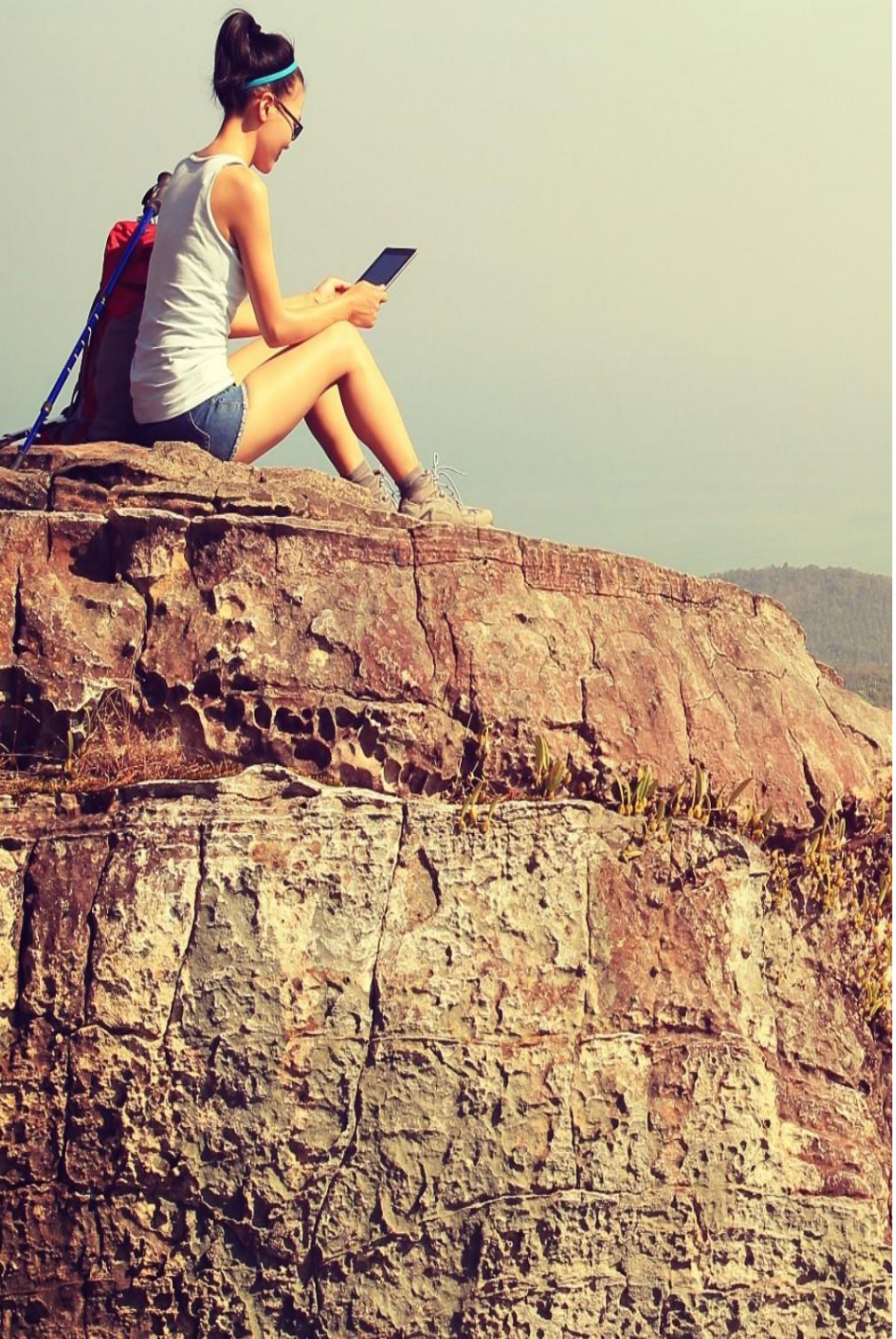


ETSI SCP & TTF001
Smart Secure Platform

ETSI MTS #82 January 2021

Alain RHELIMI-Mellonne

Terms of Reference/ Scope of the TTF

Produce 3 test specifications based on existing standards

Available in full on the ETSI Portal

STD_NUM	WORKING_TITLE
TS 103 999-1	Working title: SSP Test Specification - SSP, General characteristics
TS 103 813	SSP Test Specification - SSP, SPI interface
TS 103 999-2	SSP Test Specification - SSP, iSSP characteristics

End of project expected by October 2021

TTF Team Members

Comprion:
Olga Kaethler - Kirghizstan
Arne Marquordt - Germany
Andras Talas - Hungary

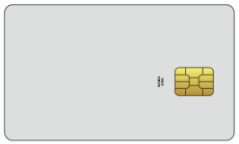
Mellone:
Alain Rhelimi, France
Bastien Lacoste, France

Idemia:
Shubham Gupta, India
Devendra Koranga, India

Virtual CTO Ireland:
Brendan McKenna – Ireland

TTF Leader

Hardware platform Ineluctable evolution



Variant	1FF	2FF ("Mini SIM")	3FF ("Micro SIM")	4FF ("Nano SIM")	e-SIM
Year of launch	1991	1996	2003	2012	2016
Dimensions (mm)	85.6 x 53.98	25.0 x 15.0	15.0 x 12.0	12.3 x 8.8	Small

Discrete component

i-SIM
2019
0x0

Secure processor integrated in a SoC*

Multiplying the HW platforms is opening the field for new opportunities for the industry:
Offering different execution environments, with a good scalability of security level, for a combination of services needed in the different segments.

*SoC: System on Chip

Secure Service agnostic from form factors

New Market Requirements

Better integration

Smaller form factors for addressing low footprint devices (e.g. Wearable device)

Lower Power consumption for addressing battery powered devices and for offering a better user experience

Easy interaction between functions of a device.

Flexibility for logistic concerns

Late personalization of a device after its issuance

Separation between hardware and software logistics.

Less/No interferences between services

Less interferences between services targeting different use cases/ecosystems

Reduce engineering cost

Improvement of the portability of the Primary Platforms supporting a diversity of services

Clear Boundaries about the responsibility between the parties

Higher security

Fast update/loading of secure services and operating systems

Crypto agility

Cost effective support of multiple certification scheme

GDPR support

Connectivity

Easy connection to new functionality then needs to support easily new presentation and application layers

The origin of integrated SSP : the GSMA & the integrated UICC

The GSMA integrated UICC Proof of Concept (iUICC POC) Group, founded 2015, targeting:

Guarantee interoperability of the integrated UICC solution

Ensure a satisfying level of security

Full control of the high level Operating System by each MNO when the iUICC is shared

Continuity of services implemented in removable UICCs when moving to an iUICC

Members : TIM, Gemalto/Thales, Qualcomm, Huawei, Intel, G&D, Idemia, KDDI, Orange, Hutchinson

A first approved document, the iUICC primary platform requirements, was published by the GSMA in May 2017:

http://www.gsma.com/newsroom/all-documents/iuicc-poc-group-primary-platform-requirements/

SSP Origin

The initial motivation did aim at bypassing of the TS 102. 221 limitations.

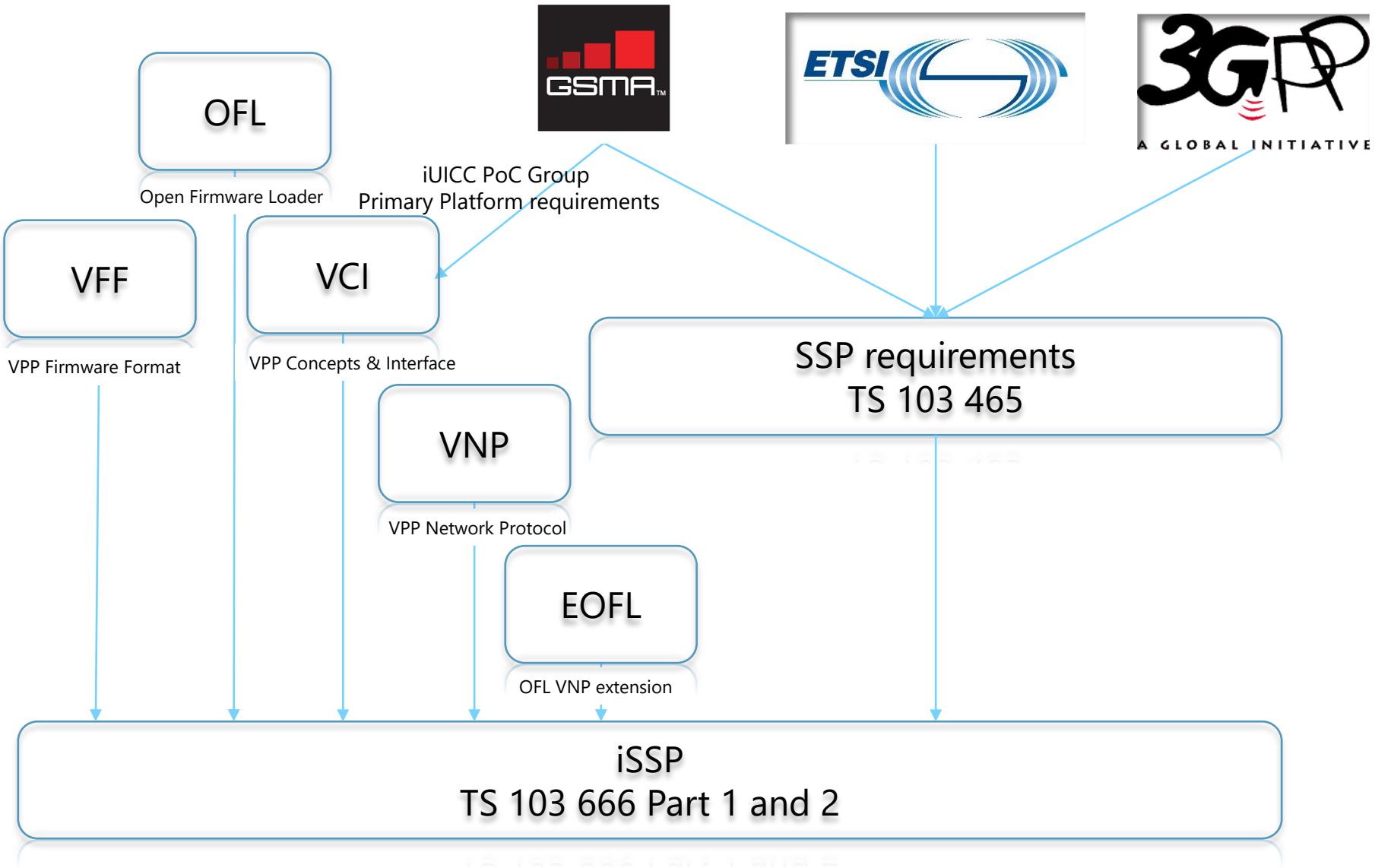
ISO 7816 interfaces was getting old and unsuitable with the requirements of modern interface then leading to:

- Suppress the possible interlocks due to basic command/response principle
- Support of simultaneous and independent channels of communication.
- Suppress of the limitations in offering:
- Any Number of parameters in the command
- Any types of the parameters (scalars and objects).
- Any length of messages
- Support of stream (endless message).
- Capability to support any presentation layers.
- The mapping of the new interface on the OSI model.

