EFT/POS 2000

Minimal Requirements for Gateway Solutions

Version 8.1.0

December 31, 2022

Revision History

Date	Version	Description	Author
December 10, 2012	6.0.0	Issuing with the ep2 specification V.6.0.0	Martin Osley
December 31, 2013	6.1.0	Software download req. updated	Martin Osley
December 1st, 2014	6.2.0	PCI PA DSS and P2PE removed	Martin Osley
November 30, 2015	6.3.0	no changes	Martin Osley
December 8, 2016	7.0.0	no changes	Martin Osley
December 22, 2017	7.1.0	no changes	Martin Osley
February 1, 2019	7.2.0	Context diagram updated	Martin Osley
December 9, 2019	7.3.0	no changes	Martin Osley
December 18, 2020	7.4.0	no changes	Martin Osley
December 31. 2021	8.0.0	TLS requirement added	Martin Osley
December 31, 2022	8.1.0	no changes	Martin Osley

1 Introduction

The Technical Cooperation *ep2* (TeCo *ep2*) defines herein the gateway approval requirements. The *ep2* certification process is focused on attended or unattended standalone terminals, i.e. all *ep2* functionality and security is implemented on a terminal device and the complete payment process is fulfilled on that terminal.

The document will be used by the *ep2* Certification Authority for the gateway approvals.

For questions and comments, please contact the *ep2* certification authority.

For all requirements in which the gateway solution does not fulfill the minimal requirements for gateway solutions a ’waiver request’ letter must be provided by the applicants to the *ep2* certification authority. The ’waiver request’ letter must be accepted by all members of the *ep2* technical working group (TWG *ep2*).

1.1 Scope

This document applies to all *ep2* gateway solutions and approvals. According to *ep2* a gateway is defined as following:

As soon as a part of the ep2 specification is implemented on a component that is not PCI PTS POI certified.

For example, gateway solutions are solutions that are used to concentrate transactions of multiple payment terminals in a single location before forwarding them to an acquirer or POS management system or if part of the *ep2* logic is divided/implemented into/on additional not PCI PTS POI certified components, it is a gateway solution.

