OSCAR FUNCTIONAL SCOPE

1 Introduction

This document describes the functional scope of OSCar implementation for the phase 2 of the OSCar project.

The success of the field trial for this phase is to be considered as a green light to deploy OSCar solutions at commercial level.

The OSCar projects main objectives are as follows:

- To prove that POIs, based on SEPA FAST and EPAS Acquirer Systems, work together,
- To set up the OSCar scheme Evaluation and Certification Infrastructure and show that it works,
- To prove the interoperability between all POI and all Acquirers implementing the EPAS Acquirer Protocol

2 Scope of the OSCar Project

An OSCar infrastructure is made up of a standalone or an integrated POI system communicating with:

- one or several Acquirer host(s) to process a card payment transaction,
- a Terminal Management System host for management functions, e.g. parameter download,
- a sale system.

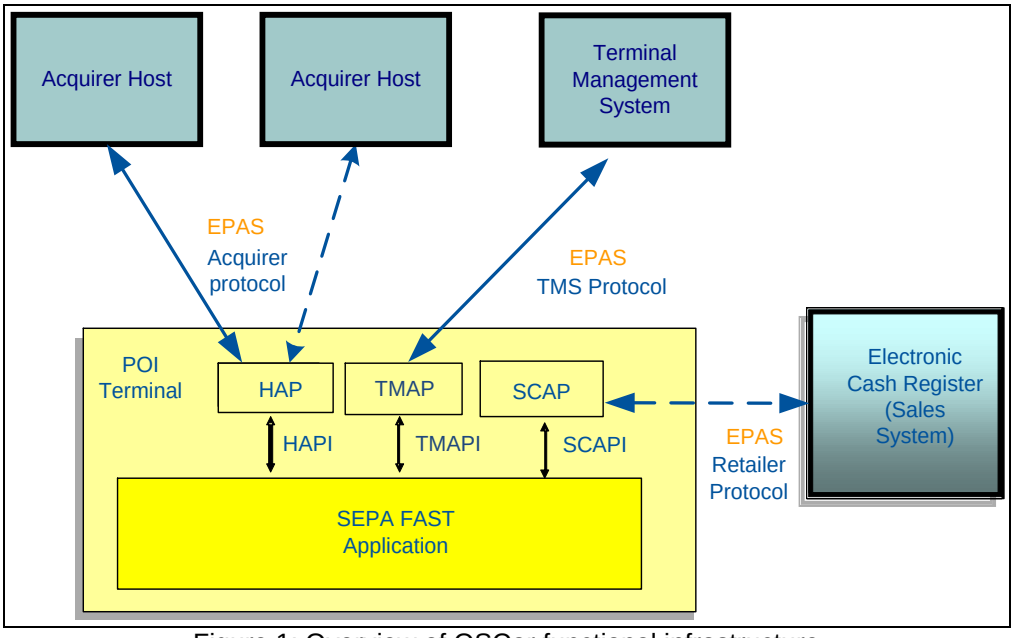

Figure 1: Overview of OSCar functional infrastructure

Note: Acquirer Host and Terminal Management System may exist on one physical host system. The dashed communication lines are mandatory for the POI test environment (except for the sales system). For the operational use of the POI the dashed communication lines are optional.

An OSCar POI terminal has to support (with limitations described below):

- A SEPA-FAST Application,

- An interface to the Host Acquirer Protocol responsible for handling the EPAS Acquirer protocol
- An interface to the Terminal Manager responsible for handling the TMS protocol,
- Connections to at least one Acquirer host in the operational environment. However the POI shall support a multi acquirer environment. The multi acquirer functionality is in scope of the OSCar test requirements,
- Connection to one TMS host for at least the purpose of OSCar parameters download,
- Cryptographic mechanisms described below,
- Optionnally, an interface to the sales system responsible for handling the EPAS retailer protocol,

An acquirer participating in the OSCar project has to support (with limitations described below):

- The EPAS Acquirer protocol,
- The cryptographic mechanisms described below,
- The TMS protocol if the acquirer is the terminal manager as well.

A Terminal Manager participating in the OSCar project has to support (with limitations described below):

- The TMS protocol
- The cryptographic mechanisms described below

2.1 POI Functional Scope

Deliver an OSCar POI in both attended and unattended environments, either as a standalone POI or as an integrated POI (up to participating vendors).

The POI shall support all the functionalities included in the scope below.

When the functionality is optional, it is clearly indicated.

2.1.1 Reference Documents

[SEPA-FAST], [EPAS RTP], [CAPE TMS MDR], [CAPE TMS MUG], [CAPE ACQ MDR], [CAPE ACQ MUG], [OIS], [VOL]

2.1.2 Card services and additional features

In scope:

- Payment,
- Cancellation,
- Refund,
- Payment with Increased Amount,
- Payment with Cashback,
- Voice Authorisation,
- Deferred Payment[1]

Out of scope:

- Cash advance
- Pre-Authorisation services,

The vendor may decide to develop a solution integrating all the services in the scope and he may develop all services except the Deferred Payment service which is used only in the petrol environment.

