GSMA Embedded SIM for Connected Cars

C-ITS ronde tafel Security
10 mei 2016

Arjan Geluk
UL Software & Security

Arjan Geluk - bio

- Principal Advisor, Software & Security
- With UL's security business since 2003
- Participates in international standardization around identification and authentication (ISO/ ICAO)
- Authored the EU regulation for eDriver's license
- Contributed to the security framework for the next generation European Digital Tachograph system
- Advises AAMVA on secure mobile driver's license
- Advises key players in public and private sectors on the security of in-vehicle software
- Serves on the ASRB Technical Steering Committee
- Develops UL's automotive security service portfolio

PROTECTING

PEOPLE
PLACES
PRODUCTS

10,842
EMPLOYEES

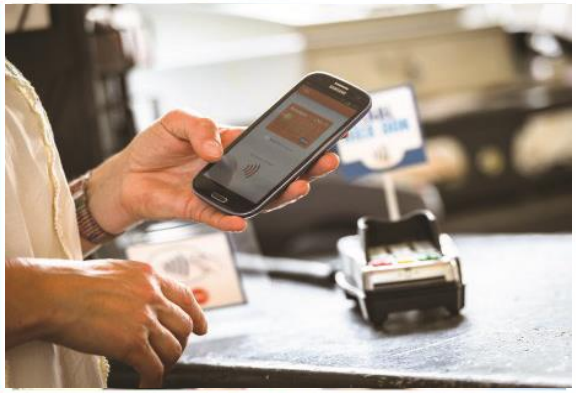
CUSTOMERS IN
113
COUNTRIES

- ✔ WORKPLACE HEALTH & SAFETY
- ✔ RESPONSIBLE SOURCING
- ✔ FIRE SAFETY
- ✔ LIFE & HEALTH SCIENCE
- ✔ TRANSACTION SECURITY

- ✔ INTEGRITY
- ✔ COLLABORATION
- ✔ COMPETITIVENESS

159
UL LABORATORY
TESTING & CERTIFICATION
FACILITIES

SECURITY



500
EXPERTS

LOCAL
EMPLOYEES IN
44
COUNTRIES

- MOBILE
- PAYMENTS
- TRANSIT
- DATA SECURITY

- INDEPENDENT
- MARKET LEADER
- GLOBAL REACH

PARTICIPATING IN
>30 INDUSTRY
ORGANIZATIONS

Newsroom
About Us
Leadership
Press Releases
Speeches & Presentations
GSMA Intelligence
GSMA Social Media
GSMA Blog
Resources
Events
Contact the GSMA
RSS Feeds

AUTOMOTIVE INDUSTRY ADOPTS GSMA EMBEDDED SIM SPECIFICATION TO ACCELERATE CONNECTED CAR MARKET

February 10, 2016 | Press Release

Press Release Archive

GSMA Blog

Use Cases for Embedded SIM

Health

- Remote Glucose Monitoring
- Assisted Living Bracelet
- Connected Ambulance
- Healthcare professional portable device

Automotive

- Emergency Services
- Infotainment
- Remote Service Management
- Fleet Management

Smart Cities

- Energy Management – demand response
- Municipal Management – waste, water, lighting, safety etc.
- Transport System Management
- Economic & Open Data projects

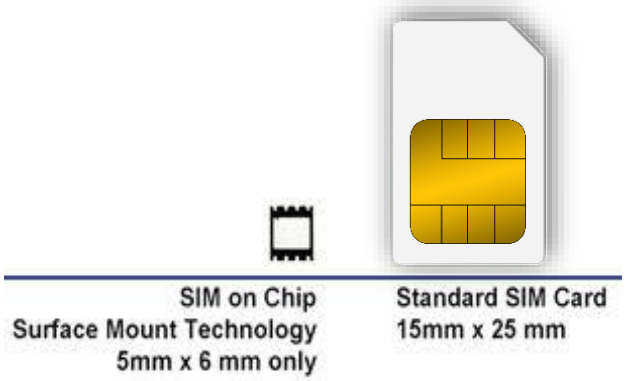
Wearables

- Health and Fitness
- Personal Medical
- Geofencing – patient care
- Child & Pet Tracking

…just the beginning!

What is Embedded SIM (eUICC)?

Embedded SIM (eUICC) is a chip soldered onto the device baseband that cannot be removed or easily accessed



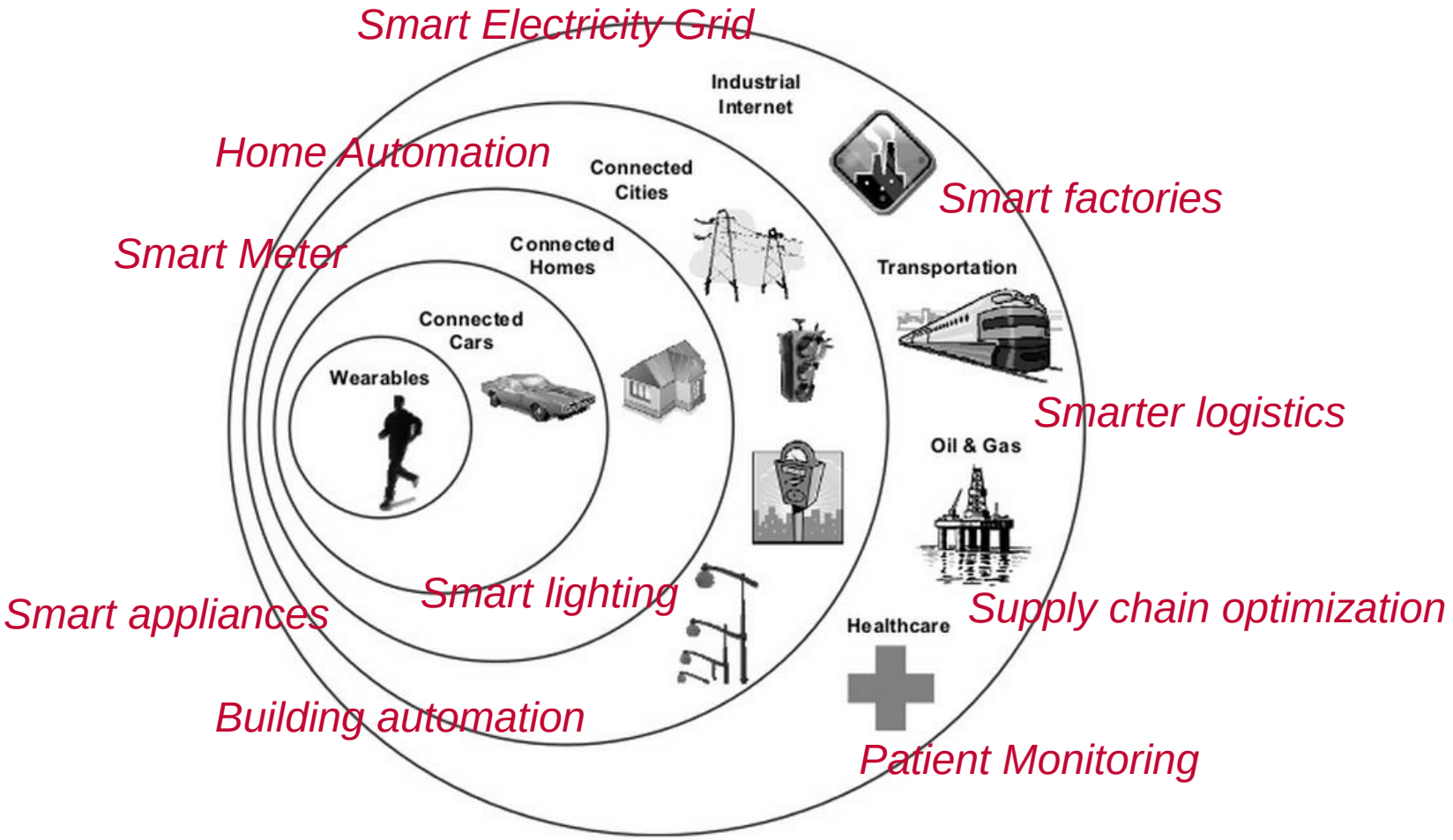
Performs most of the same functions as the traditional SIM card **with the additional ability to be remotely reprogrammed OTA with a new SIM profile on demand**

