life.augmented

# GSMA SAM (Secured Applications for Mobile)

Merging new standard technologies to empower the next generation of convergence products

Guido Abate

# Agenda

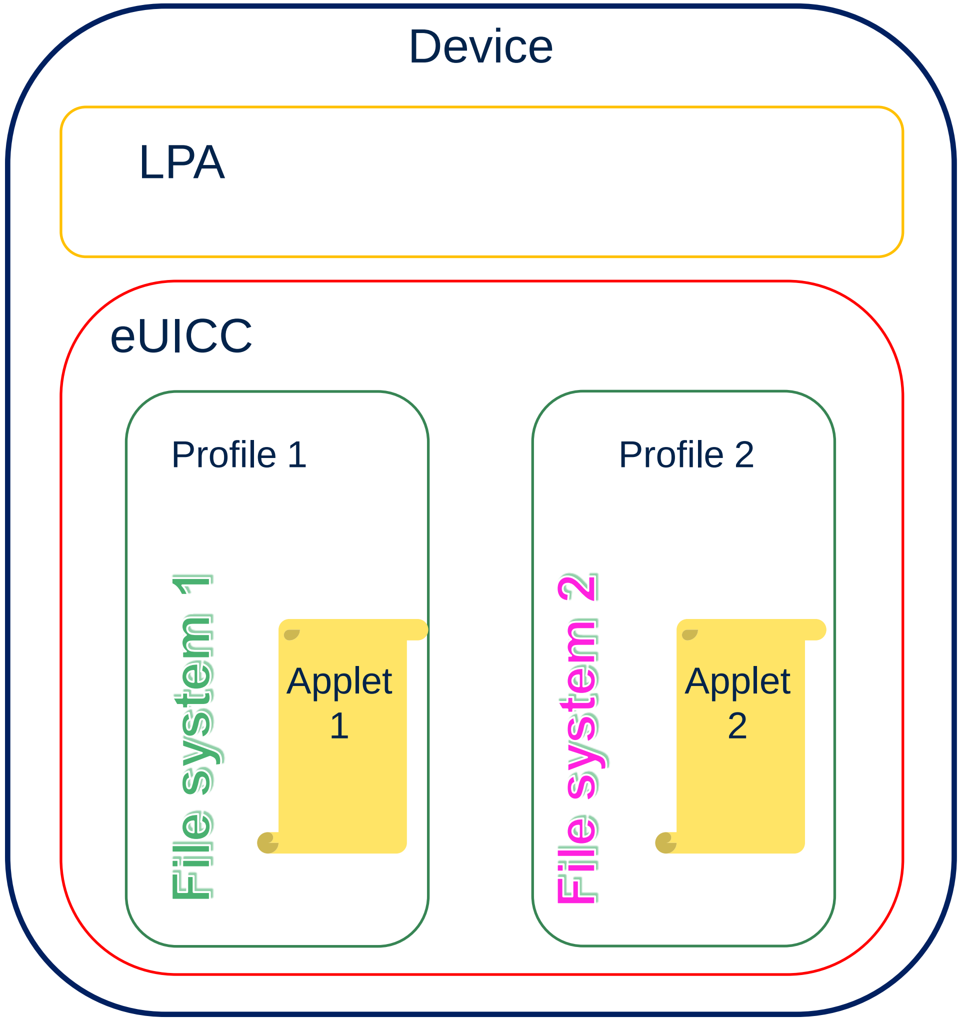
- # The consumer eUICC and its limits
- # GSMA SAM overview
- # SAM and Java Card
- # Technologies optionally to be used in SAM implementations
- # Conclusion

life.augmented

# Introduction

SAM (Secured Applications for Mobile) is a new standard technology sitting on top of Consumer eUICCs

- The eUICC is a SIM that allows a user to switch between different Telecom Operators' Profiles
- SAM allows to implement  the eUICC and the Secure Element functionalities on the same physical electronic component
- In the GSMA eSIM specifications, Java Card applets can be downloaded in the eUICC as part of a telecom Profile

