Virtualizing Secure Elements

Java Card Forum

Karl Eglof HARTEL
15 Dec 2021

Giesecke+Devrient
Creating Confidence

Server Virtualization

Use Cases

Technical Details

Impact

Server Virtualization

VPS Hosting

Virtually dedicated to you

- Dedicated resources with VMware virtualisation
- SSD SAN storage
- FREE Plesk Web Host Edition

From £1 /month excl. VAT

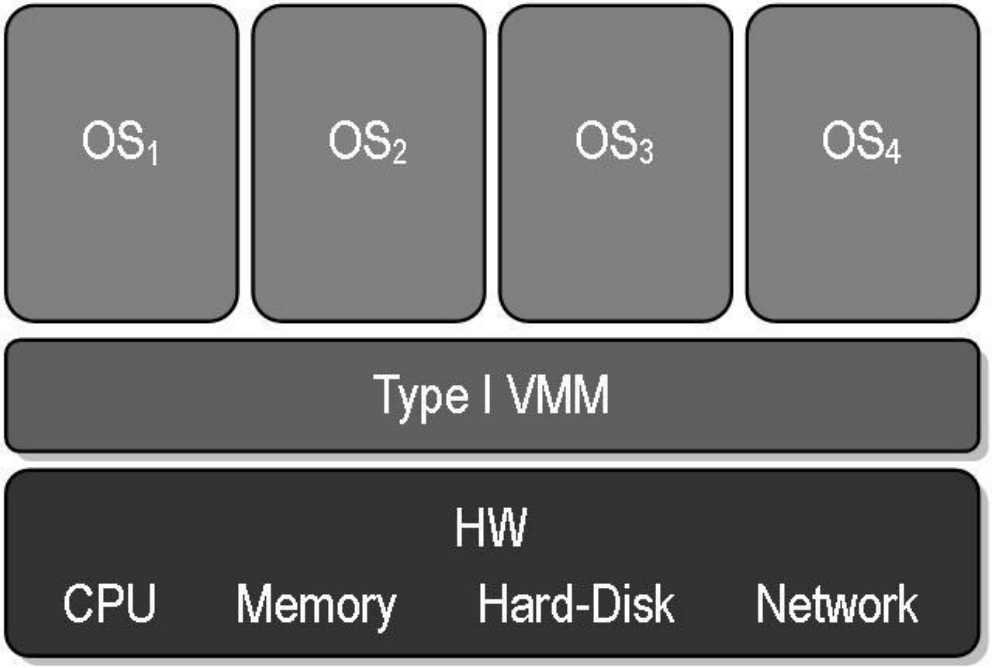
See packages

Virtual Server

Powerful flexibility: Operating system & hardware options to suit your individual needs

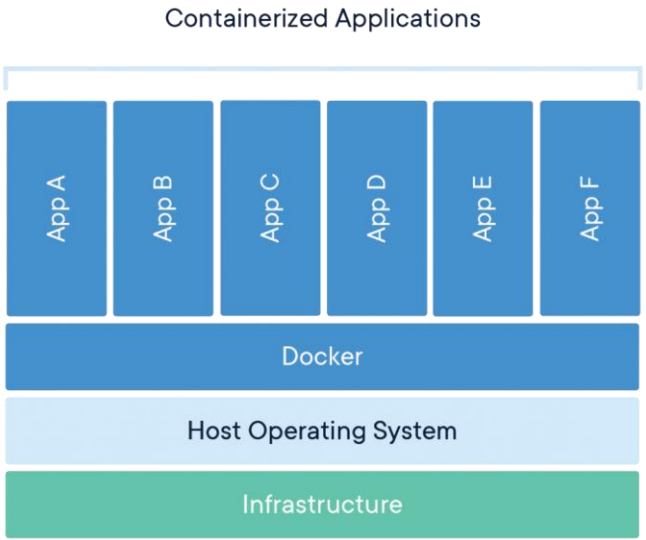
- Flexible resource options for your projects
- 99.9% uptime guarantee with 24/7 network monitoring
- SSH/Shell root access and clear user interface

