mDL Privacy Concerns

Standard: ISO/IEC 18013-5_2021

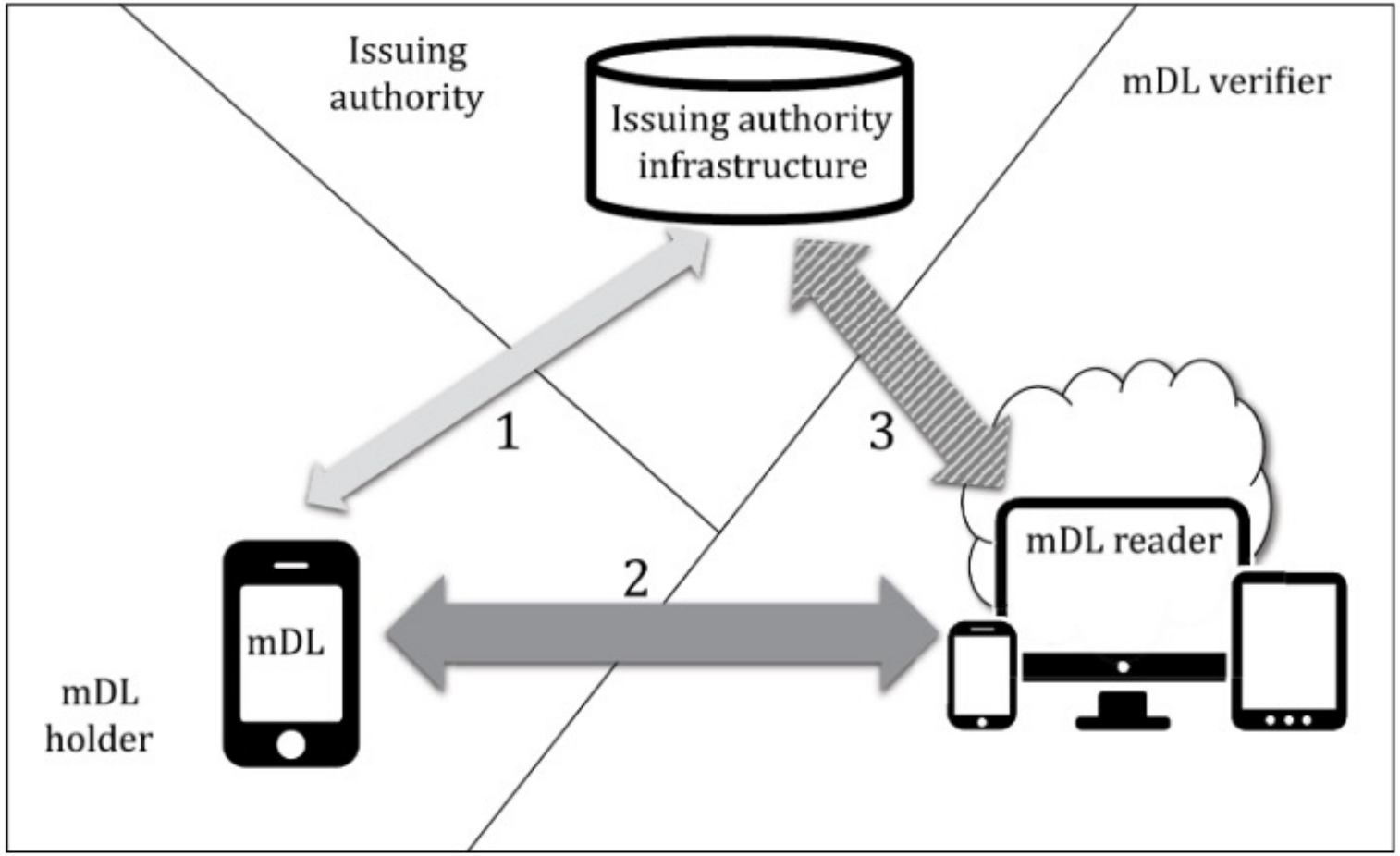
Steve McCown

Chris Bramwell

Timothy Ruff

Presented at the Internet Identity Workshop #40

How does mDL work?



