Updates on CG Report(Use Cases/Approaches)

Ryo Kajiwara @ lepidum

2019/9/19, HTTPS in Local Network CG F2F @ TPAC 2019

CG Report

We are publishing 2 reports

Use Cases and Requirements Approaches

Use Cases and Requirements Document

https://httpslocal.github.io/usecases/

Added more coverage of use cases by adding non-cross-origin cases

Clarifying usage of HTTPS in the document
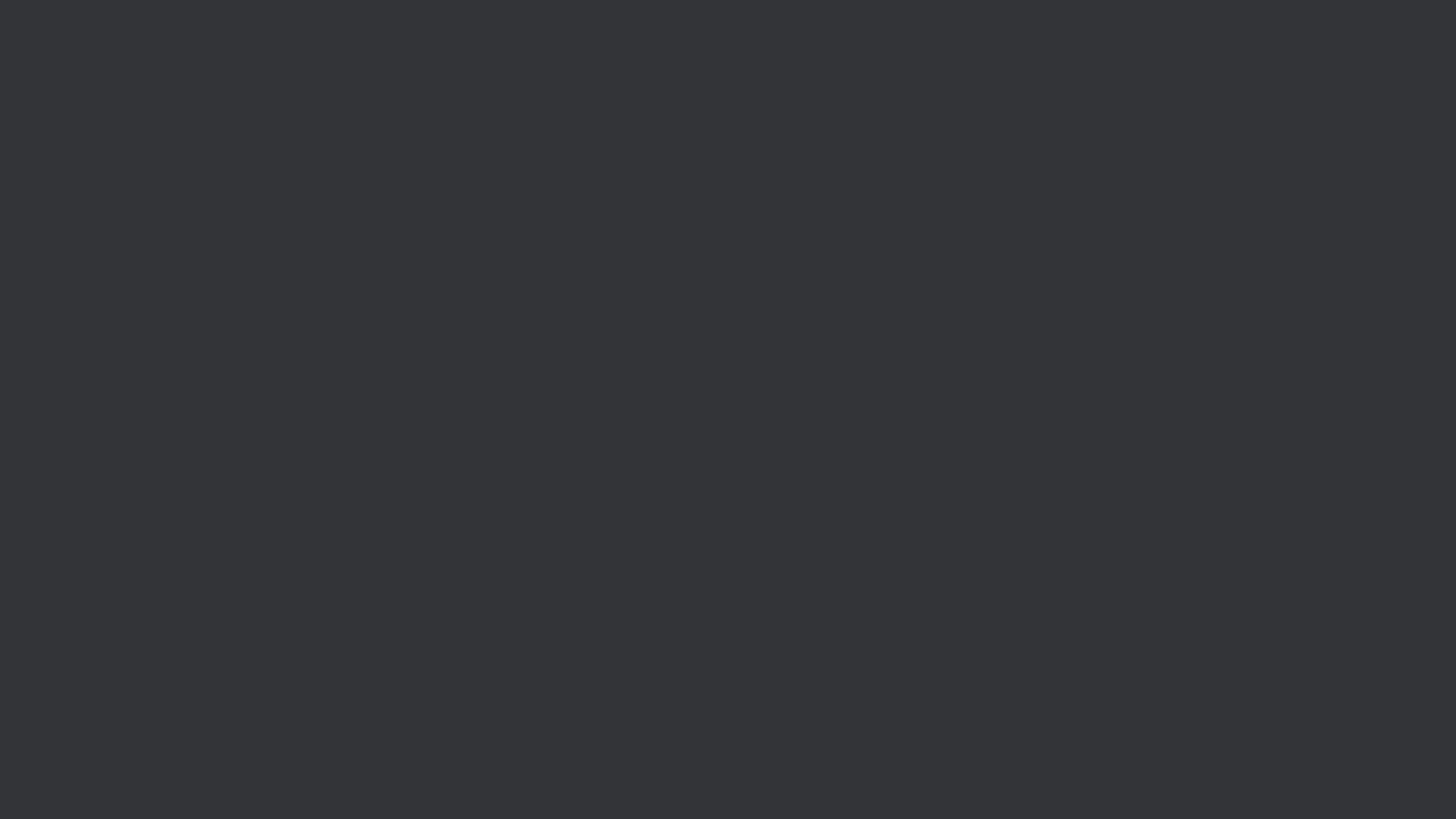
before: "HTTPS/WSS" -> too redundant

Here HTTPS is used as a subset of TLS connections negotiated by the

user-agent. It is not restricted to the HTTPS scheme (= `wss` is also included)

Refinement of Requirements

Device Discovery is optional

Organized Use Cases

"Photo sharing between online services and home NAS devices" and "Accessing audio contents in a home storage device from a cloud service" is essentially the same

Approaches to Achieving HTTPS in Local Network

Existing solutions

Mozilla's "Things Gateway"

