Authorized update to MUD URLs

Michael Richardson
IETF107 OPSAWG meeting
April 7, 2020
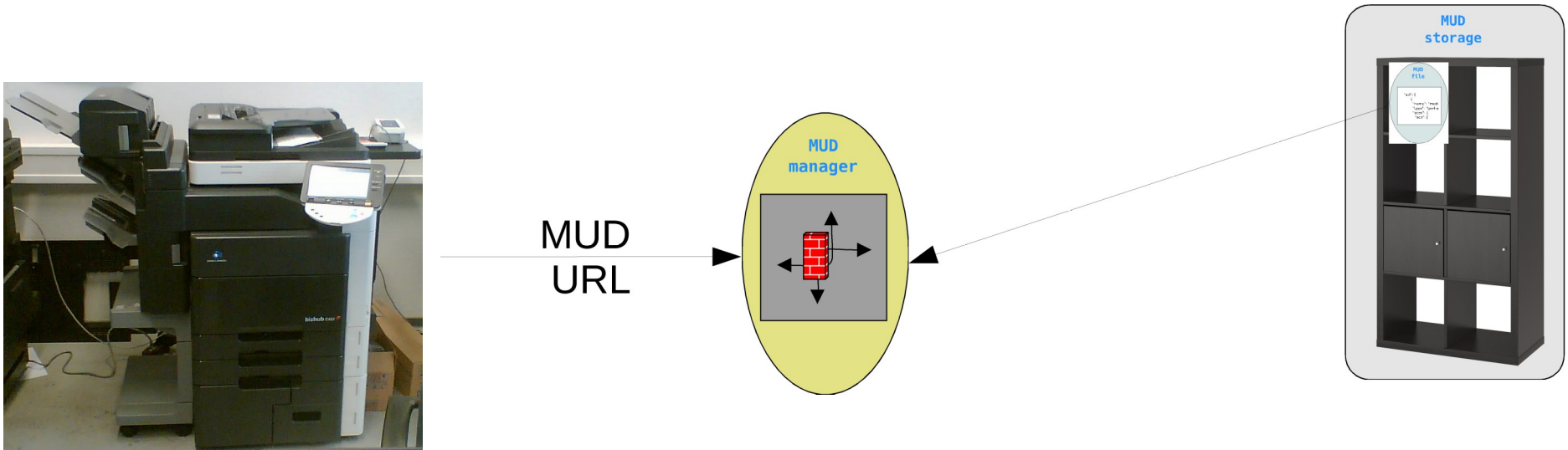
`draft-richardson-opsawg-mud-acceptable-urls-00`
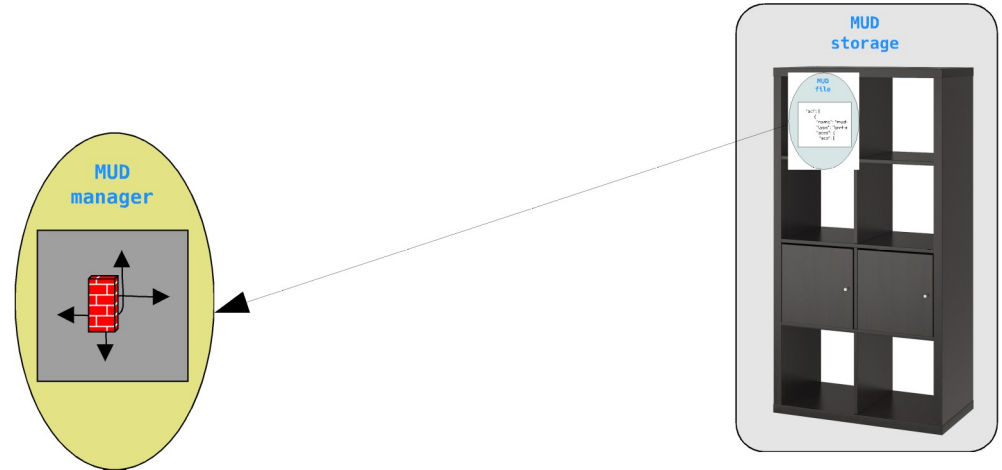
MUD URLs vs MUD files

- **Update MUD file in place**
  - PRO: no security problems
  - CON: opens issues with mis-matches of firmware
    - e.g., TLS profiles!