Some requests came from the 3GPP asking for: A new File System, a timer,…

Subsequent requirements came from the GSMA.

Where are the requirements coming from?



SSP 3 Classes

Integrated SSP (iSSP)

SSP integrated in a SoC including other functions.

Embedded SSP (eSSP)

Standalone and non removable SSP within a device

Removable SSP (rSSP)

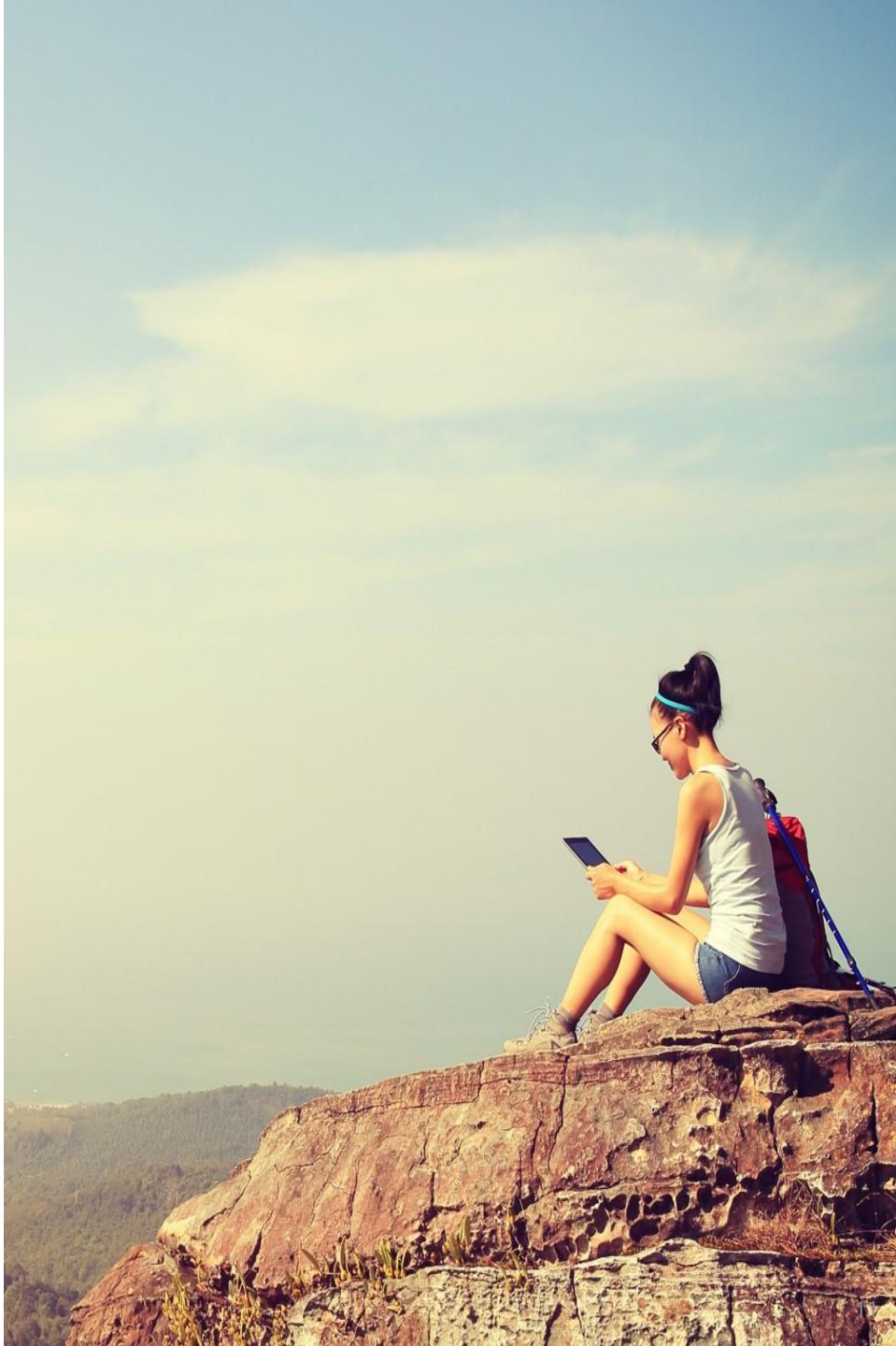
Standalone SSP within a removable card

Today, only OFL and VPP specifications are mandated for the iSSP within the ETSI.

iSSP encapsulates the following GlobalPlatform specifications:

- VPP Concepts and Interfaces [VCI]
- VPP Network Protocol [VNP]
- VPP Firmware Format [VFF]
- VPP-Network Protocol Extension for the Open Firmware Loader [EOFL]
- Open Firmware Loader for Tamper Resistant Element [OFL]

TS 103.666 Part 1 General Characteristics



TS 103.666 Part 1: General Characteristics

TS103.666 Part 1. Provides the general characteristic which are common to a least two classes.

The Part 1 provides the following description:
The SCL (SSP Common Layer)

encapsulating the GlobalPlatform VNP (VPP Network Protocol) specification.

Optional services:

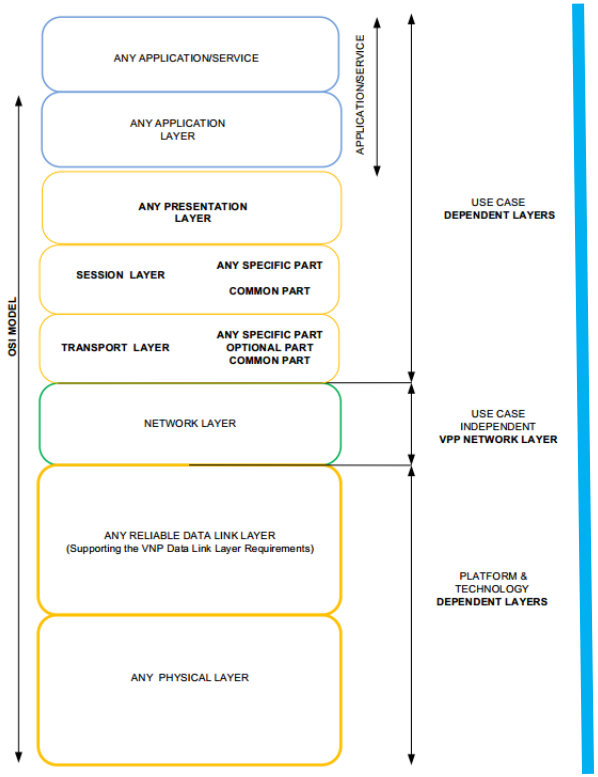
- The legacy ISO7816-4 (APDU) interface
- TCP service
- UDP service
- CRON service: timer/wakeup
- NFC services
- Encapsulation of GP VPP Network Protocol
- Enhanced File System canceling the limitations of the legacy smart cards
- Accessor Authentication service allowing multiple accessors

A product implementing the SSP Part 1 may be sized according to the use case to cover. Most of the services are independent.

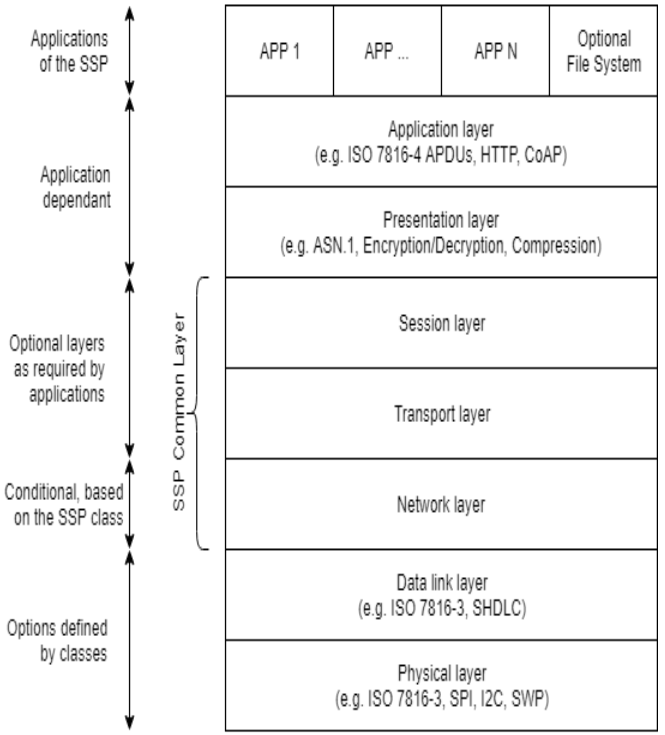
SCL Protocol Stack

- Network Layer
  - Defined by VNP specification
- Data Link Layer
  - Must support requirements specified by VNP
- Transport Layer
  - VNP defines message encapsulation & fragmentation
- Session Layer
  - Must be based on Pipe Session defined by VNP