Hypervisor based Virtualization



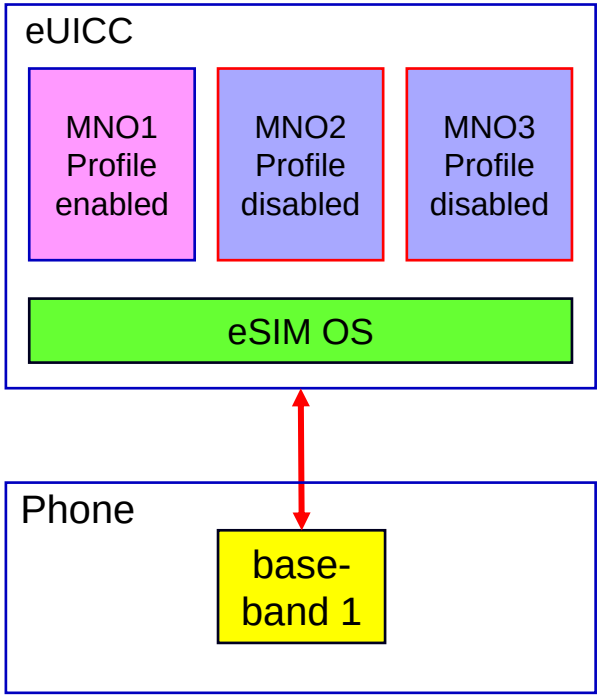
VMM
= Virtual Machine Monitor
= Hypervisor

OS Level Virtualization / Containerization

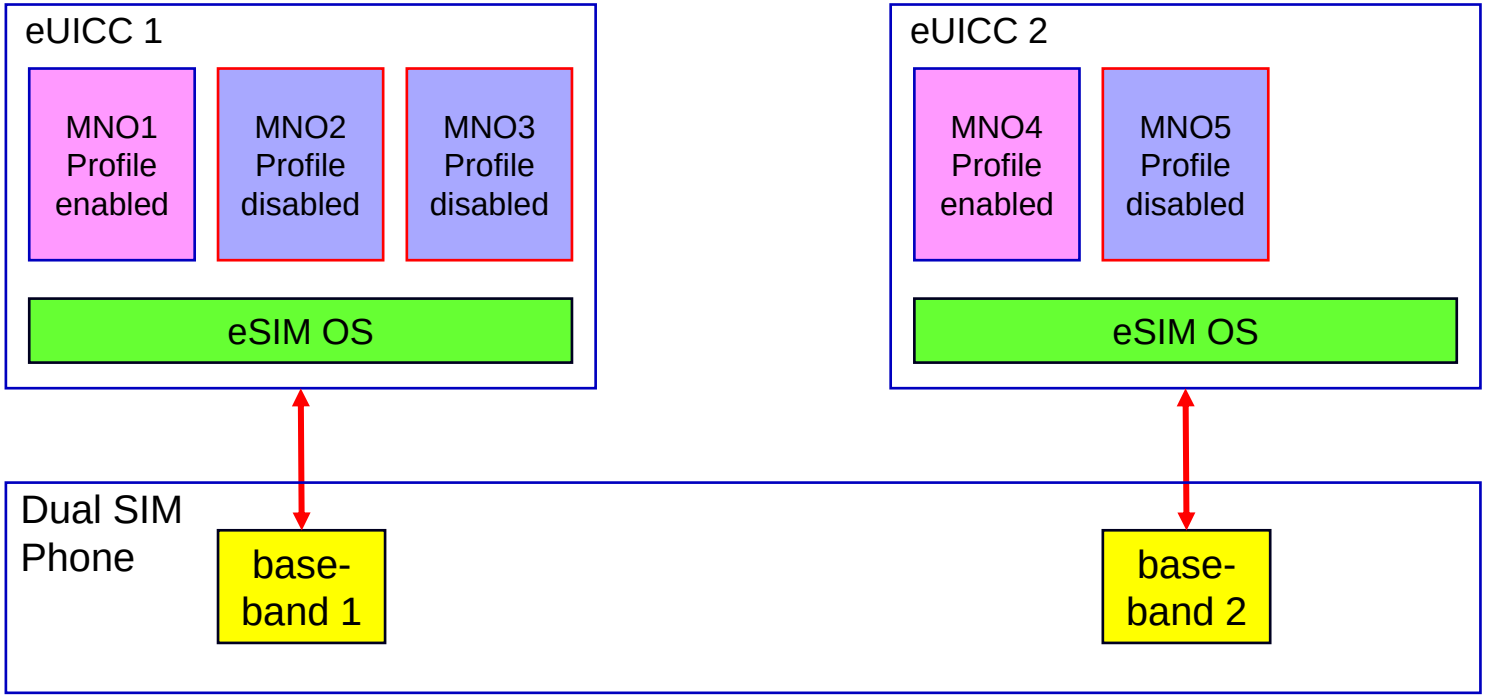


Use Cases

GSMA eSIM v2


eUICC
MNO1 Profile enabled
MNO2 Profile disabled
MNO3 Profile disabled
eSIM OS
Phone
base-band 1

