OAuth for IoT

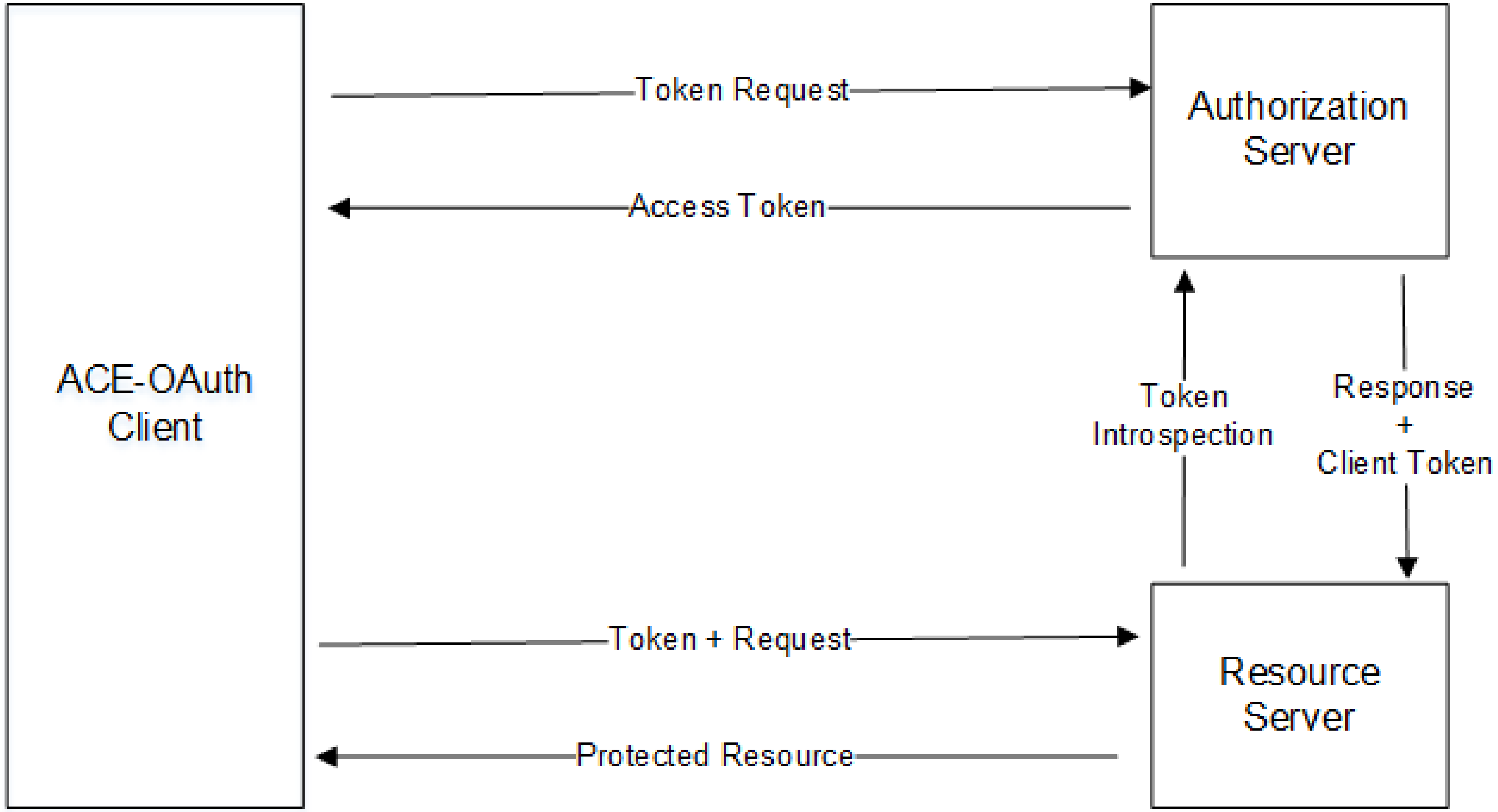
Hannes Tschofenig

OAuth Security Workshop 2018

March 2018
Trento

ACE-OAuth