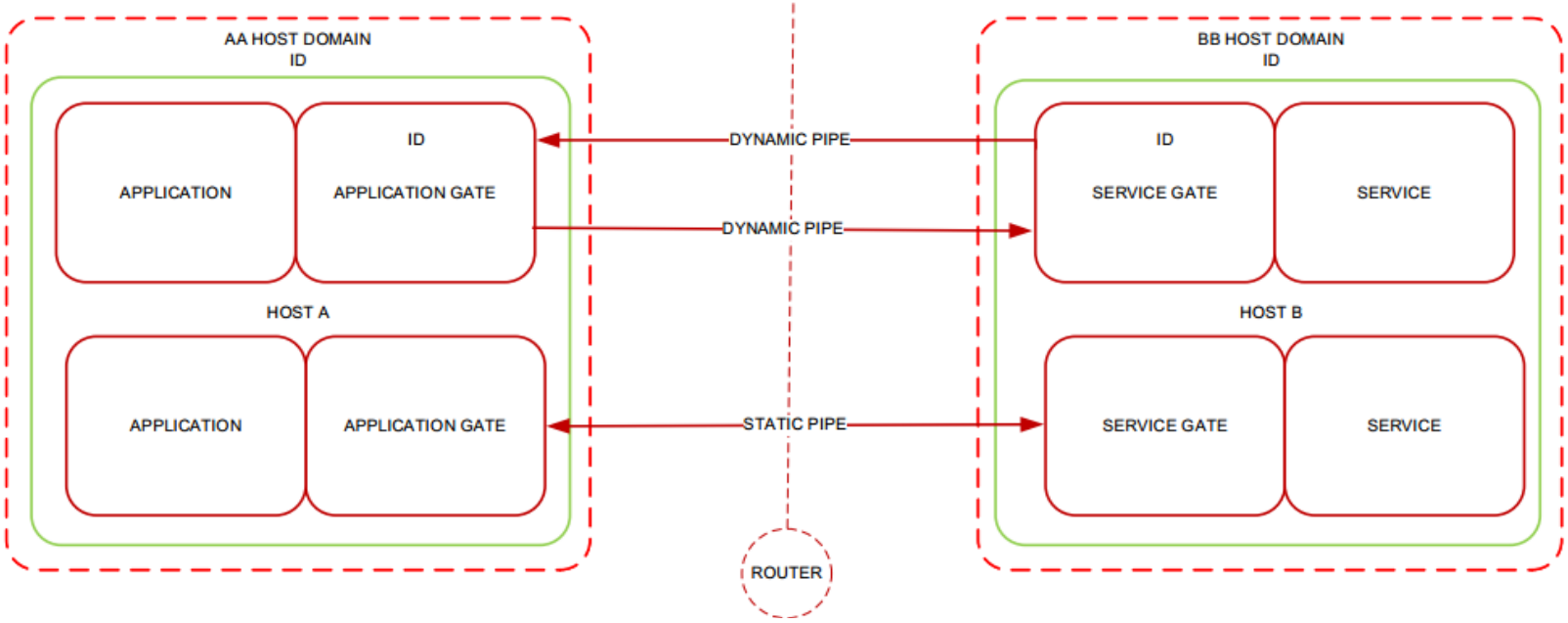
GlobalPlatform



ETSI



A Valid Network

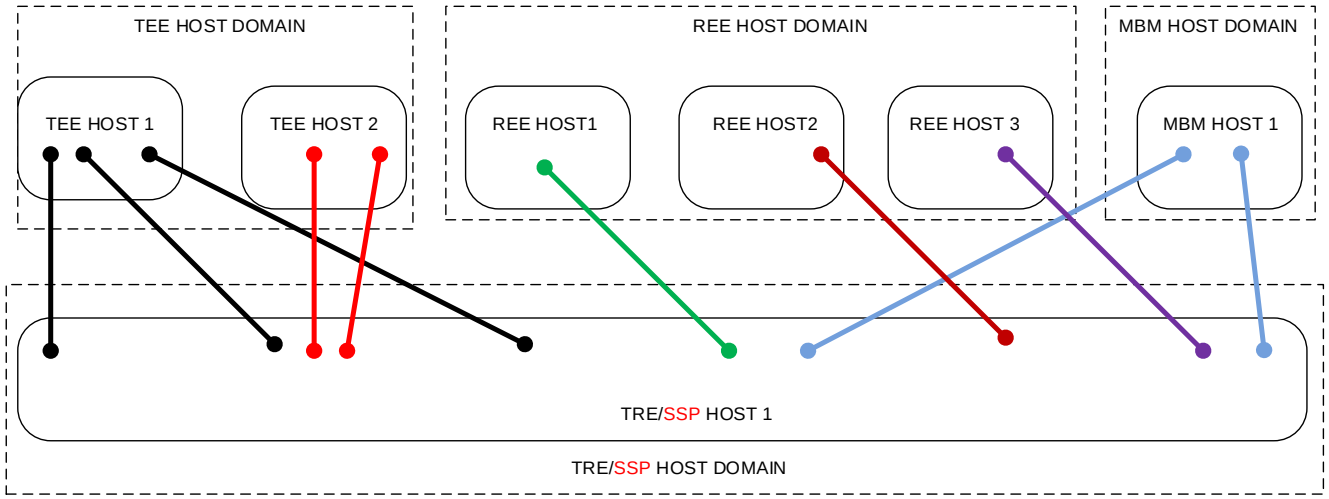


The following rules shall apply to Pipes:

- A Pipe may route Packets between two Gates located in two Hosts in two different Host Domains; and
- A Dynamic Pipe may only route Packets between two Gates sharing the same Gate Identifier.

The Gate may either interface with an Application or a Service. A Service provides a function and an Application consumes the function.

Example of Network



In red: ETSI terminology

Example of Service

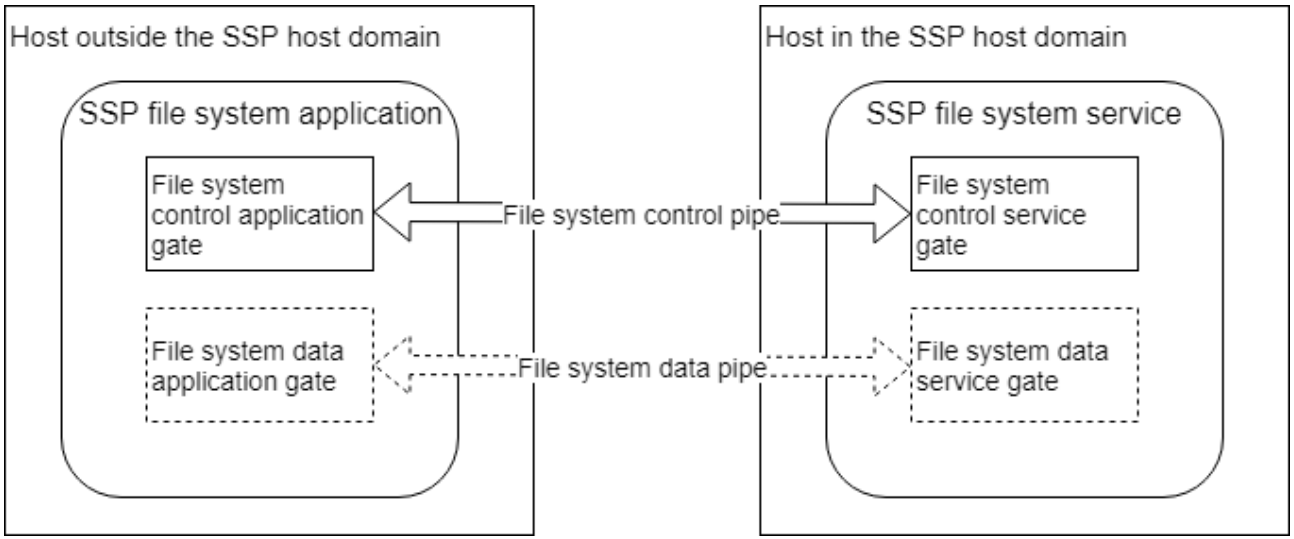
File System Control/Data service gate

The SSP file system may be accessed by entities outside the SSP using the SSP file system service over the SCL protocol.

The SSP file system service resides in an SCL host in the SSP host domain and shall contain a single file system control service gate.

The SSP file system application resides in an SCL host outside the SSP host domain and shall contain a single file system control application gate.

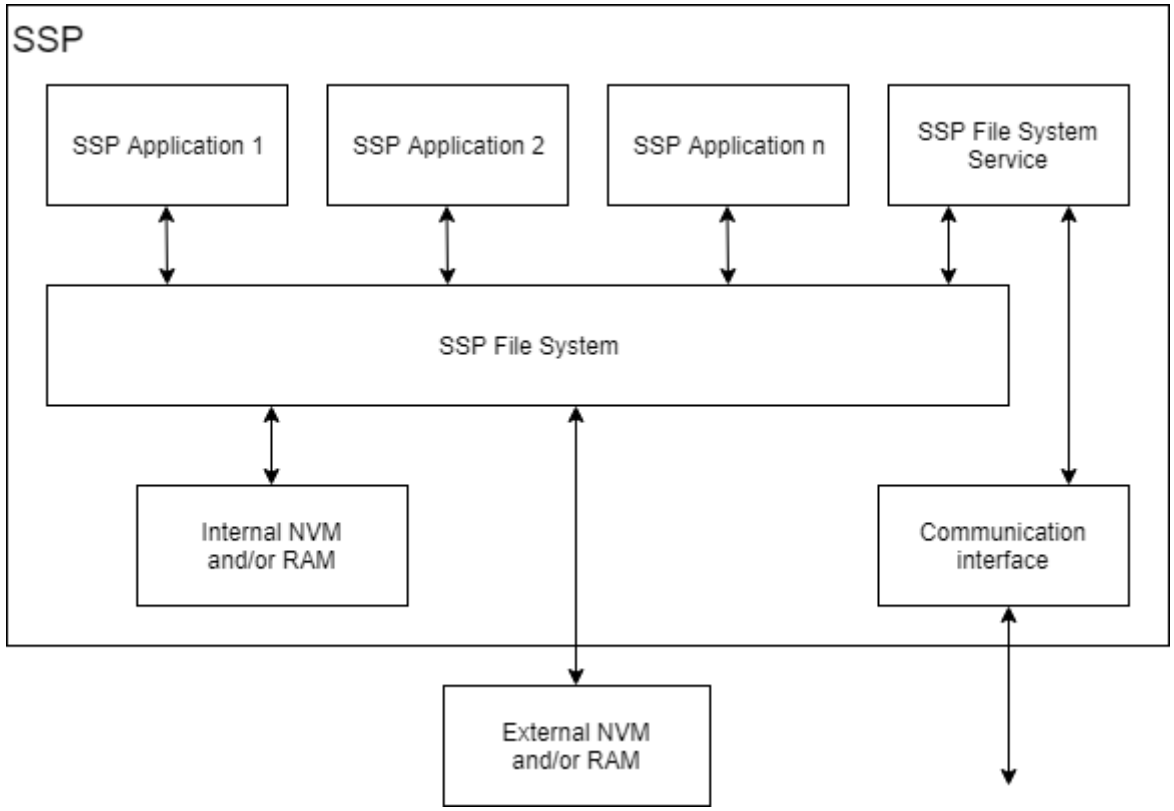
Both the SSP file system application and the SSP file system service may contain multiple file system data application/service gates.



