Muddy SUIT

draft-moran-suit-mud-01

Brendan Moran, Hannes Tschofenig

March 11th, 2021, notinprague

What MUD does

- Specifies expected network access requirements of device
- Limits allowed network access of device

- MUD URI is reported over:
  - LLDP (no authentication)
  - DHCP (no authentication)
  - Device Certificates (Signed by network manager)

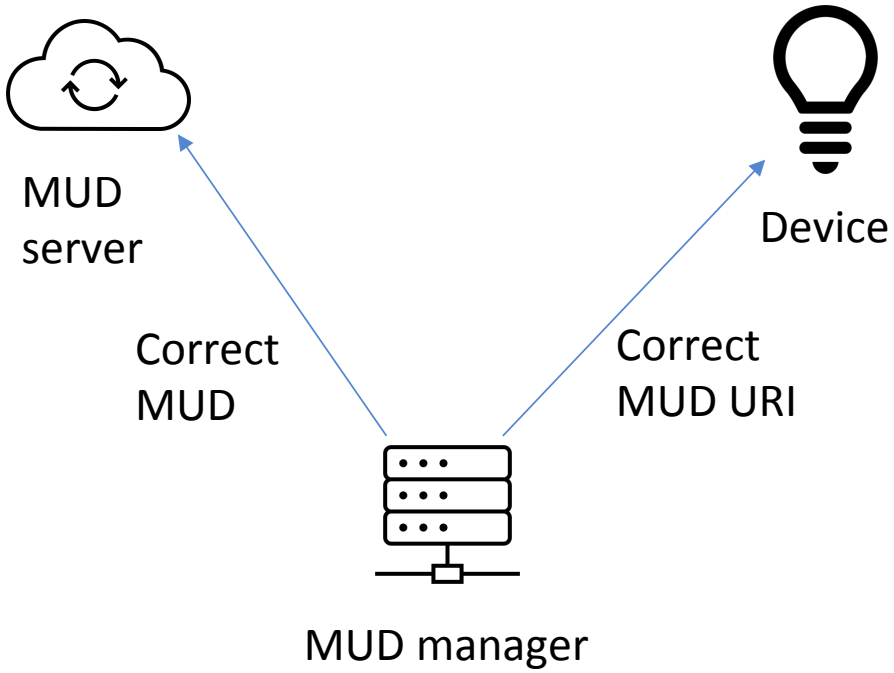
Why SUIT + MUD?

- Network Managers don’t need to know about MUD
  - Secure-by-default policies
- Target devices don’t need to know about MUD
  - MUD manager knows about SUIT instead

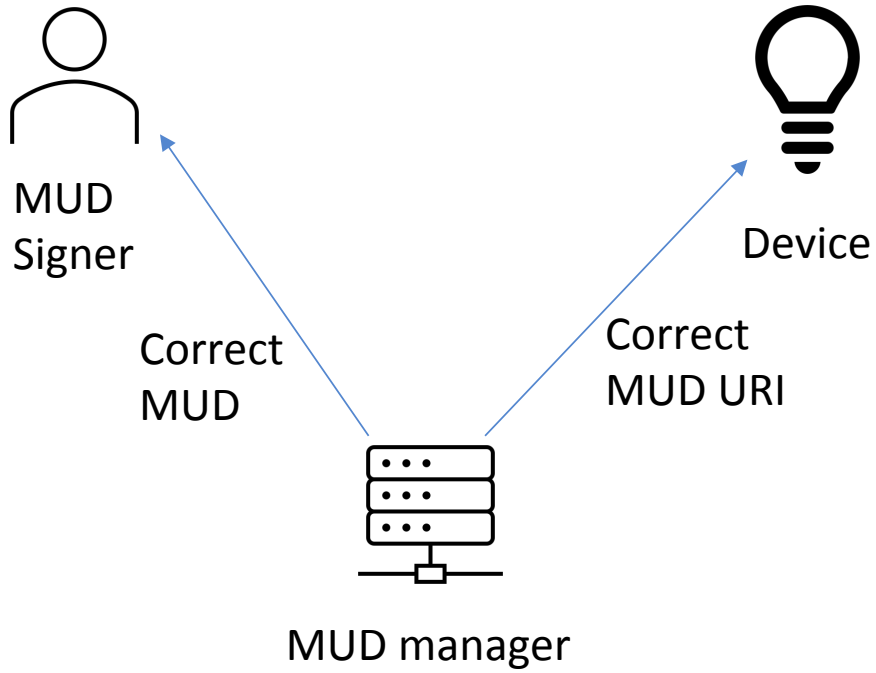
- Firmware author is best positioned to express intended access requirements
- Fewest trust relationships
- Trust in FW author is already required

