Developer Feedback

Marek Serafin

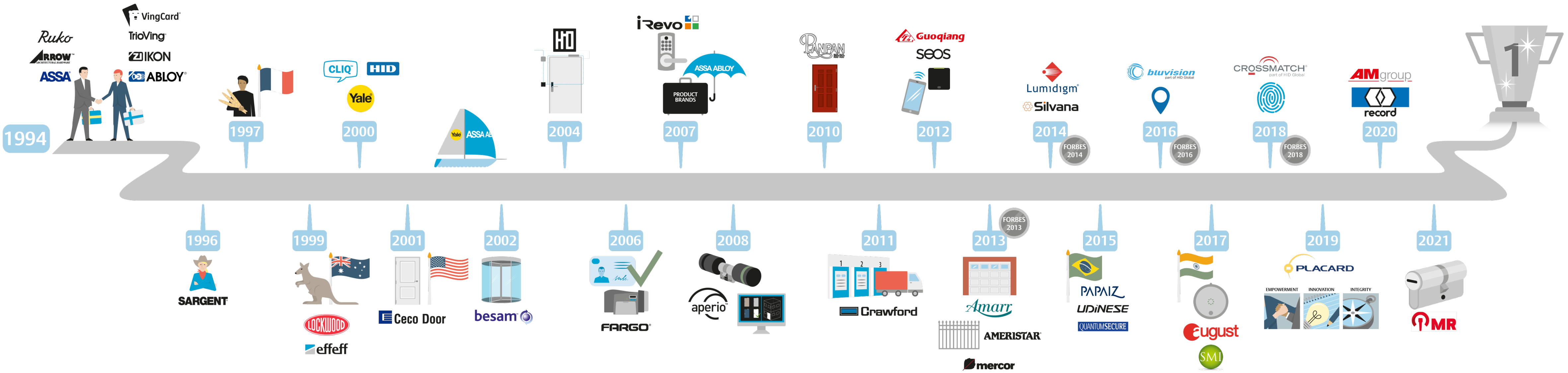
ASSA ABLOY

I’m Marek

IoT / Mobile / Solution Architect & Developer

@ ASSA ABLOY

ASSA ABLOY


1994
Ruko
ARROW
ARCHITECTURAL HARDWARE
ASSA
VingCard
TrioVing
IKON
ABLOY
1996
SARGENT
1997
1999
LOCKWOOD
effeff
2000
CLIQ
HID
Yale
2001
Ceco Door
2002
besam
Yale
ASSA AB
2004
2006
FARGO
2007
iRevo
PRODUCT BRANDS
ASSA ABLOY
2008
aperio
2010
PANPAN
2011
1
2
3
Crawford
2012
Guoqiang
seos
2013
FORBES 2013
Amarr
AMERISTAR
mercor
2014
FORBES 2014
Lumidigm
Silvana
2015
PAPAIZ
UDINESE
QUANTUMSECURE
2016
FORBES 2016
bluvision
part of HID Global
2017
august
SMI
2018
FORBES 2018
CROSSMATCH
part of HID Global
2019
PLACARD
EMPOWERMENT
INNOVATION
INTEGRITY
2020
AMgroup
record
2021
MR
1

Challenge

- Modular IoT stack to run on **Embedded**, Mobile, and Cloud
- Enable Device-to-Cloud, Device-to-Mobile and Device-to-Device E2E secure communication within Application Layer
- Work with identity formats like X.509 certificates, CWT, JWT
- Backed by **standards** so we can maintain security more efficiently with the help of Open Source