SSP File System

The SSP file system is an organization of data and metadata on an SSP providing storage capabilities.

The SSP file system includes a metadata description of the data organization and a list of commands to access and manage data storage. The SSP file system provides an access control mechanism to restrict access to the stored data.



SSP File System Nodes

Node types

The following node types are defined:

- SSP directory: an SSP directory is a particular node that contains the list of references to other nodes. It contains also a reference to the parent directory. There are two types of directories:
- SSP directory: it conforms to the above SSP directory definition.
- SSP root directory: it conforms to the SSP directory definition but does not contain any reference to the parent file object. The SSP file system shall contain only one SSP root directory.
- SSP file: an SSP file is a sequence of data bytes.
- SSP link: an SSP link contains a link to an SSP file.

Node descriptor

The SSP file system shall allocate a node descriptor per node, containing the following data:

- the node name and/or the short node name.
- the node type.
- the size of the content (only for SSP files).
- the access control list (ACL).
- additional metadata (e.g. proprietary information).

SSP File System commands

The administrative commands are:

- FS-ADMIN-GET-CAPABILITIES-Service-Command: Get the capabilities of the SSP File System.
- FS-ADMIN-CREATE-NODE-Service-Command: Create a Node.
- FS-ADMIN-DELETE-NODE-Service-Command: Delete a Node
- FS-ADMIN-UPDATE-NODE-ATTRIBUTES-Service-Command: Update the access controls and the metadata of a node

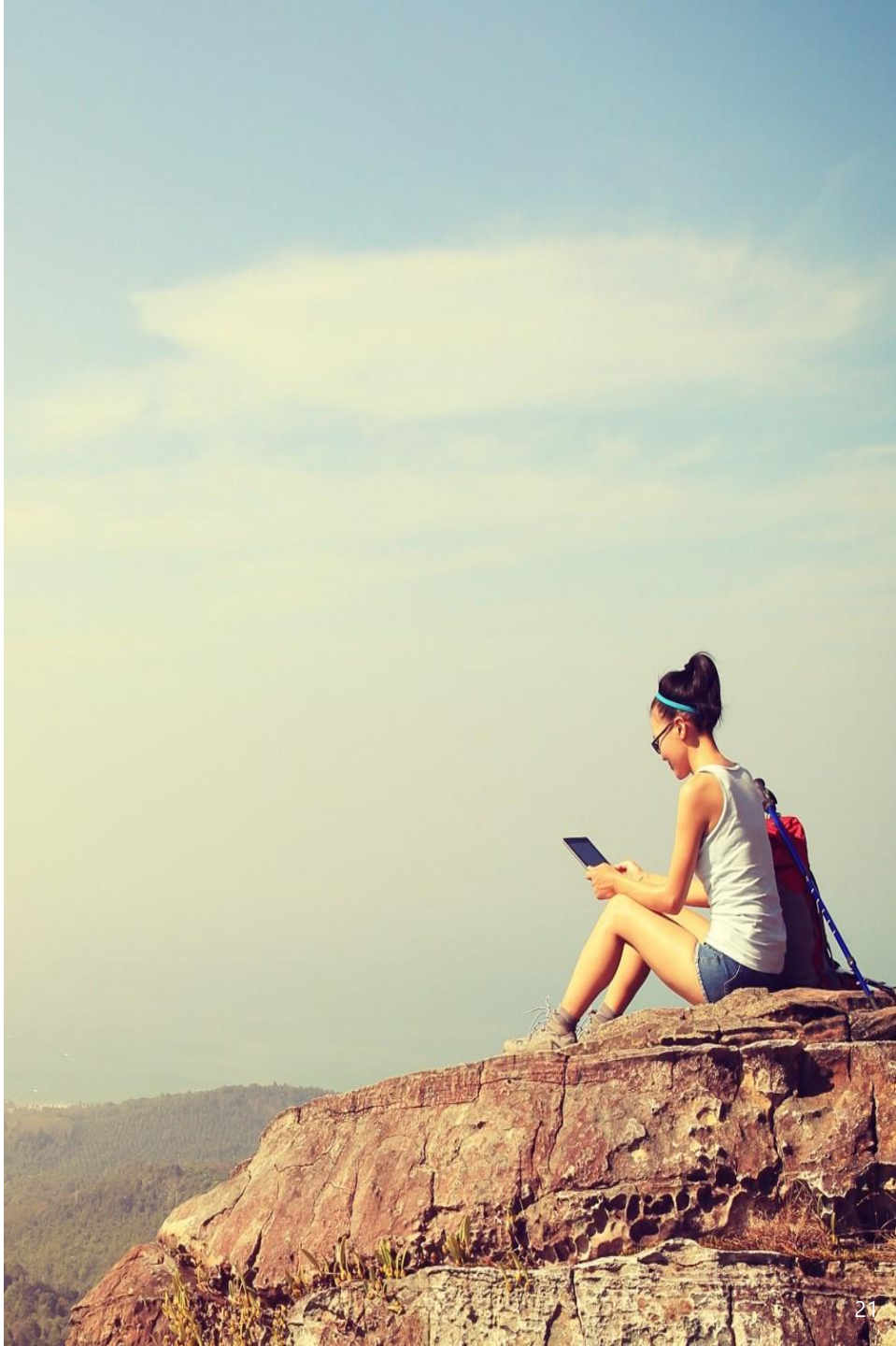
The operational commands are:

- FS-OP-GET-INFO-Service-Command: Read the information about an SSP file or an SSP directory (list of Nodes)
- FS-OP-FILE-OPEN-Service-Command: Open a file session on a specified SSP file. Flat addressing capable.
- FS-OP-FILE-CLOSE-Service-Command: Close a file session
- FS-OP-FILE-GET-POSITION-Service-Command: Retrieve the current offset position in an SSP file that was previously opened: FS-OP-FILE-READ-Service-Command
- Read data into an SSP file (any length): Data read from File System Data service gate over a stream.
- FS-OP-FILE-WRITE-Service-Command: Write data into an SSP file (any length). Data read from File System Data service gate over a stream.

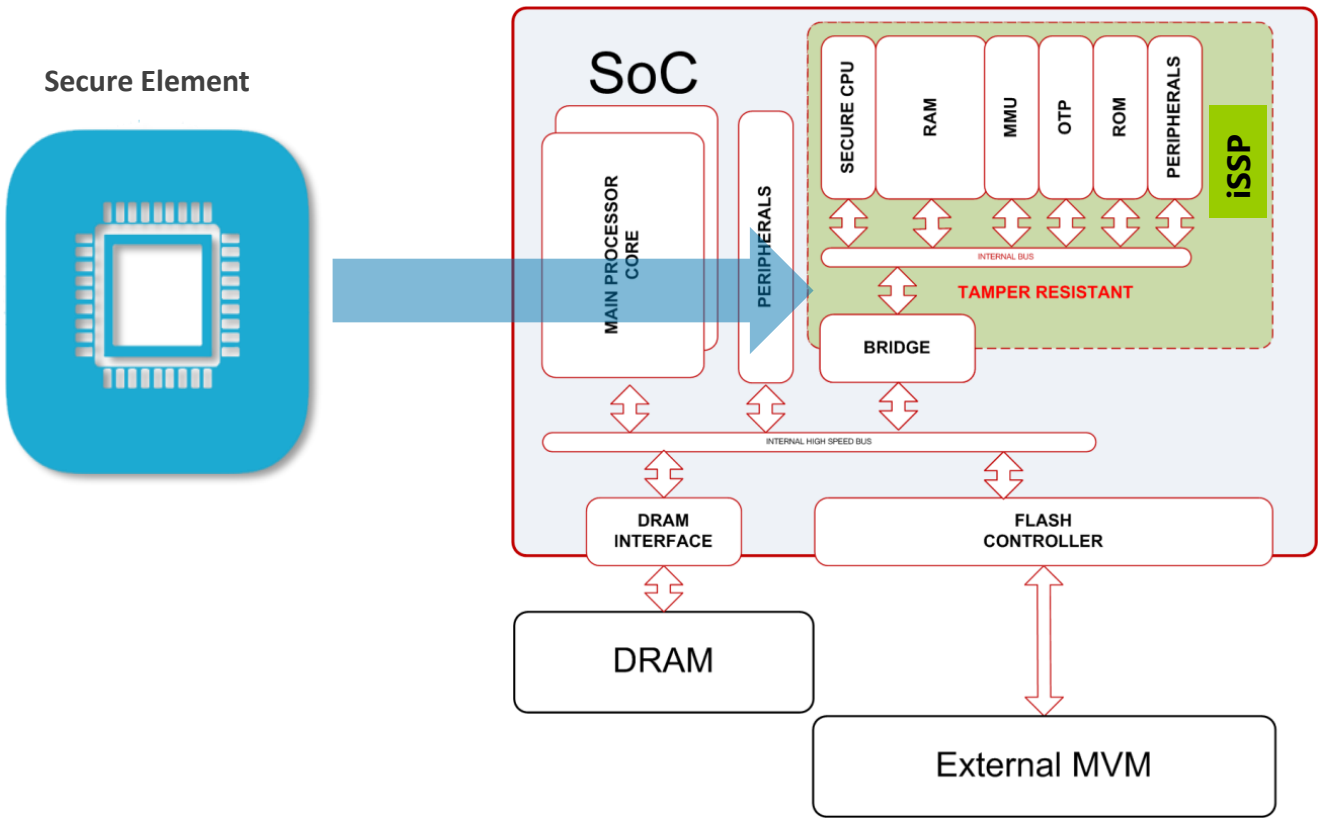
TS 103.666 Part 2:

Integrated SSP

- **VCI:VPP Concepts and Interfaces**
- **External Interfaces: based on OFL 1.3**
- **VFF: VPP Firmware Format**

