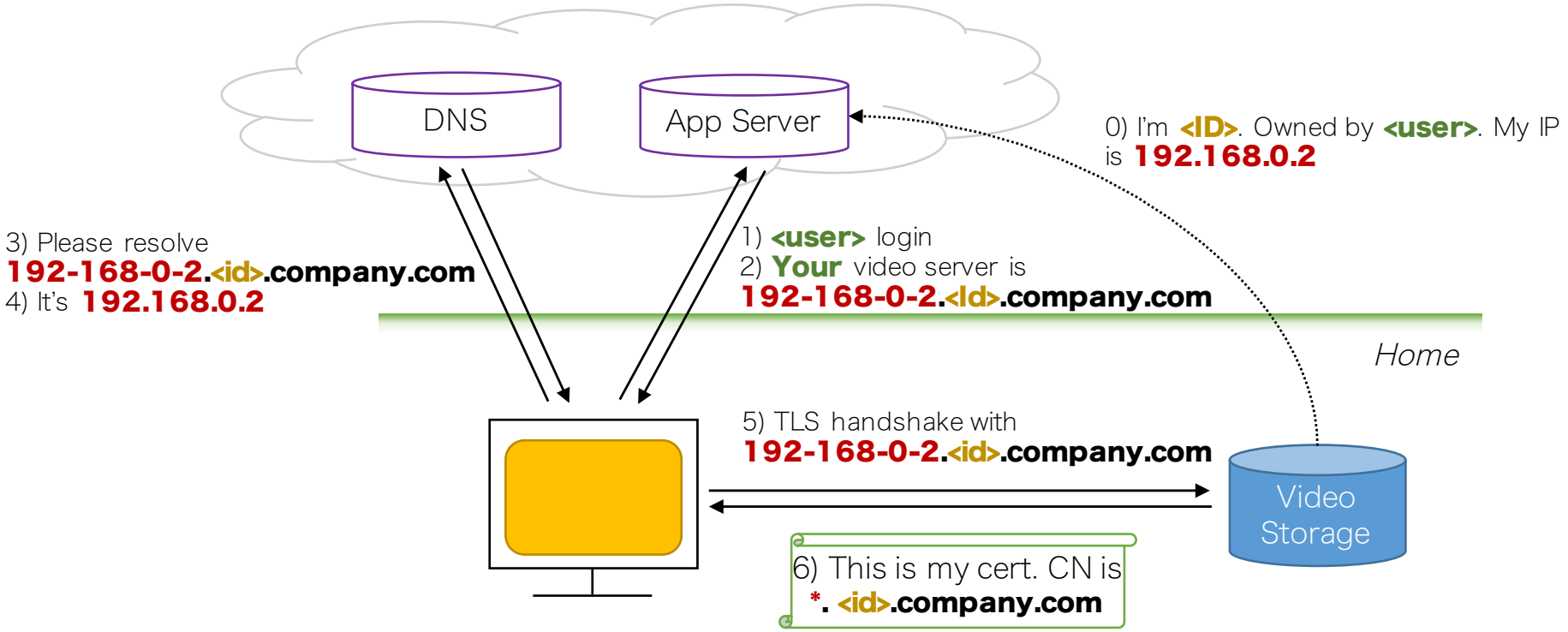


Local communication need to be secure for cross origin access

- Host name? (requires for certificate)
- How to resolve? (need to know local IP)

PLEX's solution

2015, https://blog.filippo.io/how-plex-is-doing-https-for-all-its-users/



Host Name: **<IP address>.<device ID>.company.com**

→ solves DNS scalability problem

Common Name: ***.<device ID>.company.com**

→ unique for a device and valid for any prefix

CA/Browser forum Guidance

2012, https://cabforum.org/wp-content/uploads/Guidance-Deprecated-Internal-Names.pdf