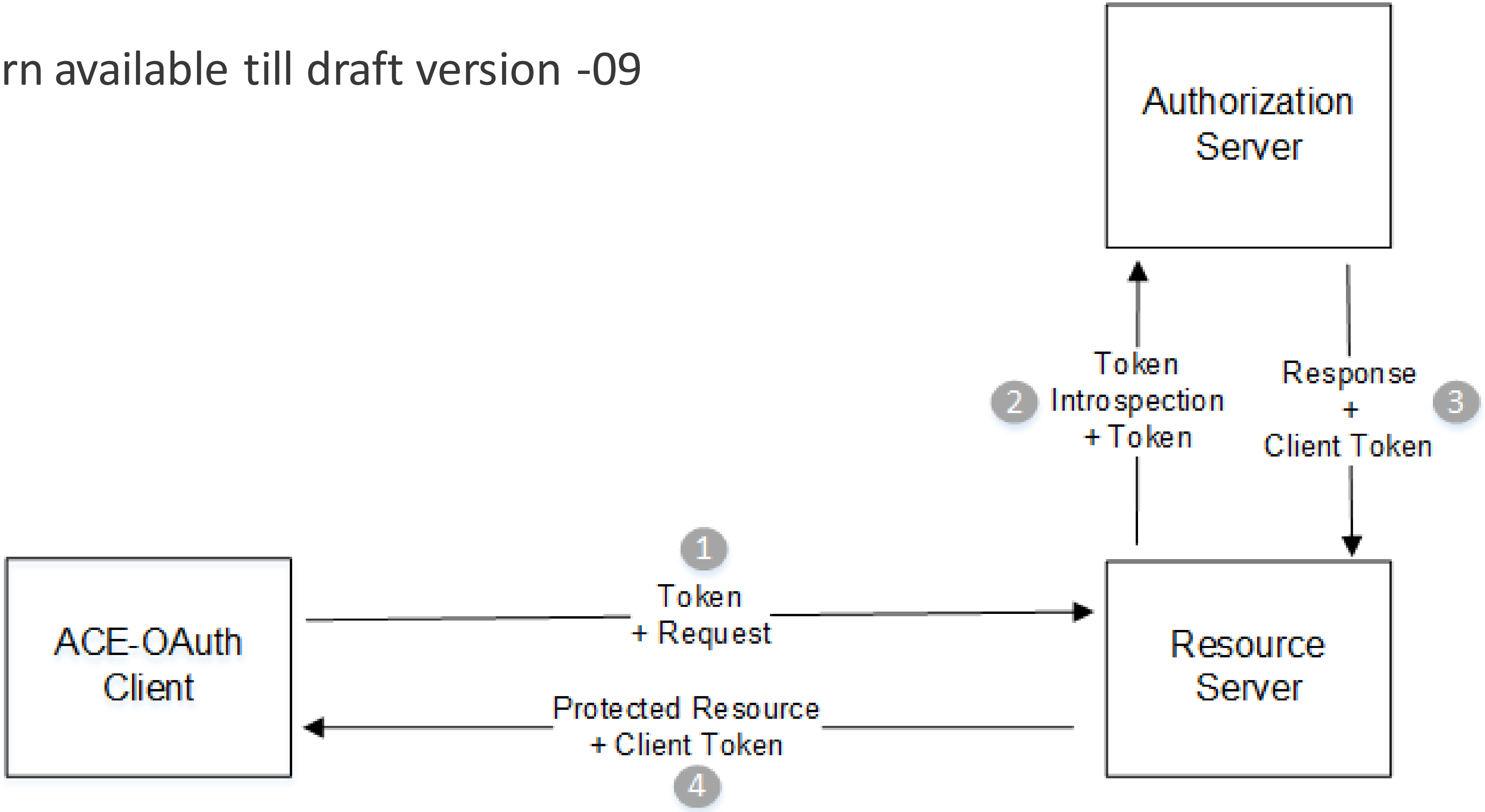
- Uses OAuth framework (OAuth for IoT)
- CoAP i.o. HTTP
- DTLS i.o. TLS
- CWT i.o. JWT
- PoP i.o. bearer