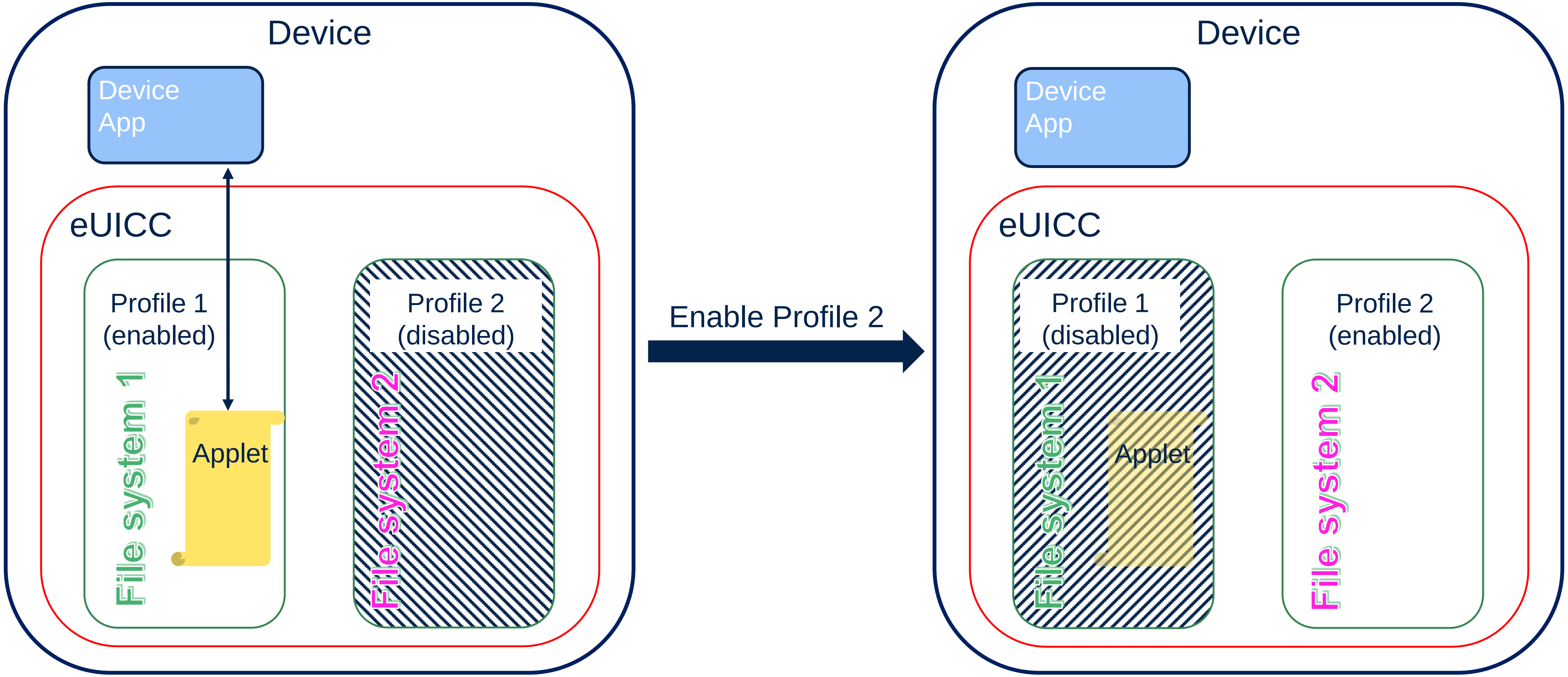


# Some use cases addressed by GSMA

- Telecom Operator (MNO1) and a bank (Bank A) owned by the same shareholder(s)
  - Due to the shareholding structure, it is important to disassociate the bank account from the telecom Profile: Bank A's customer should be able to use its bank's app even if not (or not anymore) a customer of MNO1
- eGovernment use cases
  - New ID use cases being promoted in some european countries: eGov Root of Trust shall be managed or at least authorised by the relevant Government
- The approved Use Cases list can be found in document SAM.01 v1.0, publicly available at https://www.gsma.com/newsroom/wp-content/uploads//SAM.01-v1.0.pdf

