ACE working group

Resource Directory authorization
draft-ietf-core-resource-directory-14

Peter van der Stok, Cristian Amsuss, Carsten Bormann, Michael Koster

Motivation

In the security section of Resource Directory draft
a threat to registration is described.

Hannes (and I agree) suggests that Resource Directory draft features some text to remove consequences of the threat

RD will not contain normative text (subject for another “secure RD draft”)
But may contain a guiding example.

We want to ask ACE to discuss, review, improve the suggested approach.

Threat

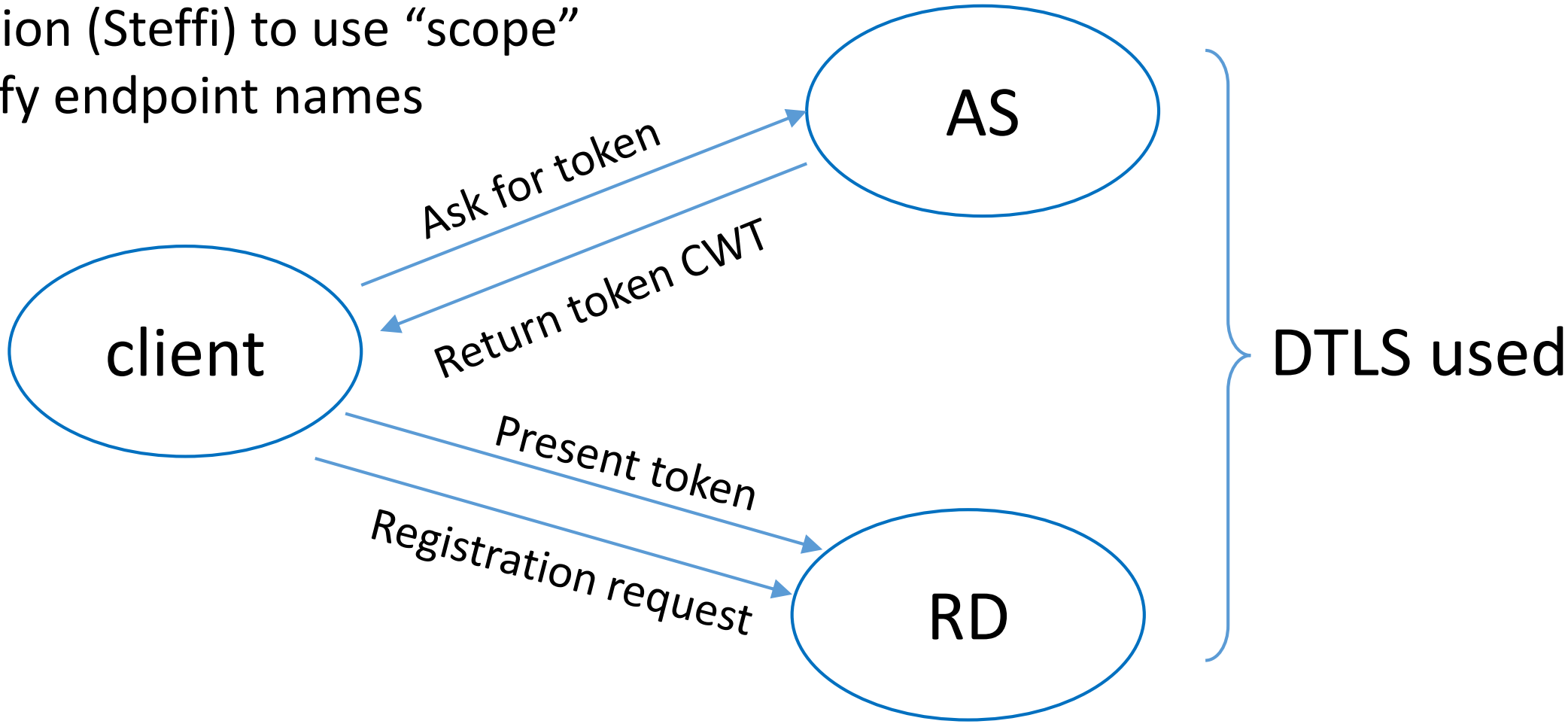
An endpoint registers with an unique endpoint name.