- Documented in framework and various profiles

Client Token

- Pattern available till draft version -09



CWT Example: MACed CWT

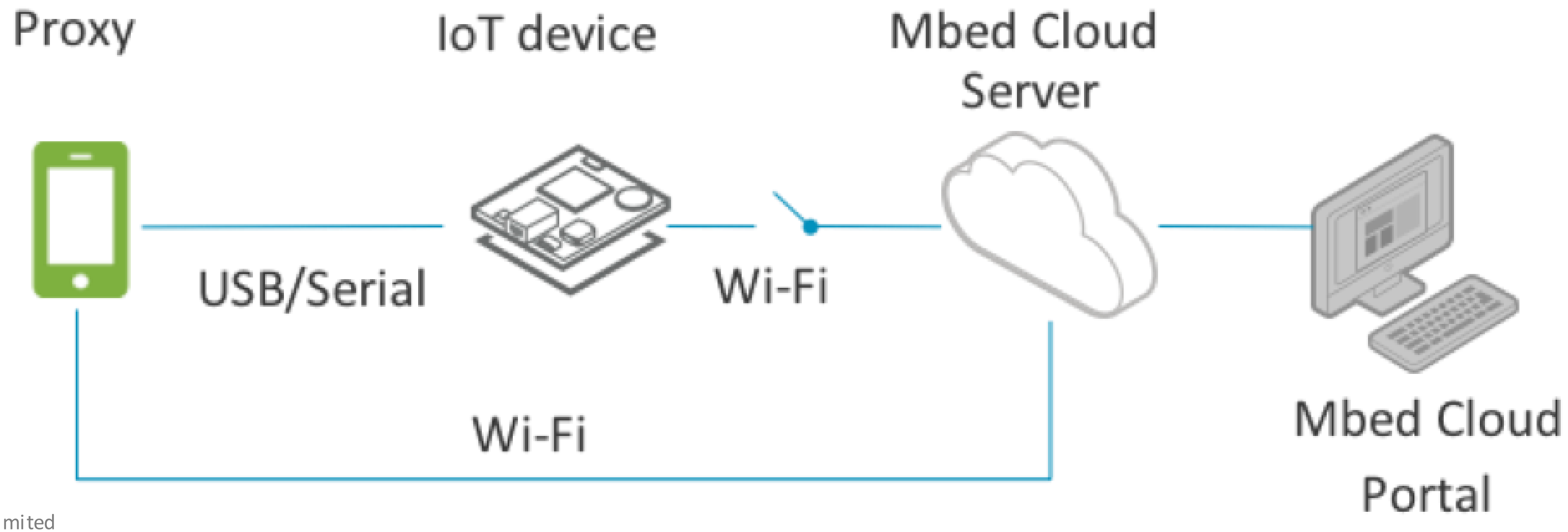
```
d83dd18443a10104a1044c53796d6d6574726963323536585 0a70175636f6170
```

Representation of an Asymmetric Proof-of-Possession Key

```
{
   /iss/ 1 : "coaps://server.example.com",
   /aud/ 3 : "coaps://client.example.org",
   /exp/ 4 : 1361398824,
   /cnf/ 8 :{
    /COSE_Key/ 1 :{
      /kty/ 1 : /EC/ 2,
      /crv/ -1 : /P-256/ 1,
      /x/ -2 : h'd7cc072de2205bdc1537a543d53c60a6acb62eccd890c7fa27c9e354089bbe13',
      /y/ -3 : h'f95e1d4b851a2cc80fff87d8e23f22afb725d535e515d020731e79a3b4e47120'
     }
    }
 }
```

