Attacks against GSMA's M2M Remote Provisioning

Maxime Meyer[1] Elizabeth A. Quaglia[2] Ben Smyth[3]

Vade Secure Inc, France

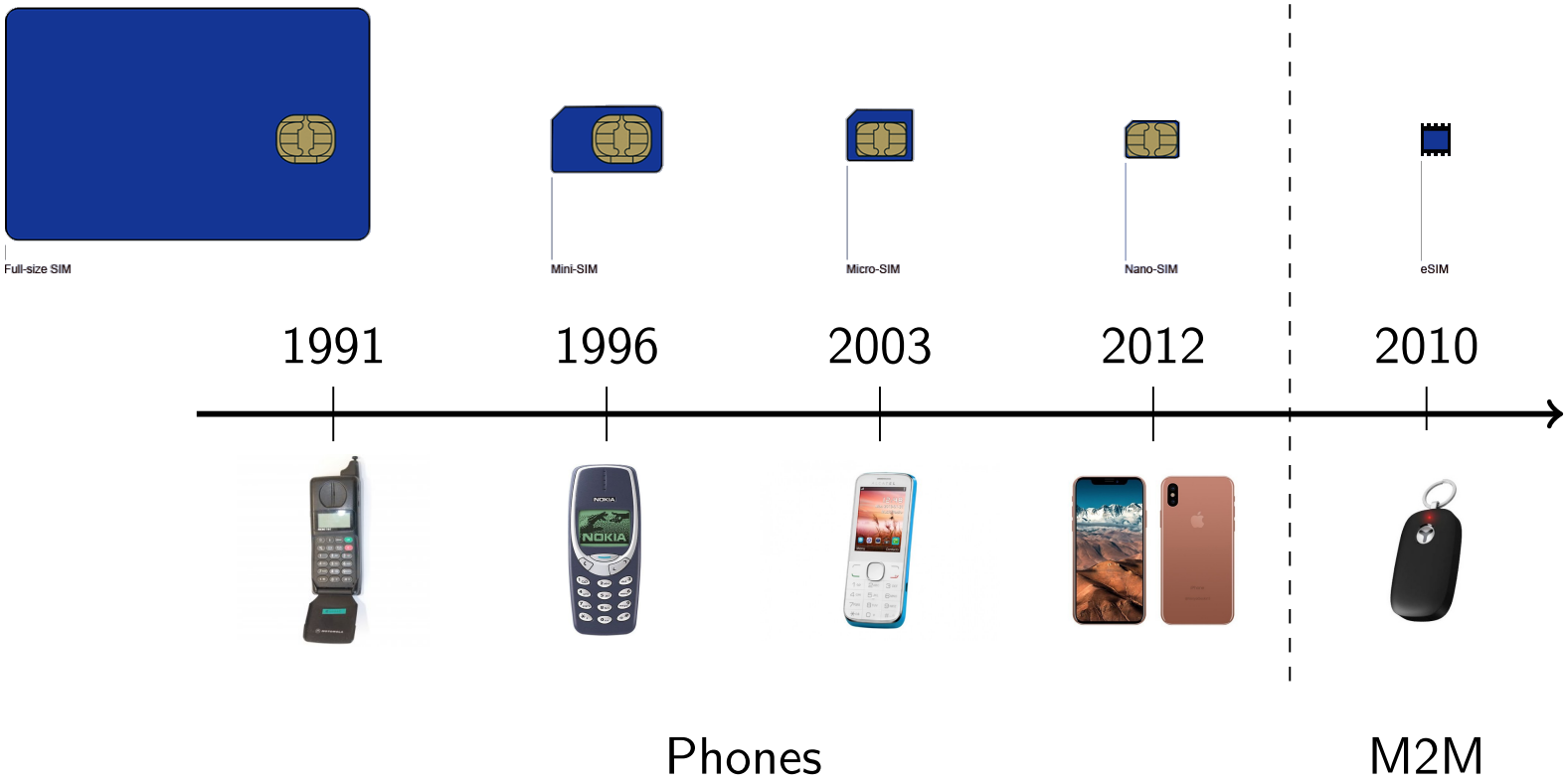
Information Security Group - Royal Holloway, University of London, UK

