TECHNICAL SPECIFICATION

ISO/IEC TS 23465-2

First edition
2023-02

Card and security devices for personal identification — Programming interface for security devices —

Part 2: API definition

Cartes et dispositifs de sécurité pour l'identification personnelle — L'interface du logiciel pour dispositifs de sécurité —

Partie 2: Definition de API

Reference number
ISO/IEC TS 23465-2:2023(E)

© ISO/IEC 2023



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2023

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

© ISO/IEC 2023 – All rights reserved

Contents

Page

Foreword ..... **v**
Introduction ..... **vi**
1 Scope **1**
2 Normative references **1**
3 Terms and definitions **1**
4 Symbols and abbreviated terms **2**
5 Graduated APIs for security devices **3**
5.1 General 3
5.2 Secure credential storage 3
5.3 Security device supporting cryptography 4
5.4 Security device supporting secure application 4
6 API pre-requisite **4**
6.1 Description language 4
6.2 Format of an API function 4
6.2.1 General 4
6.2.2 Addressing means 5
6.2.3 Parameters 5
6.2.4 Return values 5
6.2.5 Callback functionality 5
7 API error handling **6**
7.1 General 6
7.2 Exceptions 6
8 Security device identification **6**
8.1 Security device attributes 6
8.2 Security device entry 8
9 Data model definition **8**
9.1 General 8
9.2 Attributes and types 9
9.3 Methods 9
9.4 References/instances 9
10 API definition **10**
10.1 General 10
10.2 List of defined API functions 10
10.3 API function for managing, addressing and identifying security devices 11
10.3.1 Method isoIec23465_ getSecurityDeviceList 11
10.3.2 Method isoIec23465_connectSecurityDevice — Connection to the security device 12
10.4 API function derived from data model 12
10.4.1 Basic Class Object 12
10.4.2 Class SecurityDeviceApplication 14
10.4.3 Class RootApplication 15
10.4.4 Class SensitiveContainer 17
10.4.5 DataContainer 19
10.4.6 CertificateContainer 24
10.4.7 Authenticator 26
10.4.8 Password 27
10.4.9 Key 31
10.4.10 AsymmetricKey 32
10.4.11 SecretKey class 33
10.4.12 PublicKey 34

© ISO/IEC 2023 – All rights reserved

10.4.13 PrivateKey 36
10.5 API functions for cryptographic operation 38
10.5.1 General 38
10.5.2 Extension of key class 40
10.5.3 Interface methods related to keys 41
Annex A (informative) **Open Mobile API** **50**
Annex B (informative) **Support of Open Mobile API** **53**
Annex C (informative) **IDL** **54**
Bibliography **55**

© ISO/IEC 2023 – All rights reserved

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see https://patents.iec.ch).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 17, *Cards and security devices for personal identification*.

A list of all parts in the ISO/IEC 23465 series can be found on the ISO and IEC websites.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

© ISO/IEC 2023 – All rights reserved

Introduction

Integrated chip card (ICC) technologies and solutions are widely deployed around the world, but the system for identity tokens and credentials is quickly changing. In this context, the application protocol data unit (APDU) protocol outlined in the ISO/IEC 7816 series is becoming in some cases a hindrance to the integration of ICs in environments such as mobile phones, handheld devices, connected devices (e.g. M2M, IoT) or other applications using security devices.

In addition, several stakeholders are not familiar with, or not very fond of the APDU protocol because of its complexity. They would circumvent its constraints by requesting an abstraction layer hiding IC specifics such as data structures and complexity of the security policies.

A common way to reach this goal in the software development is the definition and application of application programming interface (API) functions to access the IC within the devices. Specific knowledge of ADPU protocols and details of the IC implementation is not necessary anymore. Also, the complexity and details of the implementation of the security model and the security policy can be shifted from the pure application development into the system design of the whole ID management.

However, even solutions based on those kinds of middleware are perceived as cumbersome in some systems. The market looks for a middleware memory footprint to be as low as possible and the acceptance, usage and maintenance of such a system can be simpler.

This document aims to overcome or mitigate those issues by proposing a new approach that preserves ICC functionality and allows a seamless ICC portability onto new systems.

The ISO/IEC 23465 series focuses on a solution by designing an API and a system with the following characteristics:

— It offers a set of API calls related to multi-sectorial ICC functionality, derived from the ISO/IEC 7816 series of other ICC related standards.

— It defines the sub-system to perform the conversion from the API function to the interface of the security device (e.g. APDU-interface), called “proxy”.

— It results in a description of solutions with no middleware or very little middleware memory footprint (i.e. simplified drivers).

— It defines simplified ICC capabilities, description of the discoverability (i.e. with significantly less complexity than ISO/IEC 24727) and provides examples of usages.

The present model is static and future revisions are expected to add live cycle functionality.

© ISO/IEC 2023 – All rights reserved

Card and security devices for personal identification — Programming interface for security devices —

Part 2: API definition

1 Scope

This document describes the following aspects of the programming interface between the client application dealing with the security device and the proxy, based on the framework outlined in ISO/IEC 23465-1:

— the generic API definition;

— state and security models for use cases;

— class and API definitions of functionality, defined in other standards, e.g. the ISO/IEC 7816 series.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 23465-1:2023, *Card and security devices for personal identification — Programming interface for security devices — Part 1: Introduction and architecture description*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 23465-1 and the following apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
array
indexed list of any data types with a well-known number of members

3.2
boolean
data type used to denote a data item that can only take one of the values TRUE and FALSE

3.3
char
data type containing an 8-bit quantity that encodes a single-byte character from any byte-oriented code set with a numerical value between 0 and 255

© ISO/IEC 2023 – All rights reserved

3.4
credential
set of data presented as evidence of a claimed or asserted identity and/or entitlements

EXAMPLE A user attribute (see ISO/IEC 19286) signed by the issuer as proof of authenticity is a credential that can be verified by the service provider by validating the electronic signature.

[SOURCE: ISO/IEC 29115:2013, 3.8, modified — Note 1 to entry was deleted. An EXAMPLE was added.]

3.5
integer
data type containing a sequence of digits taken from a number base

Note 1 to entry: Programming languages support integer values as a data type in different flavours, e.g. as signed integer or unsigned integer and in short or long format. To be programming language agnostic this document does not specify any of these different definitions and uses the general type integer for different types. This approach is different to the used interface description language (IDL).[6] It is the responsibility of the application programmer to define the type of integer in a relevant API function call according to the need of the function and the programming language used.

EXAMPLE Digits from the number base 10 (decimal) consisting of 0, 1, 2, 3, 4, 5, 6, 7, 8, 9.

3.6
octet
data type with 8-bit quantity

3.7
string
data type containing a sequence of characters with a definite length

4 Symbols and abbreviated terms

APDU	application protocol data unit
API	application programming interface
CPLC	Card Production Life Cycle
CPS	Cryptographic Service Provider
DLOA	Digital Letter of Approval
eID	electronic identity
eSE	embedded secure element
eUICC	embedded universal integrated chip card
GP	GlobalPlatform
ID	identification
IDL	interface description language
KMS	Key Management System
OMG	Object Management Group
OS	operating system
OSI	open systems interconnection
PII	personal identifiable information
PIV	Personal Identity Verification
PKCS	Public Key Cryptographic Standard
SD	secure digital (memory card)
TSM	Trusted Service Manager eSE

© ISO/IEC 2023 – All rights reserved