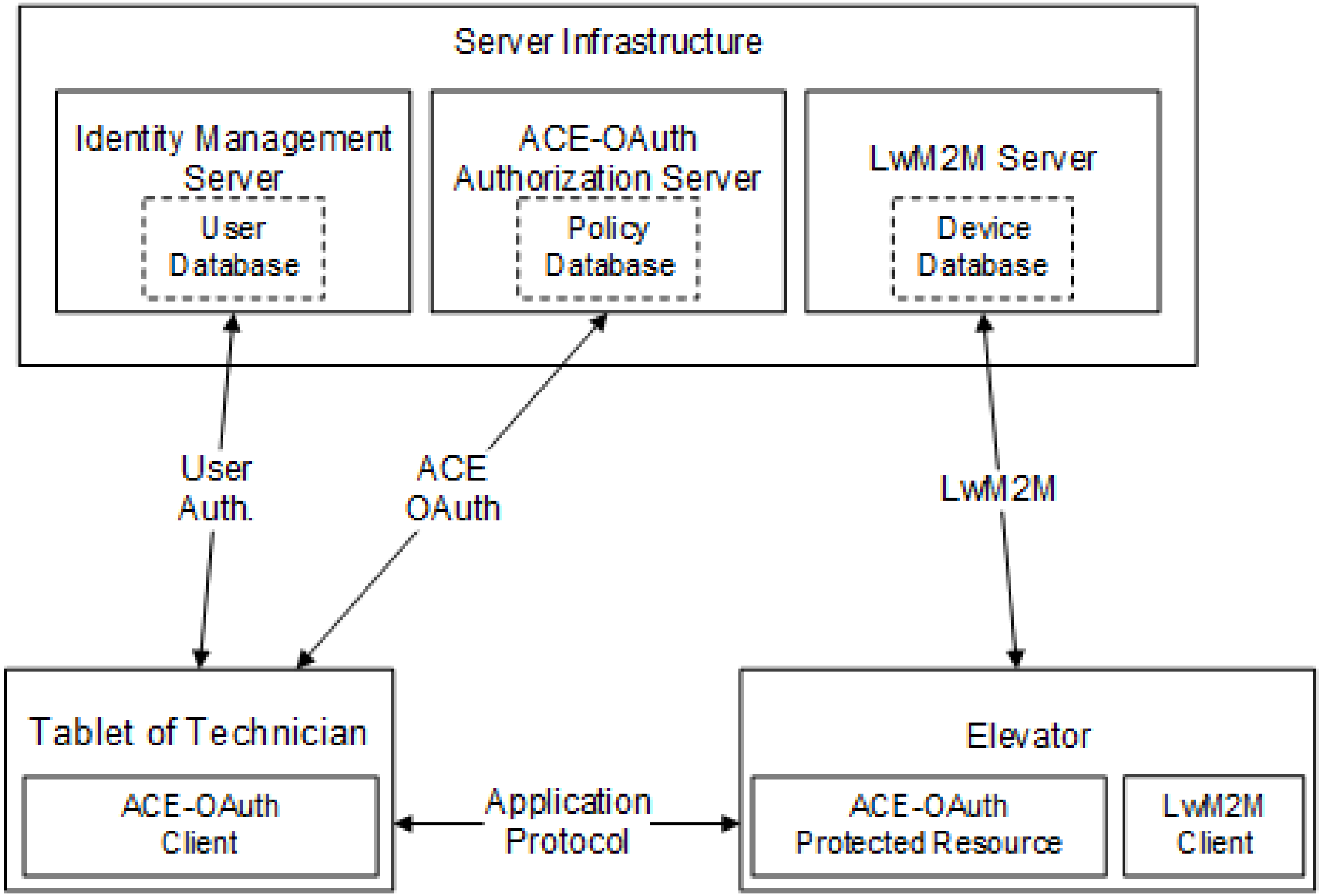
Arm Mbed Secure Device Access

- Feature is implemented in Arm Mbed Cloud product.
- Available in preview mode, available to selected partners since MWC.
- Documentation available: https://cloud.mbed.com/docs/v1.2/device-management/secure-device-access.html