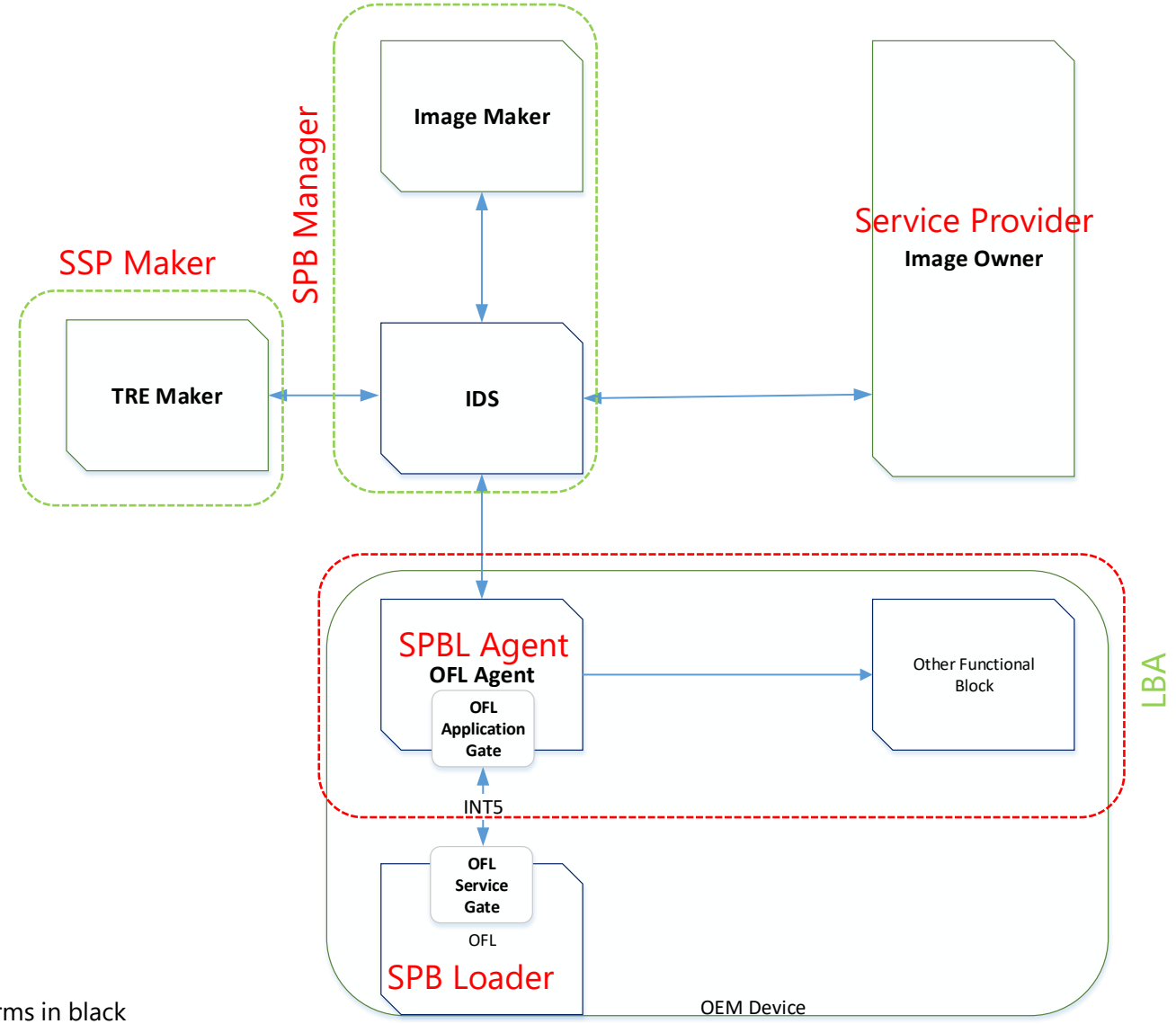


Example of a SSP integrated in a SoC (iSSP)



iUICC is an iSPP hosting supporting a least a 3GPP application

External Interfaces: The Actors/Functions Interfaces



ETSI terms in red
GlobalPlatform terms in black

Challenges of an integrated SSP on the ecosystem

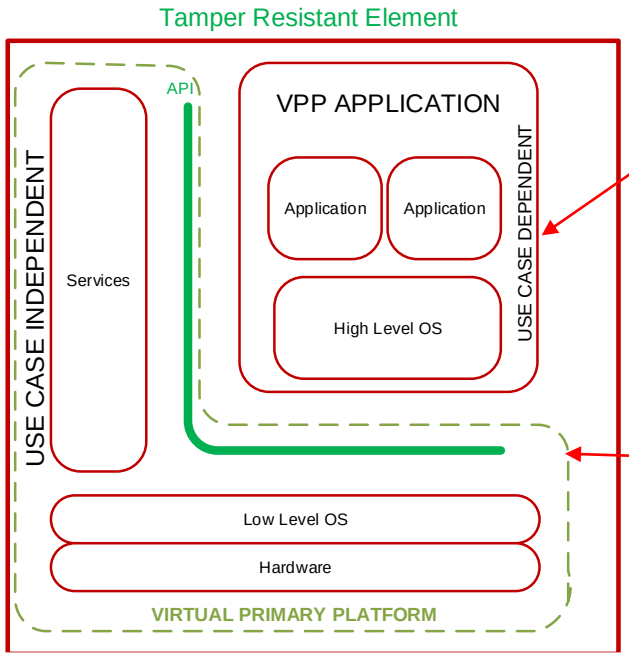
Fragmentation: There will be many different (bigger and smaller) SoC makers providing an integrated SSP based on diverging Primary Platform concepts.

Time to Market / Cost: Such fragmentation will increase the porting, validation and deployment efforts to support all different Primary Platforms.

Liability and Ownership: The iSSP on the SoC is supplied by the SoC Manufacturer directly to the Device OEMs, whereas Service Providers may want to source (and update) their own Operating System from their favorite providers.

Portability: Service Providers may want to use their Operating System on all the secure Primary Platforms in order to get an homogenous installed base.

The concept of Virtual Primary Platform by GlobalPlatform



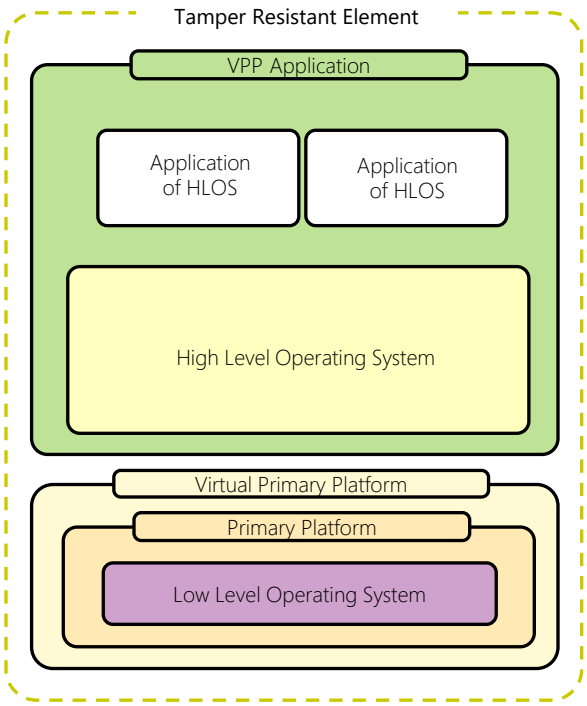
VPP Application:
A High Level OS and its applications.

VIRTUAL PRIMARY PLATFORM (VPP)
PRIMARY PLATFORM as seen from the VPP Application making all Primary Platforms virtually equivalent

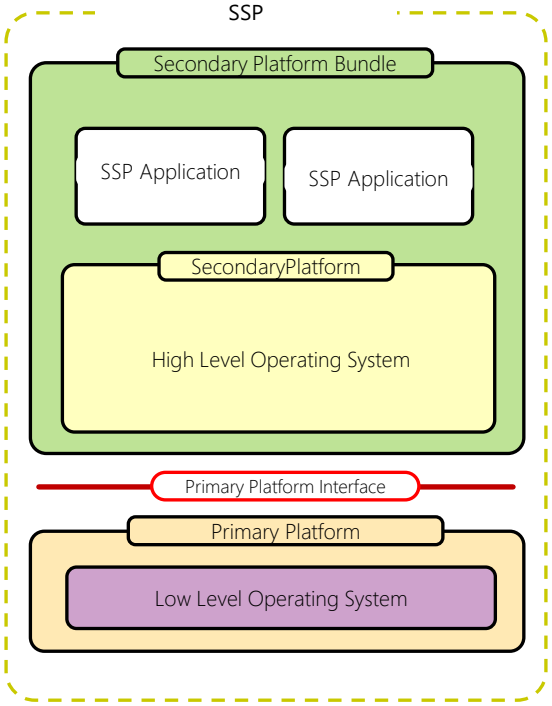
PRIMARY PLATFORM provided by TRE Maker, contains Hardware, Services and Low Level OS with **multi-processing** support

