TeleTrusT
Pioneers in IT security.

TeleTrusT-EBCA "PKI-Workshop" 2019

Bundesverband IT-Sicherheit e.V. (TeleTrusT)

Berlin, 18.06.2019

Flexibler Anbieterwechsel auf der embedded SIM

Dr. Norbert Holthöfer, achelos GmbH

Agenda

achelos

Subscription Management

- SIM Form Factors – a little history
- What is subscription management?

System Architecture

- Subscription Manager – Data Preparation (SM-DP)
- Subscription Manager – Secure Routing (SM-SR)

PKI

- Certificates
- Certification

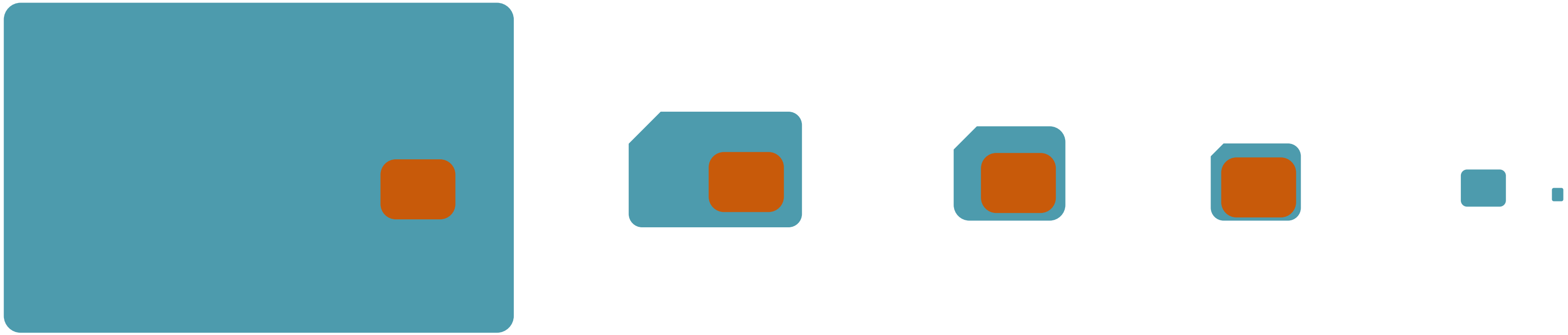
Solution Architecture

- SM-SR high level architecture
- Security Domains

Connectivity Manager

- Rule-based profile download
- Rule-based profile switch

SIM Form Factors – a little history



ID Card Size
1FF

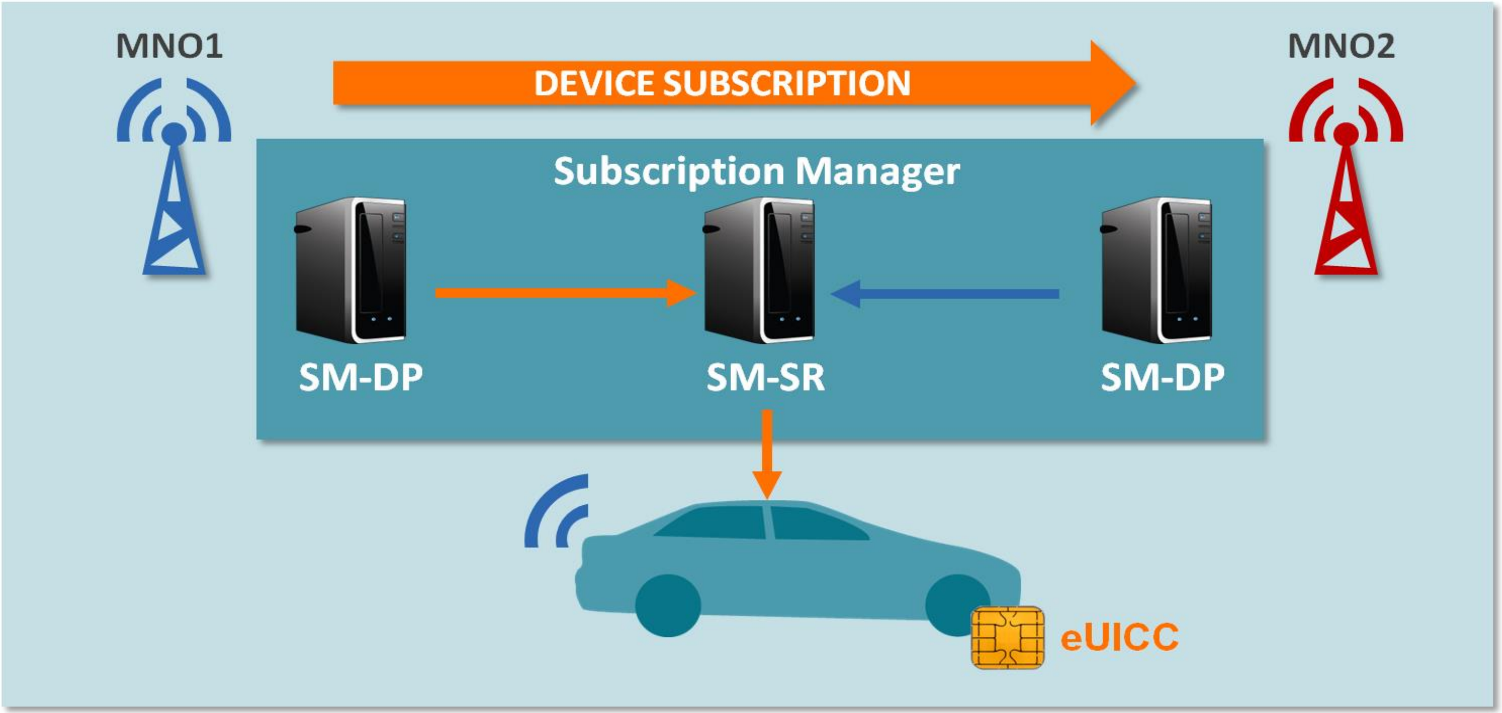
Mini SIM
2FF

Micro SIM
3FF

Nano SIM
4FF

MFF1
MFF2
Non-ETSI

Why Subscription Manager?



What is eSIM?

achelos

eSIM is a SIM card in any form factor (removable or embedded) enabled to securely store remotely provisioned network access credentials (profiles)