- Update MUD URL, provide new MUD file
  - PRO: every major revision can have specific rules
  - PRO: different operating modes for device can express different preferences
    - (commercial, pro-user, residential)
    - Features enabled via accessories
  - CON: risk that MUD file link could be changed by malware
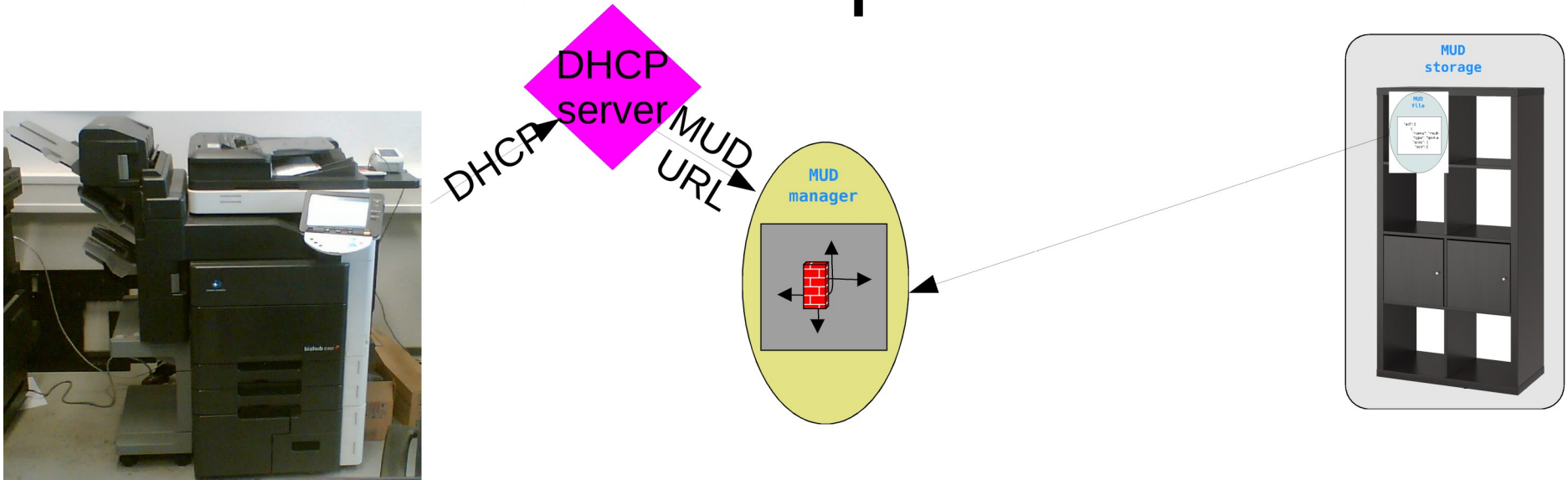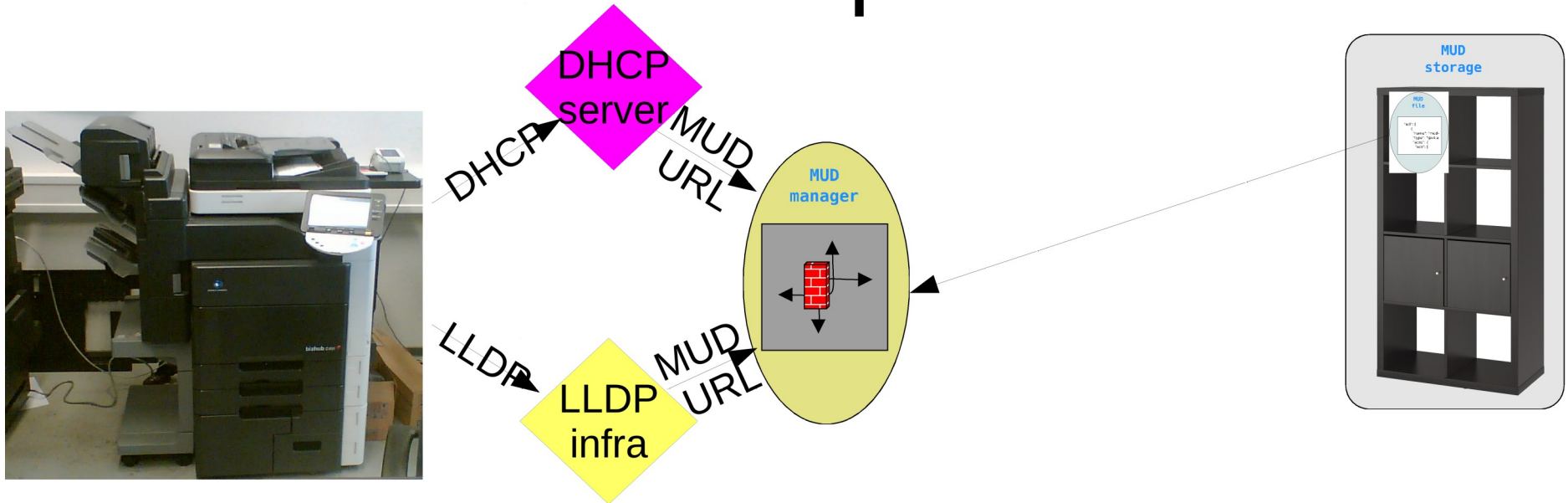
What is the problem?