Sec. 6.1, Fig 1

Sec. 6.2.3.1
“The server retrieval method relies on OpenID Connect that is not specific to mDL, or on WebAPI that relies on the generic mdoc data model.”

Where does mDL data come from?

6.3.2.5 Data retrieval methods

The following methods are defined for retrieval of mDL data. Requirements for supporting these methods are defined in Table 2.

mDL data can be retrieved in two ways:

a) using device retrieval (interface 2 in Figure 1), see 8.3.2.1;

b) using server retrieval (interface 3 in Figure 1), see 8.3.2.2, where the server retrieval token may be retrieved by the mDL reader from the mDL during device engagement or during device retrieval.

NOTE 1 For device retrieval, there is no requirement for any device involved in the transaction to be connected to the internet.

mDL Readers Must Support Both Modes

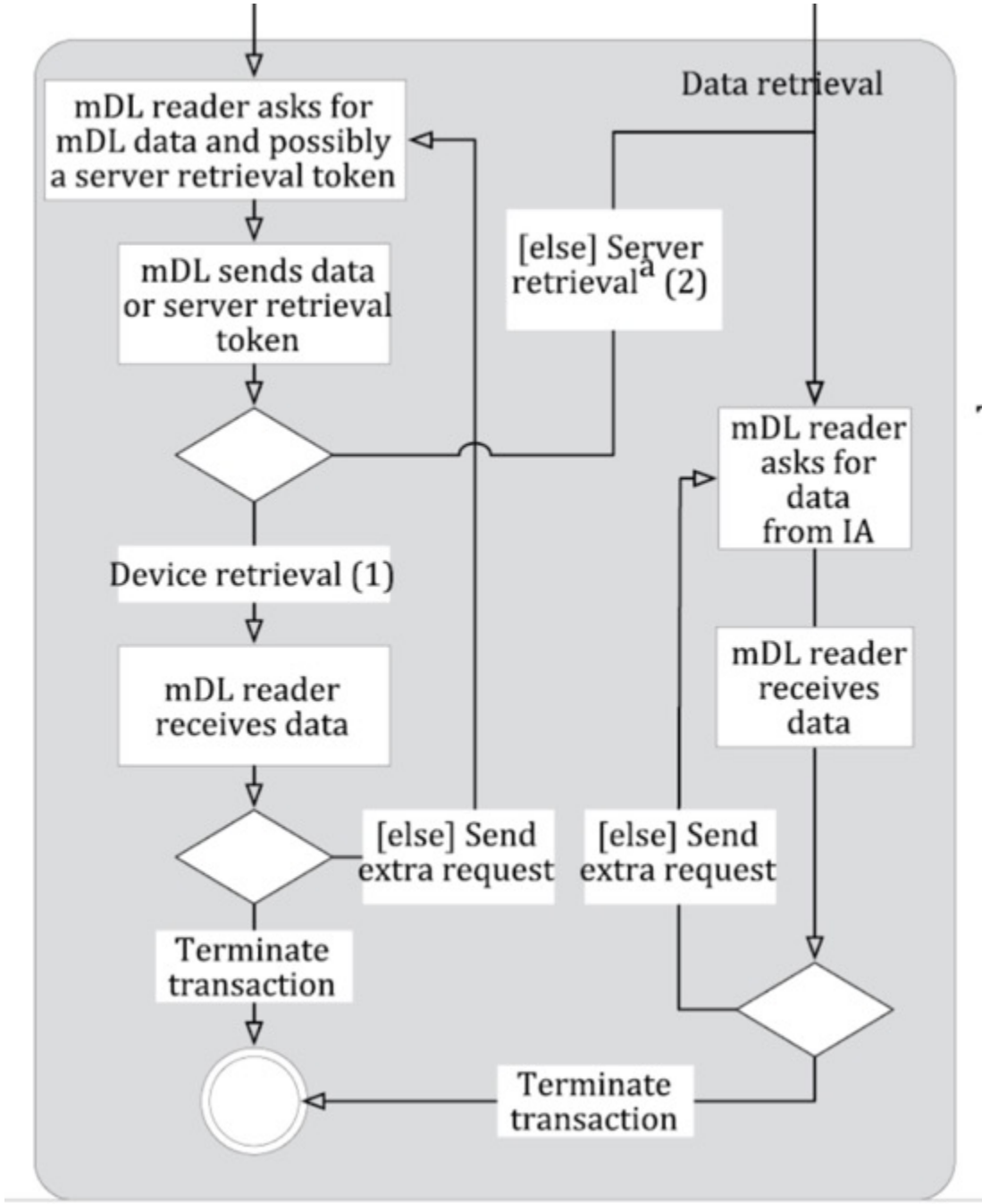
- Server Retrieval (Sec 6.3.2.4)