- Uses publicly accepted Web PKI certificates

- Device becomes accessible from the Internet

New Approaches

https://httpslocal.github.io/proposals/

Name Constraints

(will be touched on later in detail)

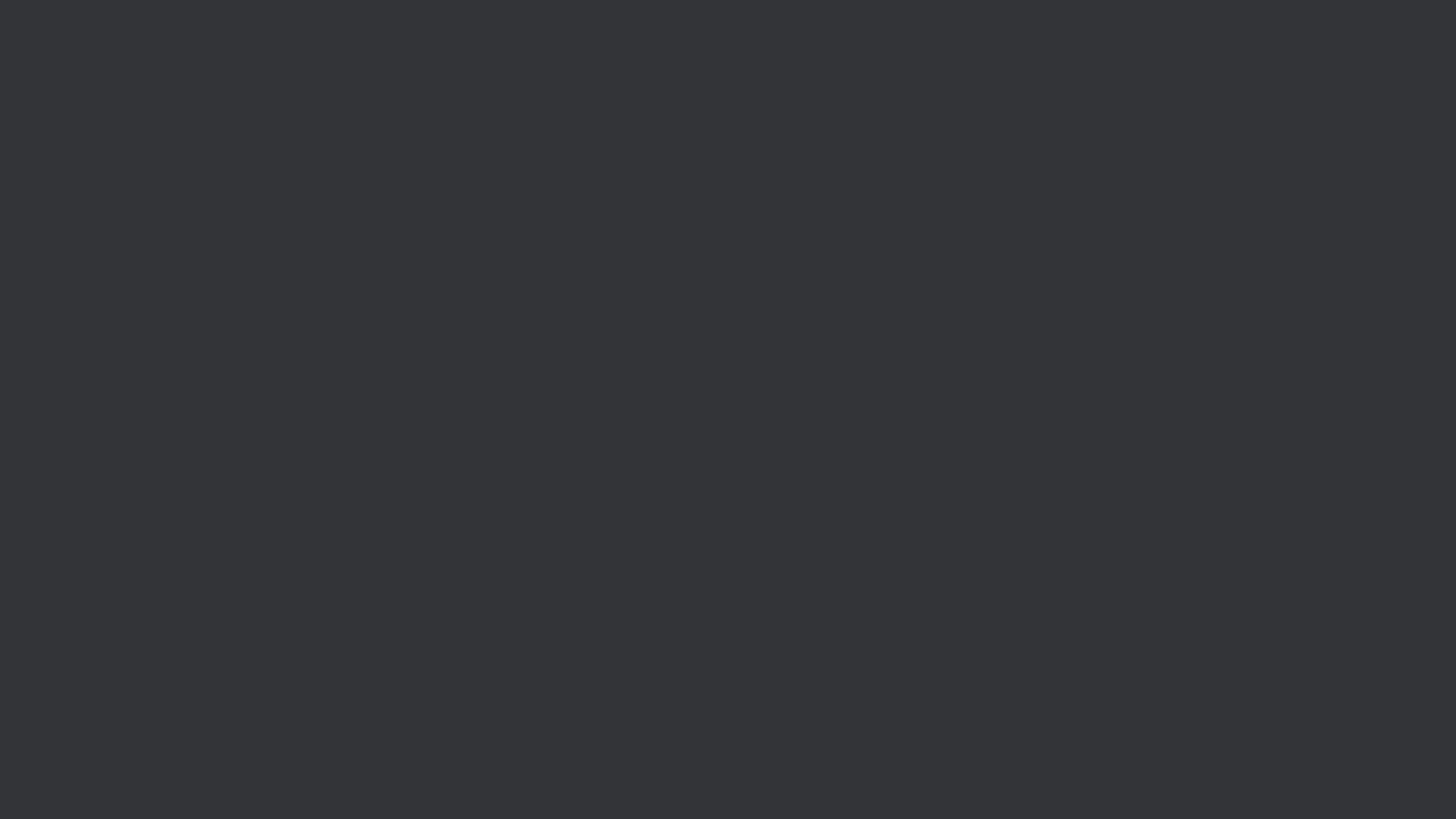"Circumvents" the need of Domain Validation in a way

Issuing Certificates to Private Domain Names

- using shared secret (PAKE-based approach)

- using application layer access token (ACE/OAuth-based approach)

- using device vendor issued certificates

Issuing Certificates to Private Domain Names

All approaches listed here will require the **extension of the "origin" notion**, which requires discussion in the W3C field.

We are releasing these CG Reports during this year (-2019/12)

Discussion items

- Any comments on use cases/proposals?

- HTTPS with private domains need the extension of origin. Is it possible/realistic?

- Place to work on this topic after the CG report?
  - We are aware that there needs to be changes in the browser (origin definition, UI, TLT cipher suite, extension of `fetch`)
  - WG? IG?
  - Any interests among browser vendors?