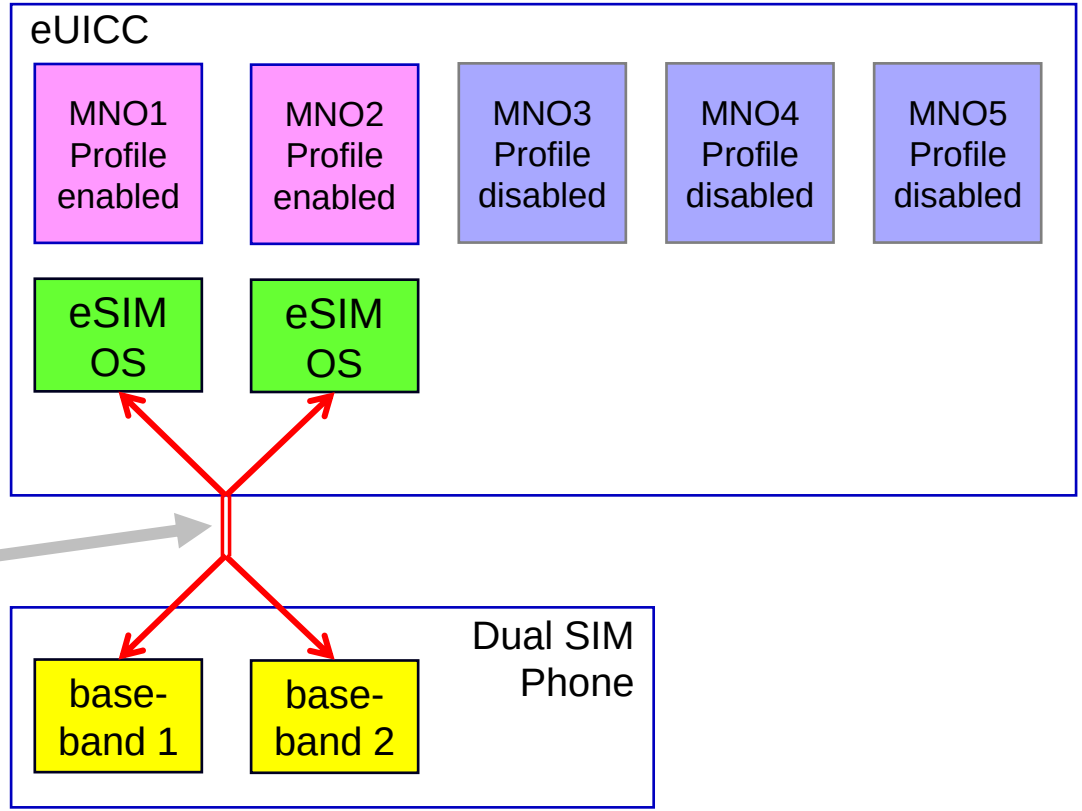
GSMA eSIM v2: The dual SIM Phone Problem



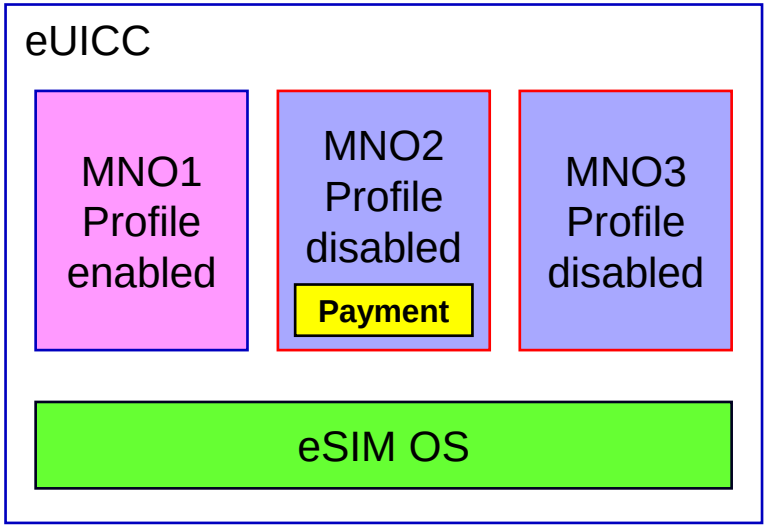
GSMA eSIM v3: Multiple Enabled Profiles

looks like 2 separate OSs to the basebands, however, it can simply be 2 threads within the same code