MUD: Where is the trust? (1/3)

HTTPS

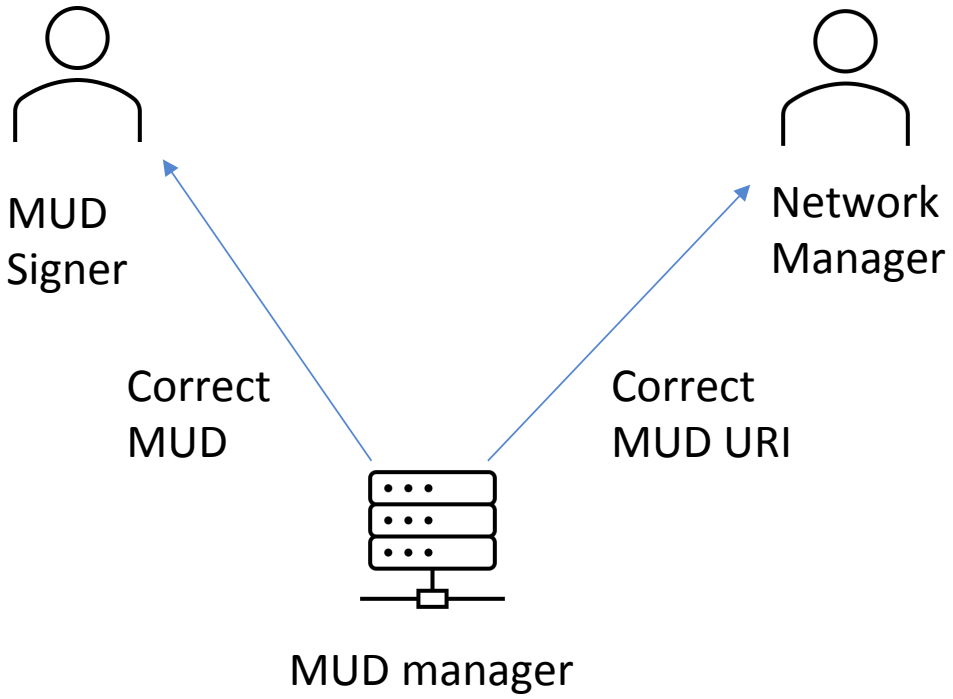


HTTPS with Signature

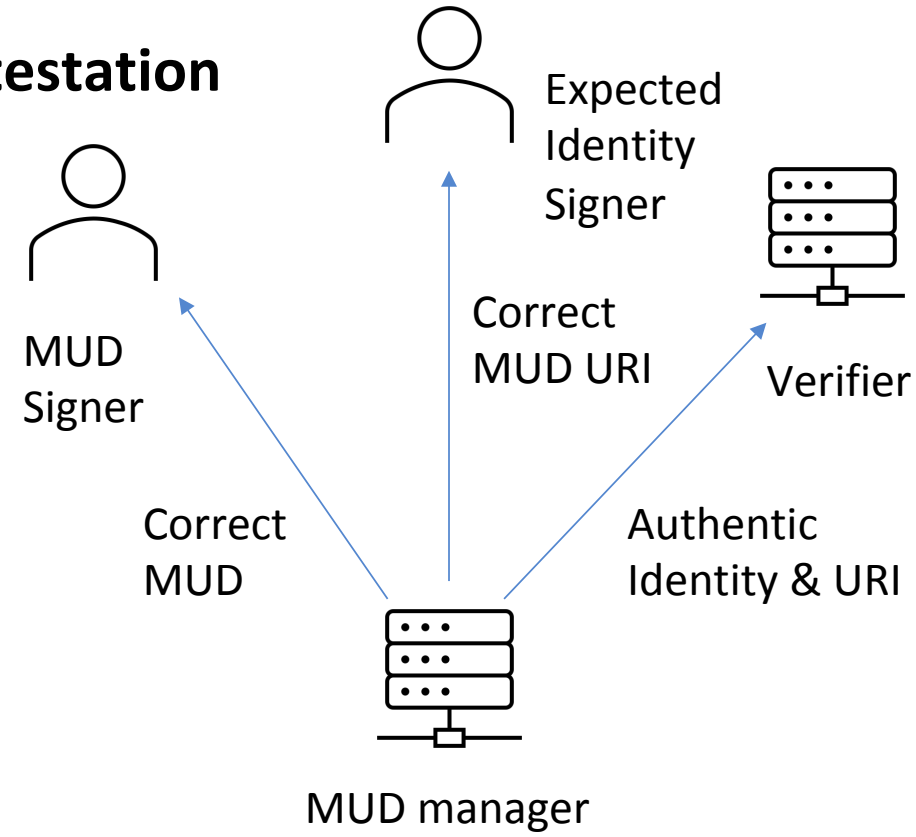


MUD: Where is the trust? (2/3)