# Limit 1

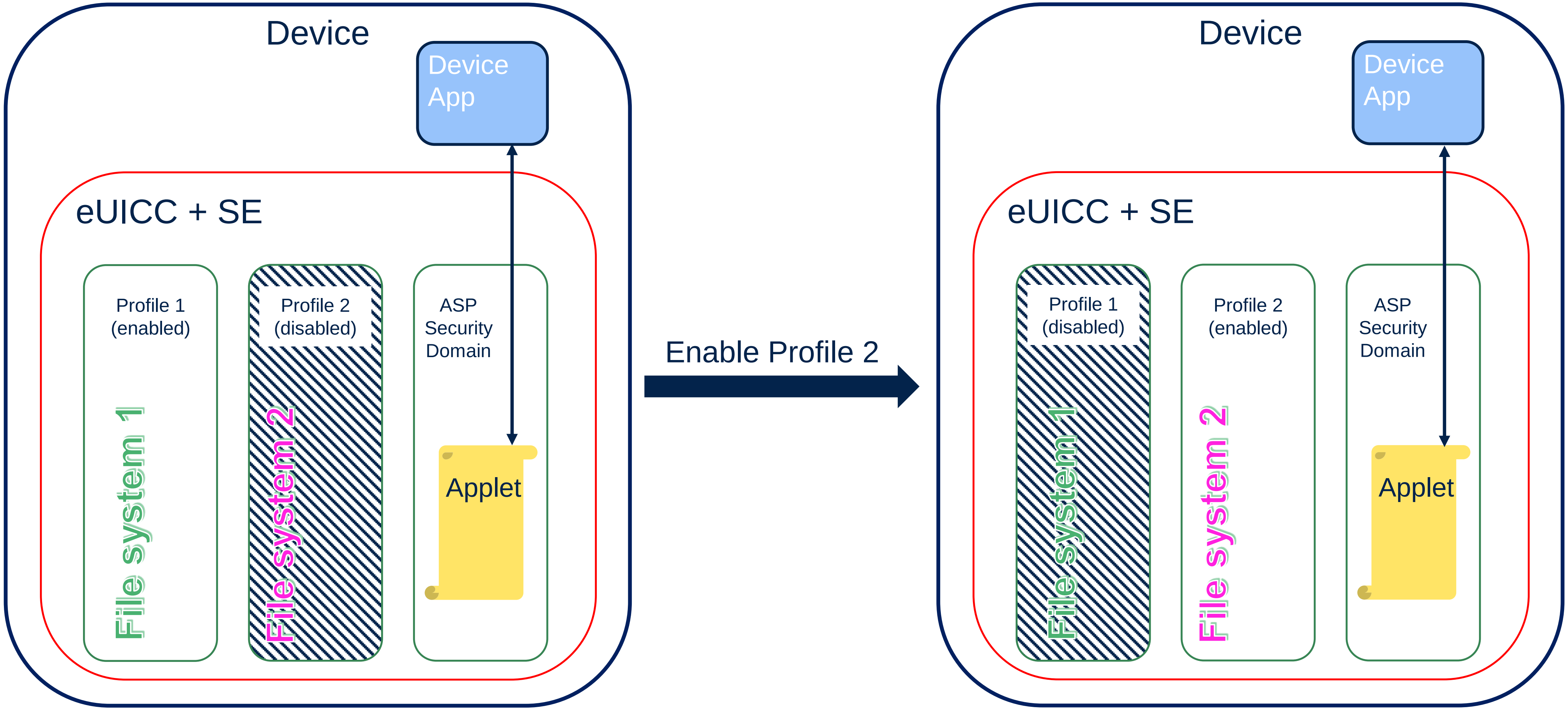
When a Profile is disabled, the applets it contains become invisible to the Device apps.