Multiplexing of “logical interfaces”



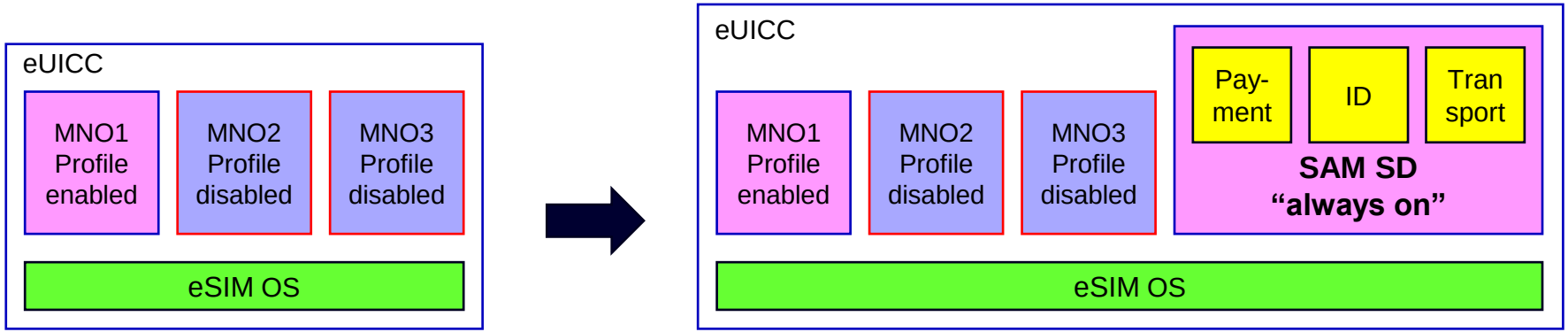
GSMA eSIM v2: 3rd Party Applications



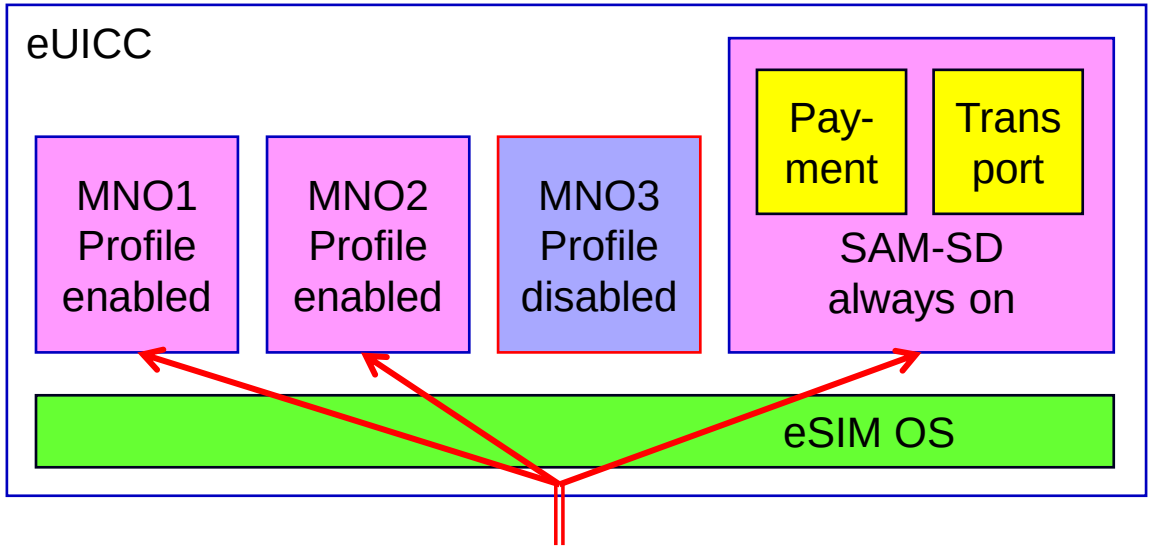
GSMA SAM: SAM Security Domain

Separate Project in GSMA TSG:

Secure Applications on Mobile (SAM)



GSMA eSIM “Next Generation”: MEP + SAM



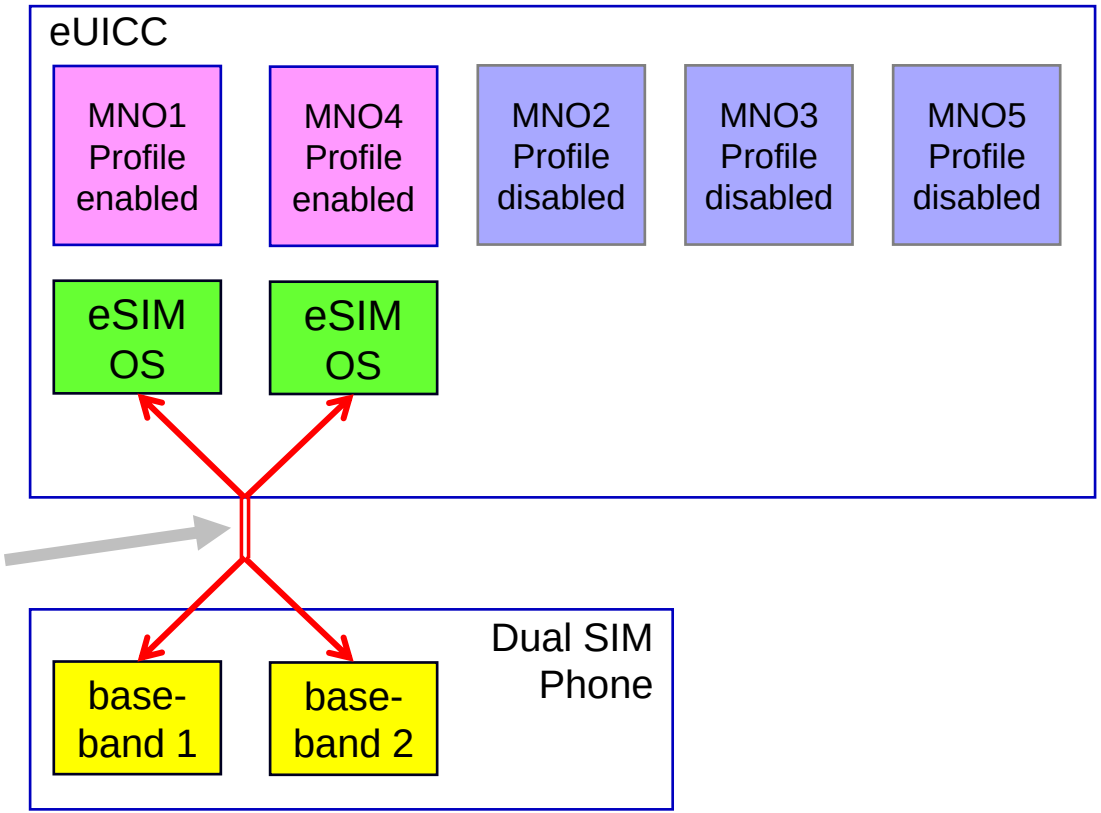
separate “logical Secure Elements”

Technical Details

GSMA eSIM v3: Multiple Enabled Profiles

looks like 2 separate OSs to the basebands, however, it can simply be 2 threads within the same code

Multiplexing of **“logical SE interfaces” (LSIs)** is being defined by **ETSI TC SET**, in cooperation with **ISO/IEC JTC 1/SC 17/WG 4**



MANAGE LSI

ETSI language: LSE = logical SE / LSI = logical SE interface

A new APDU is defined that allows multiplexing of the APDU streams for the different logical SE interfaces (LSIs). It has the following modes:

- MANAGE LSI (select LSI <LSI #>): Subsequent APDUs will go to the LSE selected on this LSI until the next MANAGE LSI (select LSI) APDU is sent.
- MANAGE LSI (reset LSE <LSI #>): This initiates a reset of the LSE selected on the indicated LSI. The ATR is sent in the APDU response. It also selects the LSI for subsequent APDUs.
- MANAGE LSI (close LSI <LSI #>): This closes the indicated LSI. Re-opening requires a MANAGE LSI (reset LSE).
- MANAGE LSI (get/set LSI configuration): For negotiation at the beginning of a card session.

