mipi®
DEVCON
MIPI ALLIANCE DEVELOPERS CONFERENCE

28-29 SEPTEMBER 2021

Giulio Follero
STMicroelectronics
ETSI SCP TEC delegate

MIPI I3C® Interface for the ETSI Smart Secure Platform

ETSI

The Standards People

MIPI I3C® Interface for the ETSI Smart Secure Platform

Presented by: **Giulio Follero**
STMicroelectronics
ETSI SCP TEC delegate

For: **MIPI DevCon 2021**
29 September 2021

Agenda

- ETSI TC Smart Card Platform (SCP)
- New Market Requirements
- Stakeholder Benefits
- The SSP Specifications
- SSP Architecture
- ETSI SSP I3C
- Status and Next Steps

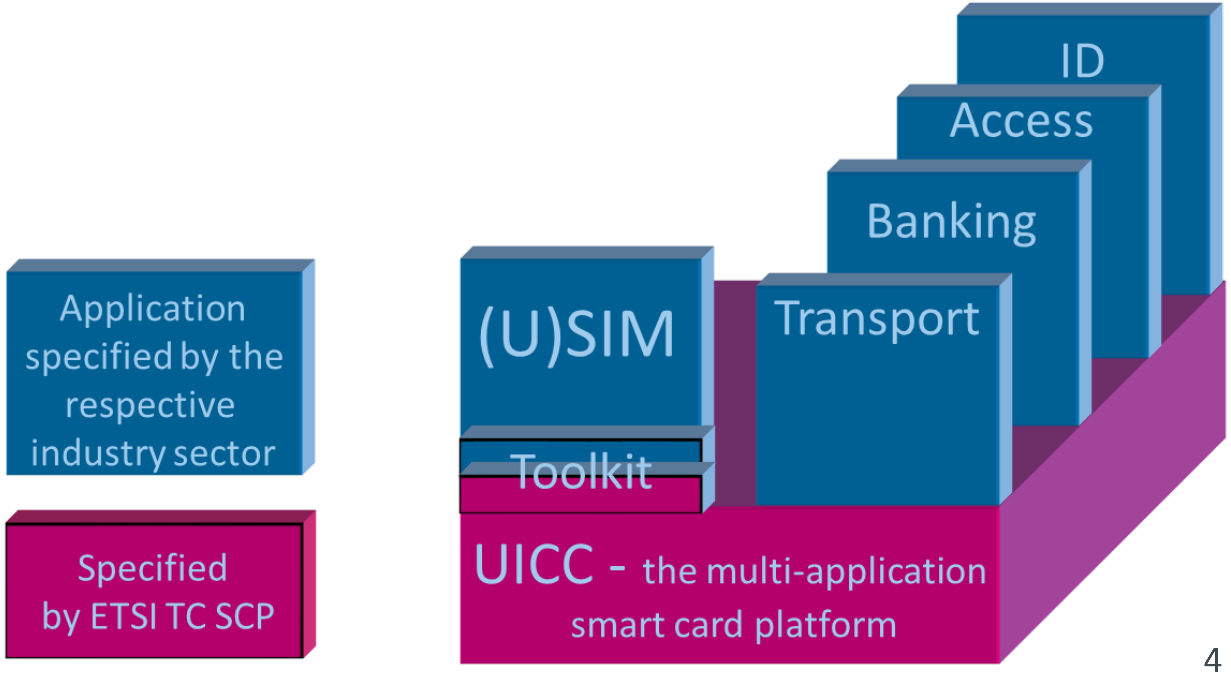
ETSI TC Smart Card Platform (SCP)

TC SCP is responsible for the development and maintenance of specifications for Secure Elements (SEs) in a multi-application capable environment, the integration into such an environment, as well as the secure provisioning of services making use of SEs

- Home of the UICC – the most widely deployed Secure Element with billions of pieces going into the market every year just as SIM cards

Visit the SCP webpage on the ETSI website
https://www.etsi.org/committee/1411-scp

For details of recent activities, see SCP Activity Report 2020


Application specified by the respective industry sector
Specified by ETSI TC SCP
ID
Access
Banking
(U)SIM
Transport
Toolkit
UICC - the multi-application smart card platform