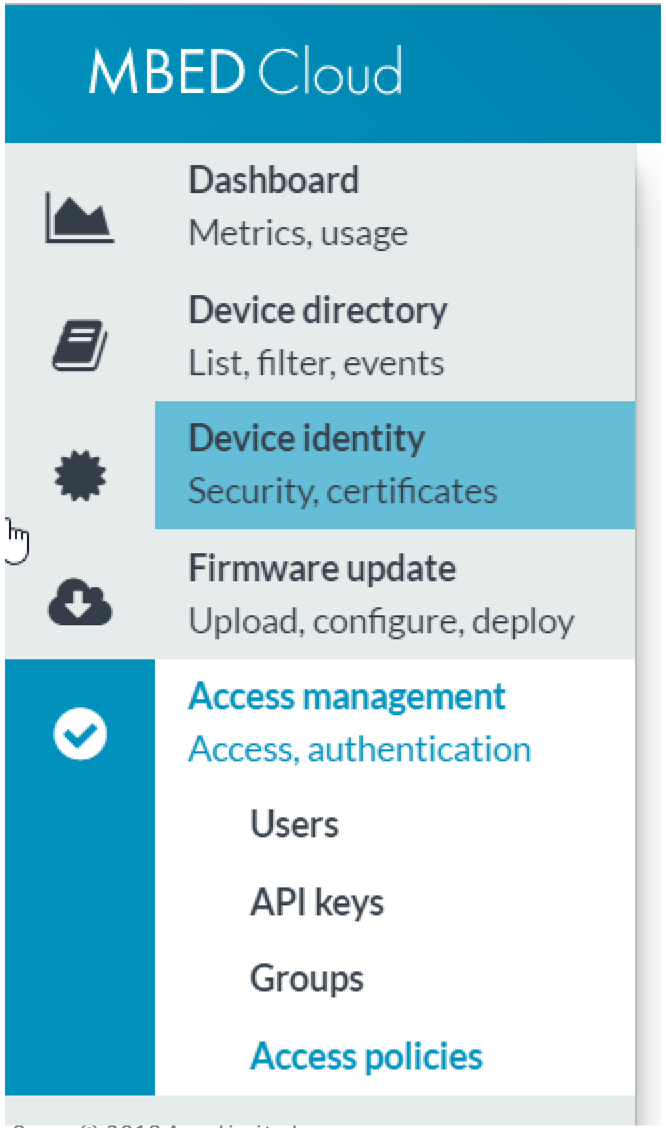


Secure Device Access

- Used in combination with our IoT device management platform.
- Latest version of the LwM2M spec (v1.0.2)