- IoT device tells MUD manager about it's URL
  - MUD manager fetches the file

What is the problem?

- IoT device tells MUD manager about it's URL
  - MUD manager fetches the file

What is the problem?

- IoT device tells MUD manager about it's URL
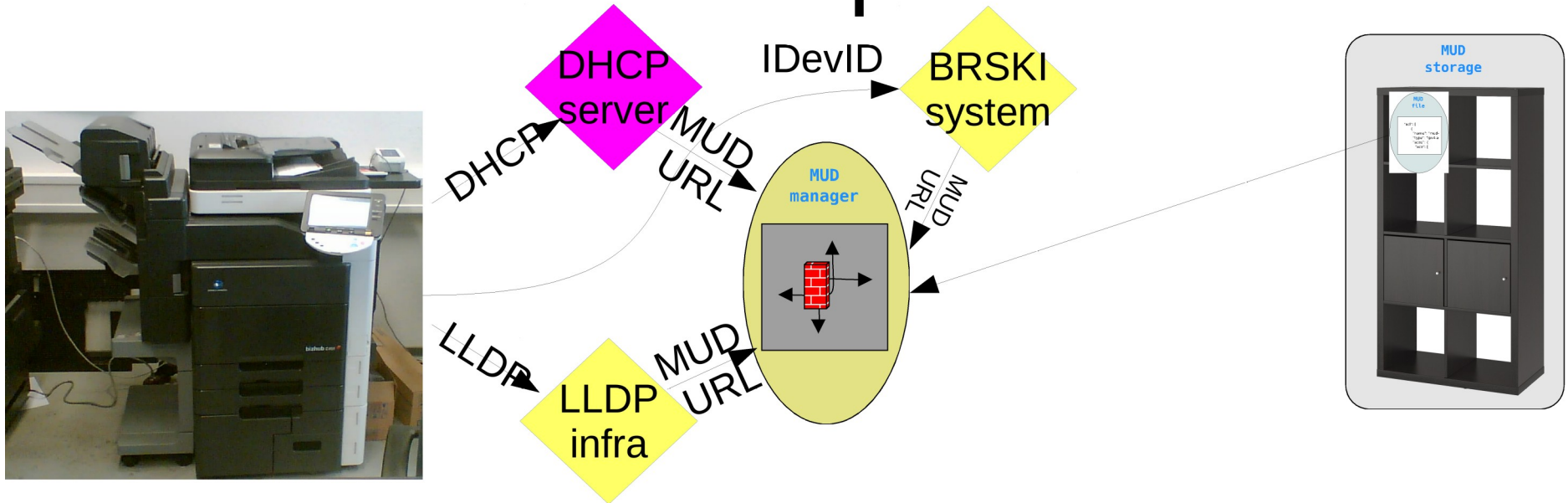 – MUD manager fetches the file
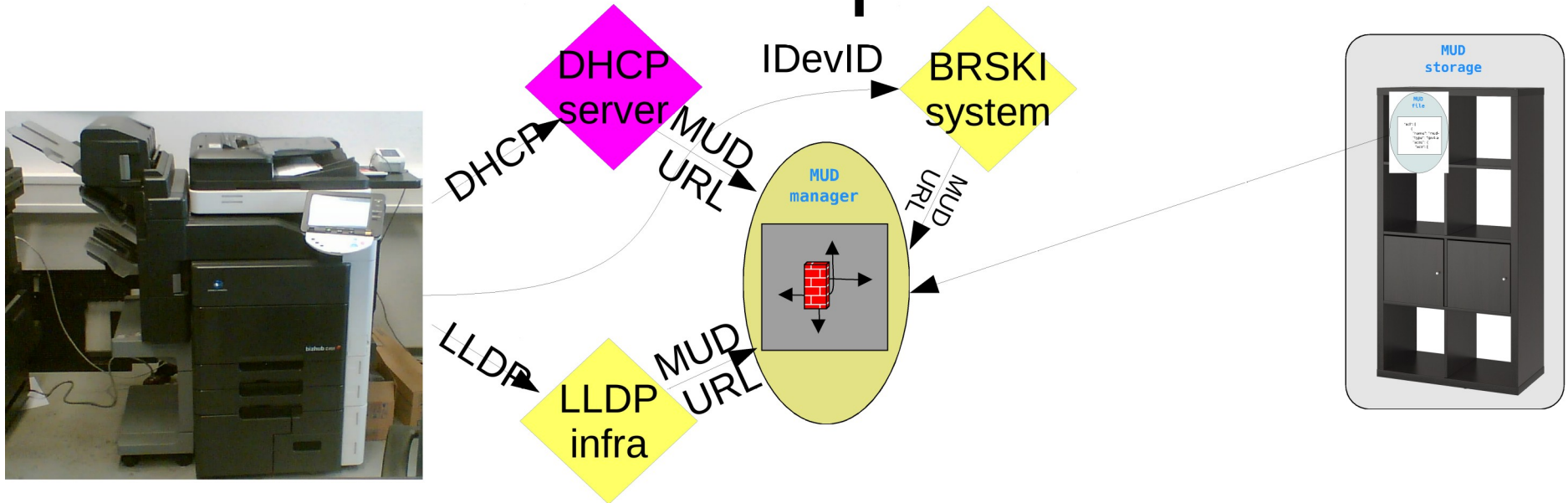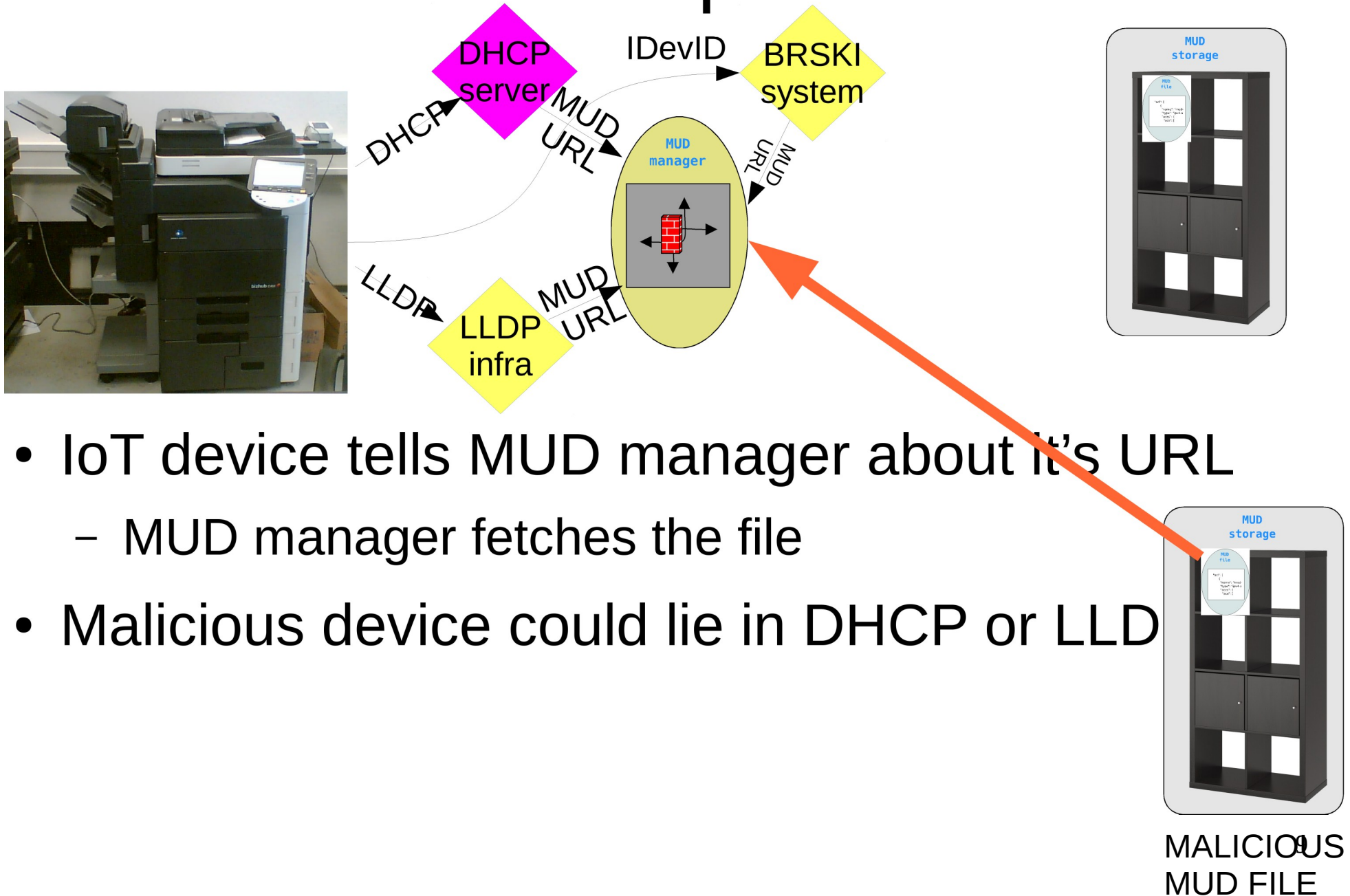
What is the problem?