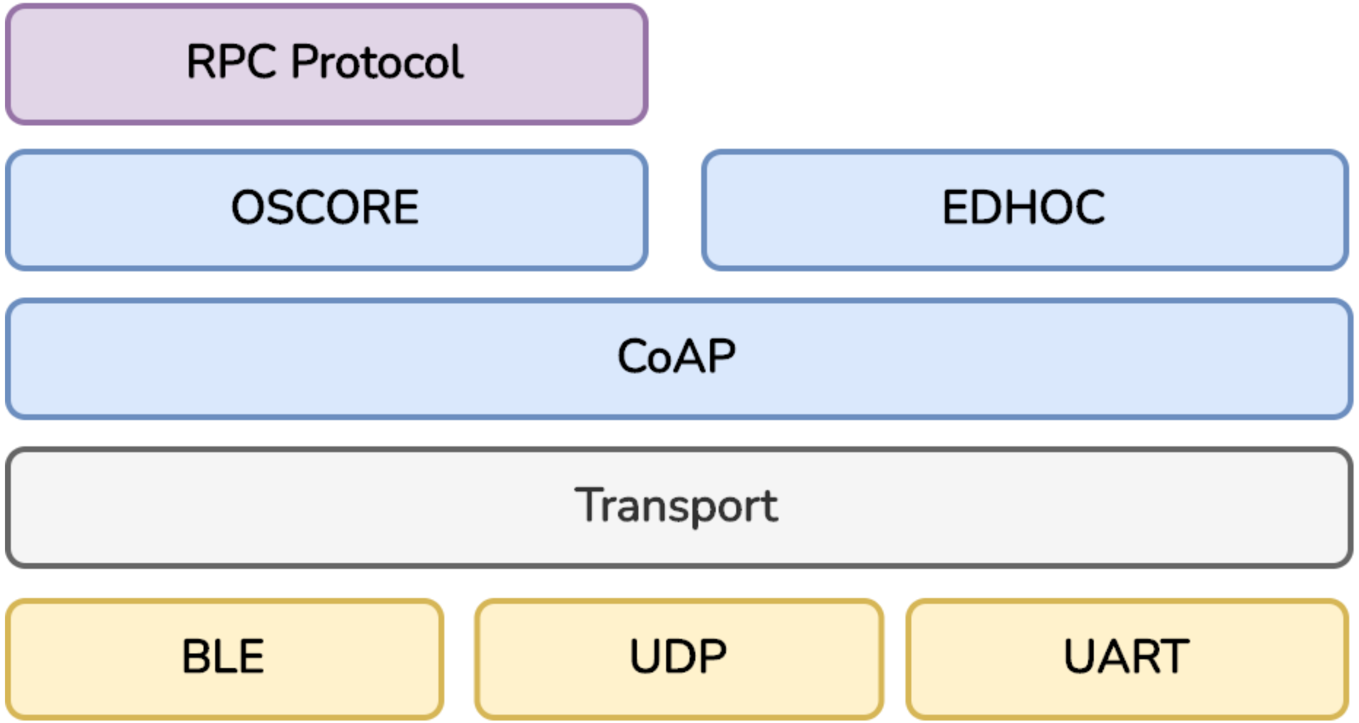
Areas

- Provisioning (Identity, etc.)
- **Communication**
- Operations (Firmware Update, etc.)