What is Embedded SIM (eUICC) – 2

- A **secure element** with a remotely managed subscription
- Eliminates the need for traditional SIM swap
- eUICC is a new business enabler for all players in the M2M/IoT ecosystem
  - New market opportunities for traditional players
    - MNO's, MVNO's
    - Card vendors, chipset vendors, handset vendors, modem vendors
  - New business opportunities for Service Providers

- Key GSMA specifications:
  - Embedded SIM specification
  - Remote SIM Provisioning (RSP) Technical specification

Smart & Connected Things



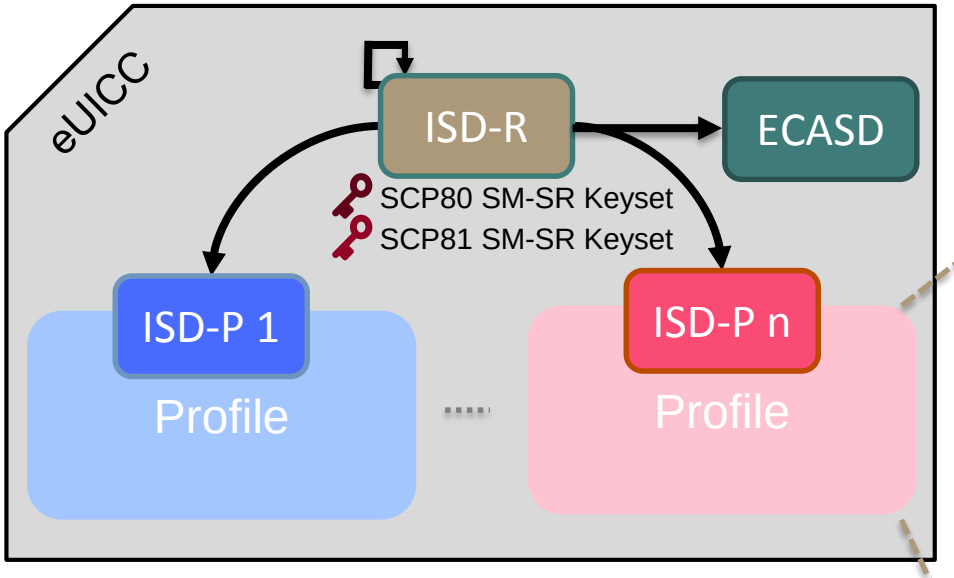
Source: Goldman Sachs

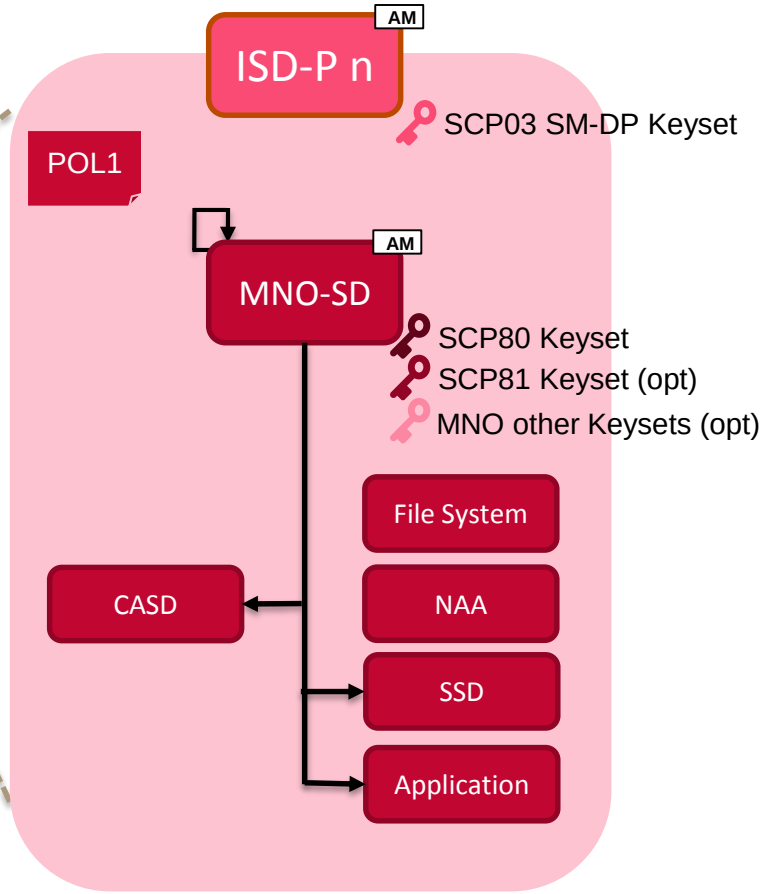
Some questions…

- Connected cars – connected street lights – connected traffic lights – …
- How do these entities communicate with each another? How do they trust each other?
- Who facilitates connectivity? Who facilitates trust?
- How and where can we store credentials securely?