- IoT device tells MUD manager about it's URL
  - MUD manager fetches the file

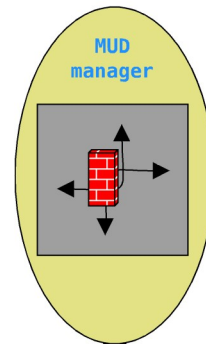# What is the problem?

- IoT device tells MUD manager about it's URL
  - MUD manager fetches the file

What is the problem?

- IoT device tells MUD manager about it's URL
  - MUD manager fetches the file
- Malicious device could lie in DHCP or LLDP

What is the problem?

- IoT device tells MUD manager about it's URL
  - MUD manager fetches the file
- Malicious device could lie in DHCP or LLD
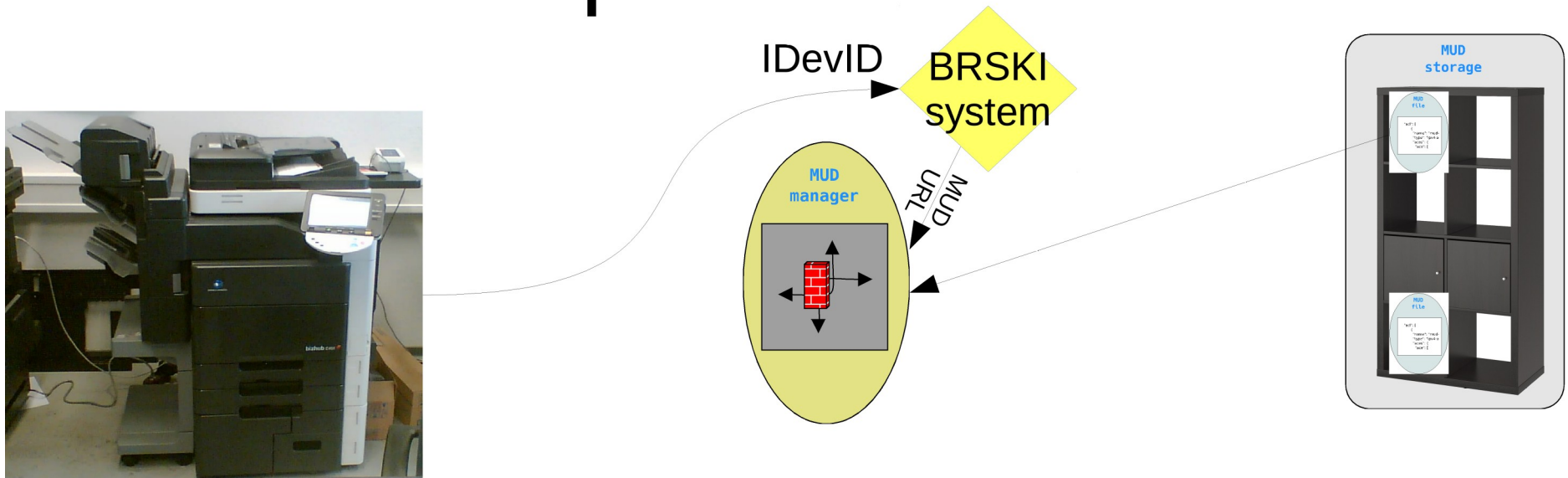
MALICIOUS
MUD FILE