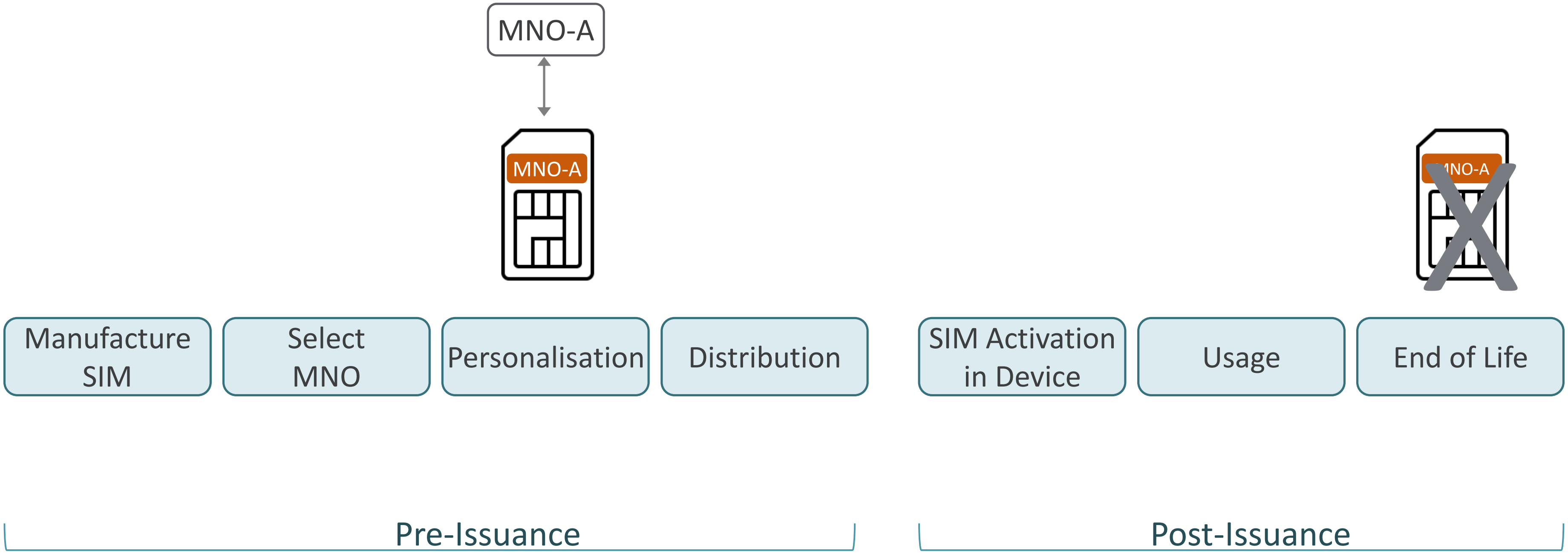
M2M and IoT devices

SGP.02: GSMA M2M Remote Provision Architecture specification v4.0

Consumer devices, mobile phones

GSMA Remote Subscription Provisioning specification v2.2

SIM Life Cycle



MNO-A

Manufacture SIM

Select MNO

Personalisation

Distribution

SIM Activation in Device