- When are standards “ready enough” to go live? Can we future proof and/or remain flexible?
- Can we leverage Embedded SIM to buy time?

eUICC Architecture – A GlobalPlatform View





- Issuer Security Domain Root (ISD-R) is the representative of the off-card SM-SR
- eUICC Controlling Authority Security Domain (ECASD) is the representative of the off-card CI
- Issuer Security Domain Profile (ISD-P) is the representative of the off-card SM-DP.
  - At least one ISD-P with a profile must be installed & first personalized by the EUM at eUICC manufacturing to allow initial connectivity to the eUICC in the future
  - An eUICC can contain multiple ISD-Ps
  - The Fall-back Attribute must be set for one ISD-P

Note: The traditional sense of the GP Issuer Security Domain (ISD) does not exist

Beyond SIM – additional eUICC applications

Leverage remotely manageable eSIM in vehicles and infrastructure for other applications (future proofing)

- Authentication – mutual authentication for remote management functions
- Secure software patching/ update/ upgrade (secure storage of trust anchors for code signing verification)
- Secure storage of credentials for V2X communication

THANK YOU.

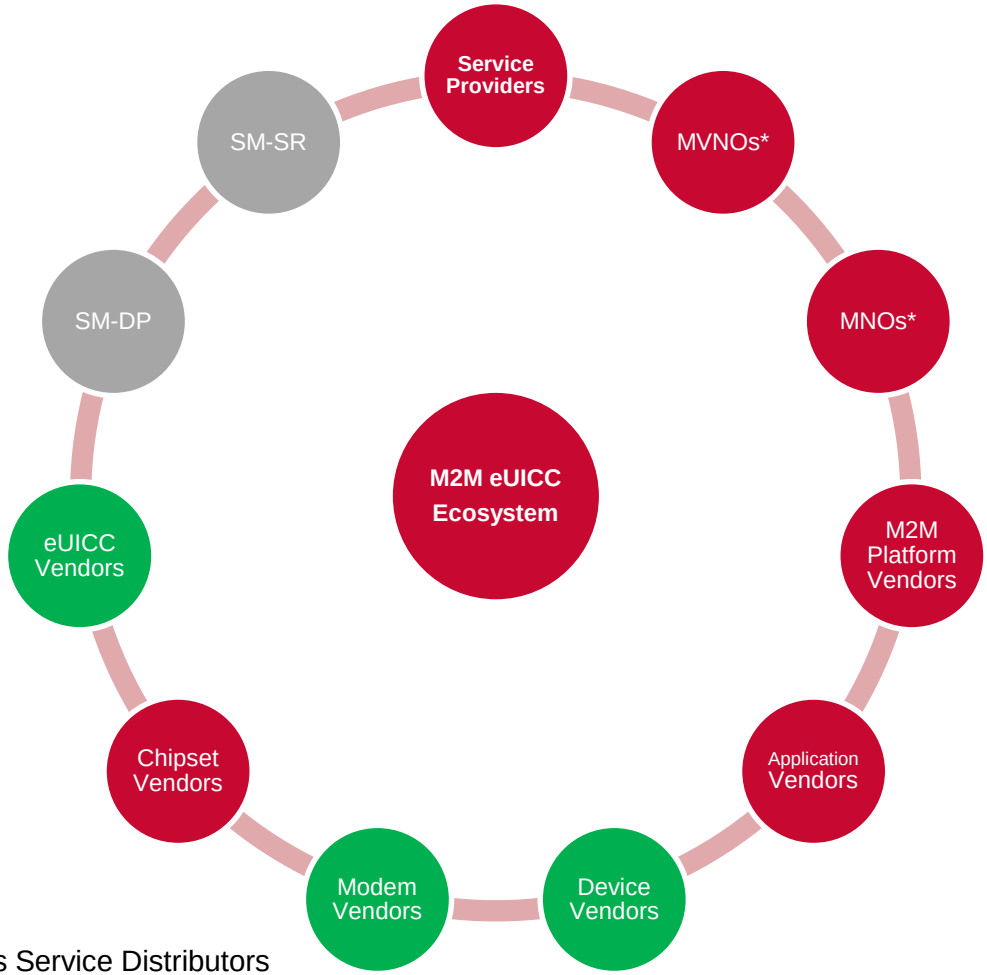
UL Software & Security
Arjan Geluk
+31 6 4476 8624
arjan.geluk@ul.com

Appendix

eUICC ecosystem, key roles, architecture & deployment

Key Roles

- Existing legacy SIM role is replaced by new eUICC role
- New Subscription Manager (SM) roles
- Modem and handset vendors play more of a central role