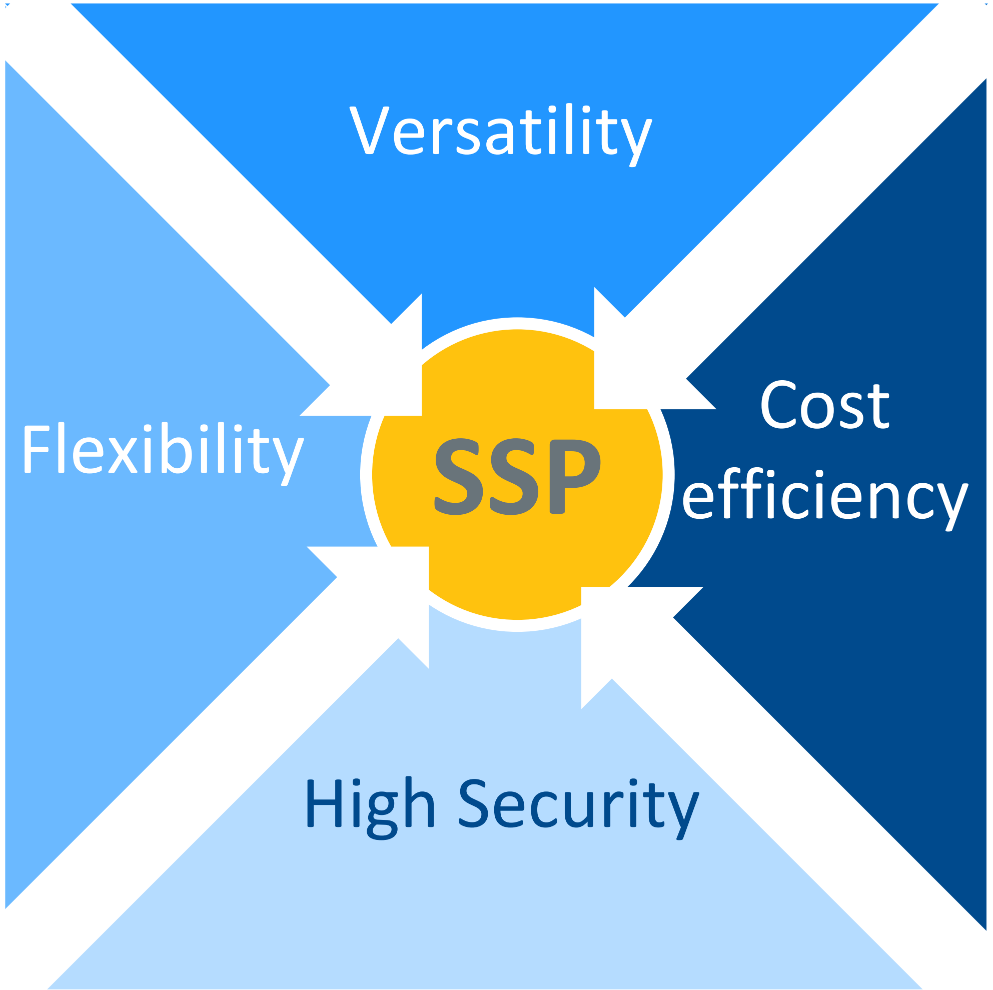
New Market Requirements

Smart Secure Platform (SSP) is the answer for new market needs: to provide independency to business players and update the technology proposal bearing in mind complexity and cost of the product, size of the hardware and allowing flexible implementations