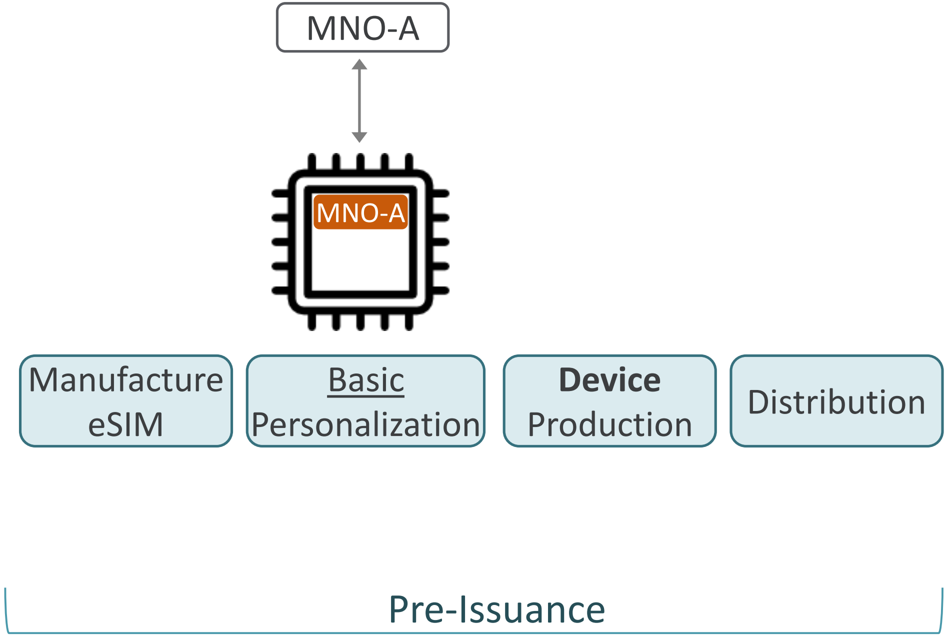
Usage

End of Life

Pre-Issuance

Post-Issuance

eSIM Life Cycle



MNO-A

MNO-A

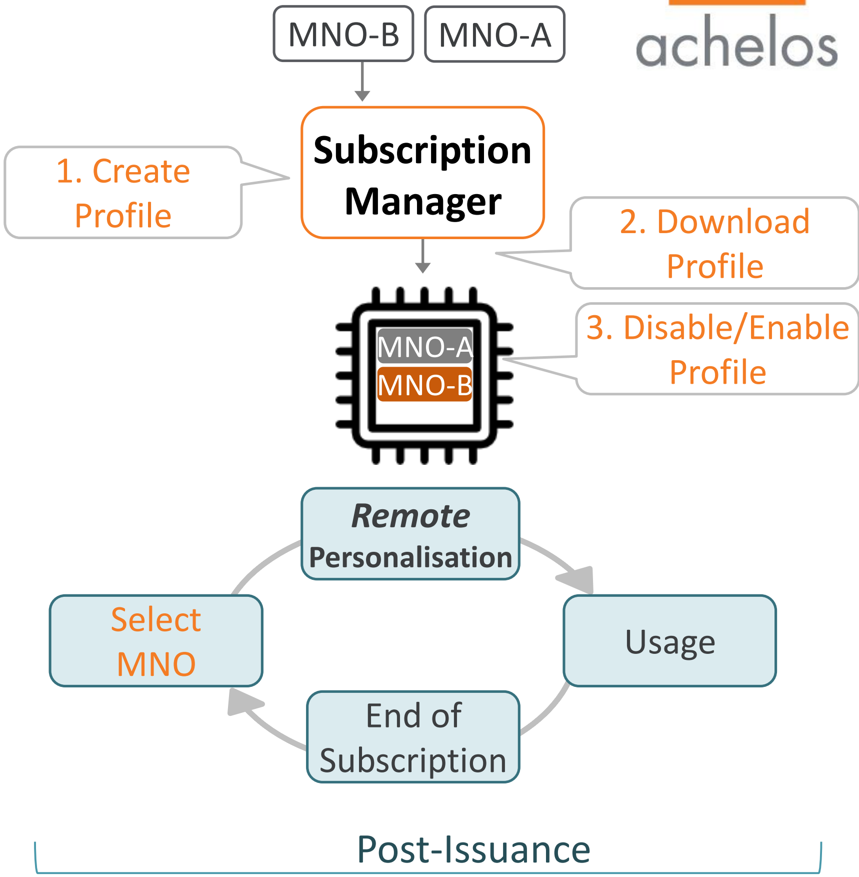
Manufacture eSIM

Basic Personalization

Device Production

Distribution

Pre-Issuance



MNO-B

MNO-A

Subscription Manager

1. Create Profile

2. Download Profile