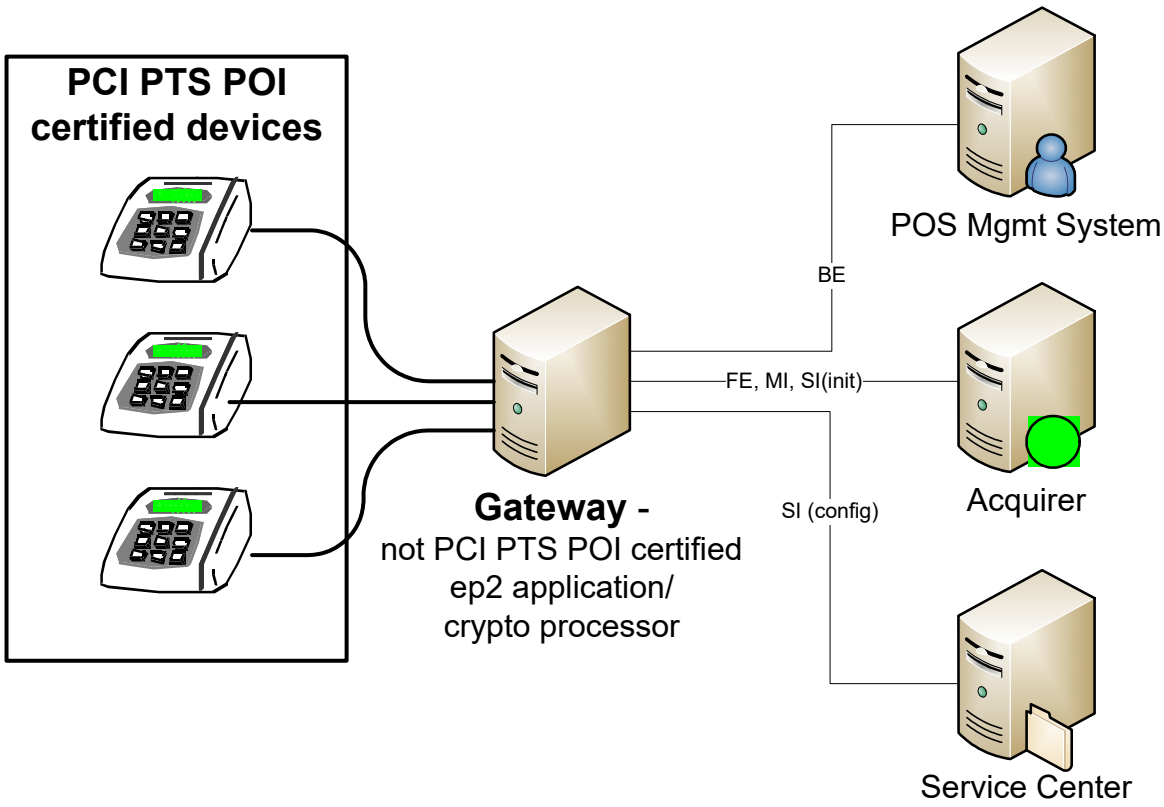

Figure 1 Definition Gateway Solution

1.2 Delimitation

The gateway approval concept does not exclude further *ep2* certification steps (e.g. SW certification).

1.3 Exclusion of Warranty

It is the sole responsibility of the applicant to ensure correct and complete functionality of the gateway solution. Conformance with these *ep2* requirements does not ensure conformance with existing functional specifications or quality requirements. Changes of international standards and specifications and changes of legal national rules also remain within the risk and responsibility of the applicant.

1.4 Gateway Concept Approval Cost

The *ep2* gateway concept approval will be charged for each request to the applicant.

Details see the *ep2* certification price list, which can be downloaded on http://www.eftpos2000.ch.

2 Roles and Responsibilities

2.1 Applicant

Members	Responsibility & Duties
SPOC	A contact person is needed for the communication with the *ep2* CA (Single Point of Contact - SPOC)
Protocol Type	Representatives of the applicant
Responsibility	- truthful delivery of information, concepts and certificates - Fulfilment of all *ep2* requirements
Duties	- Provide the required prerequisites (documents, concepts, certificates) according to the minimal requirements for gateway solutions - Answering questions of the security board and *ep2* CA - Present the gateway solution in detail and participate at the required meetings

Table 1 Responsibilities & Duties of the Applicant

2.2 ep2 Certification Authority

Members	Responsibility & Duties
Chairmanship	Head of *ep2* Certification Authority
Members	- Employees of eftpos Engineering GmbH

Table 2 Responsibilities & Duties of the ep2 Certification Authority

Members	Responsibility & Duties
Responsibility	- Central point of contact for applicants and security experts - Classification wether it is a gateway solution or not according to the *ep2* gateway definition - Organization and Scheduling of the gateway approval meetings - Ensure the flow of information among all stakeholders / participants - Neutral mediation and moderation between the stakeholders
Duties	- Answering technical question to *ep2* - Classify certification request whether it is a gateway solution according to *ep2* or not - Review of concepts and requests - Conduct and minute gateway approval meetings - Accompany the application (gateway integrator) through the *ep2* certification process, collect and communicate the results - Ensure the escalation process and prepare all waivers, requests and complaints for the security board and TWG *ep2*.

Table 2 Responsibilities & Duties of the ep2 Certification Authority

2.3 ep2 Security Board

Members	Responsibility & Duties
Chairmanship	*ep2* Certification Authority
Protocol Type	Decision with comments
Quorum	- Consensus among security experts (at least two security experts must attend) - Possible decisions: Concept approved, declined, rework or recommendation to TWG *ep2* - The *ep2* CA has no vote and no power of decision
Escalation	TWG *ep2* (first instance), Teco *ep2* Executive Board (last instance)
Members	- per Primary Acquirer one security expert - one security expert from PostFinance - a representative of the *ep2* Certification Authority
Responsibility	- Compliance with *ep2* security requirements - Equal treatment of all applicants - Safeguarding of the *ep2* principles and standard
Duties	- Review of concepts and requests - Document and report the findings to the *ep2* CA (in written form) - Make the acceptance decision within 4 weeks after a request

Table 3 Responsibilities & Duties of the ep2 Security Board

2.4 Primary Acquirer

In the gateway approval process the primary acquirer should provide a security expert to review the concept and participate on the approval meetings.

It is strongly recommended to define a primary acquirer before applying the gateway approval.