2.1.3 Acceptance technology

The vendor may decide to develop an application for ‘Chip only” terminal. He may decide also to develop the contact technology without the contactless technology or vice versa.

If the Contactless Technology is implemented, the POI shall support any combination of the 4 contactless kernels supported by the SEPA-FAST application. But it is highly recommended to support all the contactless kernels

The following options are possible:

- Chip with contact EMV,
- Chip contactless EMV (Card and Mobile) ,
- Magnetic Stripe,

[1]Volume definition: A combined service which enables the card acceptor to perform an authorization for a temporary amount and a completion for the final amount within a limited time frame. Deferred Payment is available in attended and unattended environments. This is widely used in the petrol environment.

- Manual Entry.

Or

- Chip with contact EMV,
- Chip contactless EMV (Card and Mobile),

Or

- Chip with contact EMV,

Or

- Chip contactless EMV (Card and Mobile) ,

Or

- Chip with contact EMV,
- Magnetic Stripe,
- Manual Entry.

A POI shall support a Fallback mechanism as described in [SEPA-FAST] in case of a serious error of the used chip application.

2.1.4 Acceptance environments

In scope:

- Attended for cardholder present transactions,
- Unattended for cardholder present transactions

Out of scope:

- Remote transactions.

The vendor may decide to develop a solution integrating the attended and unattended environments and he may develop only one environment: attended or unattended.

The POI Terminal type shall be “2x”

The POI can process transactions offline only, online only and offline/online depending on its configuration.

2.1.5 Cardholder Verification Methods

In scope:

- Online PIN,
- Encrypted offline PIN,
- Plain text offline PIN,
- NO CVM,
- Signature.

2.1.6 Card Authentication Methods

The POI shall support all offline card authentication methods (SDA, DDA, CDA).

2.1.7 EPAS Acquirer Protocol

The EPAS Acquirer Protocol is only supported as far as the services in scope are concerned.

The following modes/configurations of the POI Acquirer Protocol must be supported:

Mode 1:

- Online Authorisation for online transactions,
- Capture immediately after transaction finalisation of an online or offline transaction
- Reconciliation between the acceptor and the acquirer,
- Diagnostic.

Mode 2:

- Online Authorisation for online transactions,
- Capture by a batch transfer for a group of transactions (online and offline)
- Reconciliation between the acceptor and the acquirer,
- Diagnostic.

Mode 3:

- Capture with Authorisation for online transactions,
- Capture immediately after transaction finalisation of offline transactions,
- Reconciliation between the acceptor and the acquirer,
- Diagnostic.

In addition, the following configuration options shall be implemented:

- Support of both protected card data and plain card data is mandatory,
- Message Authentication Code.

The messages and scenarios used are detailed in the technical scope section of [OIS].

2.1.8 EPAS TMS Protocol

The TMS protocol is supported to configure the POI and to download the parameters of the SEPA-FAST Application and the EPAS protocol.

The minimum profiles to be supported are those concerned with the parameter downloading of the SEPA-FAST Application and the EPAS protocol by the POI:

- The message exchange of a Status Report as Request from the POI and a ManagementPlanReplacement as Response from the TMS Host,
- The message exchange of a Status Report as Request from the POI and a AcceptorConfiguration as Response from the TMS Host.

Exchanges used for key download are notmandatory to be implemented in OSCar.

The messages and scenarios used are detailed in the technical scope section of [OIS].

2.1.9 EPAS Retailer Protocol

The use of the Retailer Protocol is optional for functional testing and for operational use.

If used, the Retailer Protocol with its standard profile has to be supported by the POI to communicate with the sale system.

2.1.10 Cryptographic mechanisms & key management

In Scope:

- DUKPT as key derivation mechanism for PIN Encryption, Card Data Encryption and MAC protection,
- The Triple-DES algorithm for PIN and Card Data Encryption,
- Retail-CBC-MAC with SHA-256 for Message Authentication Code (MAC),
- Key download via TMS protocol (optional).

- Key download, requires asymmetric cryptography if implemented. - If the TMS protocol is not used for key download then keys are loaded locally in the POI or by other means.

2.2 Acquirer functional scope

An Acquirer System participating in OSCar shall support all the functionalities included in the scope below.

When the functionality is optional, it is clearly indicated.

If the Acquirer carries out the POI management, he has to use the TMS protocol for this purpose. In this case it has to support the functionalities detailed in the section 2.3 “Terminal Manager Functional Scope”.