Profile 1 enabled: services in the applet visible to the Device App and available to the end-user

Profile 1 disabled: services in the applet NOT visible to the Device App and unavailable to the end-user

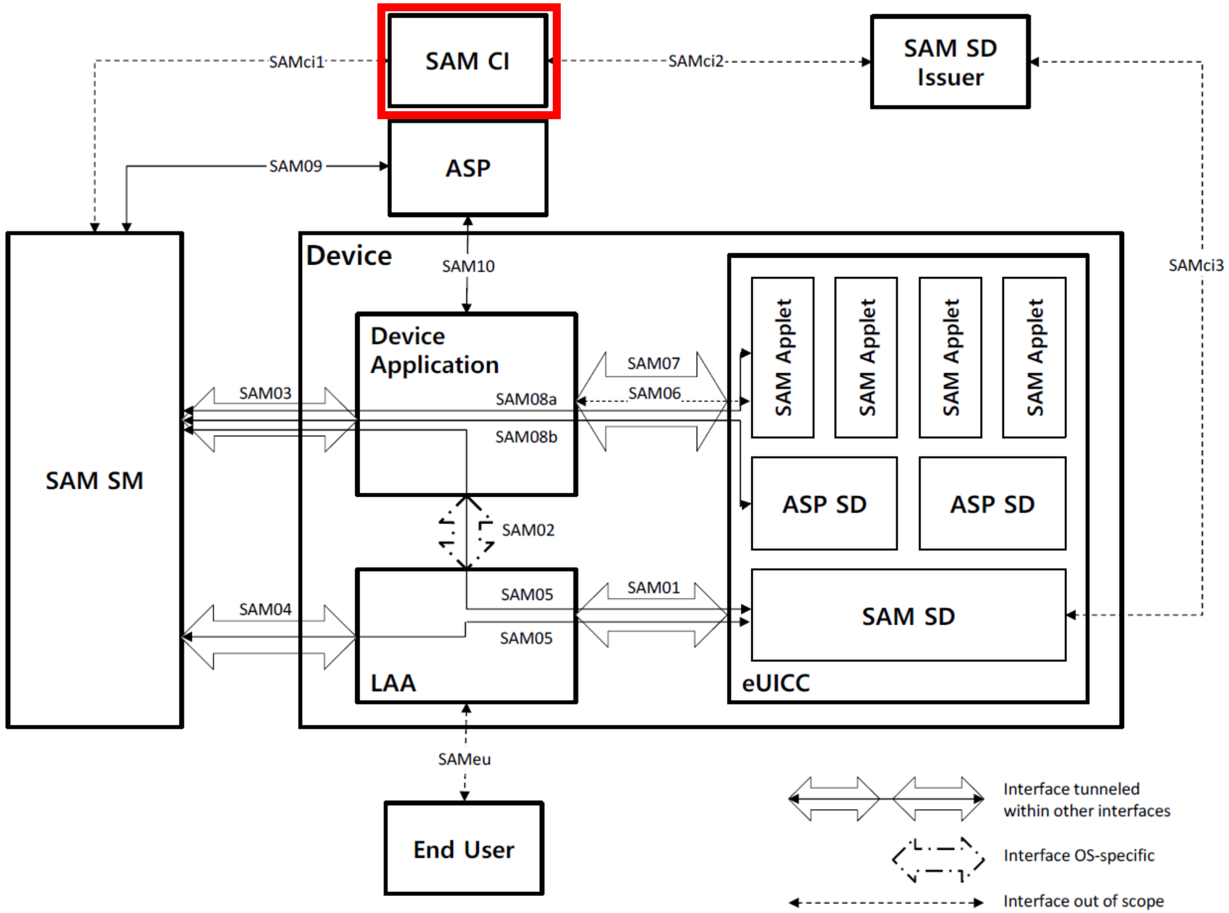
# How SAM overcomes limit 1



Profile 1 enabled: services in the applet available to the end-user

Profile 1 disabled: services in the applet keep being available to the end-user

# How SAM overcomes limit 2



- Differently from the eSIM architecture, the Root of Trust for SAM is not constrained to be a GSMA Root CI
  - For example, it may be an OEM CI
- Trust model
  - The SAM governance is out of GSMA scope
  - Each SAM Applet chains up to a Root CA domain-specific.
    - For example, for Mobile eID it would be a National Public Administration
- The functional and security certifications are not yet discussed

life.augmented

# SAM and Java Card

- Java Card is an essential enabler to develop SAM on top of a eUICC:
  - Services can be administered in an interoperable way only if they are implemented through Java Card applets
  - Applets segregation provided by Java Card is instrumental when dealing with services provided by different Service providers in the same physical chip.