2.5 Technical Working Group ep2

The TWG *ep2* (Technical Working Group *ep2*) controls the *ep2* system, treats waiver requests and is the instance for important decisions. It supervises the *ep2* certification authority. There are approximately four TWG *ep2* meetings each year, where waivers and critical approval issues may be treated. The final instance of the TeCo *ep2* association is the executive board.

3 Required Documents

3.1 ep2 HW Certificate

The applicant shall provide an *ep2* Hardware Certificate for each used PIN-pad/terminal model. Before SW-certification, additional PIN pads may be added later (separate HW-certification required).

3.2 Gateway Approval Concept

The Applicant shall provide a Gateway Approval Concept at least 14 days before the gateway acceptance meeting.

The gateway concept shall be addressee oriented for *ep2* technical working group members (TWG *ep2*) and for the *ep2* certification authority. Internal concepts are insufficient. Please avoid long extracts from the *ep2* specifications. Describe your solution as compact as possible and make references to the *ep2* specifications. Visualize as much as possible!

3.2.1 Content Priorities

1. Management Summary with context diagram and sections background, goals, purpose / motivation, intended use in the Swiss market, high level network diagram and request for a gateway approval
2. High Level description of the Gateway

3. Architectural high level and low level diagrams. Clear scoping and definitions of all components used in your solution.
4. Detailed diagrams for security, maintenance and initialization/configuration, transaction sequence diagram with focus description of differences to a standard *ep2* CAT terminal.
5. Security between terminal and acquirer
6. Functionality description of the complete solution. The gateway solution shall fulfil all *ep2* requirements according to the *ep2* specifications.
7. *ep2* use case implementation description (high level description with focus on the variations to *ep2*). Show us, how and where (component) each process transaction use case step will be performed. Create 2 separate sequence diagrams for indoor and outdoor processing (if applicable).
8. Describe how you plan to perform the *ep2* pilot with Mastercard and Visa.

Important, the concept shall be easy to understand and complemented with diagrams and pictures.

3.2.2 Visualisation

The document shall contain the following diagrams:

- high-level network diagram
- dataflow diagram and security architecture
- which data is transmitted from which component to which component/target
- which data is used in plaintext or encrypted format for transmission
- several architecture diagrams (hardware platform, software platform, software architecture, your *ep2* application structure

3.2.3 Proposed Table of Contents

1. Overview / Management Summary
   a. Motivation, Business Purpose
   b. Road Map
   c. Prerequisites, other Certificates
2. Technical Description
   a. Architecture (incl. interfaces)
   b. Functionality (use case implementation)
   c. Security
   d. Life Cycle Management (Operations)

Please note: all issues in the checklist shall be covered in your gateway concept and that the *ep2* certification authority reserves the right to ask for additional documents.

3.2.4 Minimal Concept Requirements

These concept requirements are verified at the gateway approval.

Nr.	Requirement	Type
1	Describe following aspects of your solution architecture: 1. High level component diagram with description of roles, components and interfaces 2. HW- or technology component architecture (PIN pads, gateway host, peripherals, display, card readers, printer, communication) 3. SW architecture (drivers, security, card management/EMV kernels, communication management, services 4. *ep2* application architecture (processes, interfaces, security, user interface, data storage) 5. Application architecture (the *ep2* application shall not be affected by any none *ep2* application installed on the gateway or terminal) 6. *ep2* message flow (where and how (encrypted or clear text) the *ep2* data elements are transferred	Architecture
2	Describe how the following functionality will be implemented in your gateway solution: 1. *ep2* transaction processing incl. application selection (BIN table processing) 2. *ep2* trigger implementation (describe how the *ep2* triggers are processed on the gateway) 3. Initialisation per terminal - create, read, update and delete of the Terminal Application Configuration Data (TACD) 4. Configuration per terminal - create, read, update and delete of the *ep2* configuration data objects	Functional
3	Describe your hosting location of the infrastructure (where and data center tier level) and the software download and update.Software	Operations
4	Describe following aspects of your security implementation in detail: 1. All *ep2* security mechanisms (chap. 2: ep1 to ep6) shall be described in the gateway concept (how and where implemented, refer to message flows in your architecture concept. Visualize the security architecture. 2. Explain the chain of trust: secure and authentic load/transfer of the public keys from the Service Center and from the Acquirer	Security

Table 4 Minimal Gateway Approval Concept Requirements

4 Architectural Requirements

4.1 Gateway Solution Architecture

Describe following aspects in your gateway approval concept:

1. High level component diagram with description of roles, components and interfaces
2. HW- or technology component architecture (PIN pads, gateway host, peripherals, display, card readers, printer, communication)
3. SW architecture (drivers, security, card management/EMV kernels, communication management, services
4. *ep2* application architecture (processes, interfaces, security, user interface, data storage)
5. Application architecture (the *ep2* application shall not be affected by any none *ep2* application installed on the gateway or terminal)
6. *ep2* message flow (where and how (encrypted or clear text) the *ep2* data elements are transferred

4.2 Interface Requirements

An *ep2* gateway solution shall implement following *ep2* interfaces (similar as for *ep2* standalone terminals):

1. BE for assuring the interoperability with other POS management systems (transmit)
2. MI (Subm) to submit the transactions directly to the acquirer (clearing interface)
3. FE to authorize transactions with *ep2* acquirers
4. SI (Init) individually for each PIN pad and interoperable with all *ep2* acquirers
5. SI (Config) individually for each PIN pad and interoperable with all *ep2* service centers and acquirers

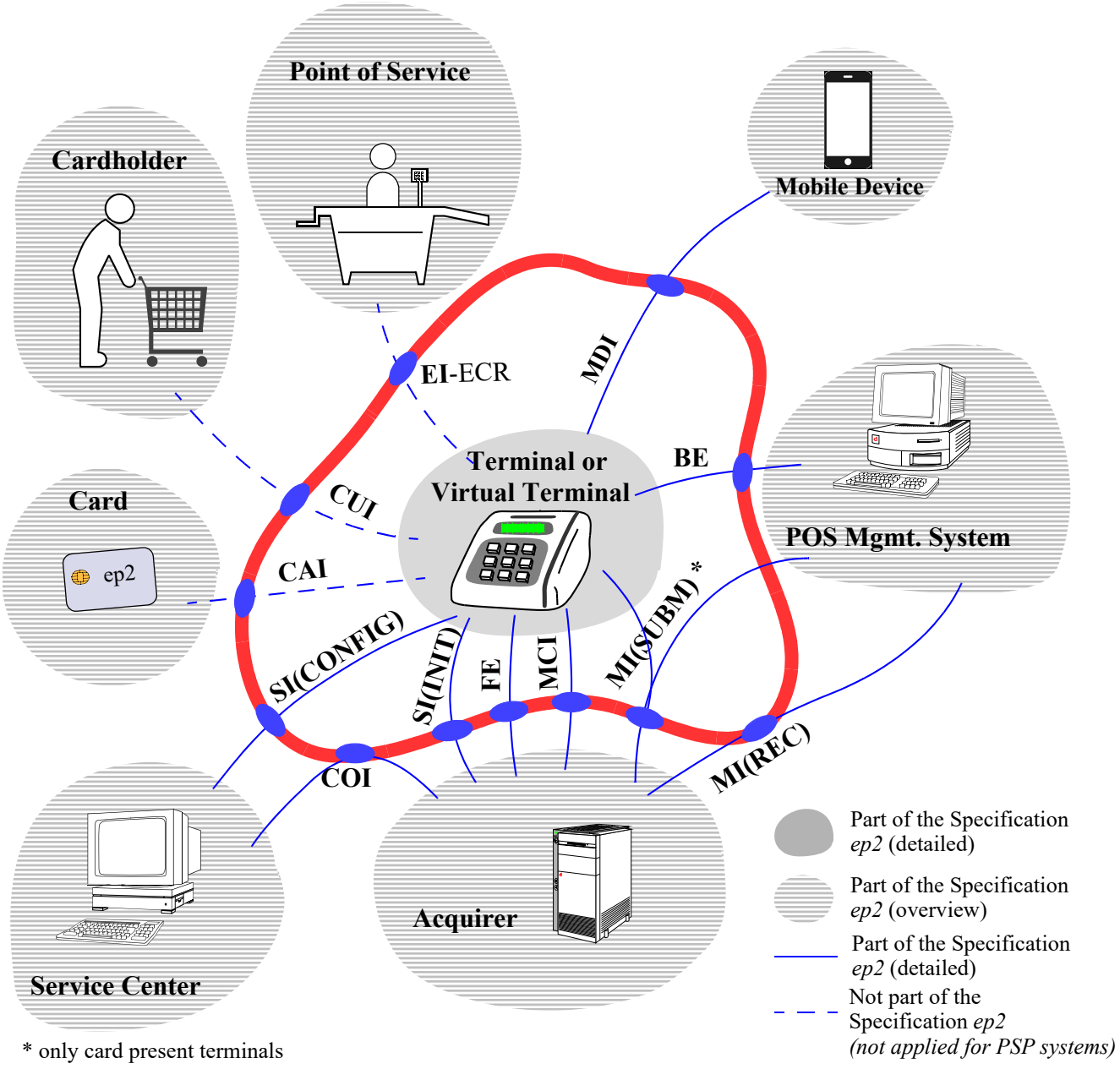

Figure 2 Required ep2 Interfaces for Gateway Solutions

4.3 Service Center Requirements

For a *ep2* gateway solution a service center is required which:

1. supports the *ep2* setup and maintenance functionality (interoperable with third-party terminals)
2. implements the COI interface to the acquirers

5 Functional Requirements

A gateway solution shall fulfil all *ep2* terminal functional and supplementary requirements. There is no difference for gateway solutions, they are treated same as a standalone terminal.

Following key requirements shall be fulfilled and described in the gateway solution concept:

1. All use cases shall be supported and implemented according to [ep2trm-func]. Note that an initialisation and configuration shall be separately possible for each PIN pad/terminal according to [ep2trm-func], chapter 18 ’Terminal Administration’ and [ep2dd], chapter 3 ’Data Model ’Setup and Maintenance”.