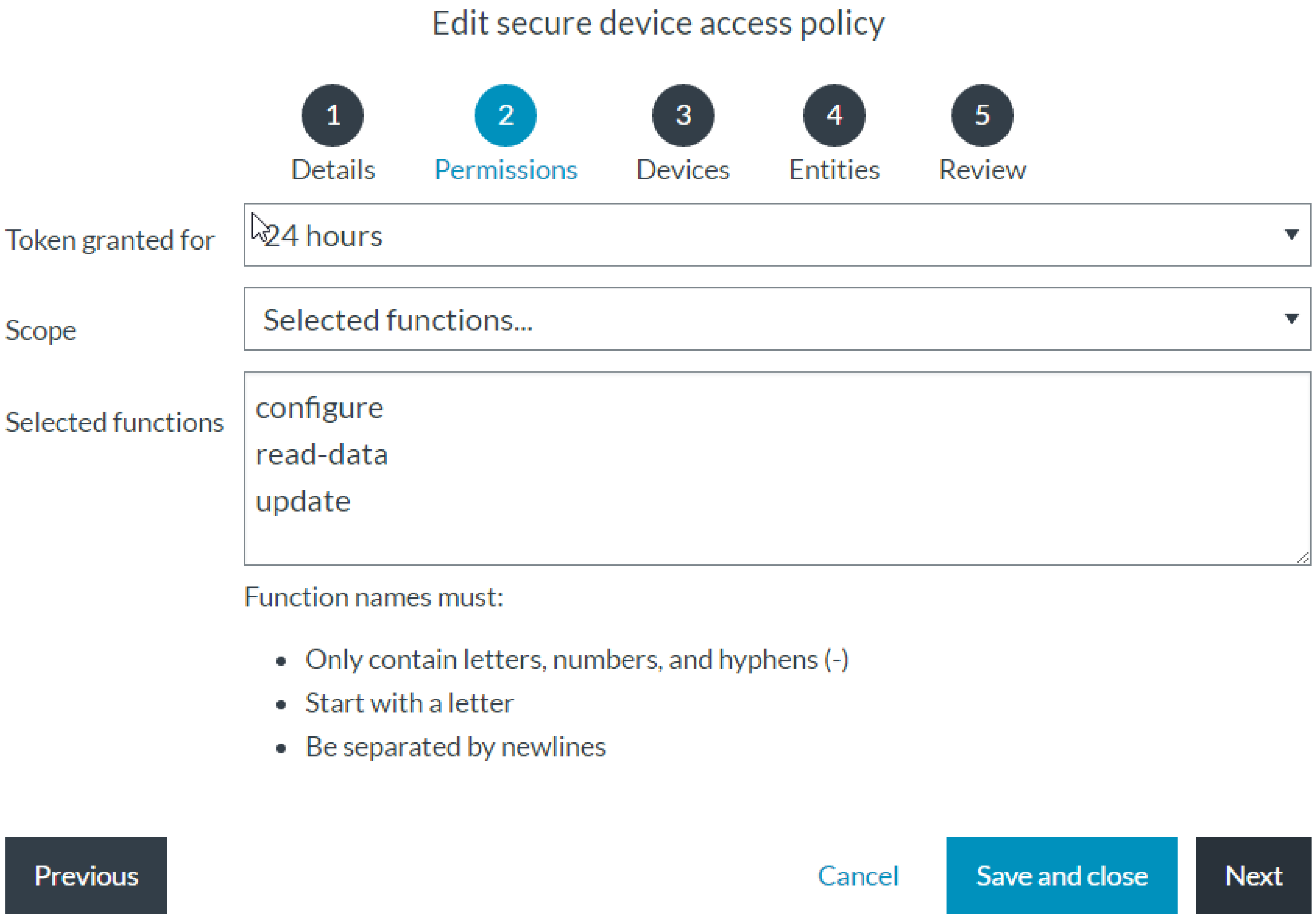


Enhancing mbed Cloud



MBED Cloud

- Dashboard
  Metrics, usage
- Device directory
  List, filter, events
- Device identity
  Security, certificates
- Firmware update
  Upload, configure, deploy
- Access management
  Access, authentication
  - Users
  - API keys
  - Groups
  - Access policies



Edit secure device access policy

1 Details — 2 Permissions — 3 Devices — 4 Entities — 5 Review

Token granted for: 24 hours ▼

Scope: Selected functions... ▼

Selected functions:

```
configure
read-data
update
```

Function names must:

- Only contain letters, numbers, and hyphens (-)
- Start with a letter
- Be separated by newlines

Video…

Lessons

- Adding support for selected ACE-OAuth functionality was smooth (particularly since we focused on the classical OAuth use)
- Ensure that HTTP-based transport is no forgotten
- Requires functionality on IoT device, Cloud/server side, and smart phone/tablet with different libraries.
  - We use COSE-Java on cloud/server and IoT side.
  - Good IoT device implementations are more difficult to find (since we want the integration with Mbed TLS crypto)
  - CWT + PoP code lacking.
- May want to re-use AppAuth (once ACE-OAuth support has been added)?!

Analysis of Client Token

- Looked at the various use cases of ACE and the functionality offered in the spec.
- High-quality specification is desirable.
- (OAuth Security Workshop also coming up where input is solicited.)
- Position paper available at http://st.fbk.eu/sites/st.fbk.eu/files/osw2018-ace.pdf
- Used Avispa and Scyther for analysis.