Interdisciplinary Centre for Security, Reliability and Trust, University of Luxembourg, Luxembourg

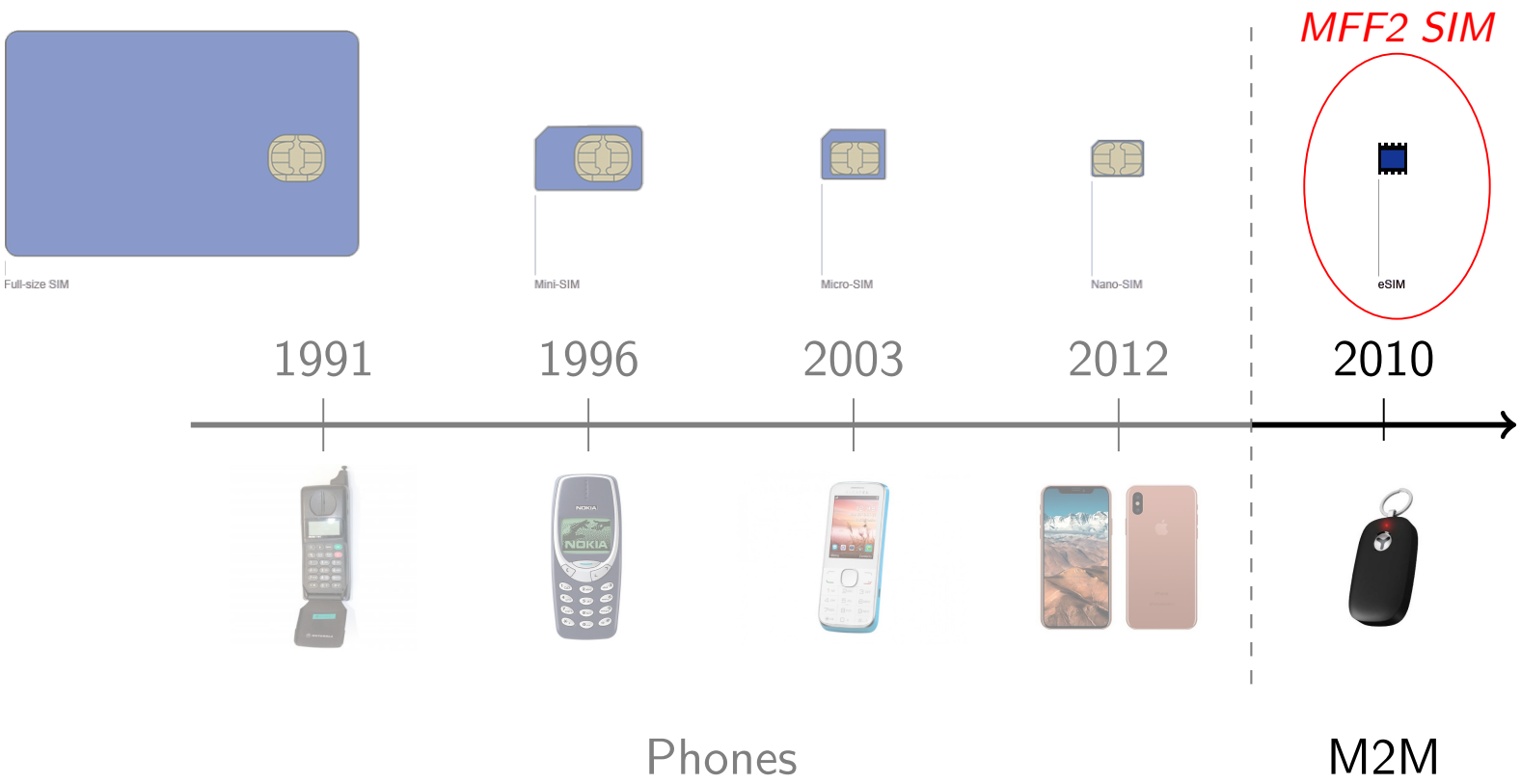
6th December, 2017


black hat®
EUROPE 2017
DECEMBER 4–7, 2017
EXCEL / LONDON, UK
#BHEU / @BLACK HAT EVENTS

Evolution of SIMs

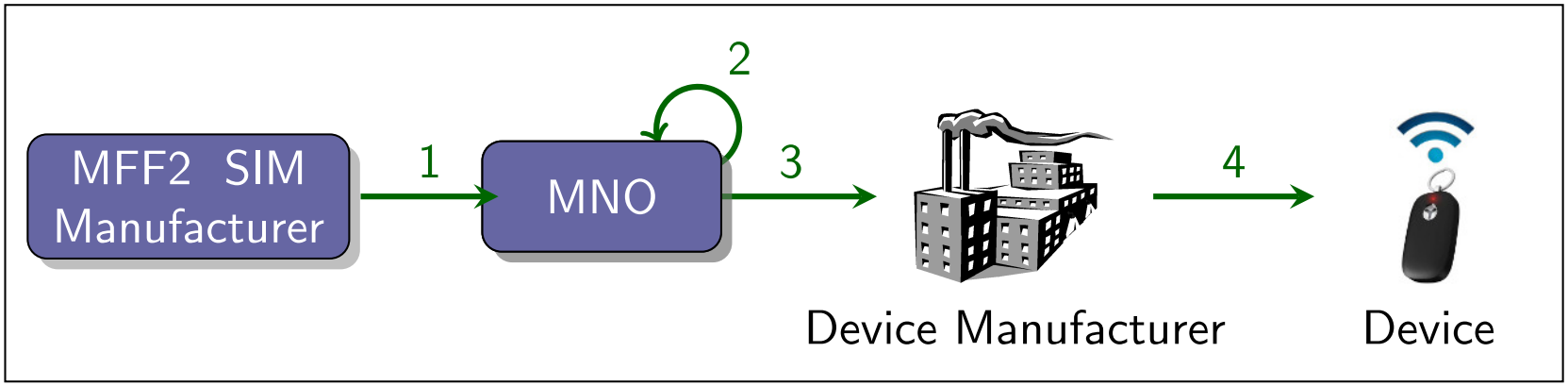


Evolution of SIMs



Distribution and provisioning of SIMs

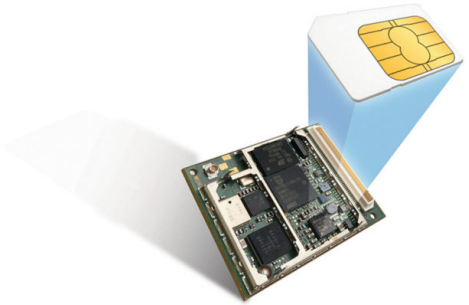
MNO : Mobile Network Operator



M2M SIMs suffer from shortcomings

Shortcomings:

- Physical installation of subscription data by operators.
- Single subscription data support by a SIM over its lifetime.
- SIMs change when buried deep inside devices.