# SDOs currently working on SAM

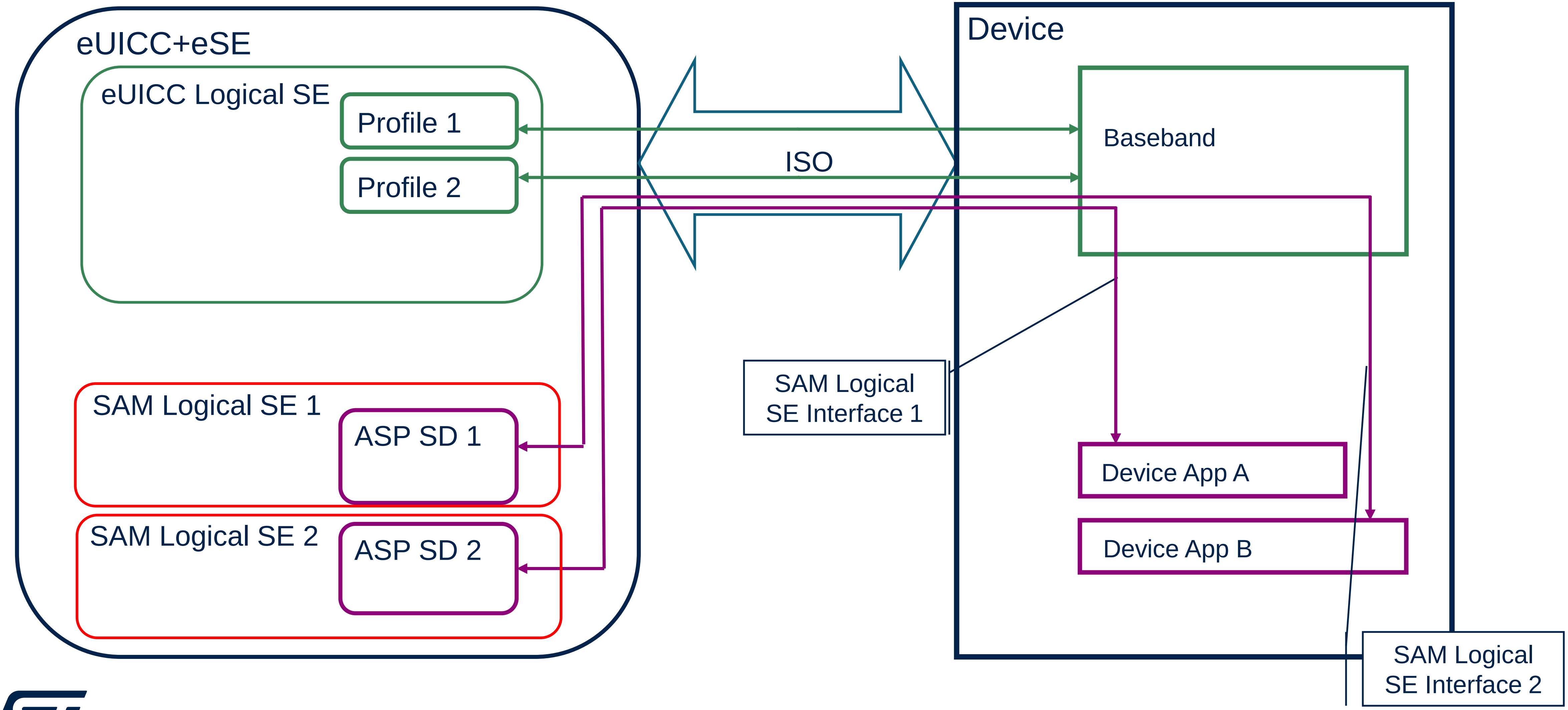
| | Current focus | Last updates |
|---|---|---|
| GSMA | Definition of Architecture and Requirements; Technical Specification defined together with GP | SAM.01 (requirements) approved and published;<br>SAM.02 (Tech Spec) ongoing |
| Global Platform® | SAM Configuration | SAM Configuration for eUICCs v0.0.0.11 under committee review |
| TCA TRUSTED CONNECTIVITY ALLIANCE | Position Paper on SAM | “Secured Applications for Mobile (SAM): TCA Position Paper” is finalized by the TCA SAM working group. Currently the doc is under the TCA approval and publication process. |
| EUROSMART The Voice of the Digital Security Industry | Liaising with GSMA | Eurosmart paper “GSMA SAM solution: opportunities and challenges for mobile identity” published here: https://www.eurosmart.com/european-mobile-identity-recommendations-on-sam-technology/ |