2. The user interface incl. cardholder display texts shall be compliant to [ep2trm-supp]
3. All receipts shall be compliant to [ep2trm-supp]
4. The application selection (incl. BIN table processing) shall fulfil the requirements of [ep2trm-func], section 19.5 ’Application Selection’
5. The cardholder verification shall fulfil the requirements of [ep2trm-func], section 19.6 ’Cardholder Verification’
6. The terminal risk management shall fulfil the requirements of [ep2trm-func], section 19.7 ’Terminal Risk Management’ and 19.8 ’Terminal Action Analysis’.
7. All *ep2* exceptions shall be covered according to [ep2trm-func], chapter 21 ’Terminal Exceptions’and the error code processing shall be fulfilled according to the *ep2* specifications.
8. All *ep2* triggers shall be supported by the gateway solution. Describe how the *ep2* triggers are processed on the gateway.

6 Security Requirements

6.1 Single Crypto-Zone

The *ep2* protocol specification is built on a single crypto-zone concept that relies on encryption at the hardware terminal and on decryption at the acquirer's or processor's site. The *ep2* end to end security (single crypto-zone between terminal and acquirer) is described in [ep2sec], section 2 ’Security Mechanisms’ and visualized in figure 3 communication channel ID 5.

The TeCo *ep2* keeps on existing security concept firmly and will not allow a multi-zone security solutions for the *ep2* software certification. This basic principle of *ep2* shall be maintained due to the equal treatment of all terminal suppliers / applicants and the loss of direct control of the terminal by the acquirer.

6.2 Sensitive Data Processing

No clear text processing of sensitive data on the gateway allowed

Encryption and decryption of sensitive data on the gateway is not allowed

6.3 Component Demarcation

PIN pad and gateway shall be treated as separate components (not as terminal subsumable). See also figure 1.

6.4 Security Communication Channels

The following security communication channel shall be considered in detail by the Applicant and mentioned in the gateway approval concept (details are described in [ep2sec], section 1 ’ep2 Security Overview’).