Next generation SIMs

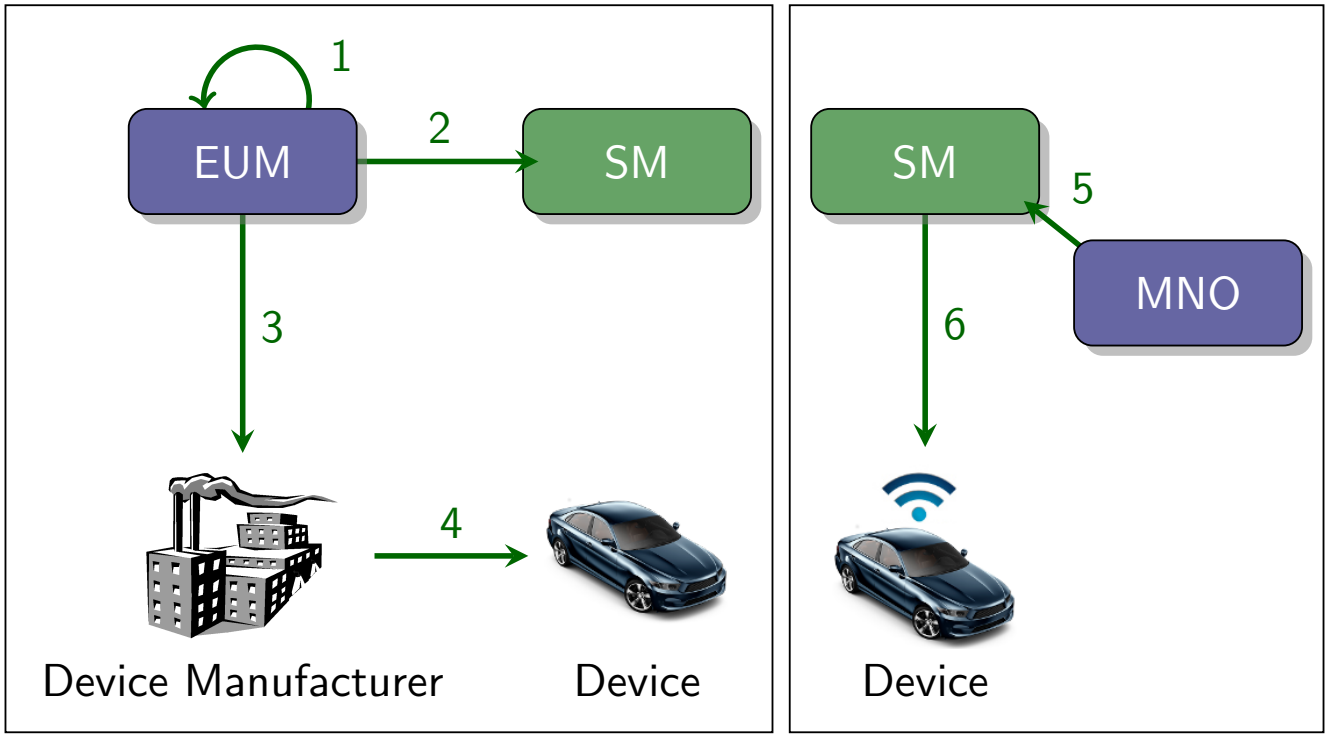
ETSI
(TS 103 383) *Smart Cards _ Embedded UICC Requirement Specification*