# Technologies optionally to be used in SAM implementations

life.augmented

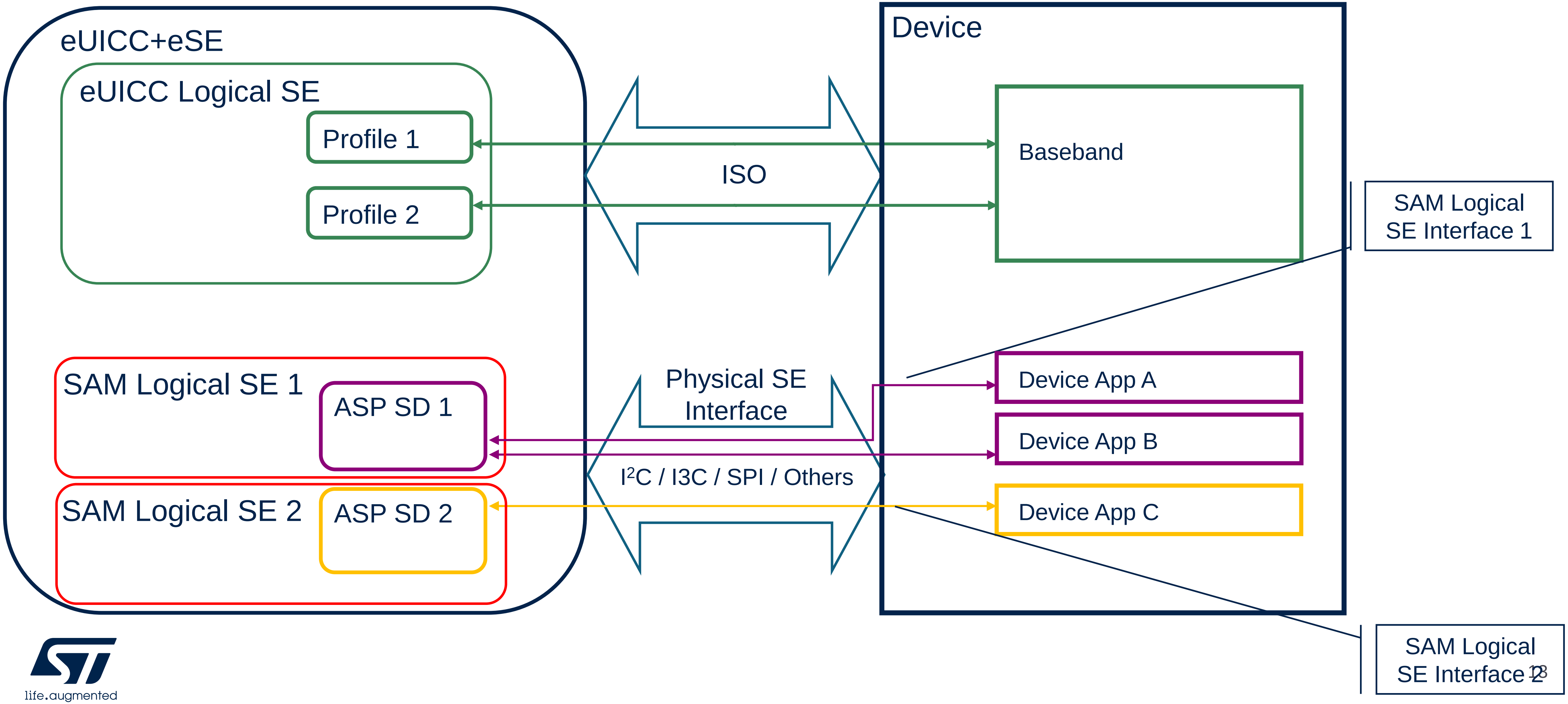
# Physical vs Logical SE Interfaces

## MLI via ISO

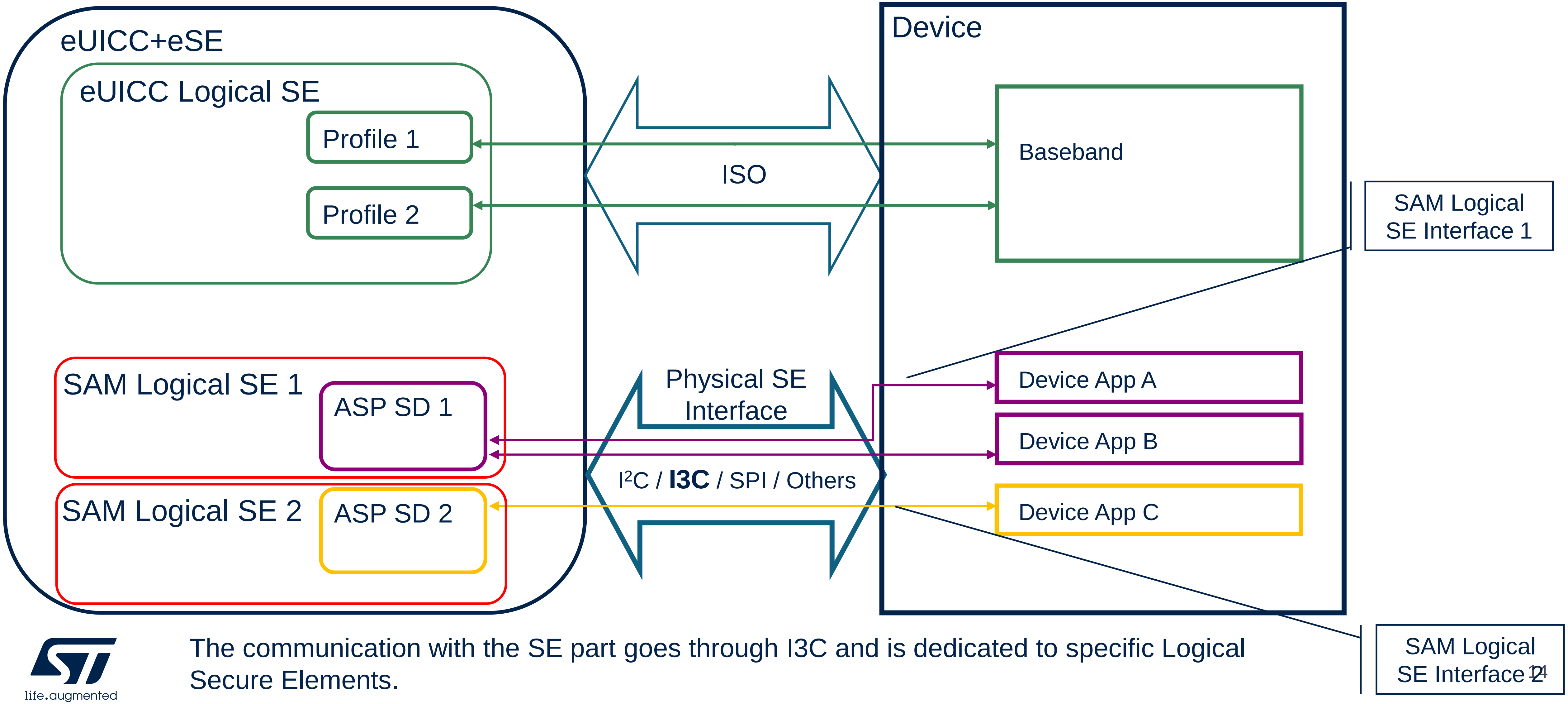


# Physical vs Logical SE Interfaces

## Logical Interfaces  over different physical interfaces

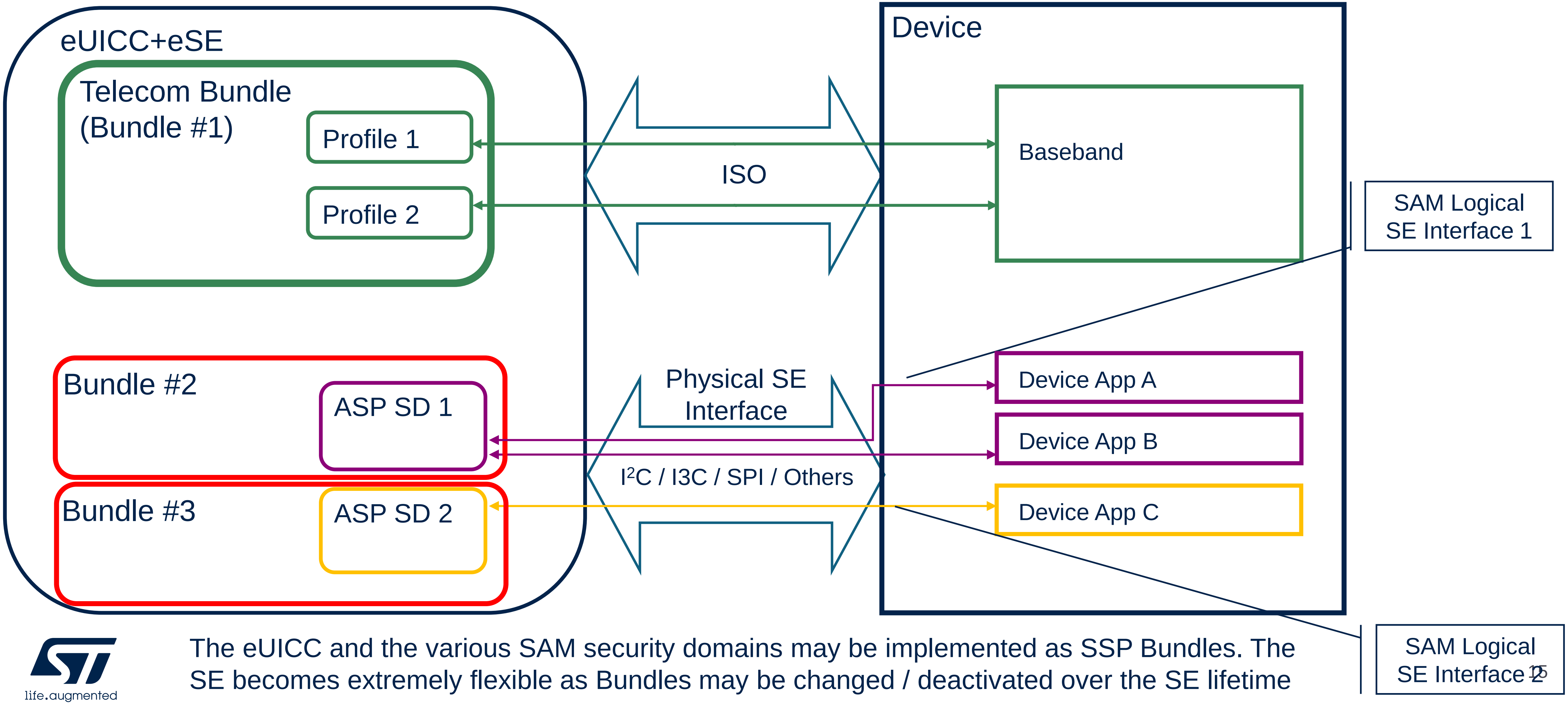


# Flexibility of this architecture



The communication with the SE part goes through I3C and is dedicated to specific Logical Secure Elements.

# Flexibility of this architecture



The eUICC and the various SAM security domains may be implemented as SSP Bundles. The SE becomes extremely flexible as Bundles may be changed / deactivated over the SE lifetime

# Potential Java Card developments

- New physical interfaces, like I3C, are potentially to be considered by JCF
- I3C specifically allows for further potential extensions:
  - The MIPI I3C spec defines the concept of Virtual Target, that can be mapped onto Virtual Secure Element
  - New Virtual Secure Elements can be dynamically downloaded in the field and immediately be accessible on the I3C bus thanks to the "Hot Join" feature defined in MIPI I3C spec.

# Conclusion

- Java Card is a fundamental building block for SAM implementations.
- New use cases open opportunities to design Java Card extensions and fulfil new user scenarios.

# Thank you

life.augmented