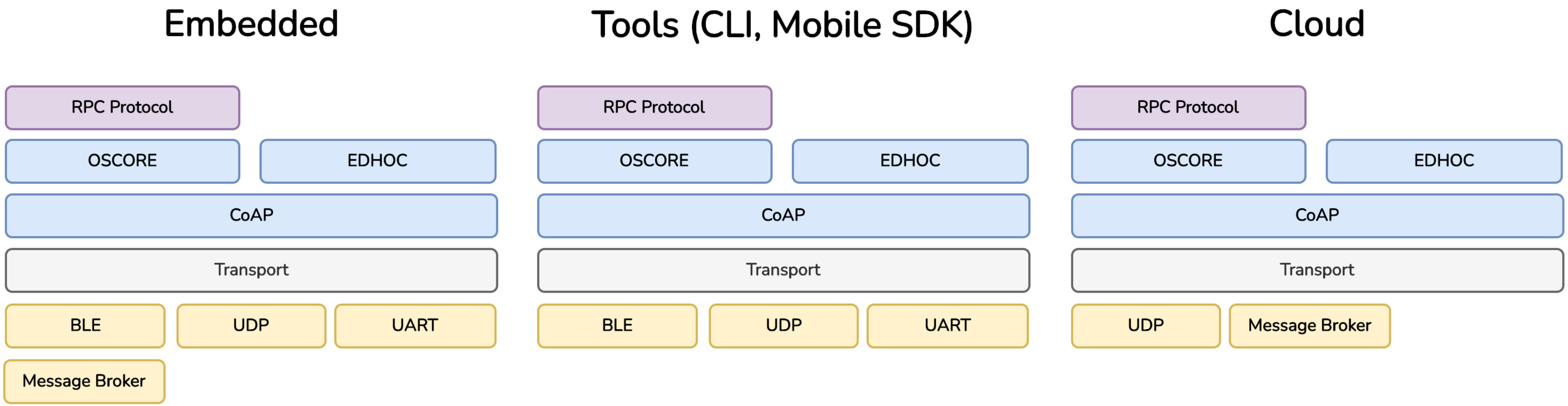
Solution

- CoAP
- OSCORE
- **EDHOC**
- X.509 certificates (p-256 keys)
- and more …

Architecture



Platforms



Embedded

- RPC Protocol
- OSCORE
- EDHOC
- CoAP
- Transport
- BLE
- UDP
- UART
- Message Broker

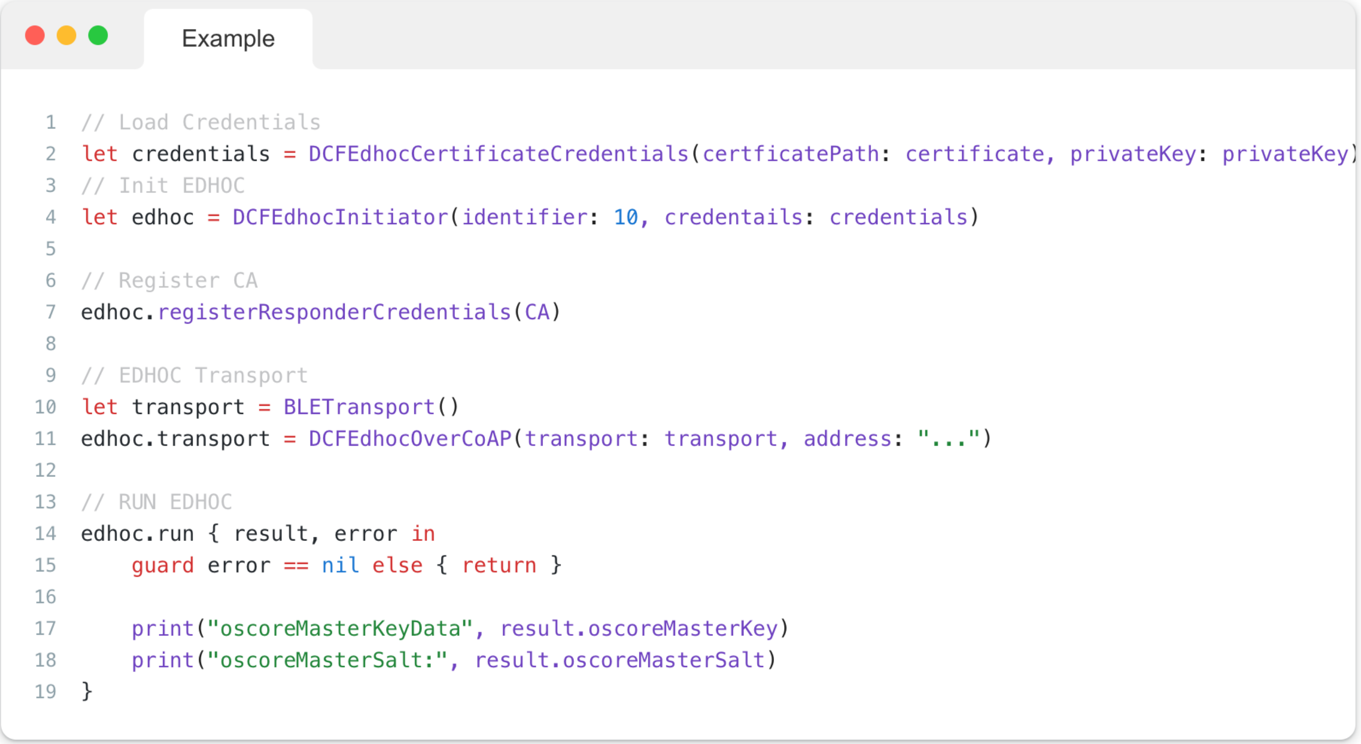
Tools (CLI, Mobile SDK)