MANAGE LSI

ETSI language: LSE = logical SE / LSI = logical SE interface

A new APDU is defined that allows multiplexing of the APDU streams for the different logical SE interfaces (LSIs). It has the following modes:

- MANAGE LSI (select LSI <LSI #>): Subsequent APDUs will go to the LSE selected on this LSI until the next MANAGE LSI (select LSI) APDU is sent. ***<- alternatives proposed***
- MANAGE LSI (reset LSE <LSI #>): This initiates a reset of the LSE selected on the indicated LSI. The ATR is sent in the APDU response. It also selects the LSI for subsequent APDUs.
- MANAGE LSI (close LSI <LSI #>): This closes the indicated LSI. Re-opening requires a MANAGE LSI (reset LSE).
- MANAGE LSI (get/set LSI configuration): For negotiation at the beginning of a card session.

T=1: LSI selection via NAD byte

Prologue field (mandatory)			Information field (optional)	Epilogue field (mandatory)
NAD (1 byte)	PCB (1 byte)	LEN (1 byte)	INF (0 to 254 bytes)	LRC (1 byte) or CRC (2 bytes)

Figure 17 — Block frame

NAD

0	DAD	0	SAD

- Use NAD byte to indicate LSI.
- Only works for T=1 (and SPI/I2C if T=1' is used there)
- Limited to 7 LSEs (unless an approach incompatible with current ISO/IEC 7816-3 specification is taken)
- NAD usage intended by ISO for physical network

T=1 vs. T=1’

T=1

- Max. payload 254 bytes
- LRC or CRC

T=1’ by GlobalPlatform for SPI/I2C

- Max. payload 64k bytes
- CRC mandatory
- S-Blocks for software reset + “ATR”

Prologue field (mandatory)			Information field (optional)	Epilogue field (mandatory)
NAD (1 byte)	PCB (1 byte)	LEN (1 byte)	INF (0 to 254 bytes)	LRC (1 byte) or CRC (2 bytes)

Figure 17 — Block frame

Table 4-1: Block Format

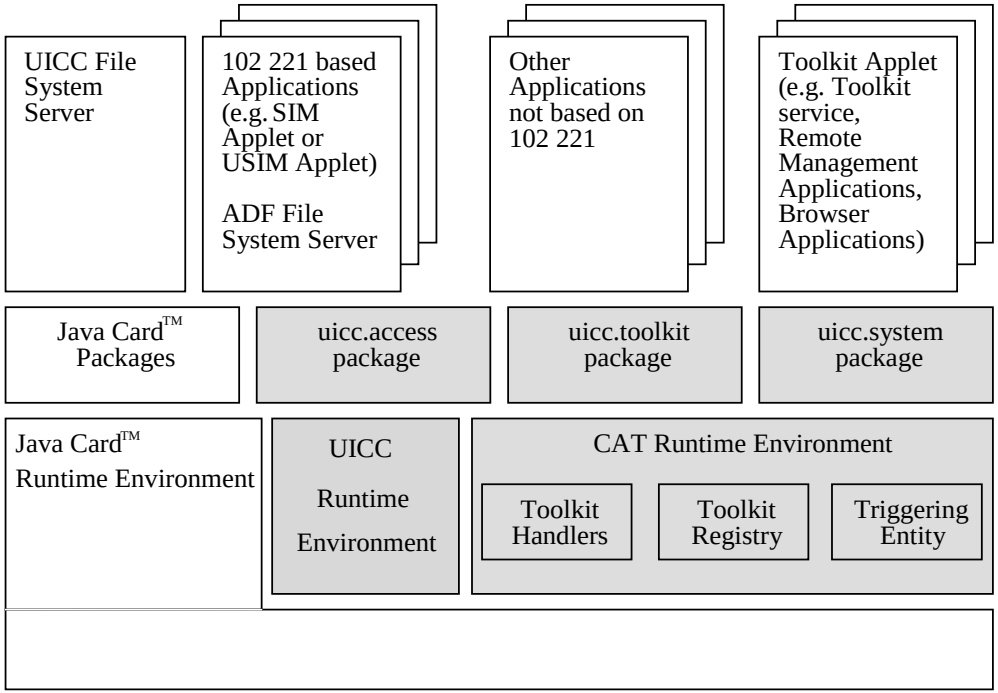
Prologue Field (mandatory)			Information Field (optional)	Epilogue Field (mandatory)
NAD (1 byte)	PCB (1 byte)	LEN (2 byte)	INF (LEN bytes)	CRC (2 bytes)