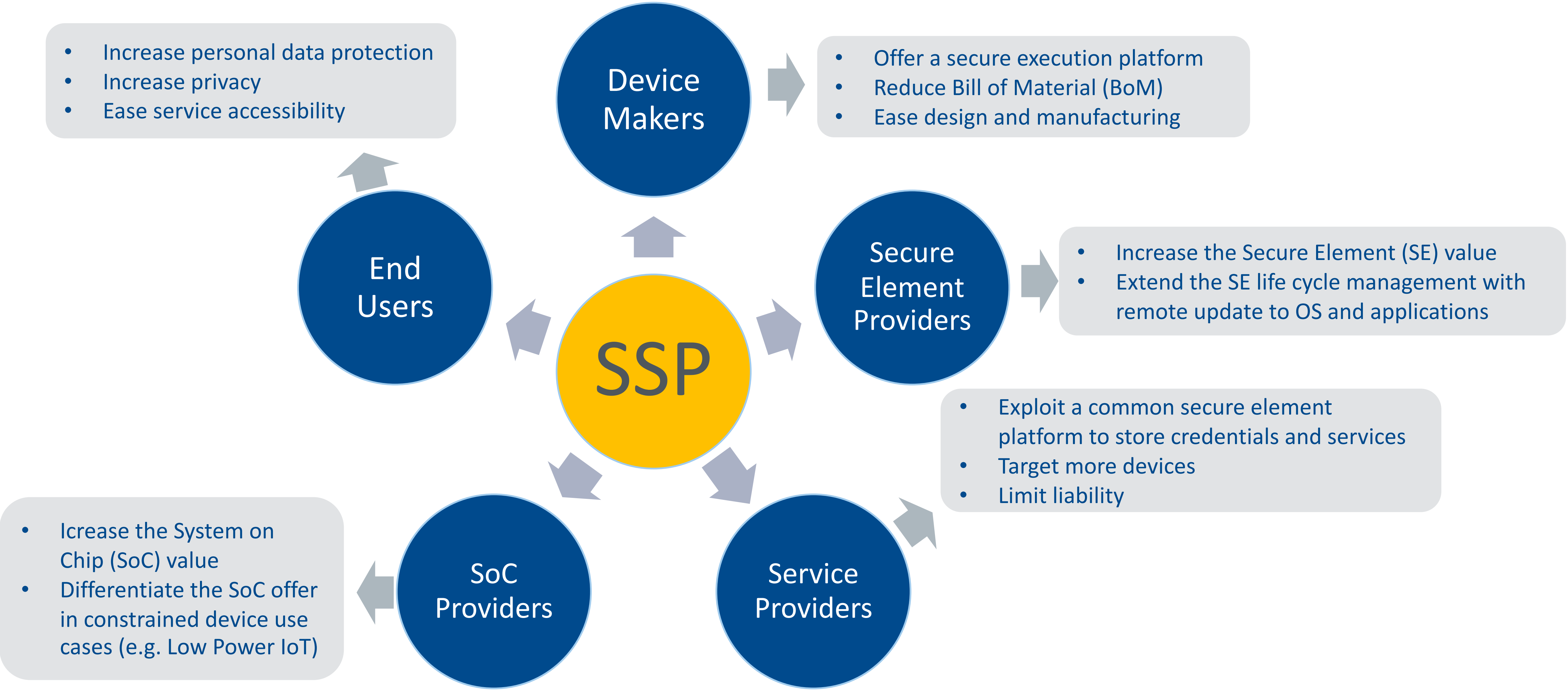
Objective: Better integration into the specific use case

Design: Modular platform offering a core set of features and a number of options

- ✓ **Flexible:** Options selected at time of implementation, application dependent
- ✓ **High Security**: extensive set of security and certification requirements
- ✓ **Versatility:** Choice of interfaces: SPI, I2C, MIPI I3C, choice of hardware
- ✓ New filesystem and transport/application protocols
- ✓ Support of existing functions: Contactless, APDU, etc.



Stakeholder benefits



SSP

Device Makers

- Offer a secure execution platform
- Reduce Bill of Material (BoM)
- Ease design and manufacturing

Secure Element Providers

- Increase the Secure Element (SE) value
- Extend the SE life cycle management with remote update to OS and applications

Service Providers

- Exploit a common secure element platform to store credentials and services
- Target more devices
- Limit liability