- RPC Protocol
- OSCORE
- EDHOC
- CoAP
- Transport
- BLE
- UDP
- UART

Cloud

- RPC Protocol
- OSCORE
- EDHOC
- CoAP
- Transport
- UDP
- Message Broker

EDHOC library



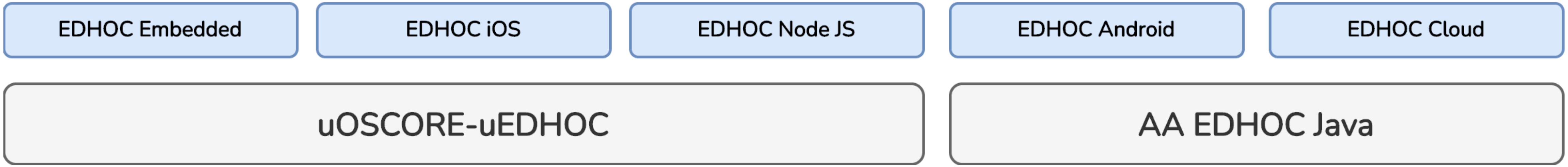
```
// Load Credentials
let credentials = DCFEdhocCertificateCredentials(certficatePath: certificate, privateKey: privateKey)
// Init EDHOC
let edhoc = DCFEdhocInitiator(identifier: 10, credentails: credentials)

// Register CA
edhoc.registerResponderCredentials(CA)

// EDHOC Transport
let transport = BLETransport()
edhoc.transport = DCFEdhocOverCoAP(transport: transport, address: "...")

// RUN EDHOC
edhoc.run { result, error in
    guard error == nil else { return }

    print("oscoreMasterKeyData", result.oscoreMasterKey)
    print("oscoreMasterSalt:", result.oscoreMasterSalt)
}
```



