Implementation report

draft-reddy-dots-signal-channel-10

March 2017

Presenter : Flemming Andreasen

Proof of concept

- Used californium framework (https://eclipse.org/californium/) to exchange DOTS messages using CoAP over DTLS.
- Californium implements DTLS 1.2

Proof of concept

- Californium framework provides APIs to
  - Use congestion control
  - Configuration of message transmission parameters and heartbeat timeout
  - Mark messages as Confirmable or Non-confirmable

Proof of concept

- Mozilla (with copper plugin https://addons.mozilla.org/en-US/firefox/addon/copper-270430/) to exchange DOTS messages to a test DOTS server.

Proof of concept

```
Constrained Application Protocol, Non-Confirmable, PUT, MID:2719
 01.. .... = Version: 1
 ..01 .... = Type: Non-Confirmable (1)
 .... 1000 = Token Length: 8
 Code: PUT (3)
 Message ID: 2719
 Token: 4ee7d4f8f01595e6
>Opt Name: #1: Uri-Host: www.example.com
>Opt Name: #2: Uri-Path: .well-known
>Opt Name: #3: Uri-Path: v1
>Opt Name: #4: Uri-Path: DOTS-signal
>Opt Name: #5: Uri-Path: signal
>Opt Name: #6: Content-Format: application/cbor
 End of options marker: 255
 [Response In: 339]
Payload: Payload Content-Format: application/cbor, Length: 27
  Payload Desc: application/cbor
 Concise Binary Object Representation
  Map: (1 entries)
   ...0 0001 = Unsigned Integer: 1
    Map: (2 entries)
     ...0 0010 = Unsigned Integer: 2
       Unsigned Integer: 123344
     ...0 1011 = Unsigned Integer: 11
      Array: (2 elements)
        Text String: Server1
        Text String: Server2
```

Proof of concept (http://cbor.me/)

Diagnostic →

```
{
   1: {
      2:99,
      11:[
         "Server1",
         "Server2"
      ]
   }
}
```

mitigation-scope

policy-id

alias

← 24 Bytes

```
a1                      # map(1)
   01                   # unsigned(1)
   a2                   # map(2)
      02                # unsigned(2)
      18 63             # unsigned(99)
      0b                # unsigned(11)
      82                # array(2)
         67             # text(7)
            53657276657231 # "Server1"
         67             # text(7)
            53657276657232 # "Server2"
```