Shape of Solution

- IoT device tells MUD manager about it's URL
  - The first time, using IDevID
  - Or may TOFU on DHCP/LLDP

Shape of Solution

- IoT device tells MUD manager about it's URL
  - The first time, using IDevID
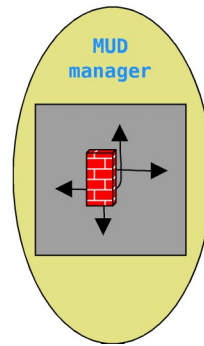 - Or may TOFU on DHCP/LLDP
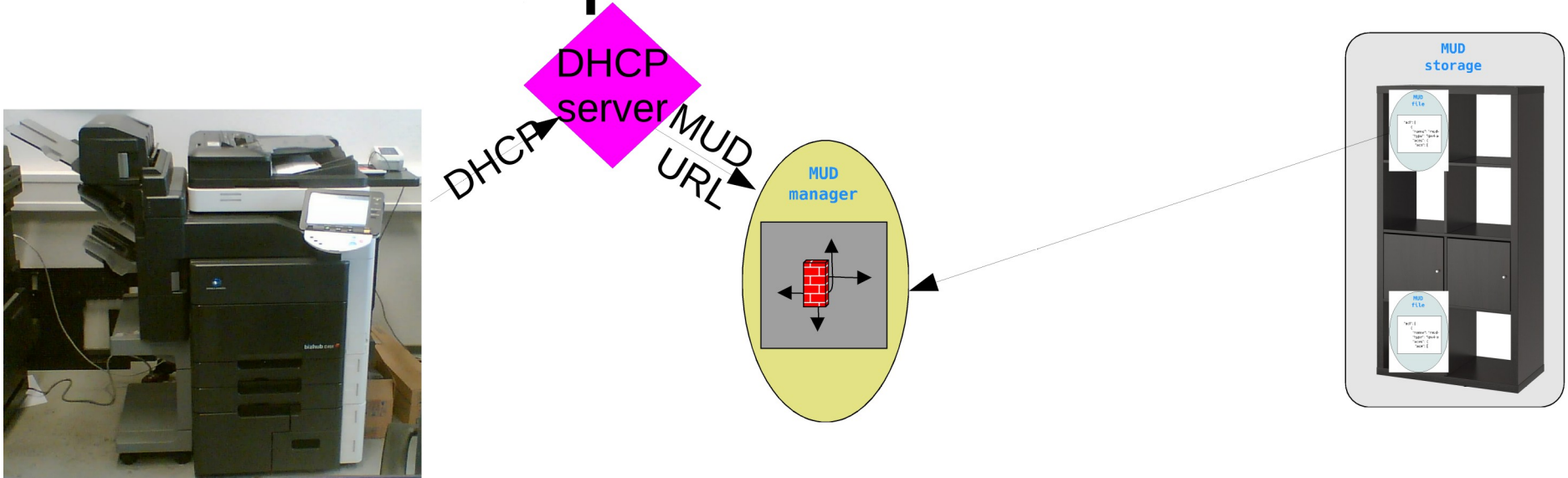
Shape of Solution