EDHOC Embedded

EDHOC iOS

EDHOC Node JS

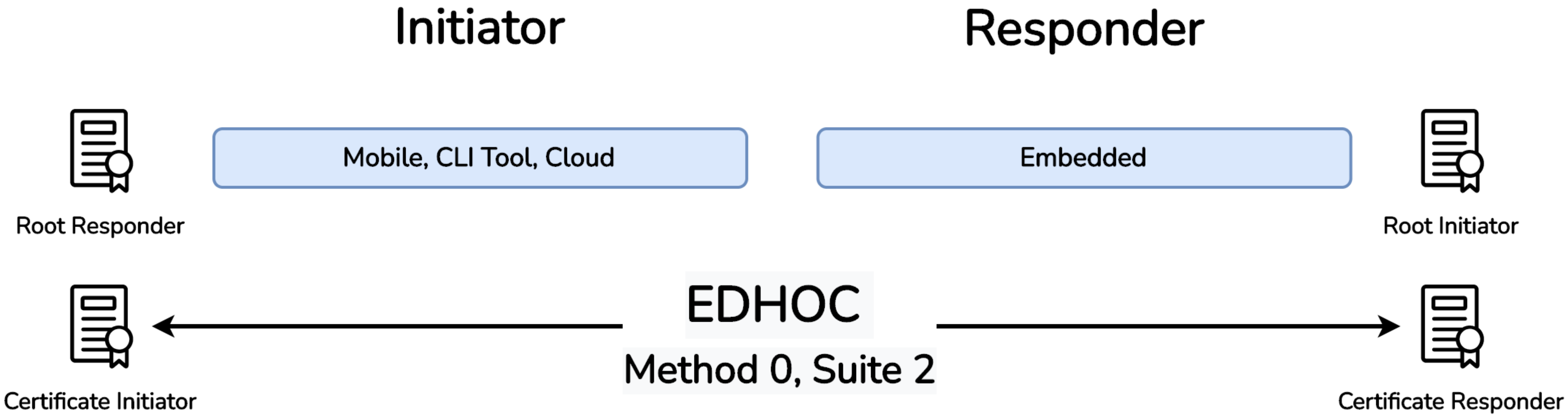
EDHOC Android

EDHOC Cloud

uOSCORE-uEDHOC

AA EDHOC Java

EDHOC use-case



Initiator

Responder

Root Responder

Mobile, CLI Tool, Cloud

Embedded

Root Initiator