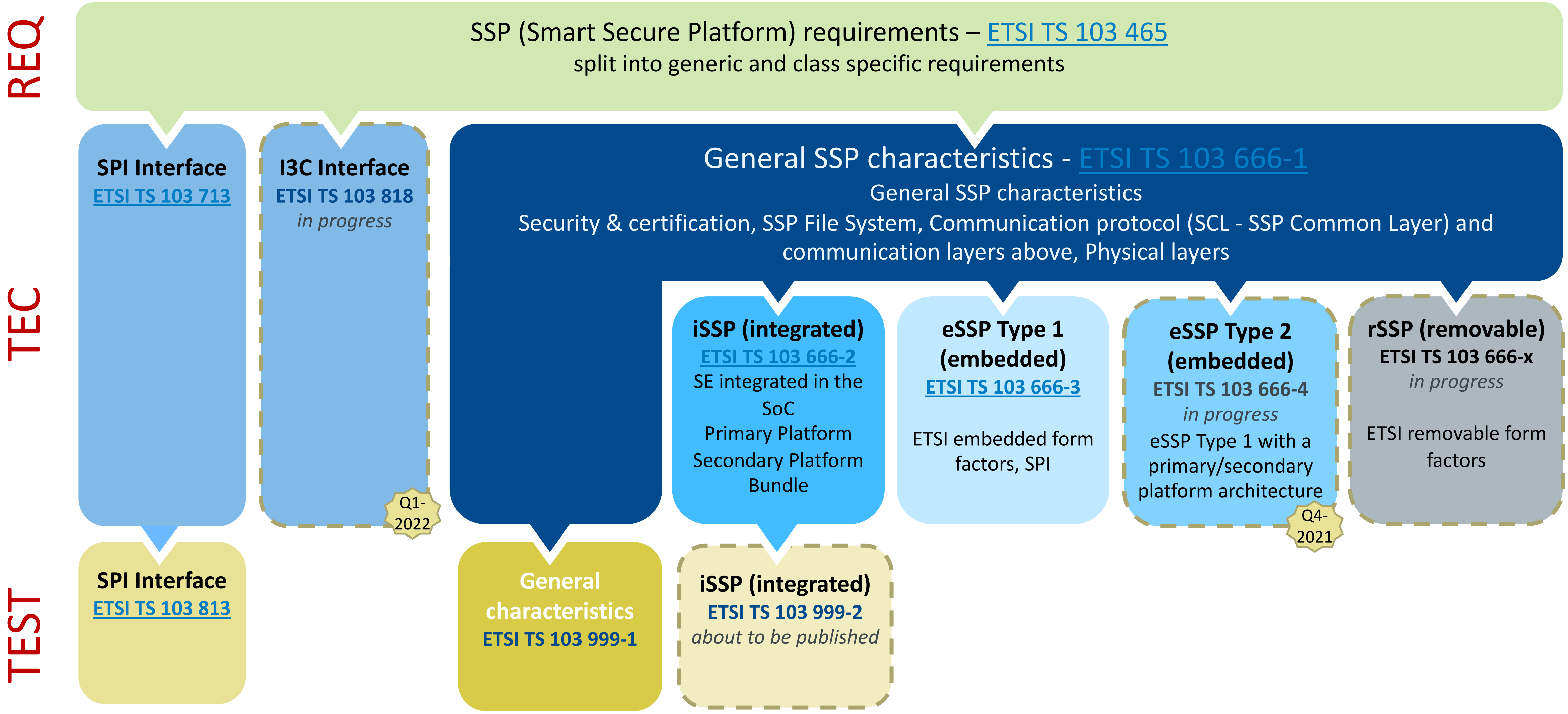
SoC Providers

- Icrease the System on Chip (SoC) value
- Differentiate the SoC offer in constrained device use cases (e.g. Low Power IoT)

End Users

- Increase personal data protection
- Increase privacy
- Ease service accessibility

The SSP Specifications



REQ

TEC

TEST

SSP (Smart Secure Platform) requirements – ETSI TS 103 465
split into generic and class specific requirements

SPI Interface
ETSI TS 103 713

I3C Interface
ETSI TS 103 818
in progress

Q1-2022

General SSP characteristics - ETSI TS 103 666-1
General SSP characteristics
Security & certification, SSP File System, Communication protocol (SCL - SSP Common Layer) and communication layers above, Physical layers

iSSP (integrated)
ETSI TS 103 666-2
SE integrated in the SoC
Primary Platform
Secondary Platform
Bundle

eSSP Type 1 (embedded)
ETSI TS 103 666-3
ETSI embedded form factors, SPI

eSSP Type 2 (embedded)
ETSI TS 103 666-4
in progress
eSSP Type 1 with a primary/secondary platform architecture