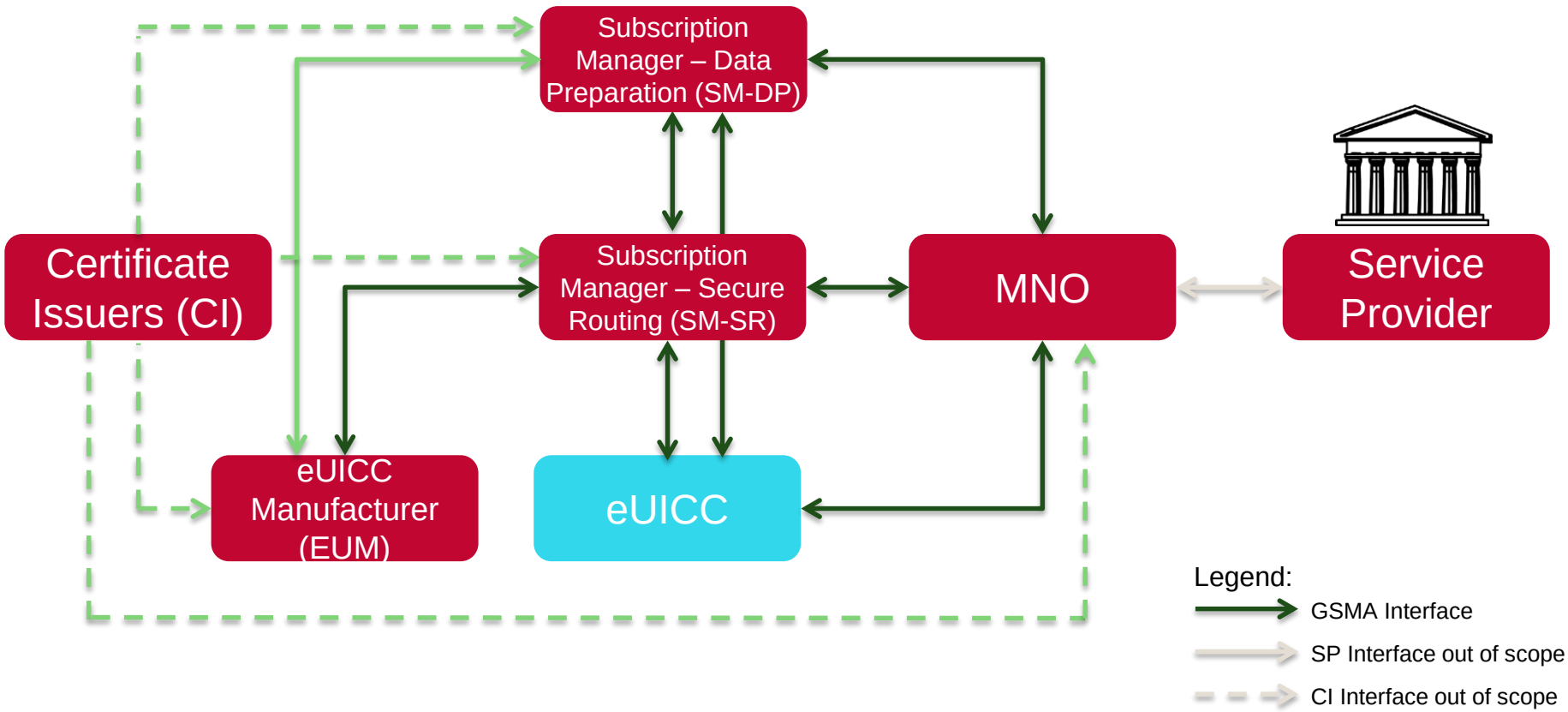
Key:
- Existing
- Changed
- New

*ETSI view MNOs as Service Distributors

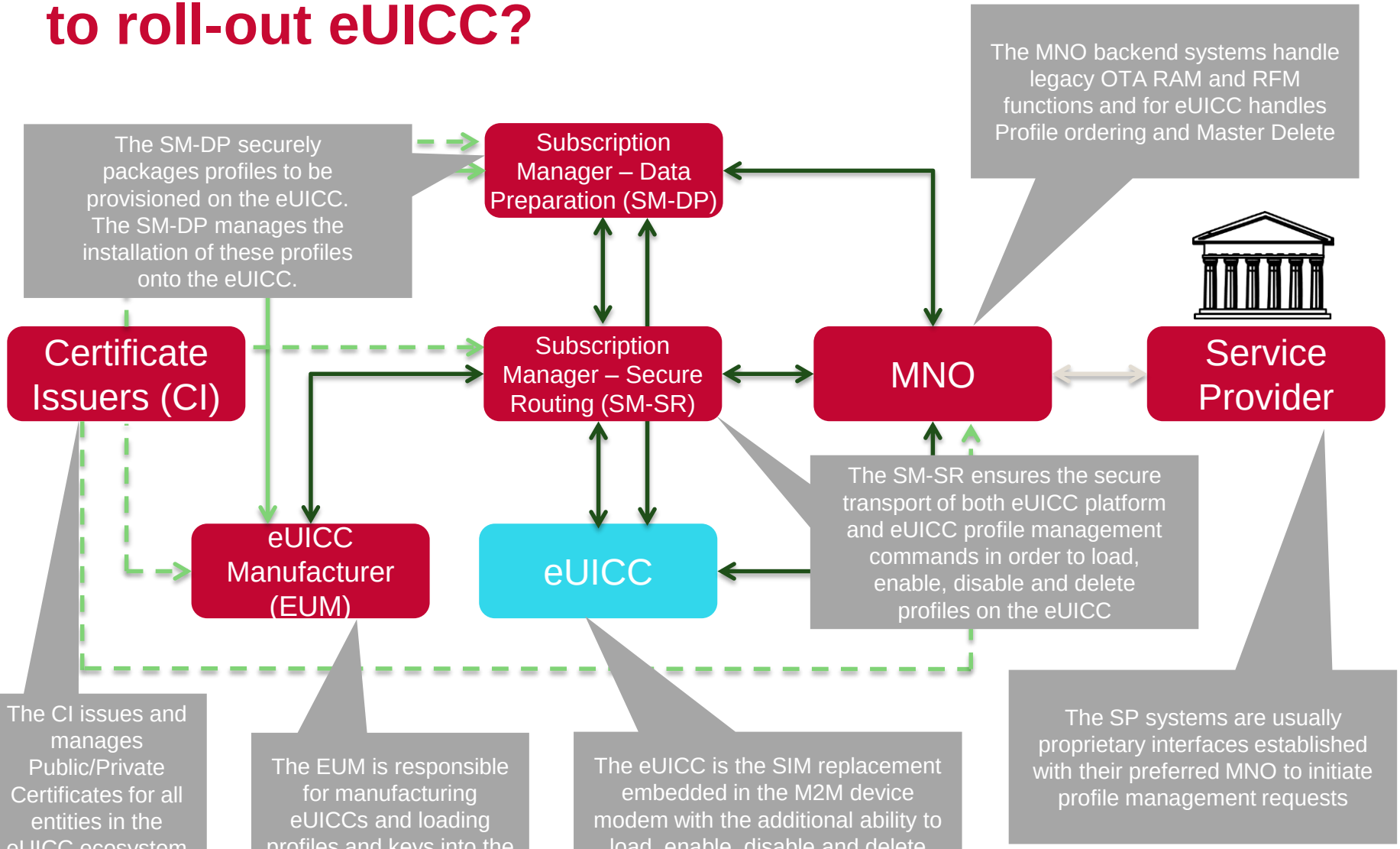
Elements Involved

Embedded SIM (eUICC)	• Functionally identical to a traditional SIM • At manufacture a ‘provisioning profile’ assigned with secret keys allowing the associated subscription manager to download & manage ‘operational profiles’ on the eUICC • Technically an initial MNO profile in the eUICC, as well as the selection of a new MNO later is possible but the implementation will depend on the commercial agreement between MNO & SP
Subscription Manager	• Manages the eUICC by; - Generating SIM profiles in real-time - Management and execution of MNO policy - Secure routing profiles to the eUICC
M(V)NO	• Uses subscription manager to manage profiles • Maximum re-use of existing provisioning interfaces and processes
Service Provider	• Signs up with initially chosen MNO or direct with EUM

General architecture: what is required to roll-out eUICC?