> After device engagement, if the mDL reader sets up a device retrieval connection, the mDL reader asks for data as defined in 8.3.2.1.2.1. The mDL sends an mdoc response according to 8.3.2.1.2.2. The mdoc request may include a request for server retrieval information used to perform server retrieval. If server retrieval information is requested next to other mDL data, the mDL shall return either the server retrieval information or the other requested data, but not both.

Server Retrieval

Is determined by data from the mDL

After device engagement, if the mDL reader sets up a device retrieval connection, the mDL reader asks for data as defined in 8.3.2.1.2.1. The mDL sends an mdoc response according to 8.3.2.1.2.2. The mdoc request may include a request for server retrieval information used to perform server retrieval. If server retrieval information is requested next to other mDL data, the mDL shall return either the server retrieval information or the other requested data, but not both.



Sec 6.2.3.1; Figure 1

Tracking *Policy*

NOTE 2 The issuing authority infrastructure is involved in each server retrieval-based transaction; therefore, the issuing authority knows when an mdoc is used and what data is shared. If tracking is a concern, the issuing authority can implement mitigating strategies to ensure the mdoc and the mdoc holder are not tracked.

Section E 2.3

Server Retrieval Determined by mDL

Sec 6.3.2.1

NOTE 1 For device retrieval, there is no requirement for any device involved in the transaction to be connected to the internet.

If the mDL reader receives the server retrieval token and URL from the mDL, either during device engagement or device retrieval, it may either use device retrieval or server retrieval. If it chooses to use device retrieval, either BLE, NFC or Wi-Fi Aware can be used to retrieve the information. If it chooses to use server retrieval, either OIDC or WebAPI can be used to retrieve the information.

Can’t we just setup Device Retrieval?

mDL Data Refresh Policy

E.15 Data accuracy and freshness

Issuers sign the mDL data and therefore are declaring the accuracy of mDL data at the time of signing.

Issuers should establish policy for how often mDL data is to be refreshed. This policy is reflected in the mobile security object (MSO). mDL solutions should endeavor to refresh mDLs at least as often as policy states.

Verifiers should implement business decisions related to that freshness if mDL data is out of date.

When do mDLs Get Updated?

General Overview

- Issuer
  - Sets up “Device Retrieval” system
  - Issues mDLs for Device Retrieval
- Holder
  - Holds mDL and presents to Verifiers
- Verifier
  - Requests mDL presentation
  - Determines Device Retrieval or Server Retrieval

Switching Models

- Issuer
  - Decides to move to a “Server Retrieval” system
  - Updates mDLs for Server Retrieval
- Holder
  - Holds mDL and presents to Verifiers
- Verifier
  - Requests mDL presentation
  - Determines Device Retrieval or Server Retrieval
  - Sends Server Retrieval Token to Issuer
- Issuer
  - Now, able to track usage of mDLs with Server Retrieval set

Do all mDLs get updated?

Can it get worse?

Issuer

- Decides to issue both “Server Retrieval” and “Device Retrieval” mDLs
- Updates *some* mDLs for Server Retrieval

Who are the lucky mDL holders that get server retrieval?

Phone Home … for Targeted Tracking of mDL usage

Thank you!

Steve McCown

https://www.linkedin.com/in/mccown/

Chris Bramwell

https://www.linkedin.com/in/christopher-bramwell-26815515/

Timothy Ruff

https://www.linkedin.com/in/rufftim/