MNO-A

MNO-B

3. Disable/Enable Profile

Remote **Personalisation**

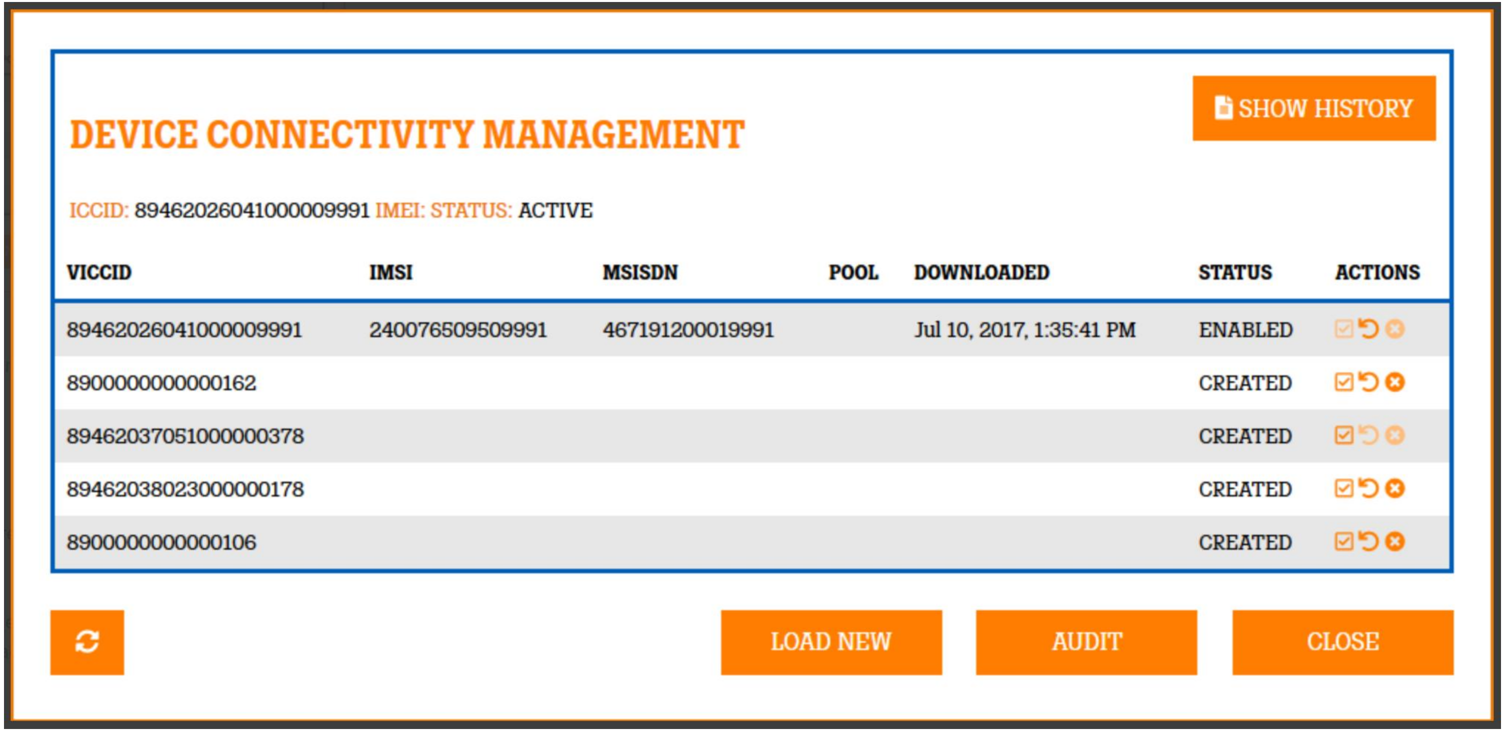
Usage

End of Subscription

Select MNO

Post-Issuance

A Real-Life Example

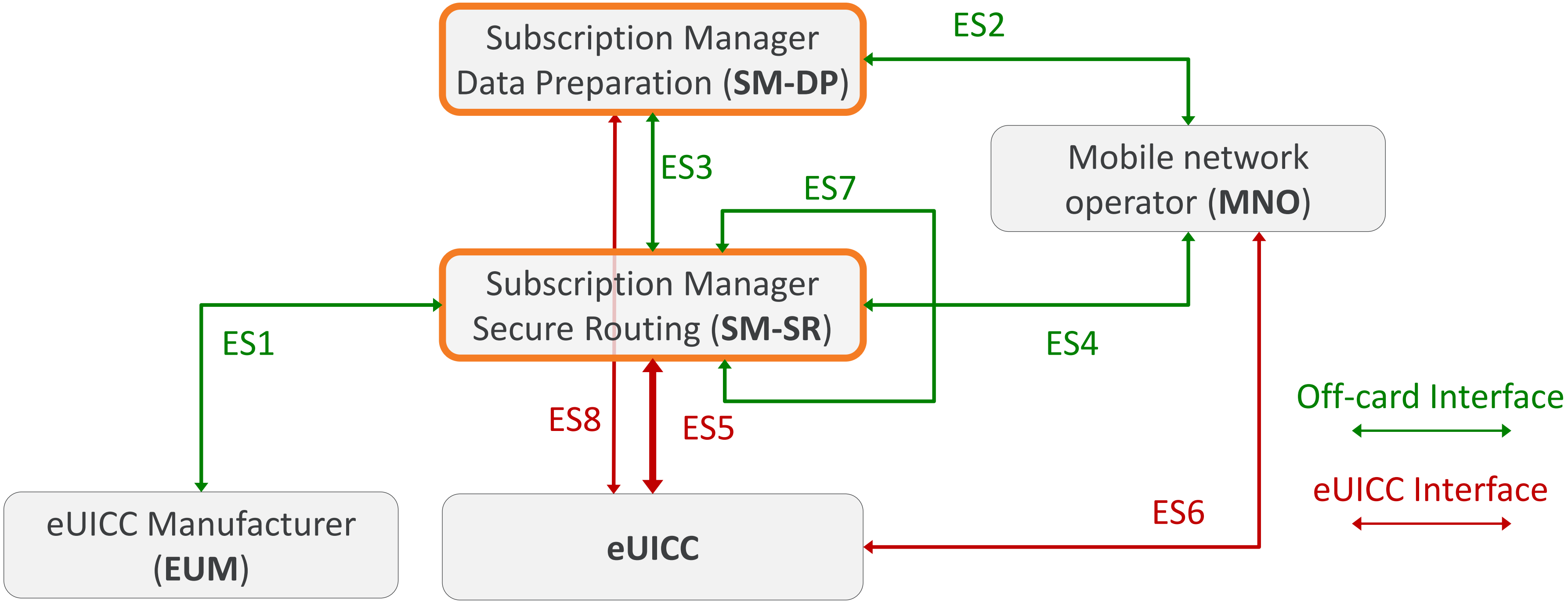


DEVICE CONNECTIVITY MANAGEMENT

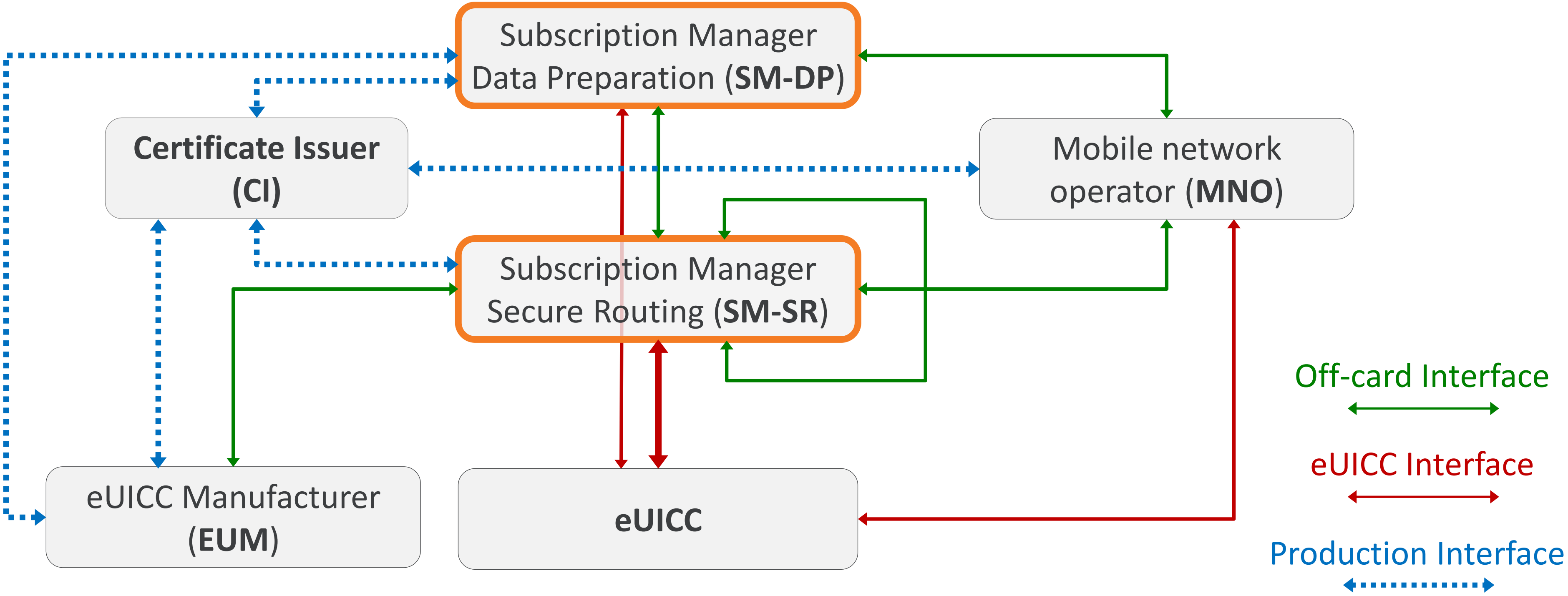
ICCID: 89462026041000009991 IMEI: STATUS: ACTIVE

VICCID	IMSI	MSISDN	POOL	DOWNLOADED	STATUS	ACTIONS
89462026041000009991	240076509509991	467191200019991		Jul 10, 2017, 1:35:41 PM	ENABLED	☑ ↺ ⊗
8900000000000162					CREATED	☑ ↺ ⊗
89462037051000000378					CREATED	☑ ↺ ⊗
89462038023000000178					CREATED	☑ ↺ ⊗
8900000000000106					CREATED	☑ ↺ ⊗