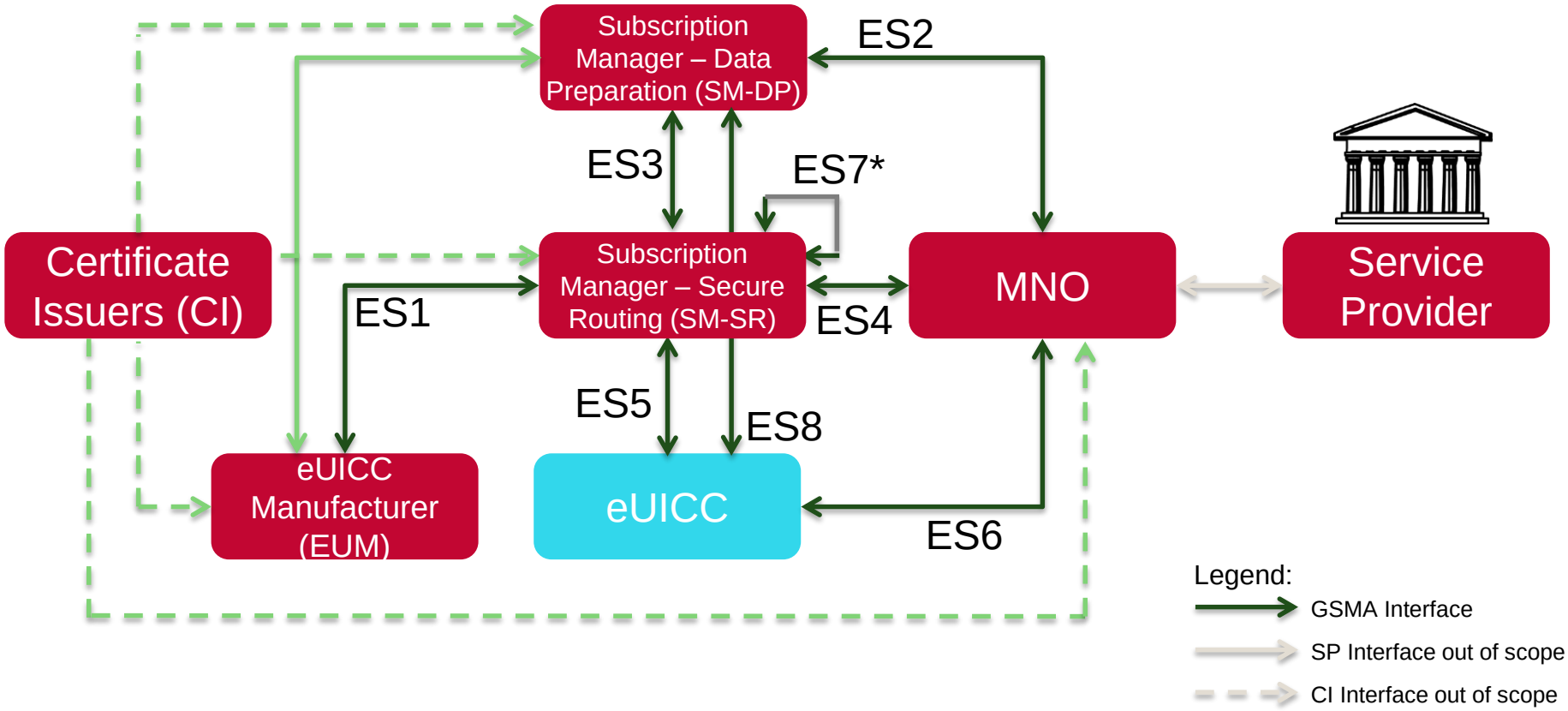


Overall system architecture: what is required to roll-out eUICC?



Interoperability

- GSMA specifications identify the following interfaces to guarantee interoperability



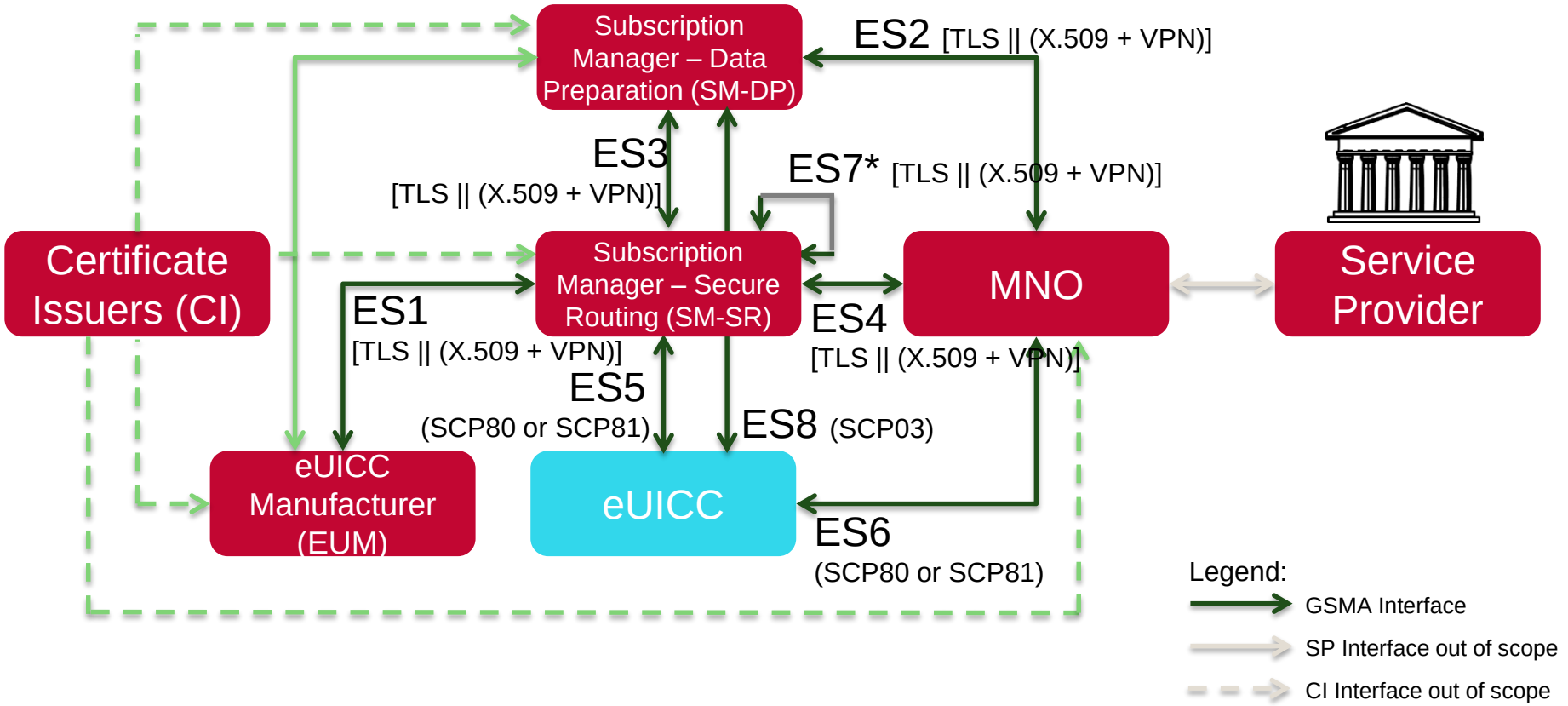
* Note: The ES7 SM-SR - SM-SR interface is between different MNOs