GSMA
(SGP 02) *Remote Provisioning Architecture for Embedded UICC*

Distribution and provisioning of eUICCs

EUM : eUICC Manufacturer

SM : Subscription Manager



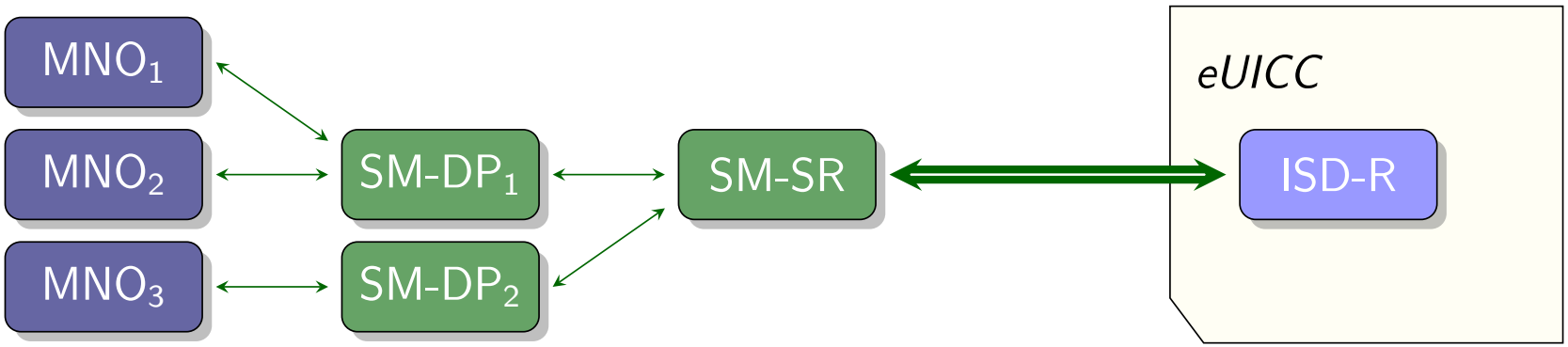
(a) Distribution chain

(b) subscription model

Subscription Manager: new entity roles

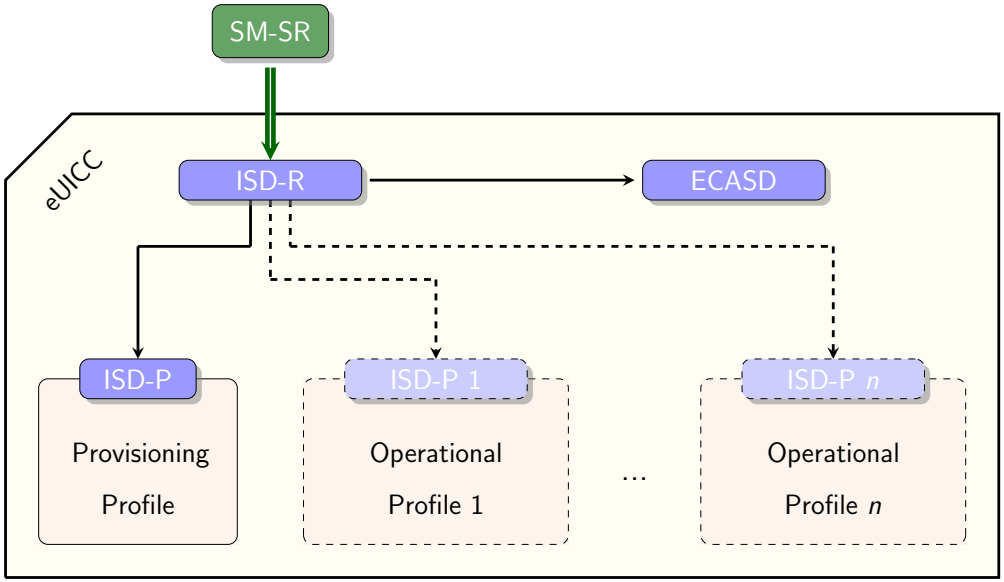
Duties split between two sub-entities

- **Data Preparation**: Generates profiles for operators, and transfers them to eUICCs.
- **Secure Routing**: Remotely manages eUICCs, and secure communication with them. eUICCs are associated to a single SM-SR which holds data in the **EIS** file about them.