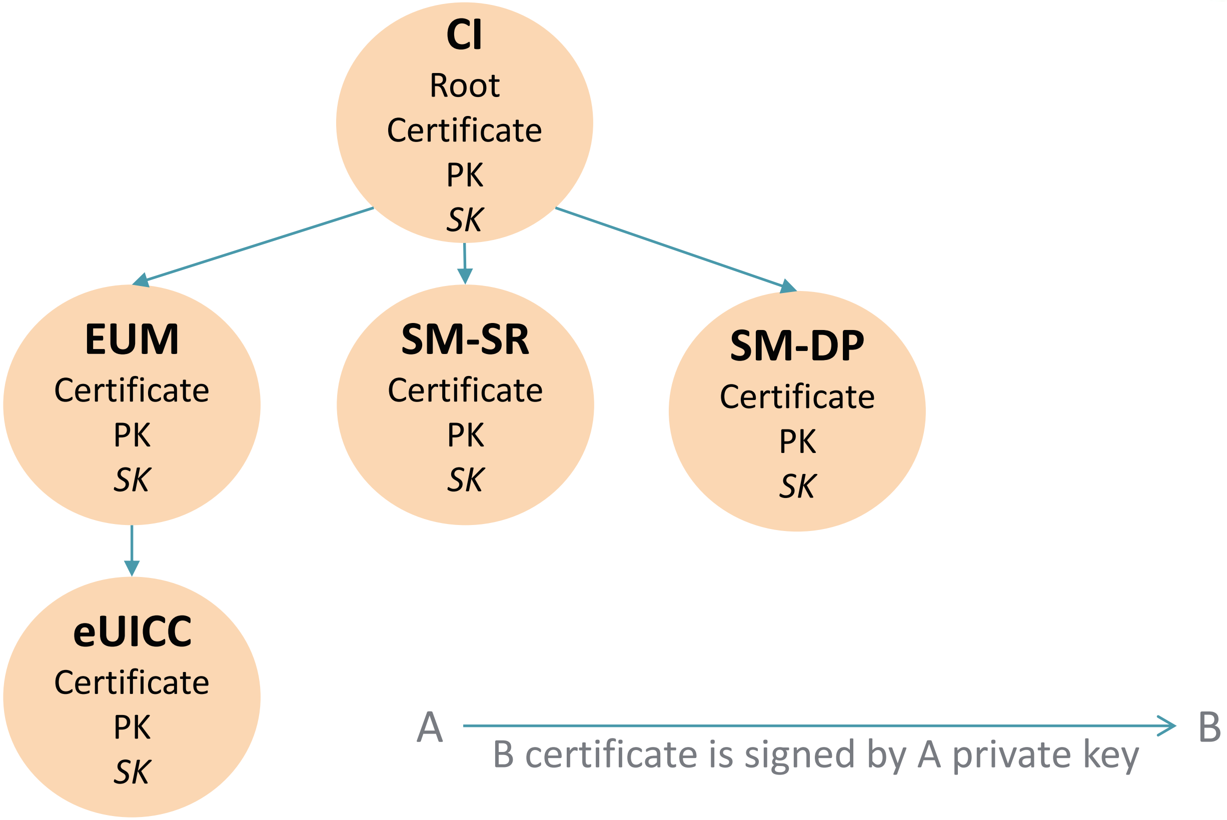
System Architecture (M2M)



System Architecture (M2M)


Subscription Manager Data Preparation (**SM-DP**)
Certificate Issuer (CI)
Mobile network operator (**MNO**)
Subscription Manager Secure Routing (**SM-SR**)
eUICC Manufacturer (**EUM**)
eUICC
Off-card Interface
eUICC Interface
Production Interface

Certification Chains (M2M)



B certificate is signed by A private key