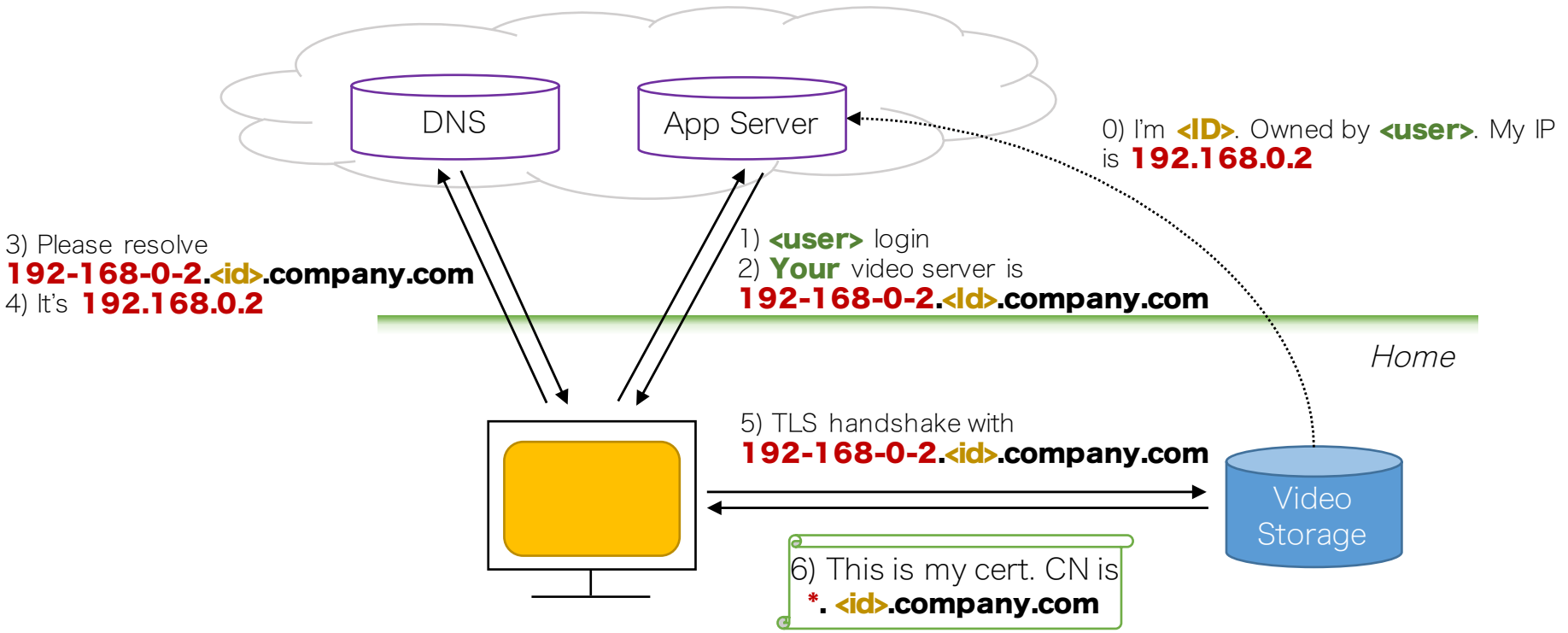
*"**Effective 1 October 2016**, CAs SHALL **revoke** all unexpired Certificates whose SAN or Subject Common Name field contains a **Reserved IP Address** or **Internal Server Name**."*

Internal Server Name: A Server Name (which may or may not include an Unregistered Domain Name) that is not resolvable using the public DNS.

- Bad hostnames
  - "**192.168.1.1**"
  - "**printer.local**"
  - ...
- Requirement

  Server name need to be resolved by **public** DNS

PLEX's solution (again)



Server name is resolved (to Local IP address) by public DNS…

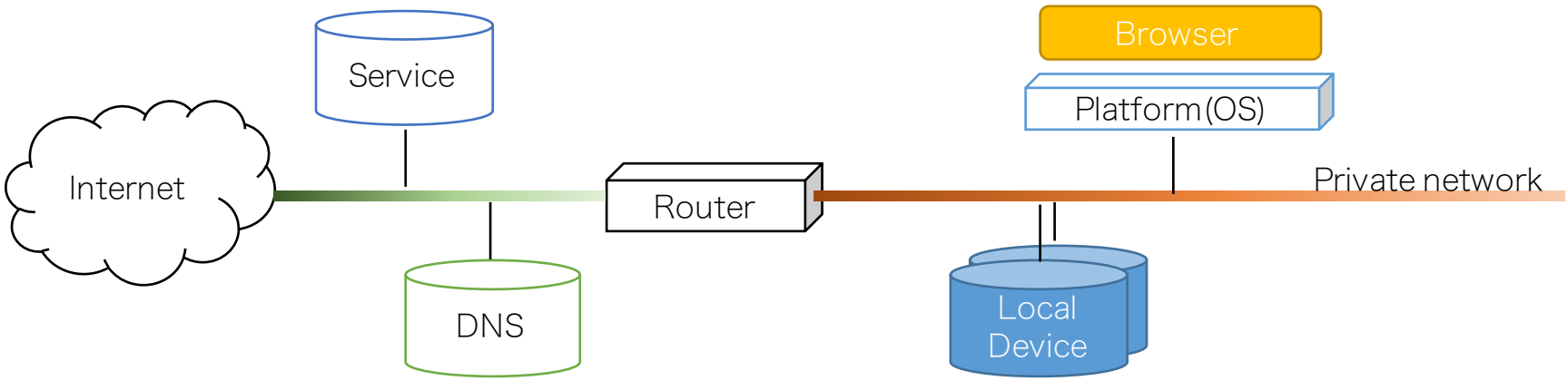
Any other approvable solution?