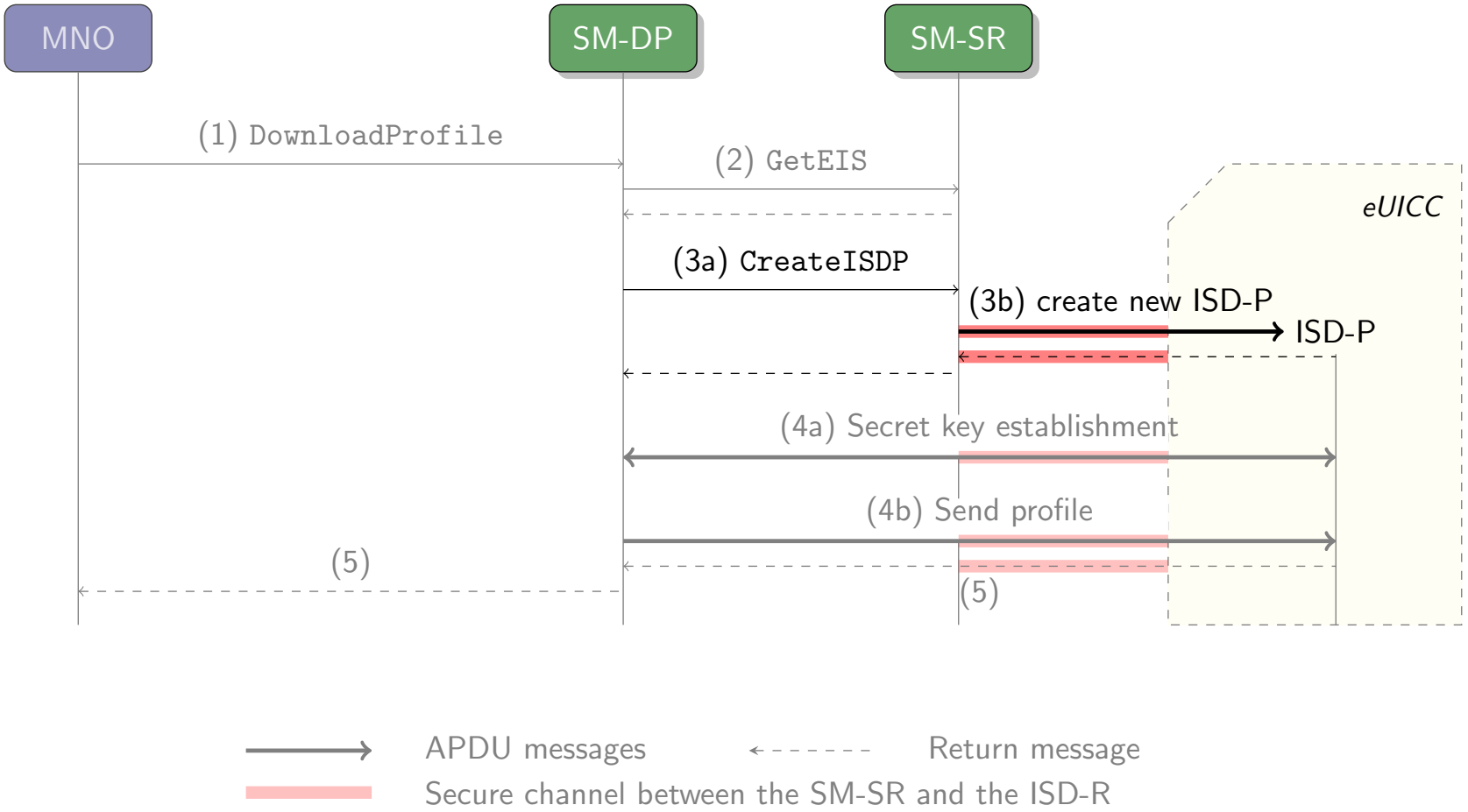
eUICC architecture

ISD-R : SM-SR representative
ISD-P : Profile Container
ECASD : Key Vault

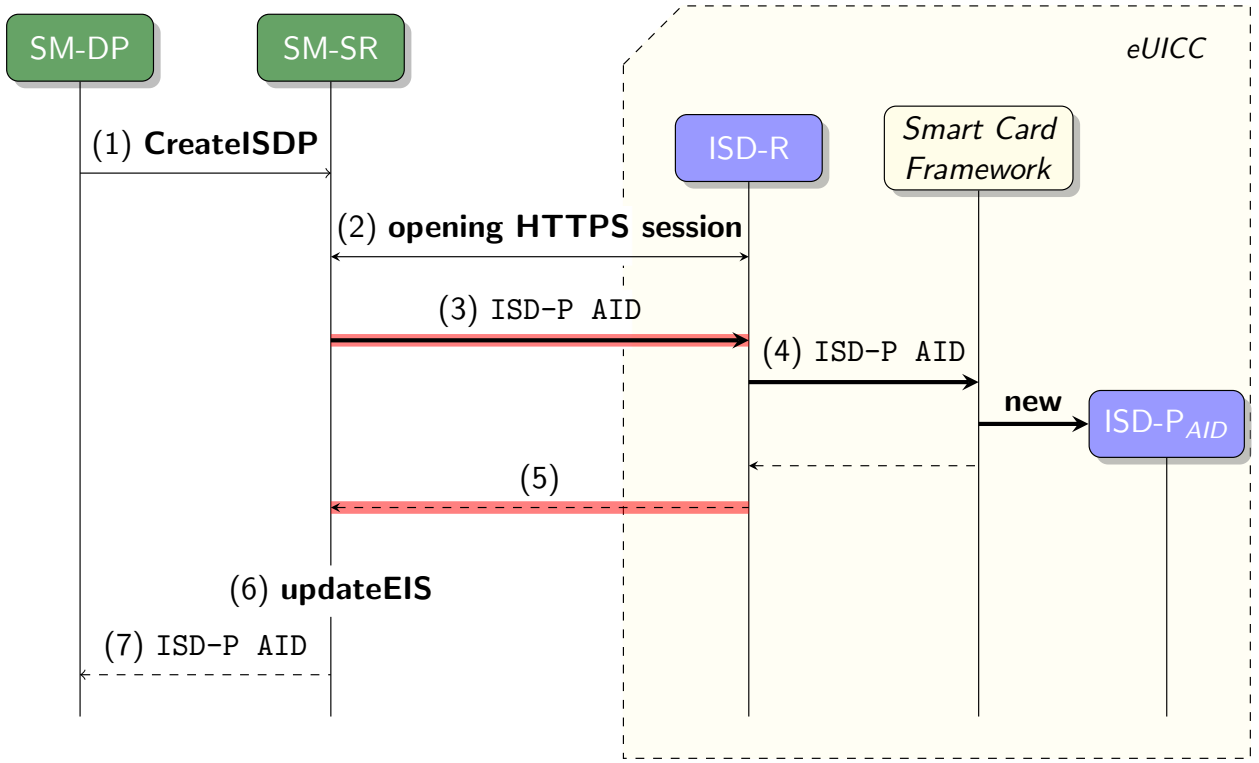


- Architecture relies on GlobalPlatform smart card standard.
- Shipped with a **Provisioning Profile** to enable remote Provisioning.
- Is provisioned with **Operational Profiles** each containing an operator's subscription data.