Q4-2021

rSSP (removable)
ETSI TS 103 666-x
in progress
ETSI removable form factors

SPI Interface
ETSI TS 103 813

General characteristics
ETSI TS 103 999-1

iSSP (integrated)
ETSI TS 103 999-2
about to be published

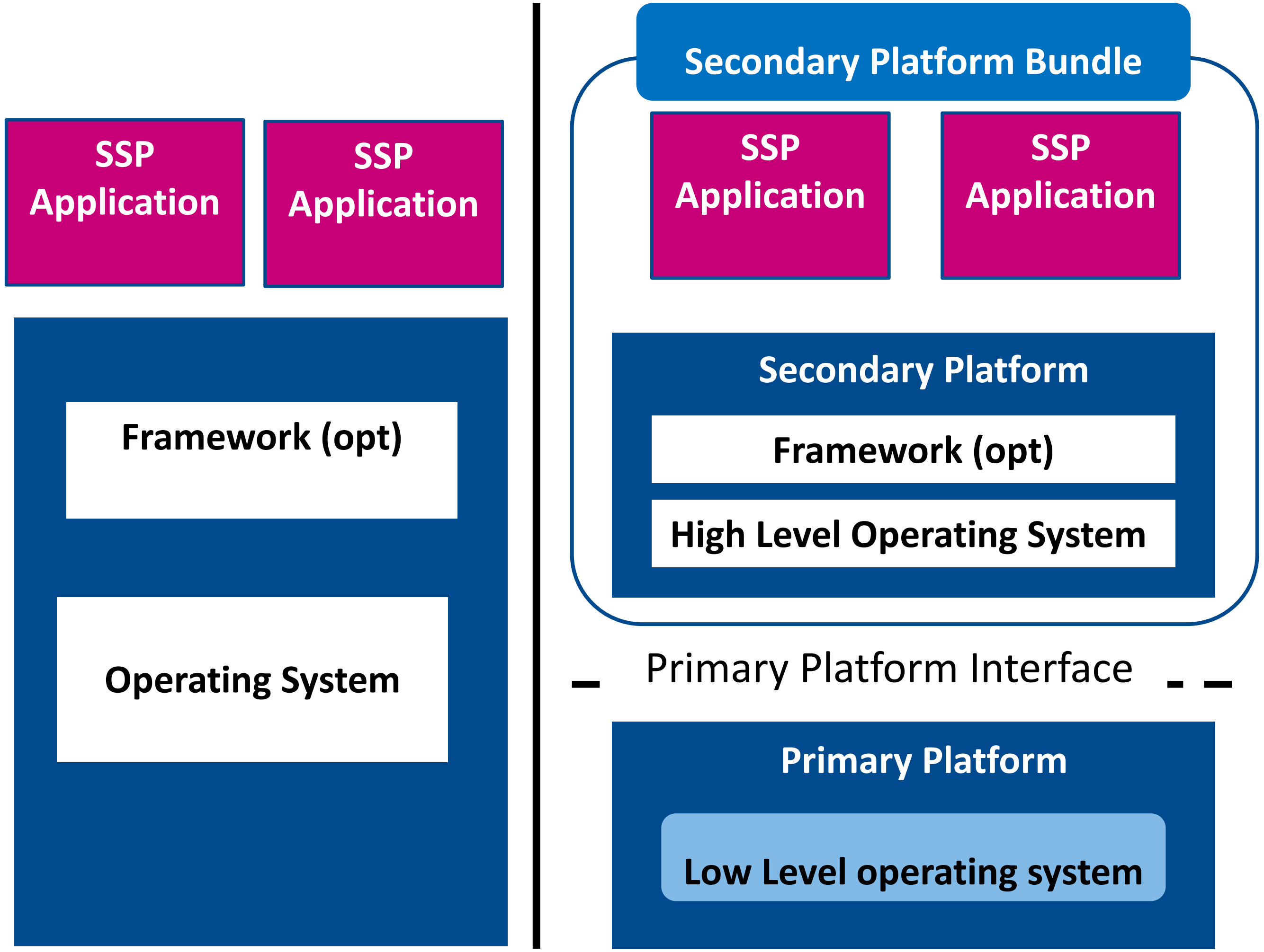
SSP possible Architectures

Two possible architectures

- SSP software running on the SSP hardware platform
- SSP software stack with Primary Platform Interface

Primary Platform: hardware platform along with a low-level operating system managing the exceptions, the hardware platform resources and their accesses

Secondary Platform: software platform using the primary platform interface and containing the high-level operating system on top of which the SSP applications are running