What we want

1. Local Devices Certificate
   - Must be equivalent to cloud server certificates
   - Need scheme to guarantee device's integrity
2. Better Mechanism than PLEX's
   - [Privacy] As a user, I'm not happy that private IP is exposed to internet.
   - [Discovery] As a 3rd party developer, I'd like to find user's device more easily.
   - [Management] As a device provider, I'd like to have a standard way to manage device certificate (update, revoke etc.)

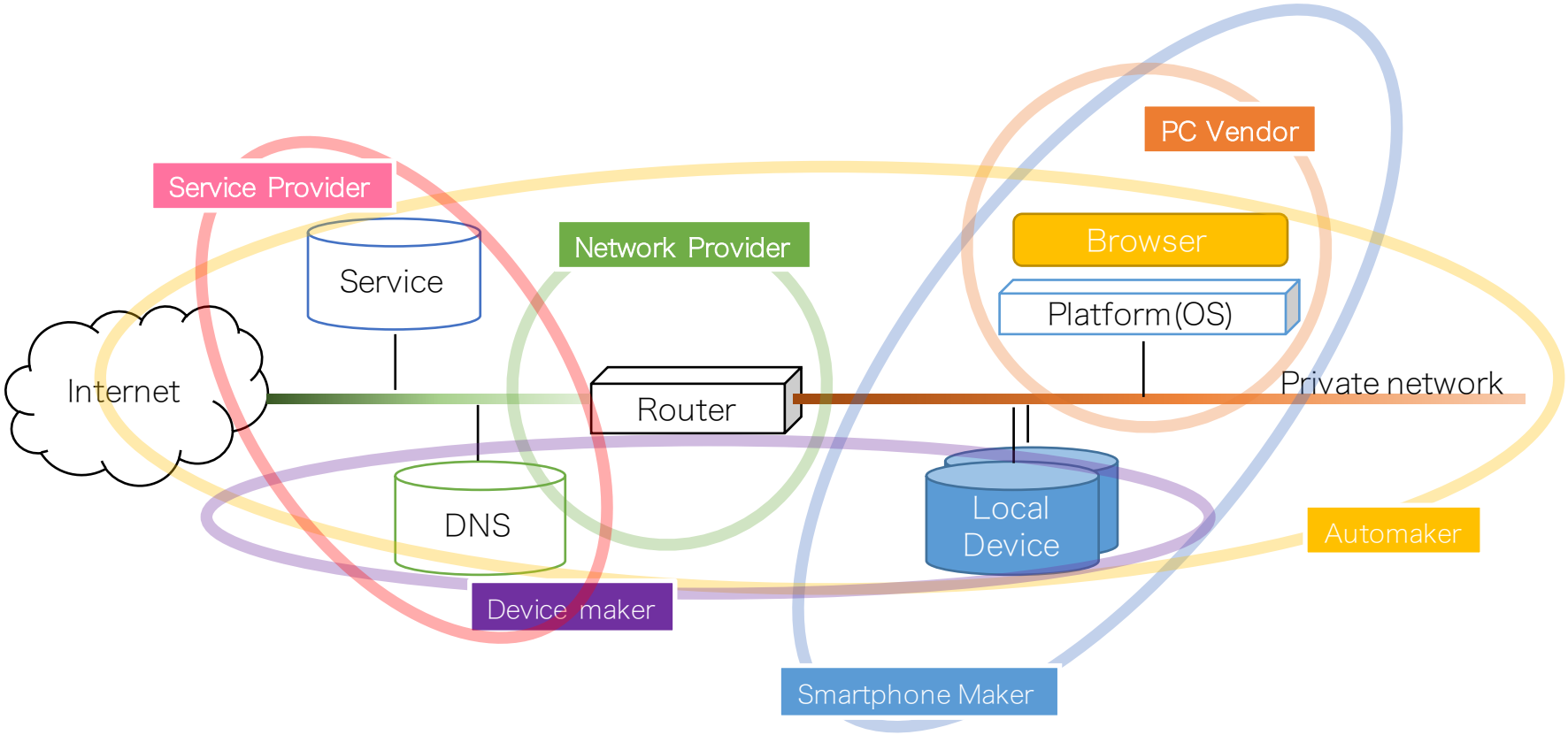
Call for Solutions!

Stakeholders



○ A solution wouldn't be a solution for others…

Stakeholders



○ A solution wouldn't be a solution for others…

Thank you