Terminology for GP and ETSI

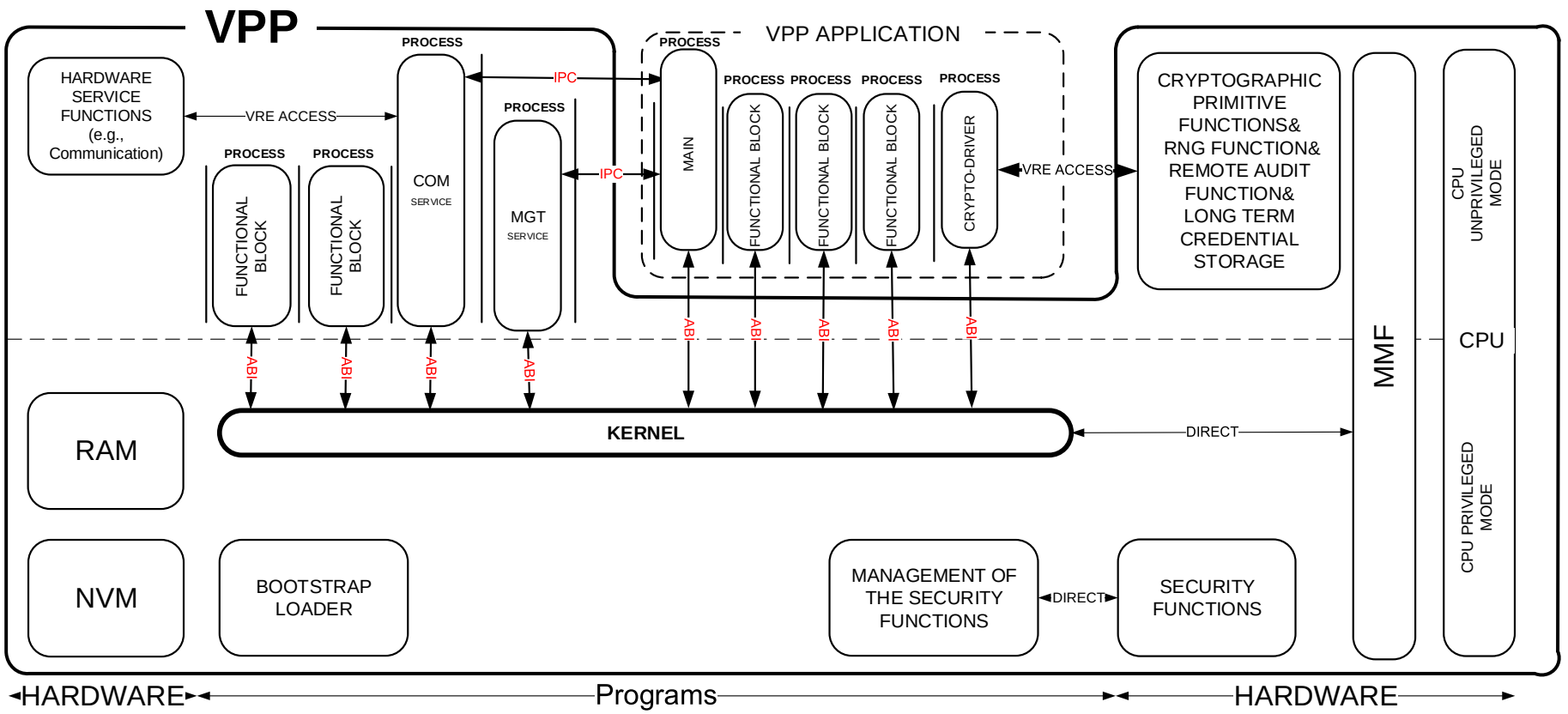
GSMA iUICC PoC & GlobalPlatform



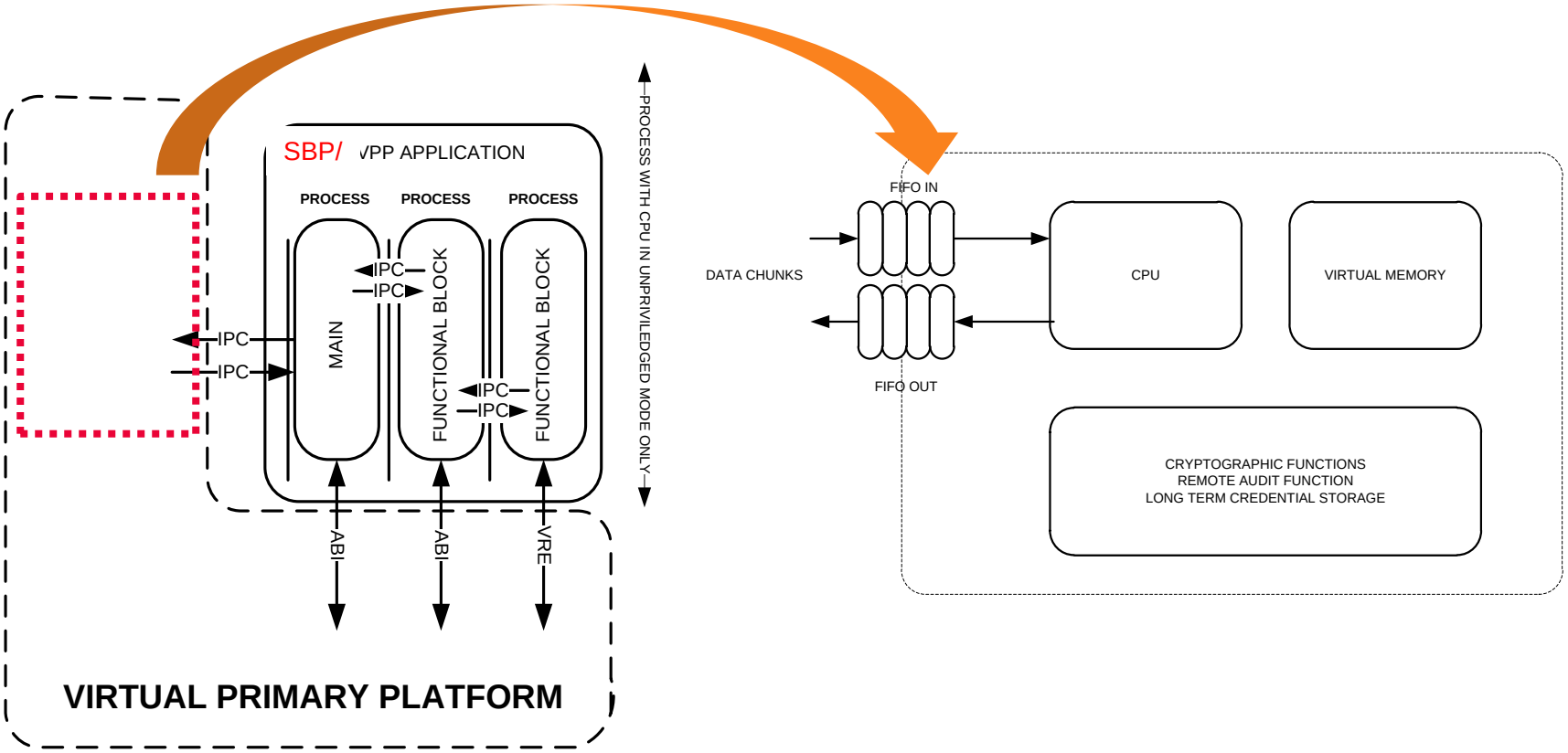
ETSI SCP "SSP"



Runtime View



View from VPP Application/SPB

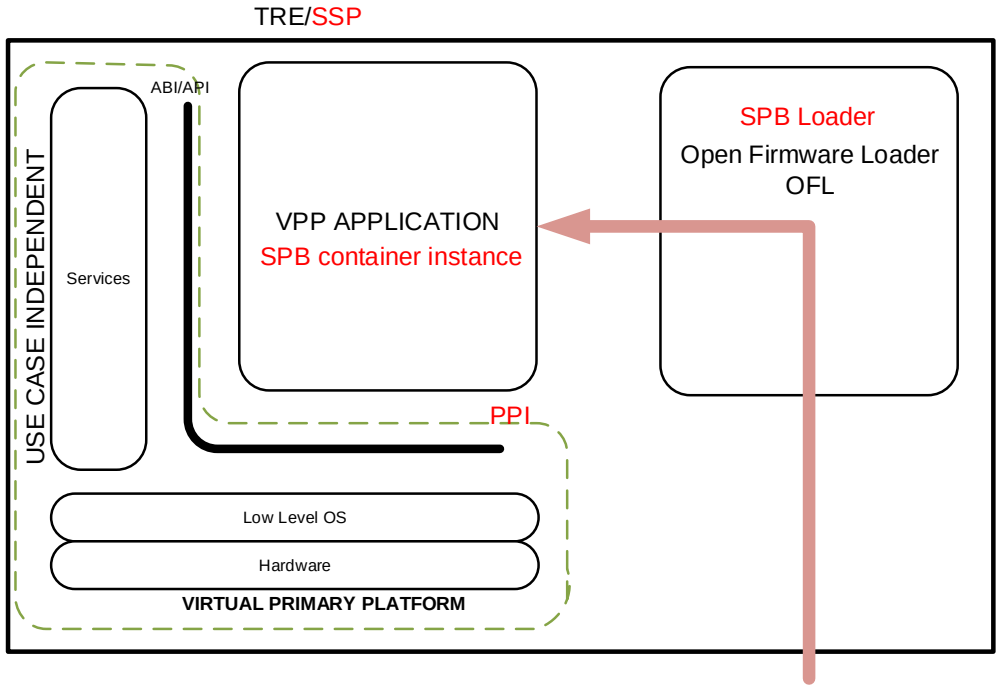


Multiple SSP bundles running sequentially

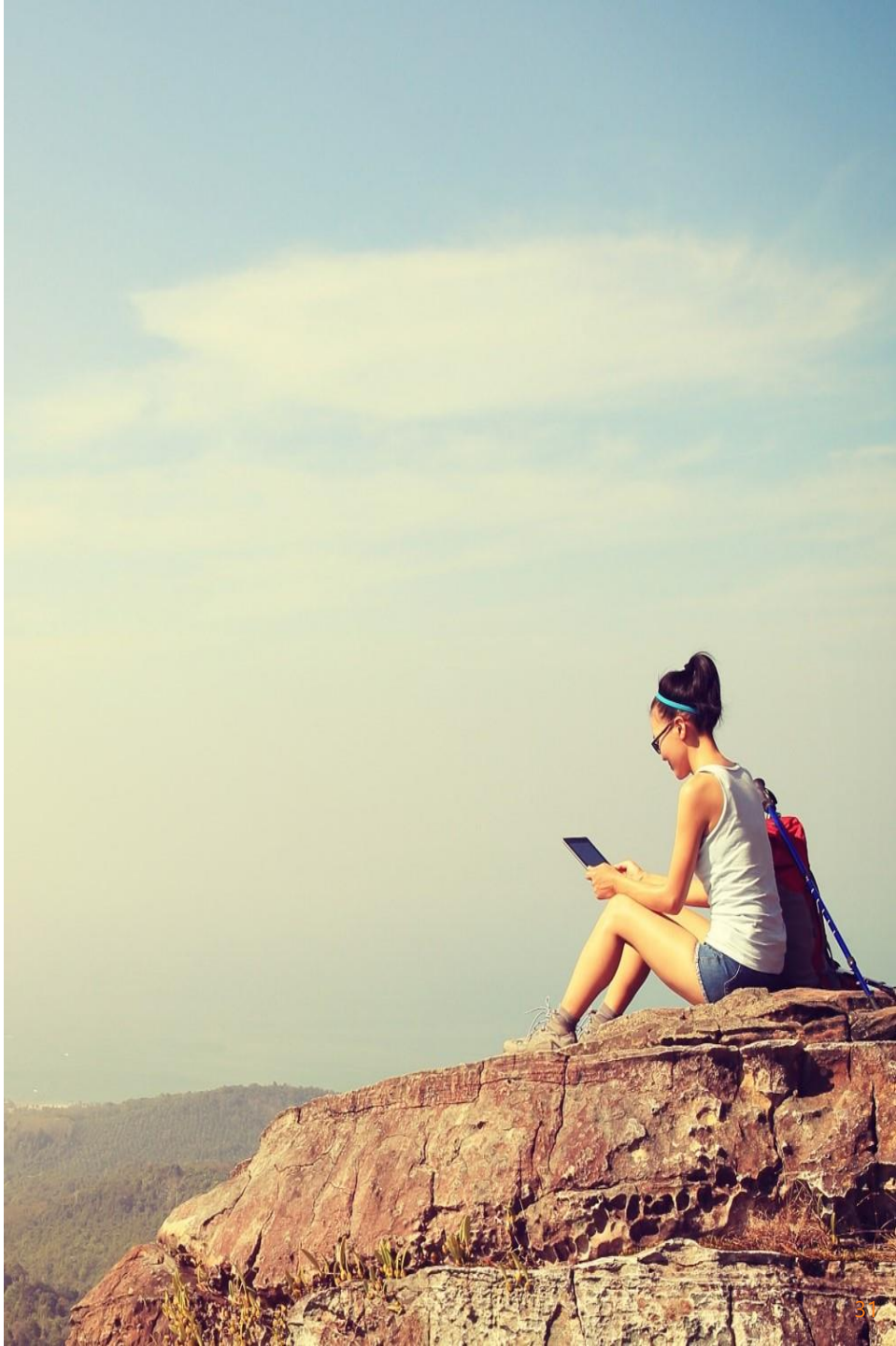
Multiple bundles/VPP applications can exist on the same VPP without interference.