Example

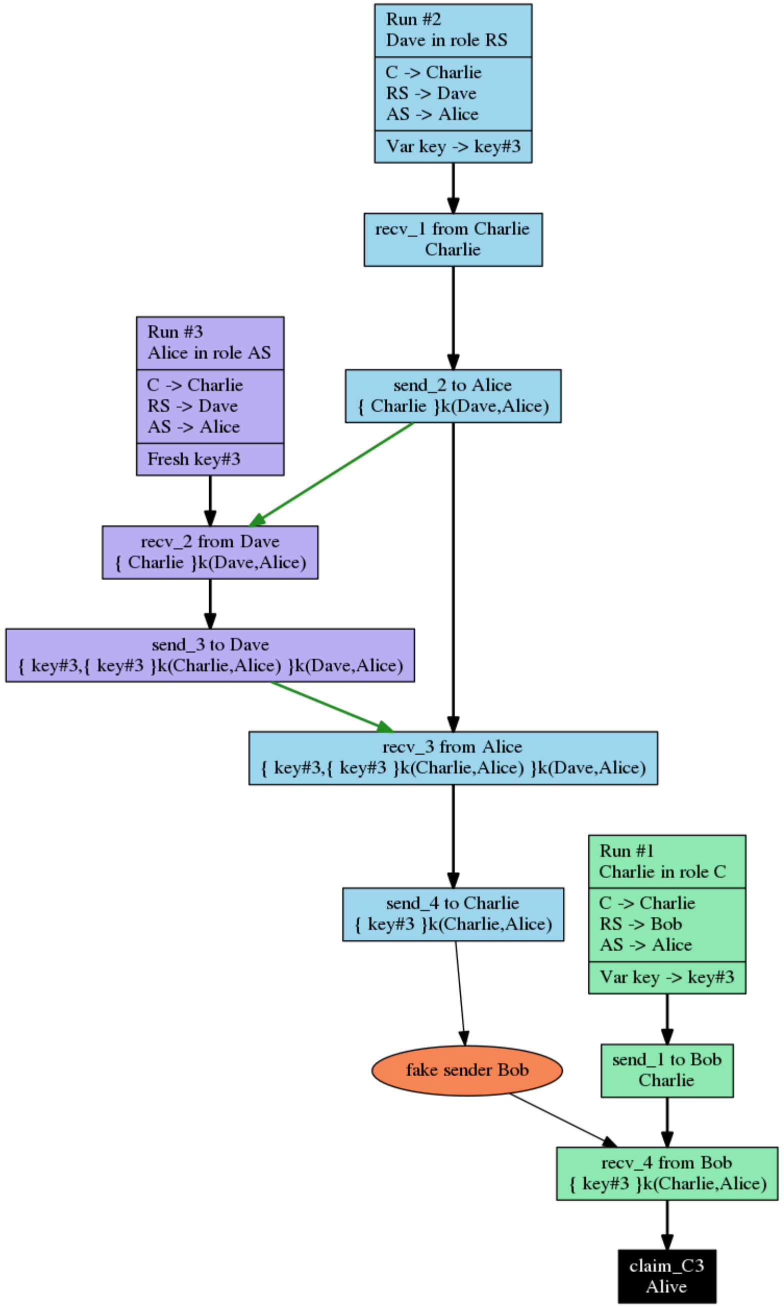
Avispa

```
% Resource Server

role client_token_R (R, A, C : agent,

         Snd, Rcv : channel (dy),

         K_RA     : symmetric_key)

played_by R

def=


 local State          : nat,

    K_SK,K_CA        : symmetric_key

 const sec_r_K_SK : protocol_id


 init  State := 0
```

```
  transition


  1. State = 0  /\ Rcv(C') =|>

    State':= 1 /\  Snd({C'}_K_RA)


  2. State = 1 /\ Rcv({K_SK'.{K_SK'}_K_CA}_K_RA)

       =|> State':= 2 /\ Snd({K_SK'}_K_CA)

          /\ secret(K_SK',sec_r_K_SK,{C,R,A})

 end role
```

Attack scenario

- Attack trace provided by Scyther. See paper for larger representation.
- The problem is that the OAuth Client is not authenticated to the Authorization Server.



[Id 4] Protocol clienttoken, role C, claim type Alive

Lessons

- Our specifications often don’t indicate what security goals the protocol (or protocol variants) are trying to accomplish.
- Details for secure implementation missing (but otherwise OK for interoperability).
- Security protocol design feels a bit adhoc and not following good engineering practices.
- Formal method tools have their own challenges: probably the most useful part is in describing the protocol in a different notation.
- Tools have limitations and tool developer support varies.
- Already in earlier workshop we promised to state security goals more clearly, provide pseudo code, etc.
  - … but we never did. Why?

Summary

- First product implementation of the ACE-OAuth available.
- Integrated ACE-OAuth with LwM2M for a selected set of scenarios.
- Started analysis of the ACE-OAuth protocol and ran into problems.
- I believe the IETF security community would benefit from the study of formal methods, and this would help them to avoid relying so extensively on researchers.
- Determining which approach is best for the analysis of IETF security protocols, where re-use and layering is a common design technique, would require further study.