Profile download and installation flow



ISD-P creation flow



Error handling during ISD-P creation

GSMA error handling during ISD-P creation

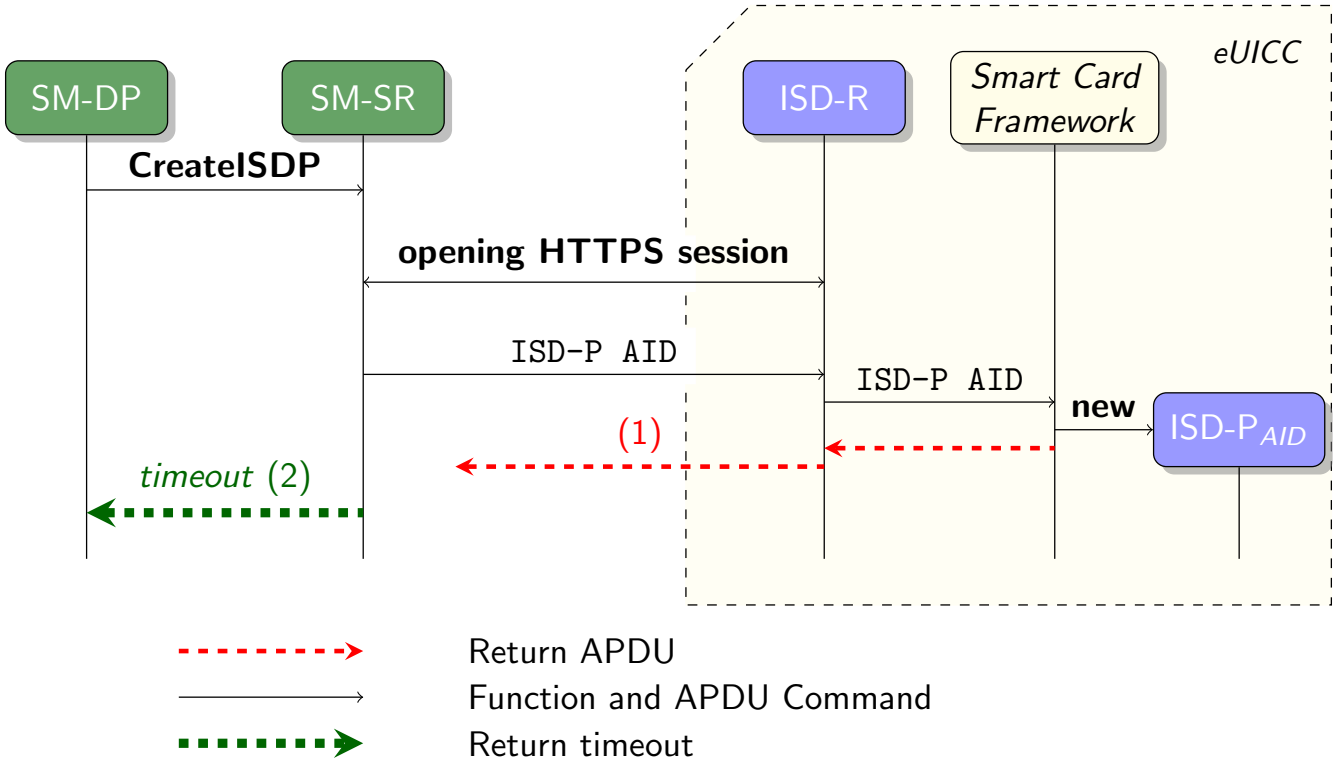
Error handling is limited to timeouts, i.e., response messages sent back when the response message from the eUICC is not received in time by the SM-SR.