- IoT device tells MUD manager about it's URL
  - The first time, using IDevID
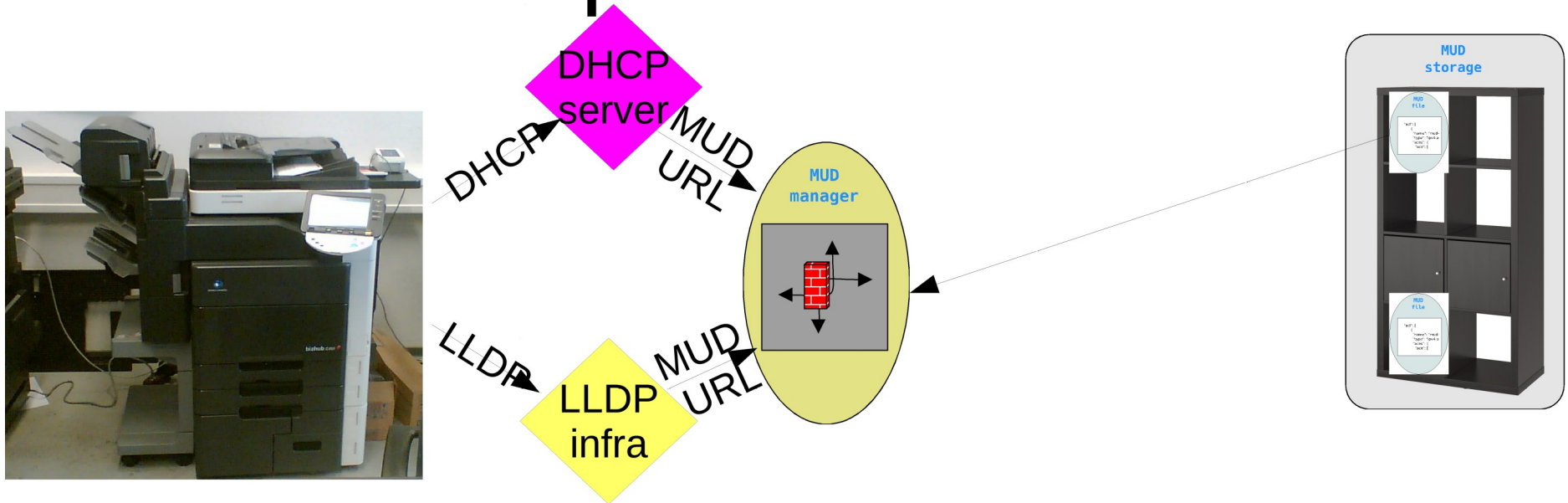 - Or may TOFU on DHCP/LLDP

