CIPURSE™ V2 Revision 2.0 Documentation Overview

10.2017

www.osptalliance.org

OSPT Alliance
Prinzregentenstr. 159
D-81677 Munich Germany
© 2017 OSPT Alliance
All Rights Reserved

Legal Disclaimer:
The information given in this document shall in no event be regarded as a guarantee of conditions or characteristics. With respect to any examples or hints given herein, any typical values stated herein and/or any information regarding the application of the device, OSPT Alliance hereby disclaims any and all warranties and liabilities of any kind, including without limitation, warranties of non-infringement of intellectual property rights of any third party.

Information:
For further information, please see the OSPT Alliance website: www.osptalliance.org or contact: info@osptalliance.org

We listen to your comments:
We are constantly striving to improve the quality of all our specification and documentation. We have spent an exceptional amount of time to ensure that it is correct. However, we realize that we may have missed a few things. If you find any information that is missing or appears to be in error, please use the contact section to inform us. We appreciate your assistance in making this a better document.

Please be aware that for the implementation of the CIPURSE specification into products, further IPR licenses may be required:

- CIPURSE cryptography IPR can be licensed from the OSPT IP Pool GmbH. Contact: info@ospt-ip-pool.com.
- The Transaction mechanism as implemented in the CIPURSE™T profile is covered by additional third party IPR, not licensable from the OSPT IP Pool. It is the responsibility of the implementer to contact the IPR owner.

Trademarks:
CIPURSE and OSPT are trademarks of OSPT Alliance.

Introduction

This document provides a brief introduction into the documents forming CIPURSE™V2 Revision 2.0.

The CIPURSE V2 standard was built to enable a broad portfolio of products that meet the demanding and diverse functional, performance, and reliability requirements of the transport applications. It supplies the issuer with a variety of products with different memory sizes, feature set, and cost positions enabling considerable flexibility in the application design.

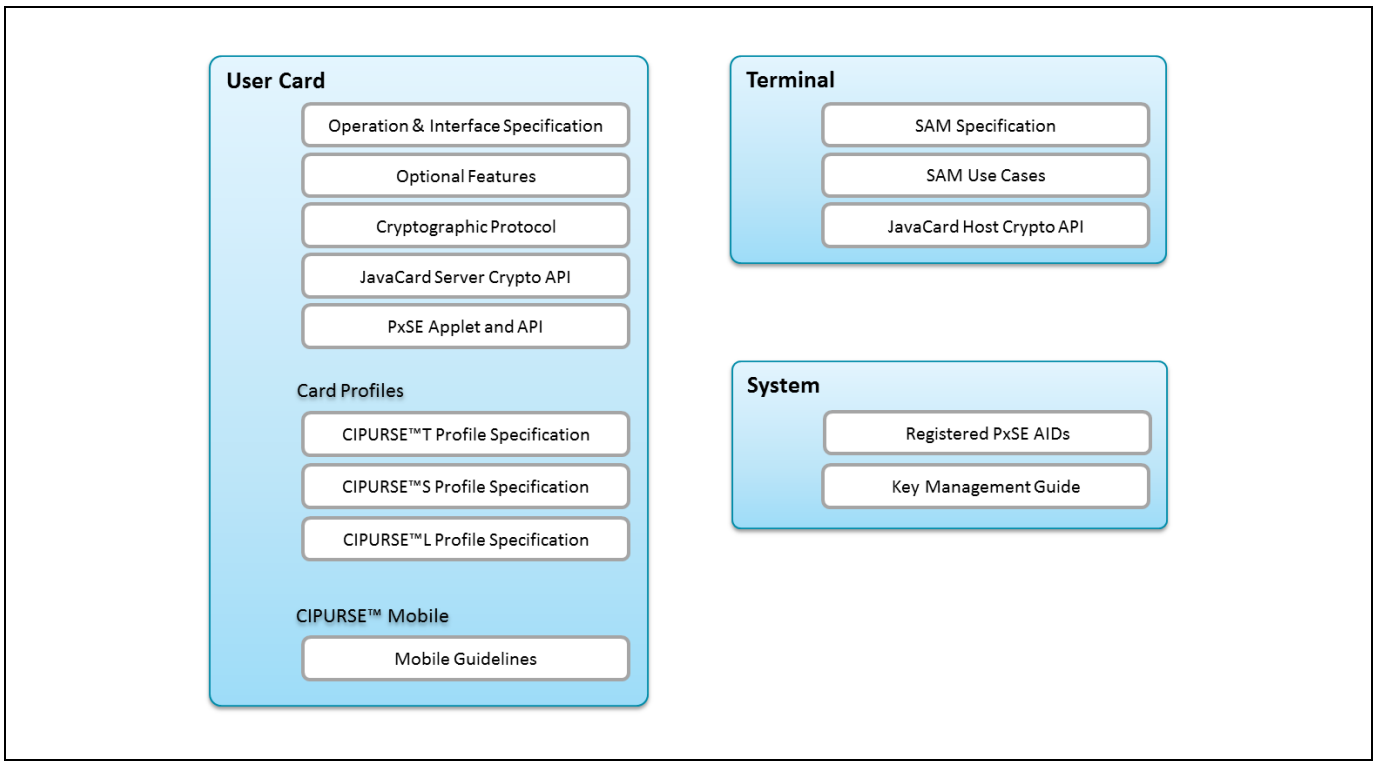
To address the diverse needs of the transit industry, the CIPURSE V2 standard offers different CIPURSE V2 profiles such as:

- **CIPURSE™T Profile:** Multiple Application Profile supporting consistent transaction mechanism – Fully configurable, supporting multiple applications on the device – In-field application download – Efficient and consistent management of data manipulations across files.
- **CIPURSE™S Profile:** Multiple Application Profile supporting several pre-defined applications – Fully flexible configuration of several applications prior issuance.
- **CIPURSE™L Profile:** The limited use ticket profile – Single application profile with a reduced file system and subset of functionality.

Nevertheless, all PICCs implementing any of these CIPURSE V2 profiles are compliant to the "CIPURSE V2 Operation and Interface" specification. This ensures interoperability across CIPURSE V2 applications and enables an easy migration from simple to more demanding applications.

CIPURSE V2 Revision 2.0

CIPURSE V2 Revision 2.0 consists of the following documents:



- **Operation and Interface Specification**: This document specifies the feature set available to all members of the CIPURSE V2 family. It describes the data objects on the card as well as the associated command set and security mechanisms by defining the interface between cards and terminals compliant to this standard.
- **Optional Features**: This document specifies optional features that can be implemented in a CIPURSE V2 product in addition to the Operation and Interface specification to support additional use cases as, for example, those commonly found in the mobile industry.
- **Cryptographic Protocol**: This document specifies the cryptographic mechanisms of cards (i.e. PICCs) and terminals (i.e. PCDs) compliant to this CIPURSE V2 specification.
- **Java Card Server Crypto API:** This package defines the interface of a library providing the CIPURSE cryptography for a card side CIPURSE application. Dividing the CIPURSE functionality into a library and an applet part allows OS manufacturers to build native performance boosters with a standard interface.
- **PxSE Applet and API**: This document specifies the feature set of a PxSE applet class and a Java Card interface allowing CIPURSE applications registering to a PxSE instance.
- **CIPURSE™T Profile Specification**: This document specifies CIPURSE™T, the multi-application profile supporting consistent transaction mechanism based on the CIPURSE V2 specification. The suffix "T" stands for the consistent "Transaction" feature.
- **CIPURSE™S Profile Specification**: This document specifies CIPURSE™S, the profile based on the CIPURSE V2 specification. The "S" suffix stands for "Standard".
- **CIPURSE™L Profile Specification**: This document specifies CIPURSE™L, the single-application profile based on the CIPURSE V2 specification. The "L" suffix describes it as a "Lite" version of CIPURSE V2.
- **Mobile Guidelines**: This document is a guideline for integrating CIPURSE V2 in an NFC environment.
- **SAM Specification**: This document specifies the interface of a CIPURSE SAM. A CIPURSE SAM provides a terminal with all of the cryptographic services required to securely communicate with CIPURSE cards.
- **SAM Use Cases**: This document describes the most common use cases of various CIPURSE SAM types.
- **Java Card Host Crypto API:** This package defines the interface of a library providing the CIPURSE cryptography for a terminal side CIPURSE application.
- **Key Management Guide**: This document provides some security requirements applicable for systems based on CIPURSE products.
- **Registered PxSE AIDs**: This document lists AIDs already registered for use by industry specific PxSE applications.

Java Card APIs

CIPURSE V2 Revision 2.0 defines APIs that can be implemented in any Java Card Classic runtime environment. Java Card technology defines file formats and deployment process different from Java. In particular, the Java Card Converter demands creation and use of export files (.EXP) as part of the software production process.

In order to enable interoperability across modules implementing an API and modules using this API the following files are provided for each API:

- **.EXP**: Export file used to provide the link between Java naming convention found in a class file and Java Card structure of the API found in a CAP file as required by the Java Card Byte Code Converter.
- **.JAR**: Java package container with interface definition to meet Java compiler needs when compiling the source code into a class file.
- **.CAP**: Only for the shareable interface defined in CIPURSE™V2 PxSE Applet and API specification, a loadable CAP file provides an implementation of `org.osptalliance.javacard.cipurse.api.pxse`.