Assume endpoints A and B with names A-1 and B-1
B is malicious.
B registers with name A-1

When A wants to register with A-1, it is toast (sic Hannes)

Suggest Authorization Server (AS)

Suggestion (Steffi) to use “scope”
to specify endpoint names



Client background

Client has certificate installed, see BRSKI
endpoint name equals certificate identifier

Unique certificate identifier:
Fairhair-01:02:03:04:05:06:07:08
Concatenated from CN field
And Serial Number field

```
Certificate: Data:
        Version: 3 (0x2)
        Serial Number: 01:02:03:04:05:06:07:08
        Signature Algorithm: md5WithRSA
        Encryption Issuer: C=US, ST=Florida, O=Acme, Inc., OU=Security,
                                                                CN=CA
      Authority/emailAddress=ca@acme.com
        Validity Not Before: Aug 20 12:59:55 2013 GMT
                                    Not After : Aug 20 12:59:55 2013 GMT
         Subject: C=US, ST=Florida, O=Acme, Inc., OU=Sales, CN=Fairhair
         Subject Public Key
         Info: Public Key Algorithm: rsaEncryption
         RSA Public Key: (1024 bit) Modulus (1024 bit):
    00:be:5e:6e:f8:2c:c7:8c:07:7e:f0:ab:a5:12:db:
    fc:5a:1e:27:ba:49:b0:2c:e1:cb:4b:05:f2:23:09:
    77:13:75:57:08:29:45:29:d0:db:8c:06:4b:c3:10:
    88:e1:ba:5e:6f:1e:c0:2e:42:82:2b:e4:fa:ba:bc:
    45:e9:98:f8:e9:00:84:60:53:a6:11:2e:18:39:6e:
    ad:76:3e:75:8d:1e:b1:b2:1e:07:97:7f:49:31:35:
    25:55:0a:28:11:20:a6:7d:85:76:f7:9f:c4:66:90:
    e6:2d:ce:73:45:66:be:56:aa:ee:93:ae:10:f9:ba:
    24:fe:38:d0:f0:23:d7:a1:3b
    Exponent: 65537 (0x10001)
```

Scope name suggestions

Three cases:

- Endpoint registers itself:
  scope: “ep-registration_ep-name_ep-sector”

- 3rd party Commissioning Tool registers endpoint
  scope: “ct-registration_ep-name_ep-sector”

- Update of Registration(s)
  scope: “rg-update_ep-name_ep-sector”

ep-sector is optional

Scope value suggestions

ep-name: certificate identifier
ep-sector: preconfigured in AS for given certificate identifiers

CWT example

Endpoint registers itself

```
{
"aud" : “coaps://rd.example.com",        /destination of token and request/
"iat" : "1360189224",
"exp" : "1360289224",
"scope" : " ep-registration_Fairhair_01:02:03:04:05:06:07:08",     / no sector /
"cnf" : {
     "COSE_Key" : {
        "kid" : ’AsymmetricRSA’,
        “kty” : ‘EC2’,
        “crv” : “p-256”,
        “alg" : “ES256",
        “signature” : 00:be:5e:6e:f8:2c:c7:8c:07:7e:f0:ab:a5:12:db:
  fc:5a:1e:27:ba:49:b0:2c:e1:cb:4b:05:f2:23:09:77:13:75:57:08:29:45:29:d0:db:8c:06:4b:c3:10:
  88:e1:ba:5e:6f:1e:c0:2e:42:82:2b:e4:fa:ba:bc: 45:e9:98:f8:e9:00:84:60:53:a6:11:2e:18:39:6e:
  ad:76:3e:75:8d:1e:b1:b2:1e:07:97:7f:49:31:35:25:55:0a:28:11:20:a6:7d:85:76:f7:9f:c4:66:90:
  e6:2d:ce:73:45:66:be:56:aa:ee:93:ae:10:f9:ba:24:fe:38:d0:f0:23:d7:a1:3b
                    }
          }
}
```