Device Certificate

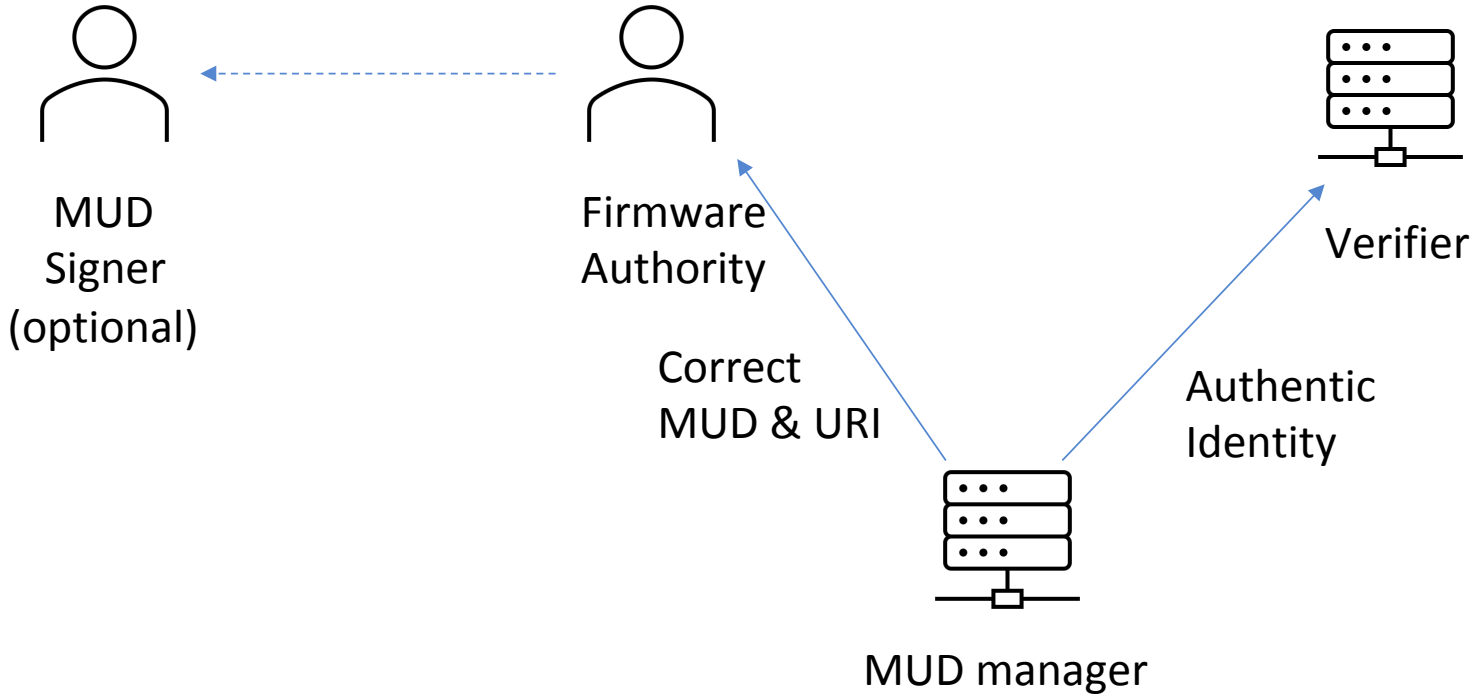


Attestation



MUD: Where is the trust? (3/3)

Attestation + SUIT



Integrating SUIT & MUD

Add a new severable value in SUIT manifest:

```
SUIT_MUD_container = {
    ? suit-mud-url => #6.32(tstr),
    ? suit-mud-ski => SUIT_Digest,
    ? suit-mud-file => bstr
}
```

- Either:
  - URI and subject key id for a remote, dynamic MUD file
  - Integrated MUD file for local, static MUD file

Open Issues:

- What about local network administration?
  - 2 manifests
    - 1 from Firmware Authority
    - 1 from local administrator
    - Combine MUD files or replace MUD files?
- Rechartering needed?

Rechartering

Proposed Text:

To support the manifest format(s) defined by this group, it will also define formats and protocols that enable a Status Tracker to determine if a particular manifest could be successfully deployed to a device, and determine if an operation was successful.

Additional specifications of names or numbers will enable the use of manifests, their precursors, and their successors within existing or future protocols.

Thanks to @mcr for feedback