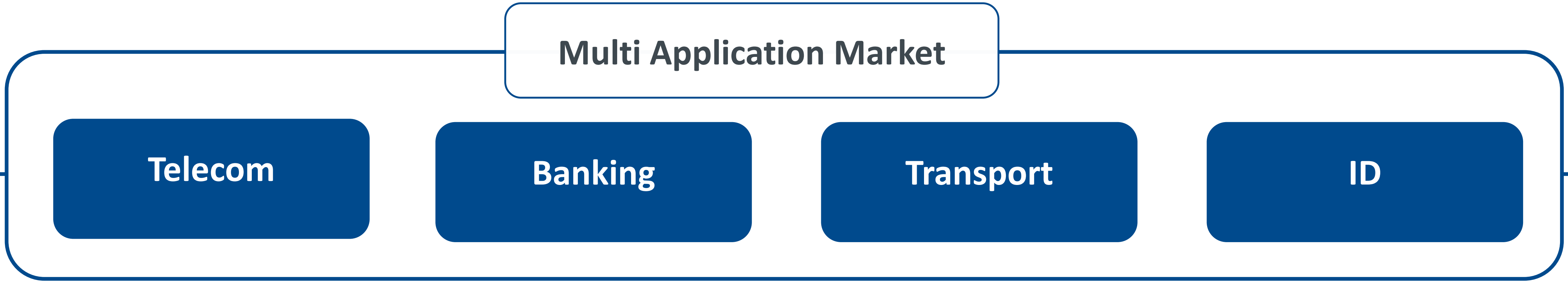


SSP possible Architectures

SSP software running on the SSP hardware: Preferably if only one application needs to be addressed and when the operating system does not need to be updated. Less complexity in the implementation.

Single Application Market

SSP software stack with Primary Platform: Different applications can be hosted, thanks to clear separation between hardware (SoC), and Operating System with applications (SPB). This architecture offers a mechanism to update operating systems and applications (SPB remote download)



Multi Application Market

Telecom

Banking

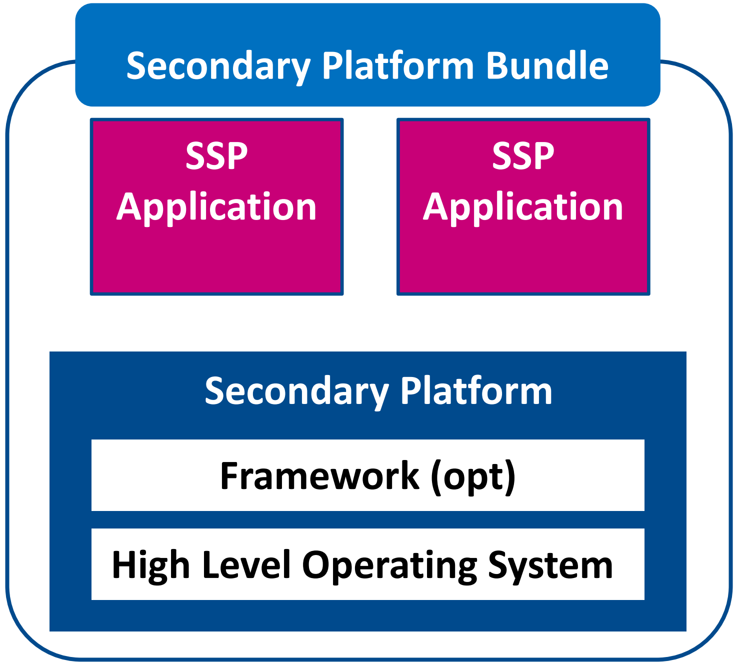
Transport

ID

SSP possible Architectures

Secondary Platform Bundle

- Software platform using the primary platform interface and containing the high-level operating system on top of which the SSP applications are running
- “Use-cases dependent” (telco, payment, automotive, transportation, etc.)
- The SSP may contain multiple Secondary Platform Bundles. At most one secondary platform bundle at time shall be loaded and executed by Primary Platform, to ensure high security, (protection of sensible data), by physical isolation between bundles