OFL/SPB Loader is an enabler for the VPP/iSSP ecosystem

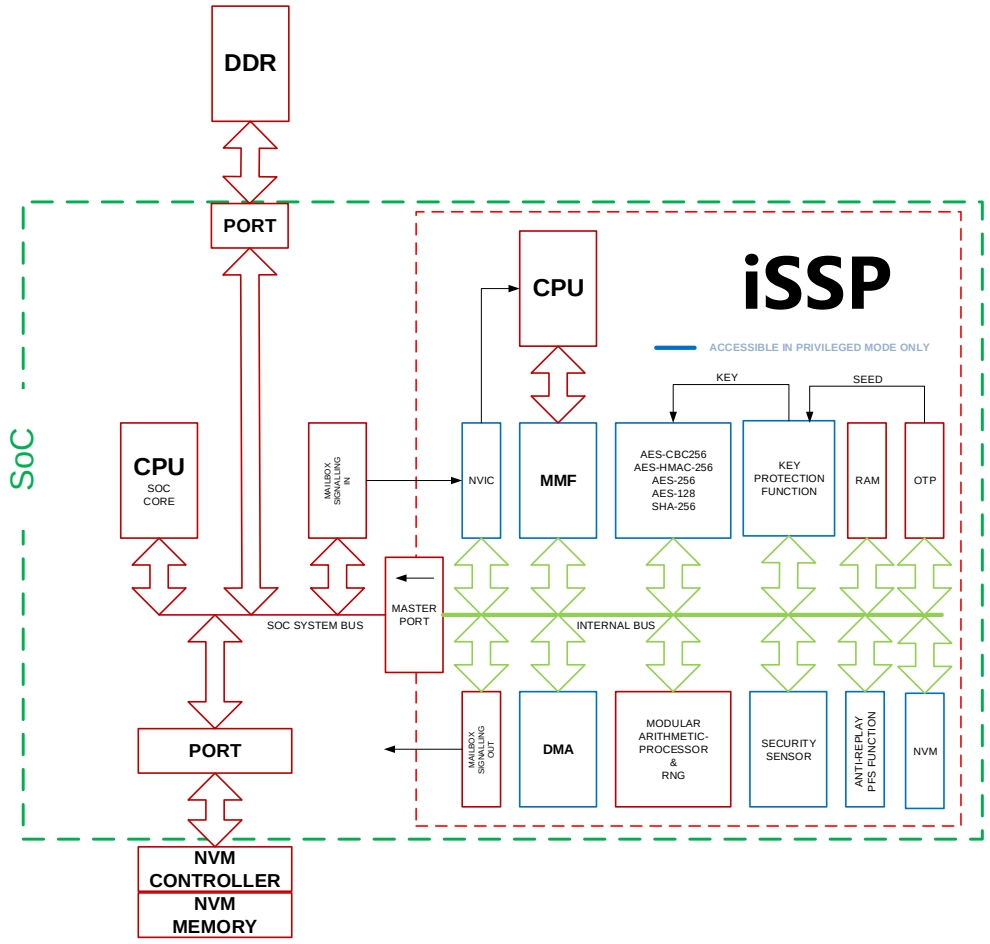
The Open Firmware Loader (OFL) is in charge of extracting the Firmware from an OFL Image and to install it into the TRE/iSSP.



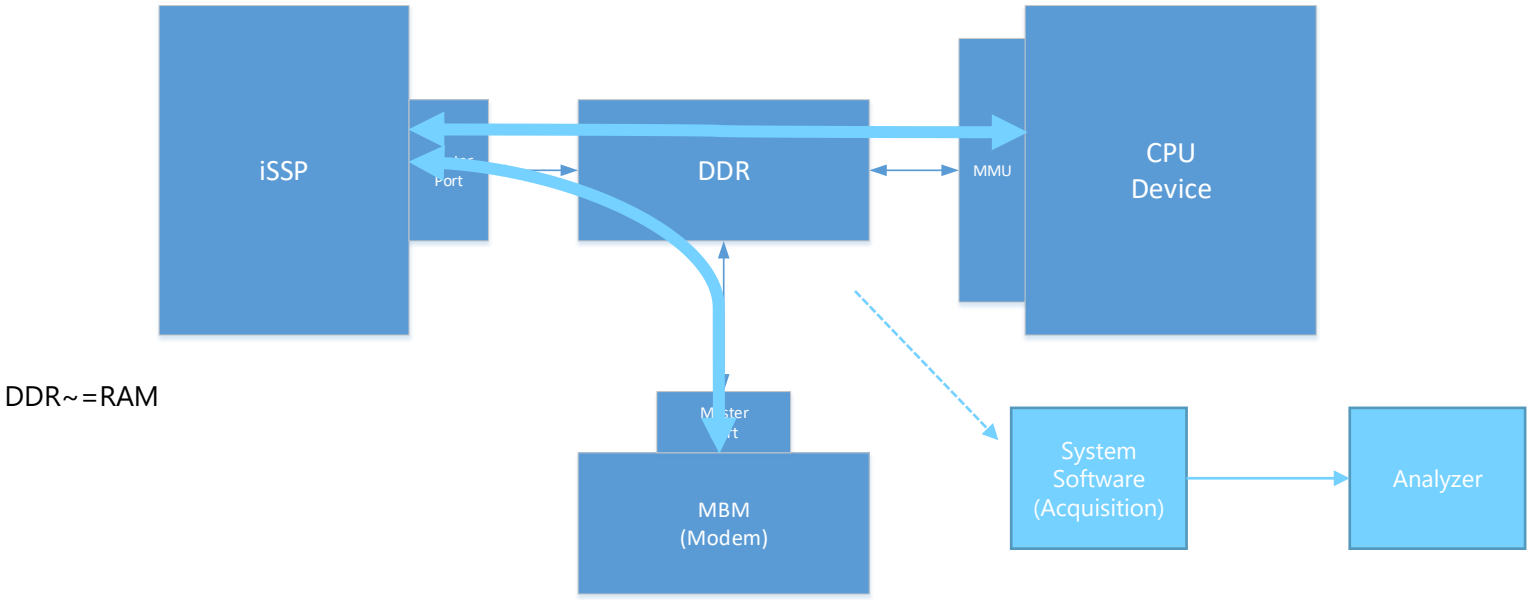
SSP Test Environment



Can we access the iSSP data?