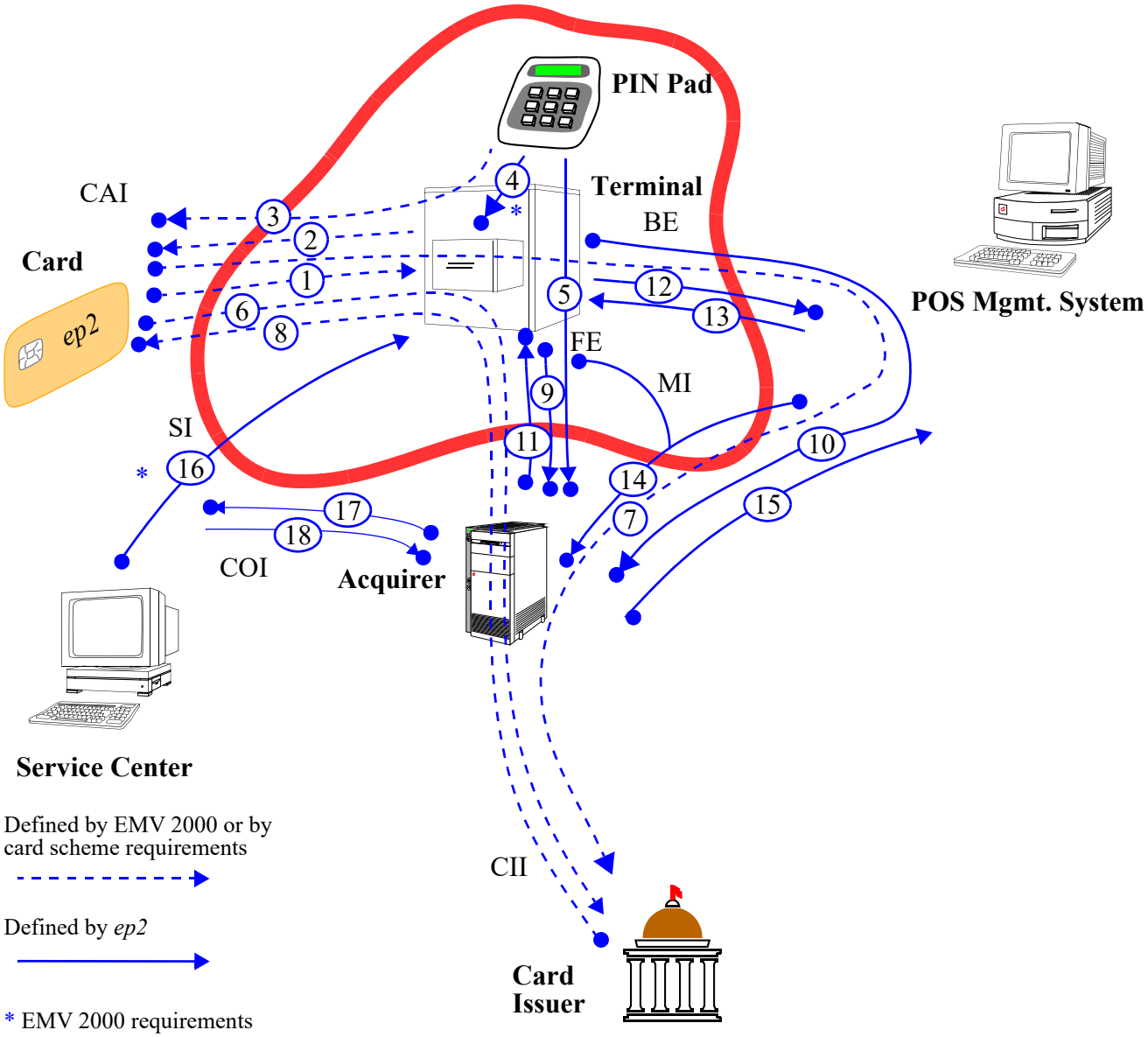

Figure 3 *ep2* Security Communication Channels

6.5 Security Mechanisms

Describe in detail the following *ep2* security mechanisms (details are described in [ep2sec], section 2 ’Security Mechanisms’):

a. ep1: Session Key Handling

b. ep2: Component Authentication

c. ep3: On-line Data Authentication

d. ep4: On-line PIN Encipherment
e. ep5: Confidential Data Encipherment
f. ep6: Acquirer Transaction Certificate Generation
g. ep7: Transport Layer Securtiy
h. trmsup1: Software Authentication
i. trmsup2: Local PIN Encipherment

6.6 Chain of Trust

Describe in the gateway approval concept the chain of trust: secure and authentic load/transfer of the public keys from the Service Center and from the Acquirer shall fulfil the *ep2* security requirements.

7 Operational Requirements

7.1 Data Center

The gateway approval concept shall contain at least following information about the data center used for the gateway solution:

a. physical hosting location of the infrastructure
b. data center tier level or certifications

7.2 Software Download

The minimal requirements for the software download as described in [ep2trm-func], section 18.3 ’Download Terminal Software’) shall be fulfilled.