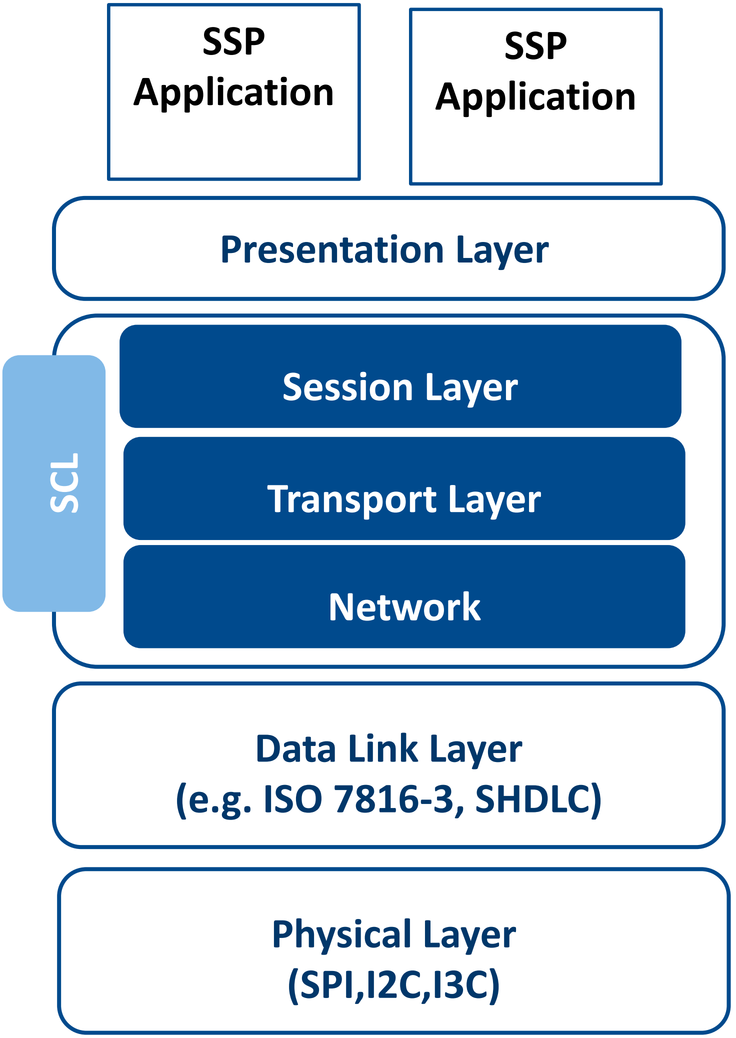
SSP Architecture – Secondary Platform

The Secondary Platform introduces the SSP common Layer (SCL) to be independent from the physical layer

SCL can support many physical layers

The following physical layers are currently specified in ETSI:

- SPI
- SWP
- ISO
- MIPI I3C (ongoing…)



ETSI SSP I3C
Services and Benefits of SSP I3C based

Consumer market: Using I3C bus, SSP improves quality of services (speed of communication, flexibility, …)

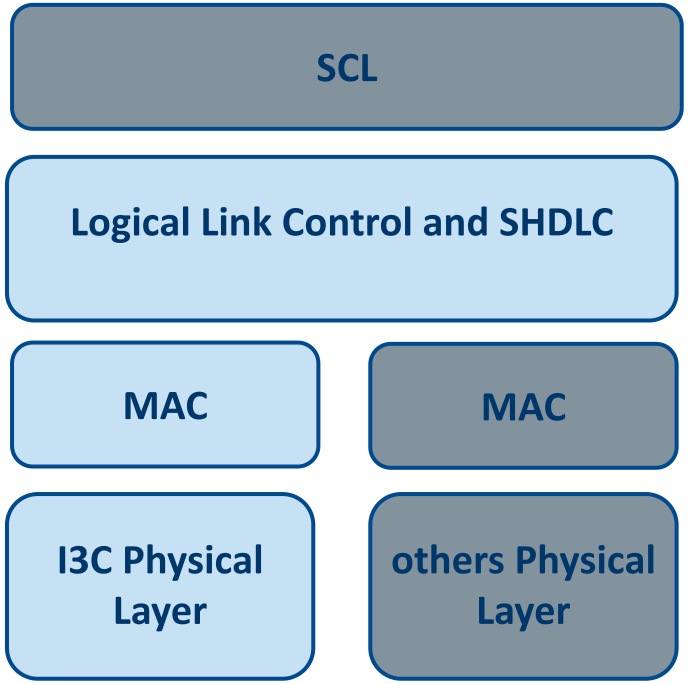
IoT market: SSP can increase security levels and decrease power consumption

Automotive market: SSP can use the I3C bus of the car, providing Cryptographic and security services

- Better integration and usage of SSP in connected devices using I3C interfaces
- All device components will be easily able to find the SSP and communicate directly with it.
- Wider SSP application field that can use data from other devices connected to the bus

ETSI SSP I3C
ETSI TS 103 818; SSP I3C specification content

- Electrical interfaces
- Physical layer
- Device STATUS
- Data Link Layer
- Link Layer Frame
- LLC Layer
- Power management