Virtual Targets for I3C

- I3C is the successor of I2C, a serial communication interface for connecting chips like sensors, actuators, power regulators, MCUs, FPGAs, etc.
- I3C allows one Target (physical device, chip) to emulate multiple I3C Target Devices.
- Applied to a Secure Element, it allows hosting of several “logical SEs” on one physical SE.

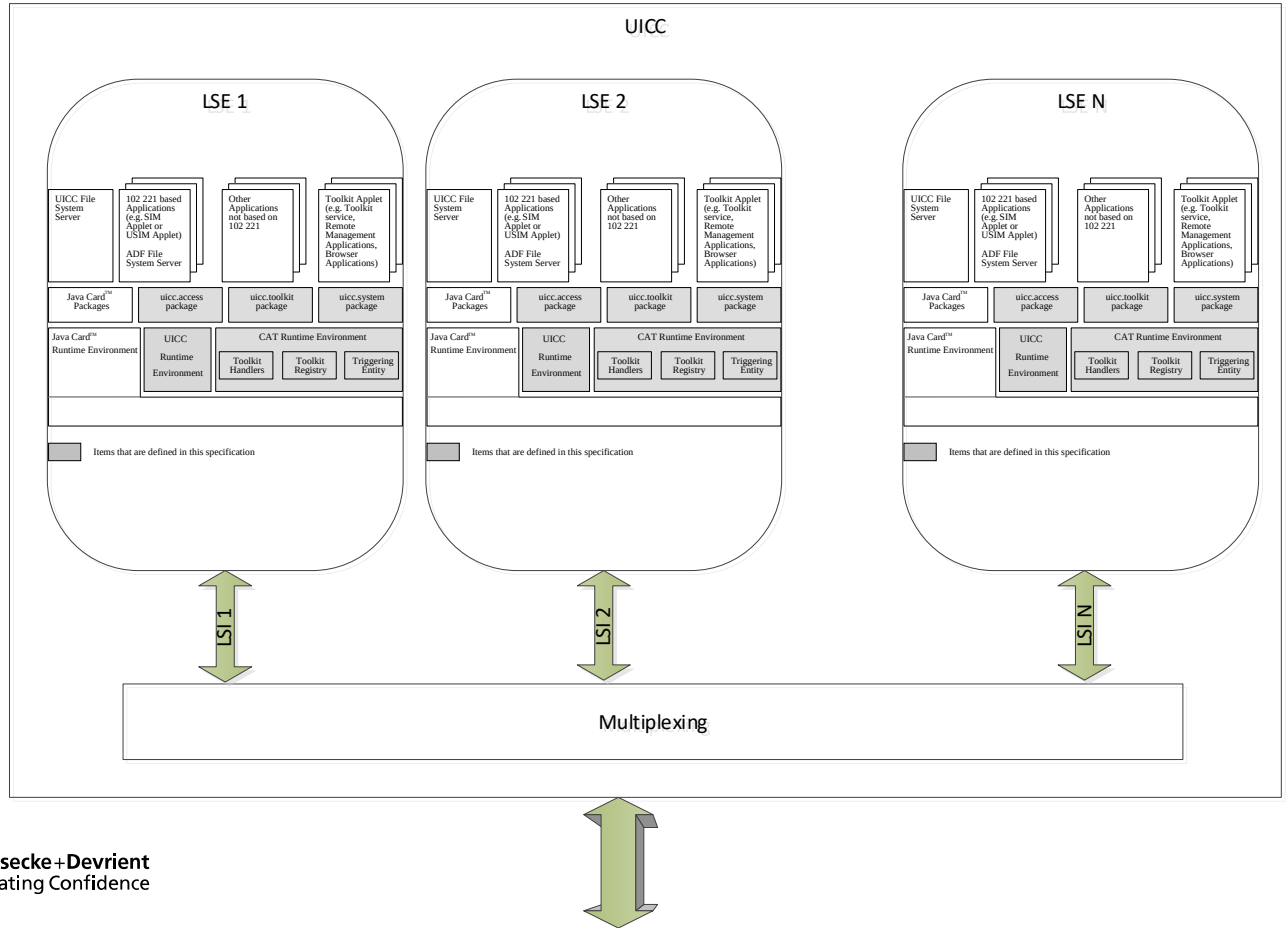
Impact

Java Card™ Impact



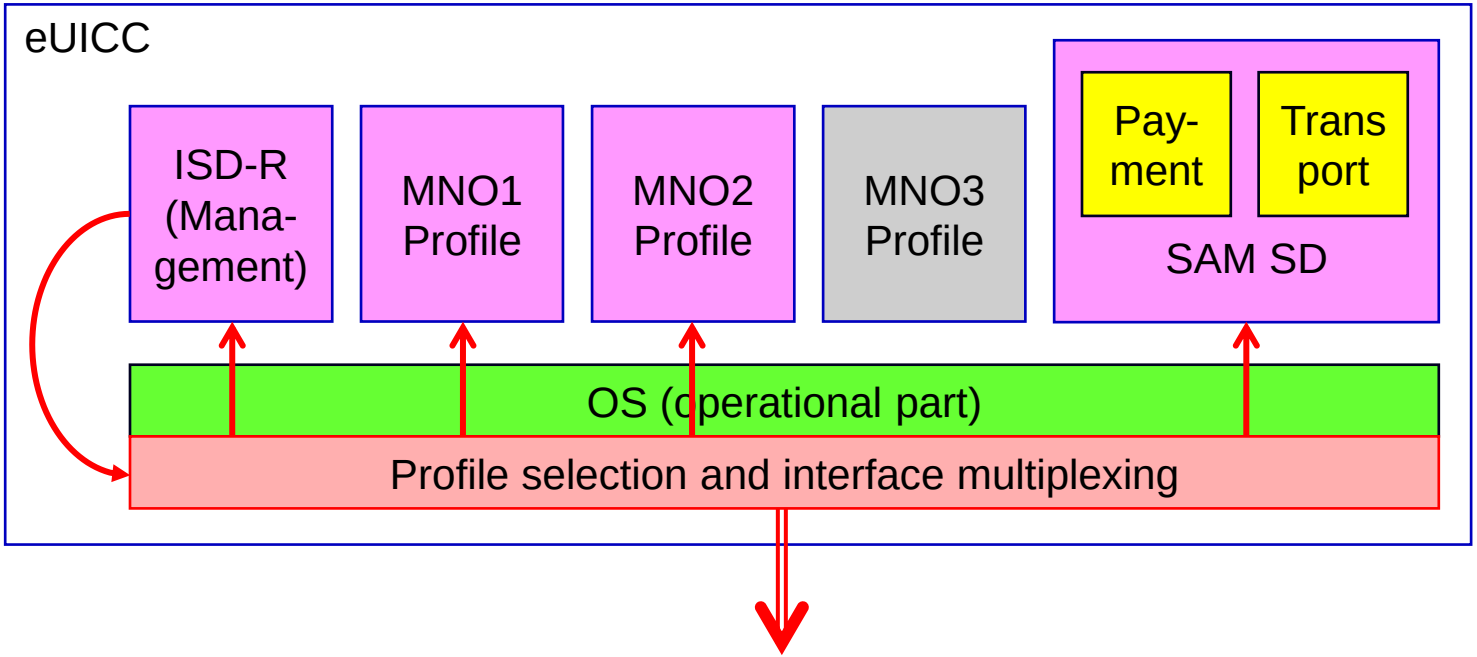
from ETSI TS 102 241

Java Card™ Impact



from ETSI TC SET SCPTEC(21)000183

Architecture of eUICC with separate Management LSI



Java Card™ Impact

- ETSI will define a new proactive command “LSI command” to trigger actions on “LSE management level”
  - Proactive session request
  - UICC platform reset
- This command shall not be available to applet. It will be a restricted system command.

- Future work may specify “LSE management services” like central proactive polling.

Questions?

Creating Confidence

Karl Eglof HARTEL

KarlEglof.Hartel@gi-de.com

Giesecke+Devrient
Creating Confidence