Certificate Issuers

eSIM Root CI

digicert®

- Specification release: SGP.21 v2.x
- Contact: Email
- Website: Visit
- GSMA Root CI Certificate: Download
- CRL Distribution Point: Download

M2M Root CI

cybertrust

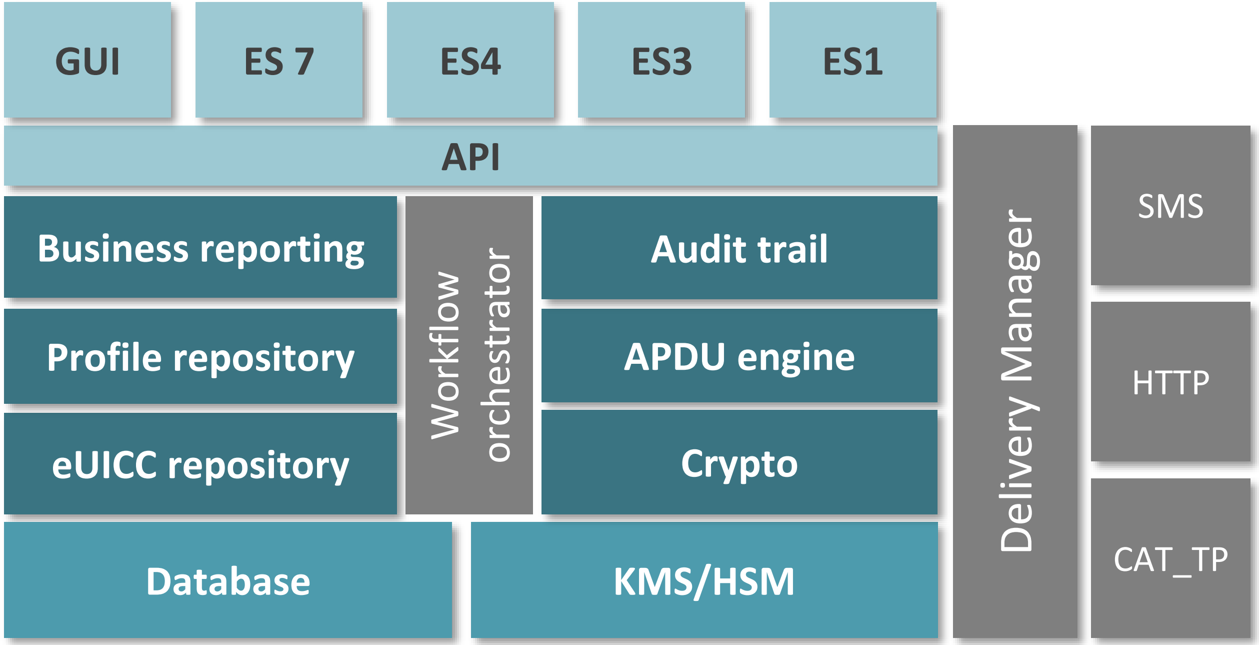
- Specification release: M2M v3.2
- Contact: Email
- Website: Visit
- GSMA Root CI Certificate: Download
- CRL Distribution Point: N/A