The gateway approval concept shall describe how the following operational requirements will be implemented:

a. Secure PIN pad software
b. Secure *ep2* software update
c. Remote update of the PIN pad and *ep2* software
d. Life cycle management process, notably the release and the change management of the *ep2* software and other applications on the gateway

8 *ep2* Gateway Approval Checklist

Checklist items		applic.	approval
	***ep2* Gateway Model:**		
3 Required Documents **3.1 ep2 HW Certificate**			
	[3.1a] For all used PIN Pads / Terminals ep2 Hardware certificates provided	m	
3.2 Gateway Approval Concept			
	[3.2a] Adherence to the concept delivery deadline fulfilled	m	
	[3.2b] The gateway approval concept is addressee oriented and suitable for the assessment/approval	m	
	[3.2c] Content priority requirements fulfilled	m	
	[3.2d] Visualisation requirements fulfilled	m	
	[3.2e] The document is complete (covers all checklist item) and correct (formal, structural and factual correctness)	m	
4 Architectural Requirements **4.1 Gateway Solution Architecture**			
	[4.1a] High level component diagram requirements fulfilled	m	
	[4.1b] HW- or technology component architecture provided	m	
	[4.1c] SW architecture described	m	
	[4.1d] ep2 application architecture described	m	
	[4.1e] Application architecture described and no affects from other applications to the ep2 application proven	m	
	[4.1f] ep2 message flow visualized and described	m	
4.2 Interface Requirements			
	[4.2a] BE interface supported	m	
	[4.2b] MI (subm) interface supported	m	
	[4.2c] FE interface supported	m	
	[4.2d] SI (init) interface supported	m	
	[4.2e] SI (config) interface supported	m	
4.3 Service Center Requirements			

Table 5 ep2 Gateway Approval Checklist

Checklist items		applic.	approval
	[4.3a] Service center functionality supported (interoperability with 3rd-party terminal fulfilled)	m	
	[4.3b] COI interface supported	m	
5 Functional Requirements			
	[5a] All ep2 use cases fulfilled and described	m	
	[5b] The user interface is ep2 compliant	m	
	[5c] All receipts are ep2 compliant	m	
	[5d] Application selection according to ep2	m	
	[5e] Cardholder verification according to ep2	m	
	[5f] Terminal risk management according to ep2	m	
	[5g] Exception handling is ep2 compliant	m	
	[5h] All ep2 triggers are supported	m	
	[5i] Complete ep2 terminal functionality is supported	m	
6 Security Requirements **6.1 Single Crypto-Zone**			
	[6.1a] Single crypto-zone requirement fulfilled	m	
6.2 Sensitive Data Processing			
	[6.2a] No clear text processing of sensitive data on the gateway performed	m	
	[6.2a] No encryption and decryption of sensitive data on the gateway performed	m	
6.3 Component Demarcation			
	[6.3a] PIN pad and gateway are treated as separate components in the concept	m	
6.4 Security Communication Channels			
	[6.4a] The security communication channels were considered by the applicant (check in presentation) and mentioned in the gateway approval concept	m	
6.5 Security Mechanisms			

Table 5 ep2 Gateway Approval Checklist

Checklist items		applic.	approval
	[6.5a] Security channel ep1: Session Key Handling described and compliant	m	
	[6.5b] Security channel ep2: Component Authentication described and compliant	m	
	[6.5c] Security channel ep3: On-line Data Authentication described and compliant	m	
	[6.5d] Security channel ep4: On-line PIN Encipherment described and compliant	m	
	[6.5e] Security channel ep5: Confidential Data Encipherment described and compliant	m	
	[6.5f] Security channel ep6: Acquirer Transaction Certificate Generation described and compliant	m	
	[6.5g] Security channel ep7: Transport Layer Securtiy described and compliant		
	[6.5h] Security channel trmsup1: Software Authentication described and compliant	m	
	[6.5i] Security channel trmsup2: Local PIN Encipherment described and compliant	m	
6.6 Chain of Trust			
	[6.6a] The load and transfer of the public keys is secure and mentioned in the gateway approval concept	m	
7 Operational Requirements **7.1 Data Center**			
	[7.1a] Hosting location mentioned	m	
	[7.1b] Data center tier level and/or certifications provided	r	
7.2 Software Download			
	[7.2a] Secure PIN pad software download	m	
	[7.2b] Secure ep2 software download	m	
	[7.2c] Remote update of the PIN pad and ep2 software by the service center	m	
	[7.2d] Life cycle management process described	m	

Table 5 ep2 Gateway Approval Checklist

Legend:

m: mandatory

r: recommended

o: optional