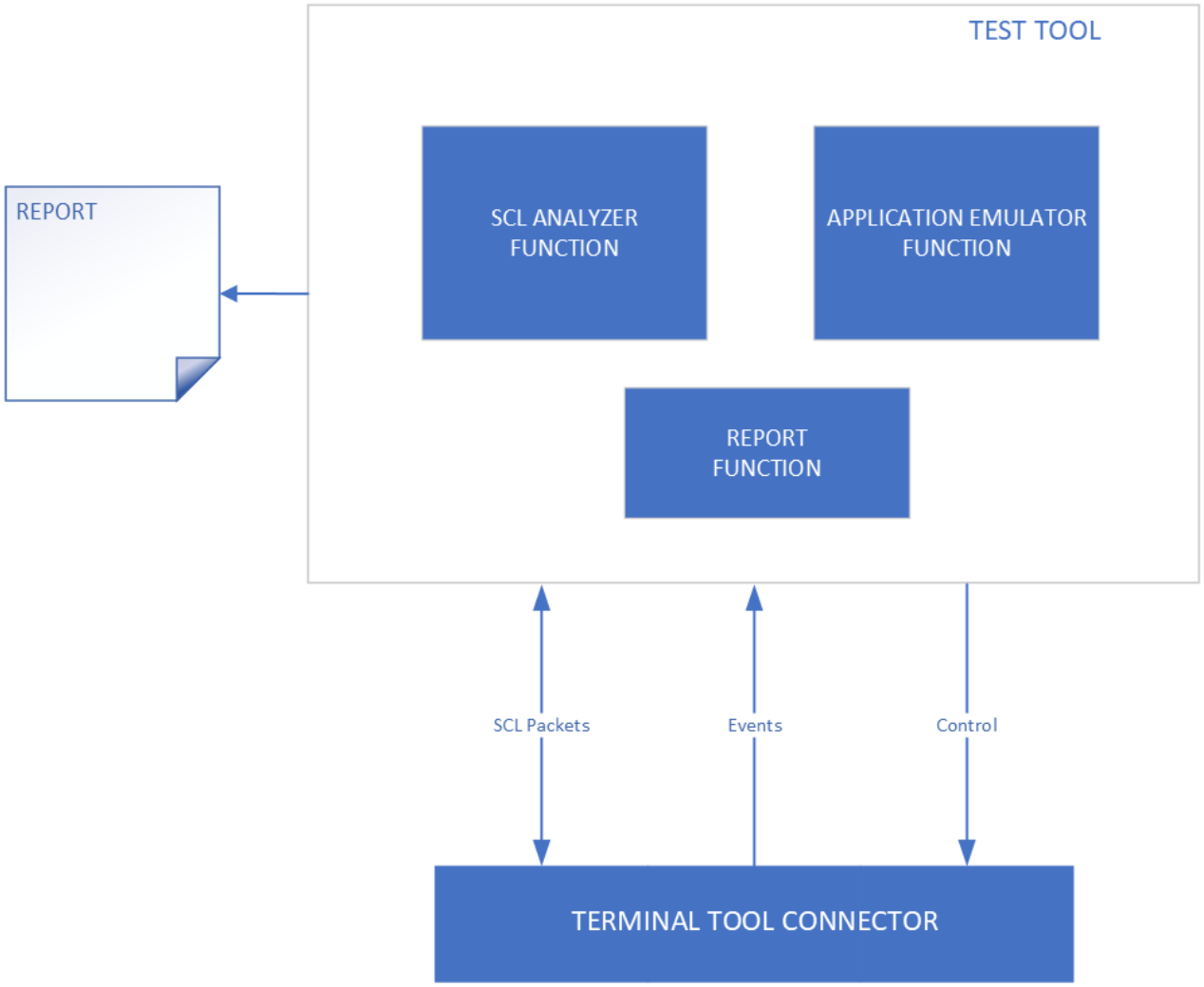


iSSP data flow observer



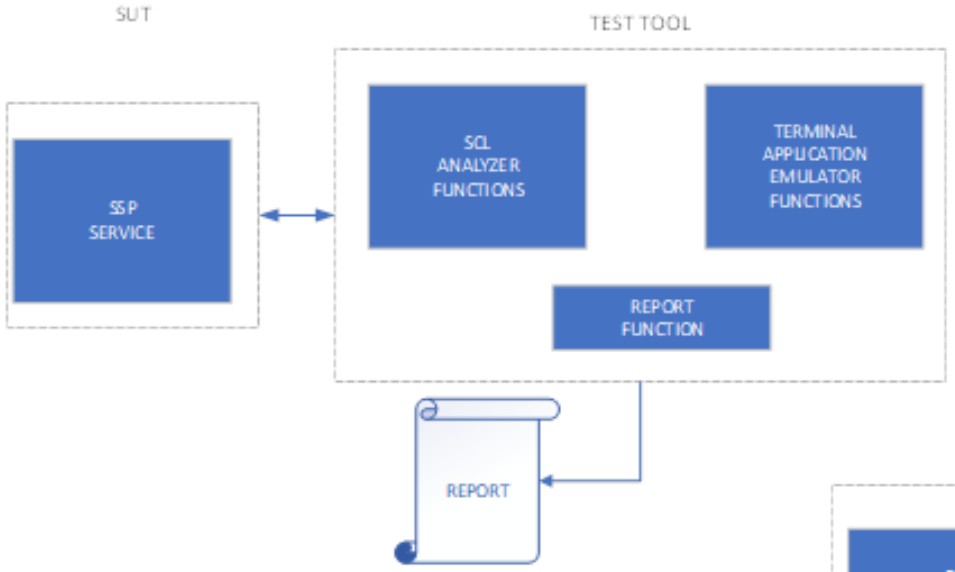
- Pipes are logical routes conveying data chunks containing Packets. By reading the DDR, the SCL packets can be acquired then be copied to the test tool.
- The device/terminal maker shall prepare the device for tests in implementing a system software able to acquire the SCL packets from the memory (DDR).

Test Tool Environment

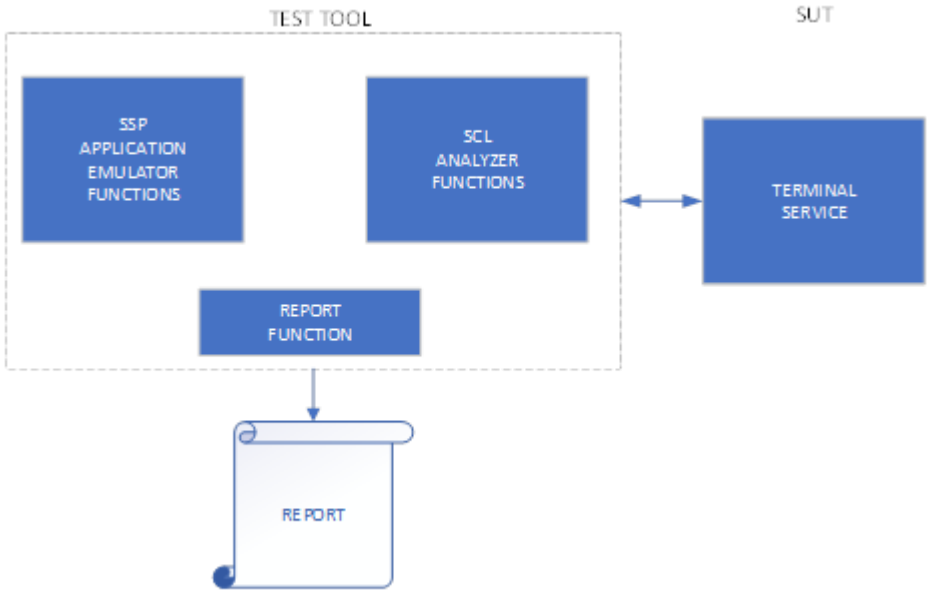


Two configurations

Test of a service in the SSP



Test of a service in the terminal



Example of usual test (not TDL based)

Test identification	AAS_0044
Test objectives	The Accessor Authentication application shall be able to authenticate an accessor from the Accessor Authentication service using an aAAS-OP-AUTHENTICATE-ACCESSOR-Service-Command. The test is successful if the authentication is failed.
Configuration reference	CAAS_003

Initial conditions

The following tests shall be successfully executed:

- AAS_0041. The TEST-1 accessor is created
- AAS_0042. A pipe session is opened with the TEST-1 Accessor Authentication Service gate.

Test sequence

Step	Description	Requirements

1	AAA gate sends aAAS-0044-command-01 command to AAS gate with:
	`-- ASN1START`
	`aAAS-0044-command-01 AAS-CONTROL-SERVICE-GATE-Commands ::= aAAS-OP-AUTHENTICATE-ACCESSOR-Service-Command : {`
	`  aCredential aPinNumericCredential : "1235"`
	`}`
	`-- ASN1STOP`	

2	AAS gate sends an aAAS-0044-response-01 response to AAA gate with:
	`-- ASN1START`
	`aAAS-0044-response-01 AAS-CONTROL-SERVICE-GATE-Responses ::= aAAS-OP-AUTHENTICATE-ACCESSOR-Service-Response : {`
	`  aAAS-Service-Response eAAS-NOT-AUTHENTICATED,`
	`  aParameter aCredentialsStatus : {`
	`  aPinNumericStatus {`
	`  aCommonStatus {`
	`  aIsDisabled FALSE,`
	`  aRemainingAttempts 2`
	`  }}}}`
	`-- ASN1STOP`
	The test is successful if the aAAS-Service-Response is eAAS-NOT-AUTHENTICATED.
		RQ0613_137
		RQ0613_141

TDL: Test Purpose Example

```
//Structured test objective specifications
Package objectives {
    import all from AAS_DOMAIN;
    import all from AAS_DATA;
    Test Purpose {
        TP Id TP_CREATION_ACCESSOR_OK
        Test objective "Valid Creation of an Accessor."
        PICS Selection ACCESSOR_CREATION_OK
        Expected behaviour
        ensure that {
            when {
                the AAA entity sends the aAAS_ADMIN_CREATE_ACCESSOR_Service_Command  containing aAccessor_OK ;
            } then {
                the AAS entity sends the aAAS_ADMIN_CREATE_ACCESSOR_Service_Response containing eAAS_OK;
            }
        }
    }
    Test Purpose {
        TP Id TP_CREATION_ACCESSOR_NOK
        Test objective "Invalid creation of an Accessor."
        PICS Selection ACCESSOR_CREATION_NOK
        Expected behaviour
        ensure that {
            when {
                the AAA entity sends the aAAS_ADMIN_CREATE_ACCESSOR_Service_Command containing aAccessor_E_OK ;
            } then {
                the AAS entity sends the aAAS_ADMIN_CREATE_ACCESSOR_Service_Response containing eAAS_E_NOK;
            }
        }
    }
```

TDL: Test Description Example

```
//Creation an instance of AAS_ADMIN_CREATE_ACCESSOR_Service_Command

AAS_ADMIN_CREATE_ACCESSOR_Service_Command aAAS_ADMIN_CREATE_ACCESSOR_Service_Command (
    aAccessor=_aAccessor,  // Accessor to be created
    aCredential=_aAccessorCredentials,  // Credentials for the accessor
    aCredentialsPolicy=_aAccessorCredentialsPolicy   // Policy for the provided accessors
) with  {Note AAS_ADMIN_CREATE_ACCESSOR_Service_Command_Type_Creation : "Creation an instance of AAS_ADMIN_CREATE_ACCESSOR_Service_Command";};



Test Description AAS_TD_CREATE_01 uses configuration AAS_TC_001
{
    //Pre_conditions and preamble from the source document
perform action preambles with {PREAMBLE;};
perform action preConditions with {PRECONDITION;};

//Open a session between AAS and AAA
//---------------------------------
execute ADM_TD_BIND_01(pipe_application= PIPE_AAA,serviceId=accessor_sut) with {
STEP:"Preamble";
PROCEDURE: "Binding of the AAA and the AAS";
};

//Test sequence
AAA.g sends aAAS_ADMIN_CREATE_ACCESSOR_Service_Command to AAS.g with {
STEP : "1" ;
PROCEDURE : "AAA transmits a AAS_ADMIN_CREATE_ACCESSOR_Service_Command to AAS " ;
} ;


alternatively {
      AAS.g sends aAAS_ADMIN_CREATE_ACCESSOR_Service_Response(status =eAAS_OK)  to AAA.g with {
       STEP : "2" ;
          PROCEDURE : "Check: Does the AAS transmit an
          eAAS_OK to AAA?" ;
       test objectives : AAS_TP1 ;
          } ;
      set verdict to PASS ;
   }
or
   {
```

THANK YOU

This presentation has been created from the ETSI SCP presentations