https://www.gsma.com/esim/ceritificateissuer/ (May 2019)

Trial Phase

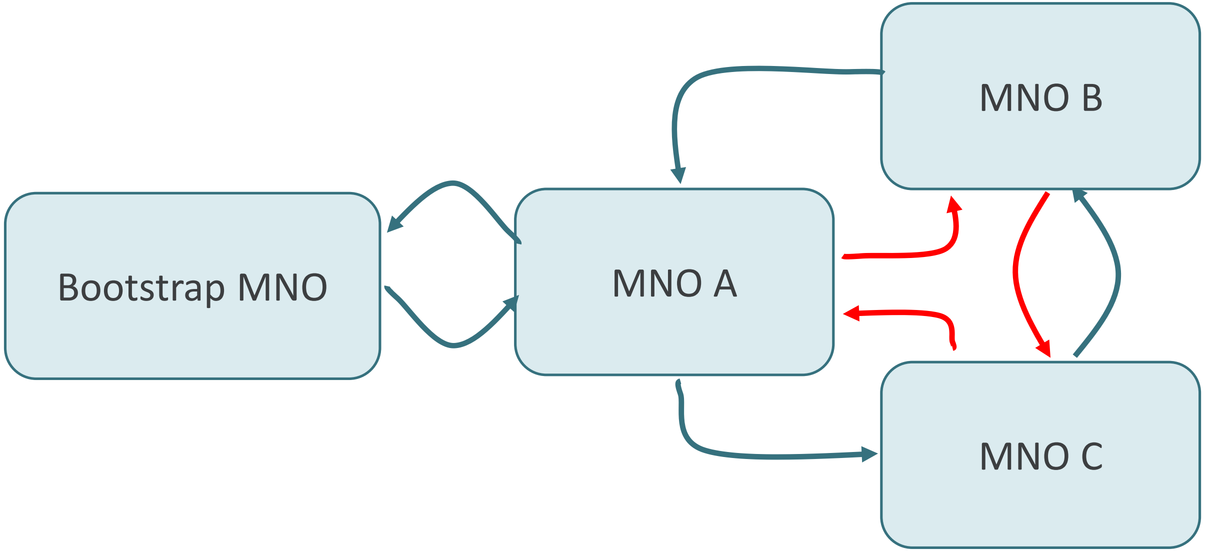
- The trial phase can be rolled out without the SAS SM certificate (self-signed infrastructure instead)
- GSMA SAS SM does not mandate the SAS certification being prerequisite for the GSMA certificate issuance
- The SAS SM certification can be applied if the trial phase has been proved successful

SM-SR high level architecture



We provide Subscription and Connectivity Management technology enabling our partners to offer the services to their customers

Connectivity Orchestration



Resume

- The eSIM has many benefits for all stakeholders
- The market for eSIM will rapidly grow with the IoT market
- Subscription Manager enables flexible and efficient handling of connectivity profiles
- Connectivity Manager enables automatic profile switches

Vielen Dank | Thank you

achelos GmbH
Vattmannstraße 1 | 33100 Paderborn | GERMANY
T +49 5251 14212-0 | info@achelos.de
achelos.de | IoT.achelos.com

security health mobility public IoT

SecurITy made in Germany
Trust Seal www.teletrust.de/itsmig