GSMA error handling once ISD-P is created

Specific error handling process.

- The SM-DP initiates the process by requesting the SM-SR to delete the ISD-P and relevant data onto the eUICC using ISD-P AID.
- The SM-SR manages the eUICC to delete the ISD-P.

Timeout resulting from lost message



Flaw based on deletion mechanism

Results of the timeout

- ISD-P creation status is unknown for the SM-SR.
- ISD-P is neither associated to an SM-DP nor to an MNO.
- Memory space has been reserved for the profile on the eUICC.

Deletion mechanism

- SM-SR cannot delete ISD-P.
- Only MNO or SM-DP can initiate deletion of ISD-P given that they know the AID of that ISD-P.

Network adversary (i.e., MITM) attack

→ Drop the return message.

Attack motivation and rewards

Attack characteristics

- Recovery is not possible.
- Attack trace is minimal.
- Causes financial loss to operators.

Potential attacker

- Lonely hacker trying to disrupt service.
- A adversarial SM-SR or a competitive operator.
- A business competitor

Fixing GSMA's specification

Possible fix ideas:

- Setup a retry mechanism before the timeout.
  This will result in a failure message as there is already an ISD-P with the same AID on the eUICC.
- Authorize deletion by SM-SR.
  This rely on a trust assumption (not the best idea) and deletion message could be dropped by adversary.

Recommended fix:

Create an eUICC internal mechanism to manage ISD-P creation.
The mechanism could be an extension of the GlobalPlatform smart card framework.

Other attacks against the specification

Attack relying on trust assumptions between network entities.

- Undersizing memory attack by SM-SR.
  During profile creation, the SM-SR can deceive the SM-DP into thinking that the eUICC has no remaining memory left for another profile.
- Inflated profile attack by network operators.
  Operators or SM-DPs can easily fill the memory of an eUICC with *big enough* profiles.

Attack relying on lock functionality.

Locking profile attacks is made possible for an attacker if the eUICC is not locked to a profile.
If the eUICC is locked to a profile, the operator owning the profile can abuse the lock functionality.

Notifying GSMA

- We notified GSMA's CVD Programme
- We also notified GSMA's eSIM working group
- GSMA acknowledge all the attacks present in the paper
- GSMA ESIMWI4 is working on a countermeasure (latest SGP02 version 3.2 contains a fix to some of our attacks)

Response

We would like to confirm that our remote SIM provisioning experts have acknowledged the existence of the four attacks and confirmed the vulnerabilities have the ability to impact the mobile industry and its customers.

Black Hat Sound Bytes

Takeaways

- An understanding of next generation SIMs and networking technology.
- An understanding of our attacks and of the importance of attacks against specifications at an early stage.
- An overview of GSMA vulnerabity disclosure process and an insight to next specifications.

What to do:

- Companies: Release public specifications as early as possible. Invest into standard verification for standards used in your products.
- Hackers: Do not only focus on products or websites, also hack specification as they affect all products based on them.

Closing remarks

Thanks for listening!

Maxime Meyer[1] Elizabeth A. Quaglia[2] Ben Smyth[3]

Vade Secure Inc, France
http://maximemeyer.com/

Information Security Group - Royal Holloway, University of London, UK
https://lizquaglia.wordpress.com/

Interdisciplinary Centre for Security, Reliability and Trust, University of Luxembourg, Luxembourg
https://bensmyth.com/