Interoperability

Security

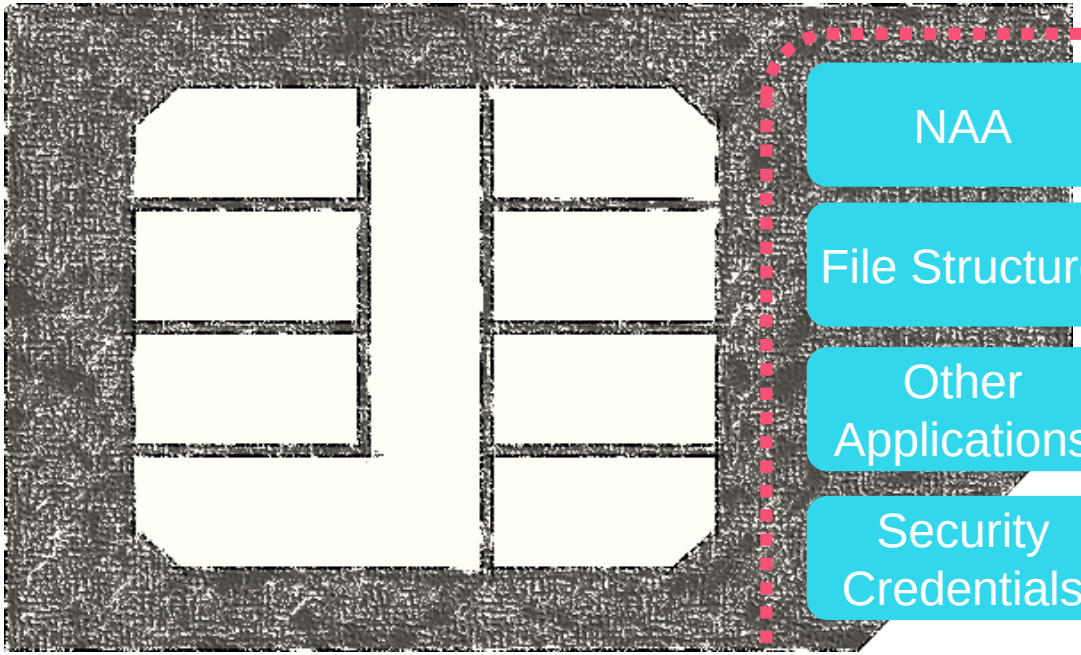
Interoperability & Security

- The security applied on these interfaces is via:
  - TLS 1.2 or X.509 Certificates and VPN for off-eUICC activity, or
  - Global Platform Secure Channel Protocol (SCP) for on-eUICC activity



* Note: The ES7 SM-SR - SM-SR interface is between different MNOs

GSMA Embedded SIM Profile & SIM Subscription



NAA

File Structure

Other Applications

Security Credentials

Today's SIM cards contain different types of data, collectively called a **SIM Profile**

Network Access Application (NAA) Is everything required to allow the SIM to register onto the MNOs network. This includes home network, tower frequencies, location data, authentication algorithms keys & IMSI. All of this is referred to as a **SIM Subscription**

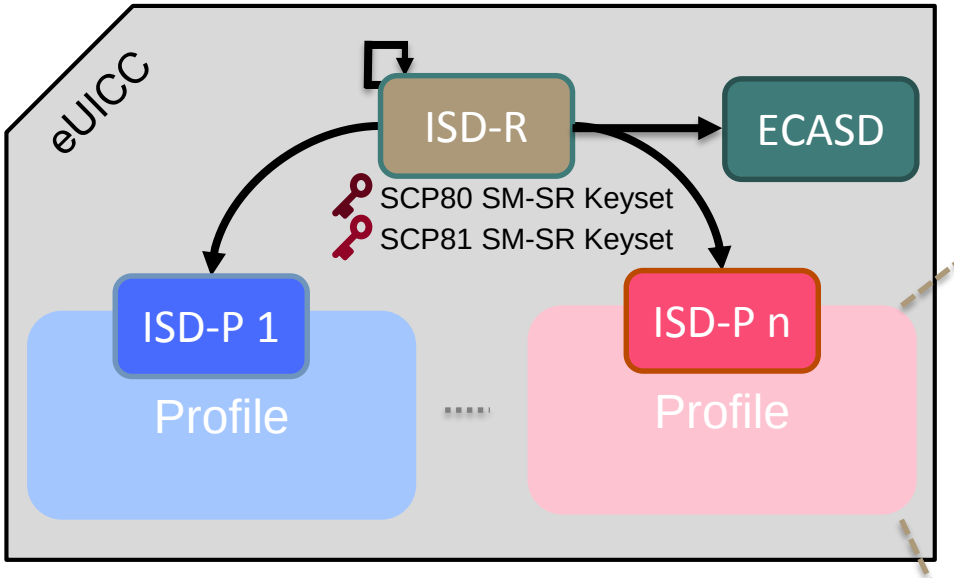
Just like a PC the SIM has a file structure, with each file having a specific purpose.