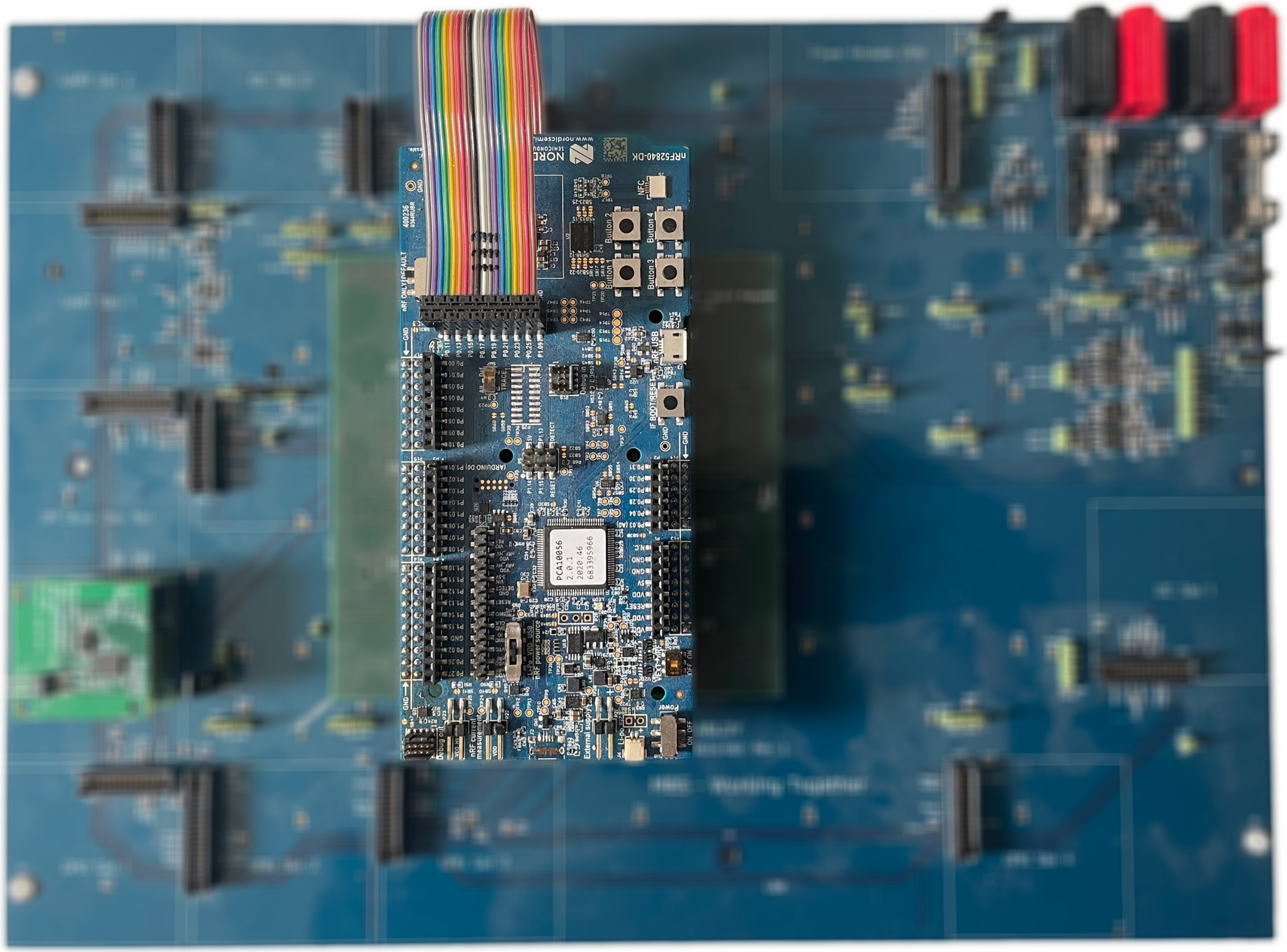
EDHOC

Method 0, Suite 2

Certificate Initiator

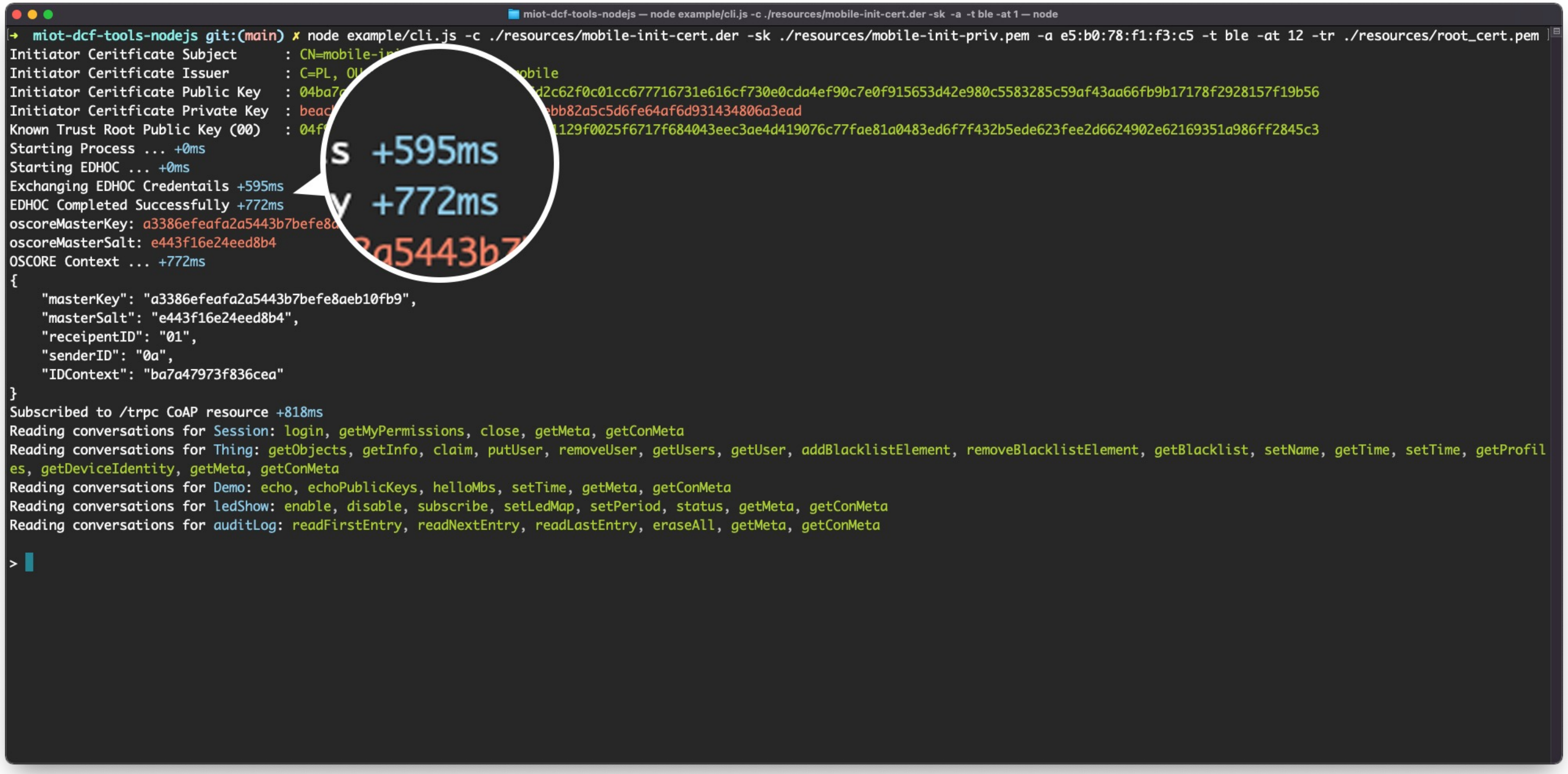
Certificate Responder

Embedded



- NRF52840 FreeRTOS
- Lobaro CoAP
- uOSCORE
- **uEDHOC**
- HW Crypto (mbedTLS)