2.2.1 Reference Documents

[SEPA-FAST], [CAPE ACQ MDR], [CAPE ACQ MUG], [OIS], [VOL]

2.2.2 Card services and additional features

In scope:

- Payment,
- Cancellation,
- Refund.
- Payment with Increased Amount (TIP),
- Payment with Cashback,
- Voice Authorisation,
- Deferred Payment

The following services are not mandatory to be supported by the acquirer:

- Payment with Increased Amount (TIP),
- Payment with Cashback,
- Deferred Payment

The acquirer configures the POI to activate or deactivate these services..

Out of scope:

- Cash advance
- Pre-Authorisation services

2.2.3 Acceptance technology

In scope:

- Chip with contact EMV,
- Magnetic Stripe,
- Manual Entry.
- Chip contactless EMV (Card and Mobile),

Or

- Chip with contact EMV
- Chip contactless EMV (Card and Mobile),

Or

- Chip with contact EMV,

Or

- Chip contactless EMV (Card and Mobile),

Or

- Chip with contact EMV,
- Magnetic Stripe,
- Manual Entry.

The Acquirer configures the terminal to support an Acceptance technology per profile for the operational use. This means that the acquirer has to support at least one of these acceptance technologies in the operational use.

2.2.4 Acceptance environments

In scope:

- Attended for cardholder present transactions,
- Unattended for cardholder present transactions

Out of scope:

- Remote transactions.

2.2.5 Cardholder Verification Methods

In scope:

- Online PIN (optional),
- Encrypted offline PIN,
- Plain text offline PIN,
- NO CVM,
- Signature.

It is up to the Acquirer to decide to support the online PIN or not. The POI has to be configured consequently.

2.2.6 EPAS Acquirer Protocol

The EPAS Acquirer Protocol is only supported as far as the services in scope are concerned and only with one of the following profiles and options.

The following modes/configurations of the POI Acquirer Protocol are possible

Mode 1:

- Online Authorisation for online transactions,
- Capture immediately after transaction finalisation of an online or offline transaction,
- Reconciliation between the acceptor and the acquirer,
- Diagnostic.

Mode 2:

- Online Authorisation for online transactions,
- Capture by a batch transfer for a group of transactions (online and offline)
- Reconciliation between the acceptor and the acquirer,
- Diagnostic.

Mode 3:

- Capture with Authorisation for online transactions,
- Capture immediately after transaction finalisation of offline transaction
- Reconciliation between the acceptor and the acquirer,
- Diagnostic.

The support of Refund online is optional for the acquirer

2.2.7 Cryptographic mechanisms & key management

In Scope:

- DUKPT as key derivation mechanism for PIN Encryption, Card Data Encryption and MAC protection,
- The Triple-DES algorithm for PIN and Card Data Encryption,
- Retail-CBC-MAC with SHA-256 for Message Authentication Code (MAC),

2.3 Terminal Management functional scope

The Terminal Management System carries out the POI management, andhas to support the functionalities detailed in the scope below. When the functionality is optional, it is clearly indicated.

2.3.1 Reference Documents

[SEPA-FAST], [CAPE TMS MDR], [CAPE TMS MUG], [OIS], [VOL]

2.3.2 EPAS TMS Protocol

The minimum profiles to be supported are those concerned with the parameter downloading of SEPA-FAST Application and the EPAS protocol by the POI:

- The message exchange of a Status Report as Request from the POI and a ManagementPlanReplacement as Response from the TMS Host,
- The message exchange of a Status Report as Request from the POI and a AcceptorConfiguration as Response from the TMS Host.

In addition, the following configuration options shall be implemented:

- Message Authentication Code.

Exchanges used for keys download are not mandatory to be implemented in OSCar.

The messages and scenarios used are detailed in the technical scope section of [OIS].

2.3.3 Cryptographic mechanisms & key management

In Scope:

- DUKPT as Key derivation Mechanism for MAC protection,
- Retail-CBC-MAC with SHA-256 for Message Authentication Code (MAC),
- Key download via TMS protocol (optional).

3 Reference Documents

[VOL] SEPA CARDS STANDARDISATION (SCS) “VOLUME”

[SEPA-FAST] SEPA-FAST Financial Application Specification for SCF Compliant EMV Terminals, Part 1: Attended POS Environment Technical Specification, Draft Version 3.0

[CAPE ACQ MDR] ISO 20022, Card Payment Exchanges, Message Definition Report, Edition May 2013 (Acceptor to Acquirer)

[CAPE ACQ MUG] CAPE, Card Payments, Message Usage Guide, Edition December 2013

[CAPE TMS MDR] ISO 20022, Card Payment Exchanges - Terminal Management, Message Definition Report, Edition May 2013

[CAPE TMS MUG] Card Payment – Terminal Management Message Usage Guide, Edition December 2013

[EPAS RTP] Sale to POI Protocol Specifications, Retailer Protocols Working Group, EPASOrg, Version 2

[OIS] OSCar Integration Specification for SEPA compliant terminals, Draft Version 3.1