Shape of Solution

- IoT device tells MUD manager about it's URL
  - The first time, using IDevID
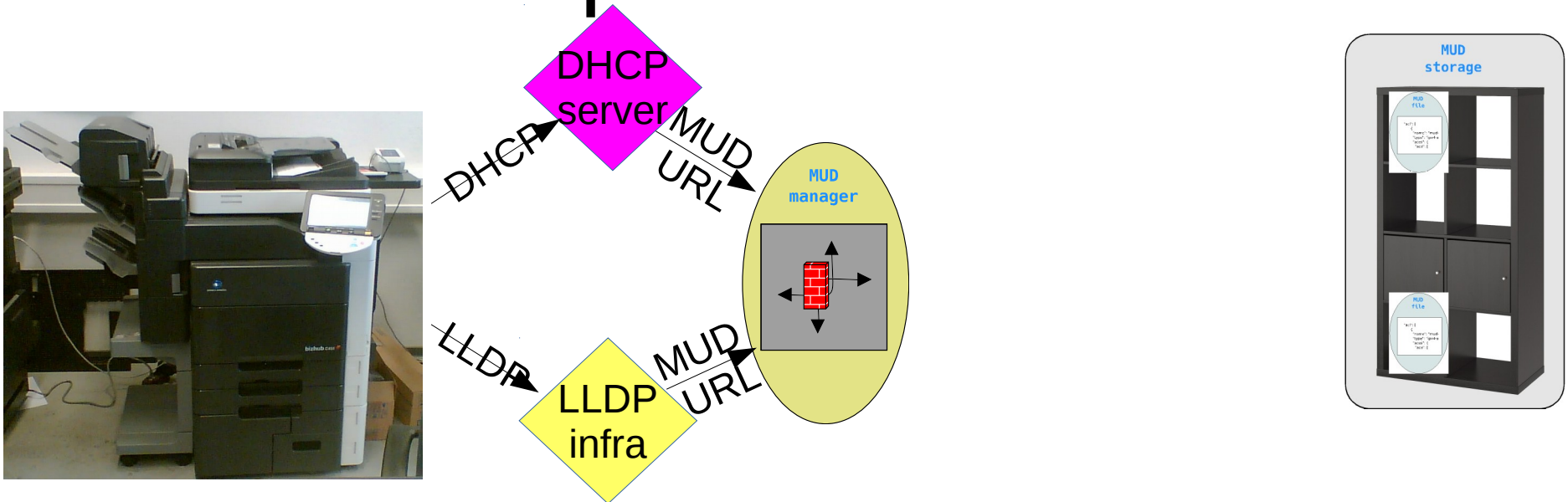 - Or may TOFU on DHCP/LLDP
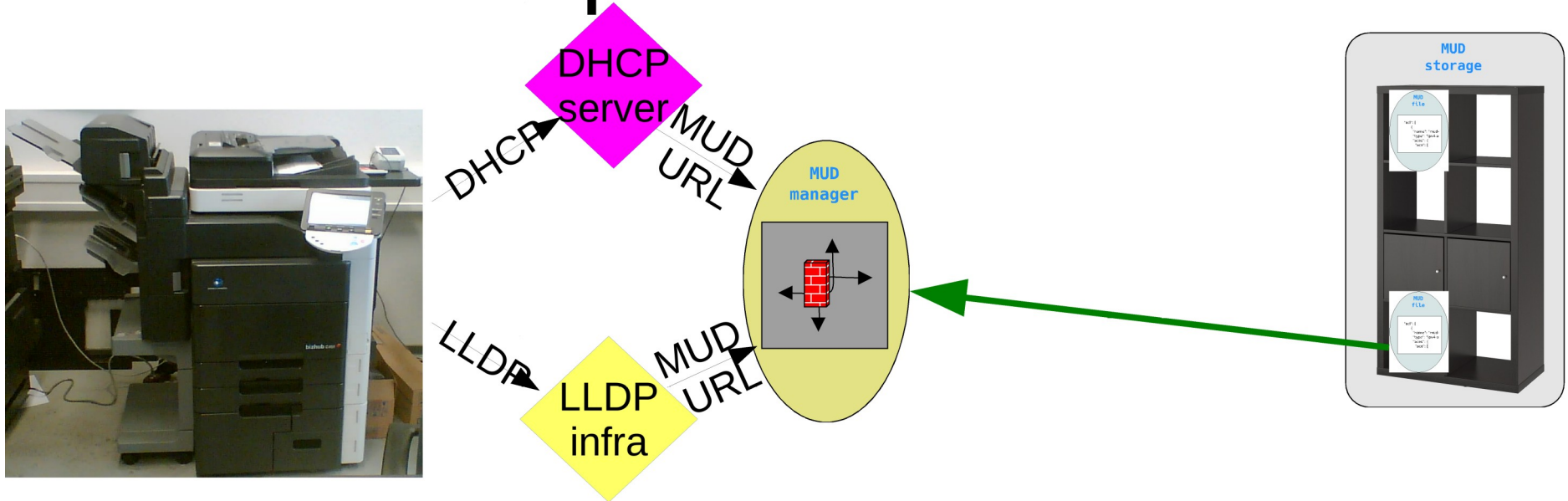
Shape of Solution

- IoT device tells MUD manager about it's URL
  – The first time, using IDevID
  – Or may TOFU on DHCP/LLDP

Shape of Solution

- IoT device tells MUD manager about it's URL
    - The first time, using IDevID
    - Or may TOFU on DHCP/LLDP
- Updates to URL would be restricted to the last component

Shape of Solution

- IoT device tells MUD manager about it's URL
  - The first time, using IDevID
  - Or may TOFU on DHCP/LLDP
- Updates to URL would be restricted to the last component

Updates to IdevID?

- If IDevID is the most secure, why not update that?
  - Not easy to do for many products, IDevID is ideally stored in TPM

- If the IDevID can be updated, then can a malware update it too?

Two ideas

- Update RFC8520 to say that the base URL must always be the same

- Add extension to RFC8520 say allow base URL to be specified

What to do next

- This is aimed at being a BCP for MUD

- Is this a problem for you?

  – Do you have a preference for solution?

- Adopt?

- QUESTIONS?