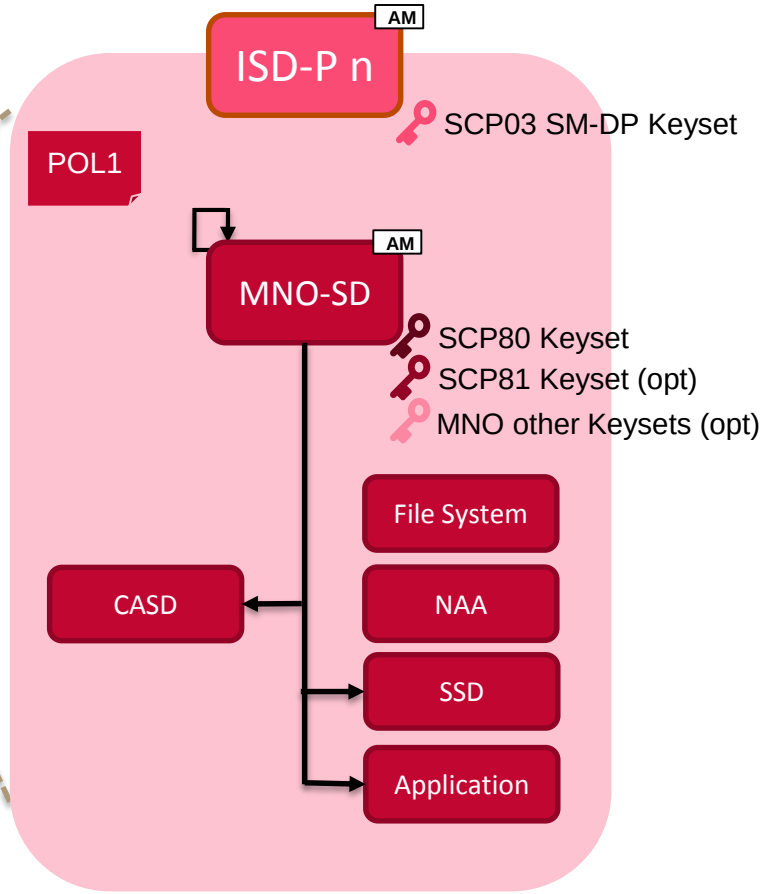
The SIM typically contains a number of other applications, each providing some kind of value-added service e.g. Call Control or mCommerce etc.

The SIM may have a wide range of secret keys, algorithms, certificates and other cryptographic data

- Provisioning Profile is the initial profile that manage Operational Profiles
- Operational Profile is used as the initial Provisioning Profile

eUICC Architecture – A GlobalPlatform View

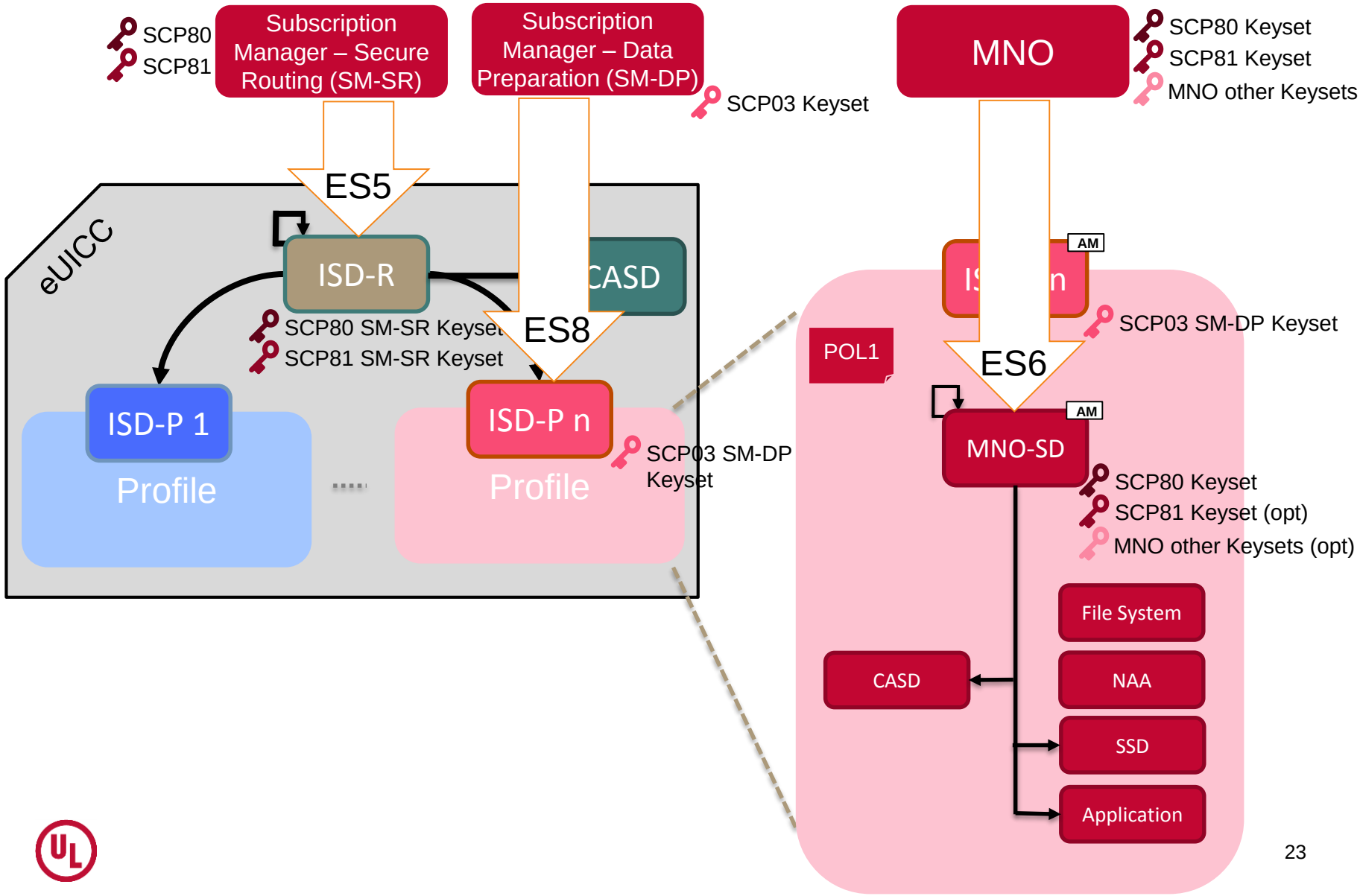




- Issuer Security Domain Root (ISD-R) is the representative of the off-card SM-SR
- eUICC Controlling Authority Security Domain (ECASD) is the representative of the off-card CI
- Issuer Security Domain Profile (ISD-P) is the representative of the off-card SM-DP.
  - At least one ISD-P with a profile must be installed & first personalized by the EUM at eUICC manufacturing to allow initial connectivity to the eUICC in the future
  - An eUICC can contain multiple ISD-Ps
  - The Fall-back Attribute must be set for one ISD-P