SCL

Logical Link Control and SHDLC

MAC

MAC

I3C Physical Layer

others Physical Layer

🟦 In the scope of SSP I3C spec

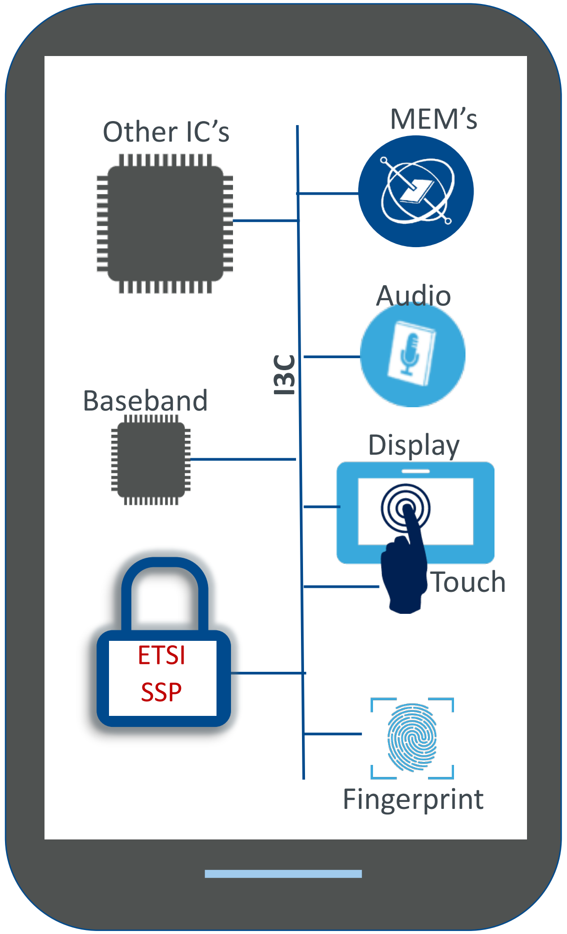
⬤ Out of the scope of TS 103 818 spec

ETSI SSP I3C
ETSI SSP I3C implementation

MIPI Alliance: "Specification for I3C^{SM} - Improved Inter Integrated Circuit" Version 1.0”

The main MIPI I3C features used in the ETSI specification

- IBI support with payload
- Single Data Rate
- Power management
    - Power saving mode
- Operating voltages
- Dynamic Addressing
- Hot-join (in case of removable SSP TBD)

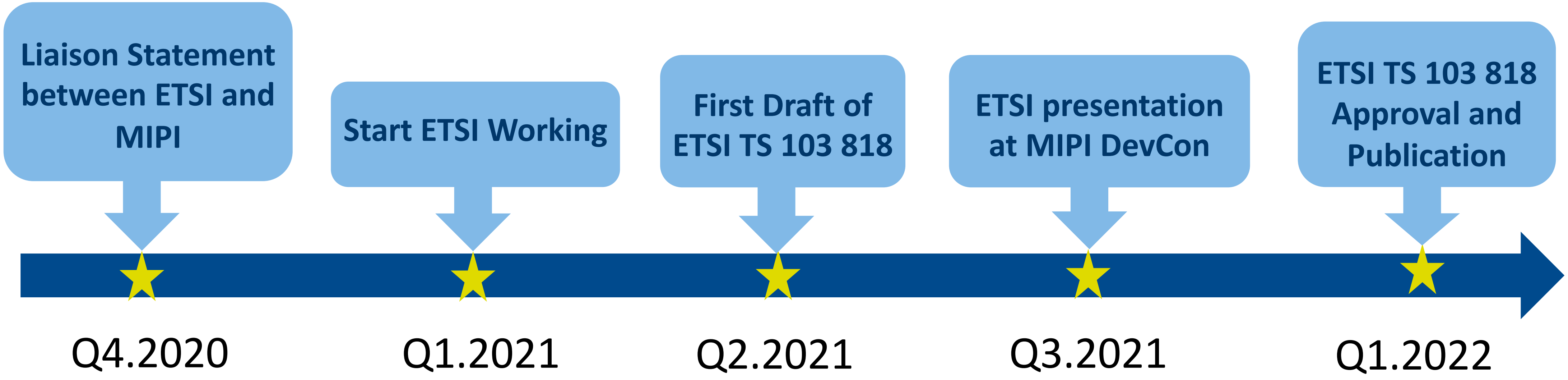


The SSP features in I3C

- The SSP is Target Only
- One SSP per system

SSP I3C Status and next Steps

- The first version of SSP over I3C has been presented in ETSI
  - Physical and Electrical Interfaces
- Mac and Data link layers under definition
- Asking for a specific Device ID for the SSP in the DCR
- TEST specification


Liaison Statement between ETSI and MIPI
Q4.2020
Start ETSI Working
Q1.2021
First Draft of ETSI TS 103 818
Q2.2021
ETSI presentation at MIPI DevCon
Q3.2021
ETSI TS 103 818 Approval and Publication
Q1.2022

Thank you