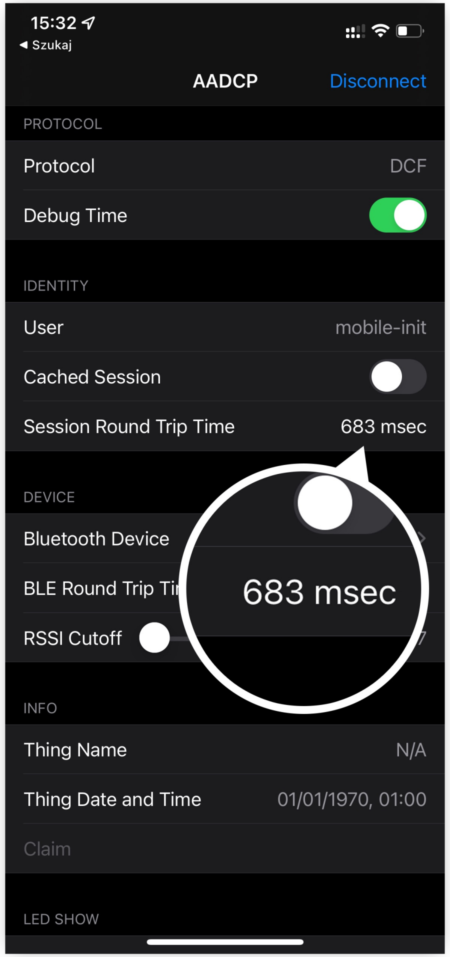
EDHOC Performance


miot-dcf-tools-nodejs — node example/cli.js -c ./resources/mobile-init-cert.der -sk -a -t ble -at 1 — node
s +595ms
y +772ms
2a5443b7

```
→  miot-dcf-tools-nodejs git:(main) ✗ node example/cli.js -c ./resources/mobile-init-cert.der -sk ./resources/mobile-init-priv.pem -a e5:b0:78:f1:f3:c5 -t ble -at 12 -tr ./resources/root_cert.pem
Initiator Ceritficate Subject      : CN=mobile-in
Initiator Ceritficate Issuer       : C=PL, OU                   obile
Initiator Ceritficate Public Key   : 04ba7c                     d2c62f0c01cc677716731e616cf730e0cda4ef90c7e0f915653d42e980c5583285c59af43aa66fb9b17178f2928157f19b56
Initiator Ceritficate Private Key  : beac                       ebb82a5c5d6fe64af6d931434806a3ead
Known Trust Root Public Key (00)   : 04f                        1129f0025f6717f684043eec3ae4d419076c77fae81a0483ed6f7f432b5ede623fee2d6624902e62169351a986ff2845c3
Starting Process ... +0ms
Starting EDHOC ... +0ms
Exchanging EDHOC Credentails +595ms
EDHOC Completed Successfully +772ms
oscoreMasterKey: a3386efeafa2a5443b7befe8a
oscoreMasterSalt: e443f16e24eed8b4
OSCORE Context ... +772ms
{
    "masterKey": "a3386efeafa2a5443b7befe8aeb10fb9",
    "masterSalt": "e443f16e24eed8b4",
    "receipentID": "01",
    "senderID": "0a",
    "IDContext": "ba7a47973f836cea"
}
Subscribed to /trpc CoAP resource +818ms
Reading conversations for Session: login, getMyPermissions, close, getMeta, getConMeta
Reading conversations for Thing: getObjects, getInfo, claim, putUser, removeUser, getUsers, getUser, addBlacklistElement, removeBlacklistElement, getBlacklist, setName, getTime, setTime, getProfil
es, getDeviceIdentity, getMeta, getConMeta
Reading conversations for Demo: echo, echoPublicKeys, helloMbs, setTime, getMeta, getConMeta
Reading conversations for ledShow: enable, disable, subscribe, setLedMap, setPeriod, status, getMeta, getConMeta
Reading conversations for auditLog: readFirstEntry, readNextEntry, readLastEntry, eraseAll, getMeta, getConMeta

> 
```

EDHOC Performance



15:32
◂ Szukaj

AADCP Disconnect

PROTOCOL

Protocol DCF

Debug Time ☑

IDENTITY

User mobile-init

Cached Session ☐

Session Round Trip Time 683 msec

DEVICE

Bluetooth Device

BLE Round Trip Ti

RSSI Cutoff

683 msec

INFO

Thing Name N/A

Thing Date and Time 01/01/1970, 01:00

Claim

LED SHOW

<1 sec for

1. BLE Scan,
2. Connect,
3. Discover GATT
4. EDHOC with X.509 Certificates
5. Setup RPC Session

Future

- Cloud HTTP to CoAP proxy with EDHOC and OSCORE
- Open Source contributions (Already uOSCORE-uEDHOC)
- Develop modern Test Vector Generator

Thank you!

✉ marek.serafin@assaabloy.com

https://github.com/stoprocent

in https://www.linkedin.com/in/marekserafin