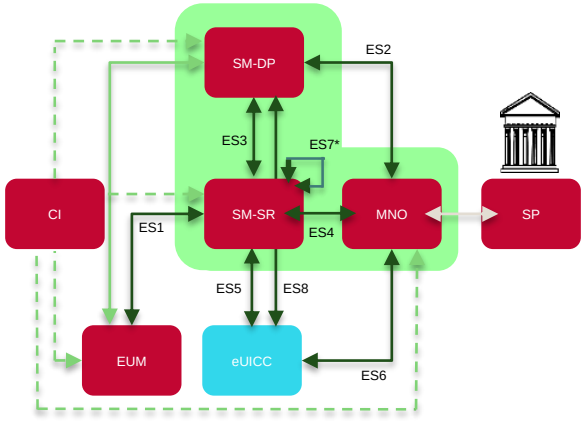
Note: The traditional sense of the GP Issuer Security Domain (ISD) does not exist

SM to eUICC Architecture

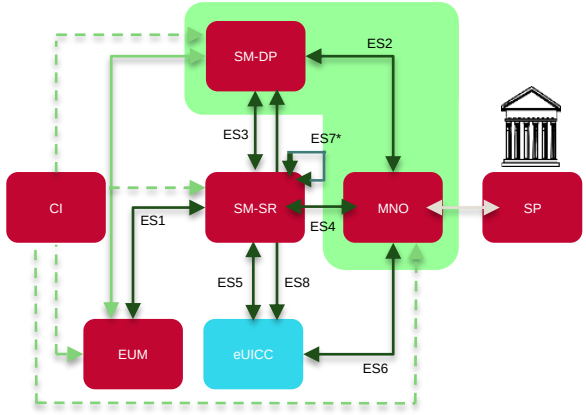


SM Deployment Architecture Options

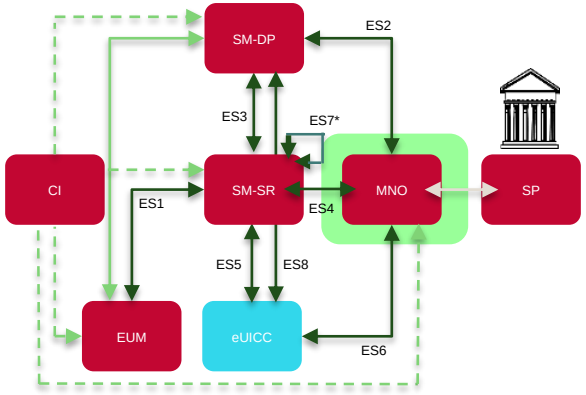
1. M(V)NO Owns SM-DP & SM-SR



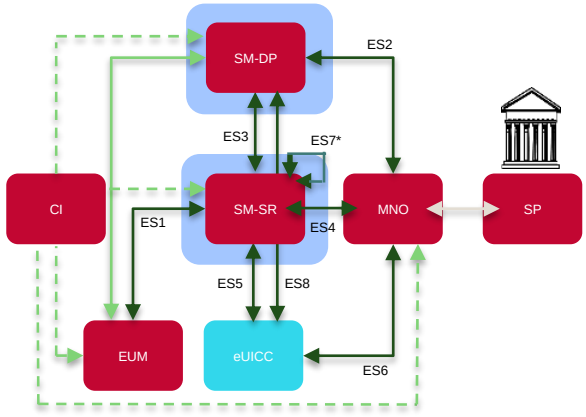
2. M(V)NO Owns SM-DP



3. M(V)NO Owns no SMs



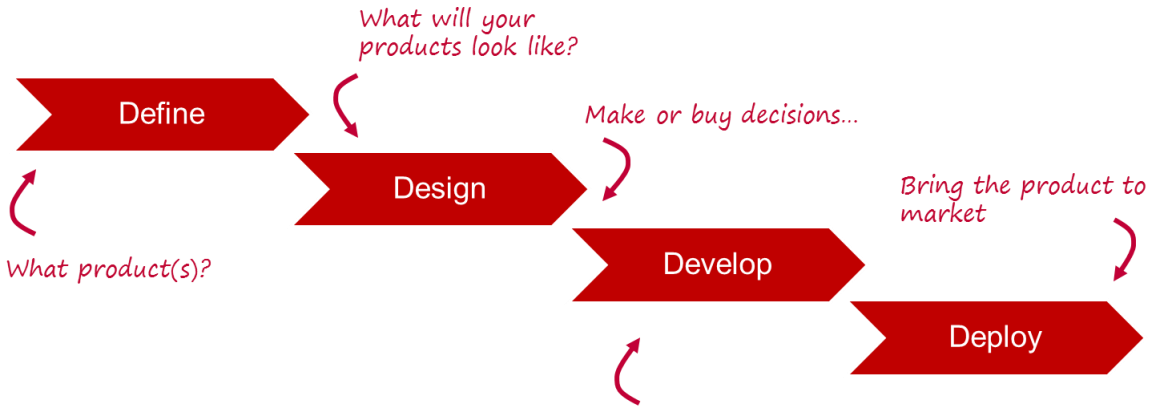
4. Third Party SM-SR and/or SM-DP



- What is the business use case and ROI per option?

UL support

UL advisory services to support your implementation project



UL can support , building on a strong and relevant knowledge base

- Remote management of secure applications via TSM & SM
- Mobile authentication mechanisms, MNO-centric (SIM-based applets, and network authentication) as well as non-MNO-centric
- mPKI

References

- Extensive experience in projects where Mobile Authentication is central
  - Many mobile payments projects (KPN, Softcard, Vodafone, Valyou, Swisscom, ING, etc)
  - TRA – smart Government, providing consultancy for and managing the implementation of the National TSM
  - Banco Itaú – advisor for mobile wallet implementation, where Mobile authentication is a crucial element

- Hands-on experience with Mobile authentication in the MNO domain, e.g.
  - KPN eCommerce and SCP81 RAM over HTTP
  - VALYOU SCP81 RAM over HTTP
  - Softcard (AT&T, T-Mobile & Verizon) 4G IMS Authentication
  - Softcard SCP80 push SMS
  - Softcard SCP81 RAM over HTTP
  - Orange Switzerland 3G Milenage Authentication
  - Telia Sonera SMS Secured Data for RAM & RFM OTA services

THANK YOU.

UL Software & Security
Arjan Geluk
+31 6 4476 8624
arjan.geluk@ul.com