INTERNATIONAL STANDARD

ISO/IEC 23465-1

First edition
2023-02

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

Part 1: Introduction and architecture description

Cartes et dispositifs de sécurité pour l'identification personnelle — Interface de programmation pour dispositifs de sécurité —

Partie 1: Introduction et description de l'architecture

Reference number
ISO/IEC 23465-1:2023(E)

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

Contents

Page

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.

Introduction

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

Several stakeholders are not familiar with, or not very fond of the APDU protocol because of its complexity. They will often circumvent its constraints by requesting an abstraction layer hiding IC specifics. Although the security mechanisms of security devices are well defined in ISO/IEC 7816-4 their implementation and application differ from vendor to vendor and the complexity overstrains most of the application developers.

In software development, a common way to simplify the usage of complex systems is the definition and application of application programming interface (API) functions to access the IC within the devices. Specific knowledge of APDU 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 pure application development into system design of the electronic device and its related software.

Therefore, this document is geared towards software (SW)-architects, application programmers or specification developers developing software applications using and addressing ICs as security devices within operating systems or their components.

The projected applications can run on different software and hardware environments. Generalisation of the API definition is key and the dependencies on specific runtime environments and equipment are kept out in principle.

Existing runtime environments already support the access to IC as security devices using different specific APIs, e.g. OpenMobileAPI,[10] PKCS#11,[12] but they always implement a proprietary interface and middleware, which is not commonly applicable. 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. This document also aims to overcome or mitigate those issues by proposing a new approach that would preserve ICC functionality and allows for a seamless ICC portability onto new systems.

Since the system is designed for easy support by mobile operation systems, mobile operating system (OS) designers/ implementers are encouraged to support these standardized APIs to access any embedded secure element (eSE) within the mobile device.

In the context of mobile devices, there is a necessity for trusted computing, e.g. by dedicated security hardware. The proposed API helps the application implementer with a standardized common interface to such trusted IC.

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

The ISO/IEC 23465 series is comprised of three parts each focusing on a specific topic:

— ISO/IEC 23465-1 (this document): provides an introduction to the series and a short overview of the architecture;

— ISO/IEC TS 23465-2: defines the API for client applications allowing incorporation and usage of security devices;

— ISO/IEC TS 23465-3[1]: describes the software called Proxy which provides different services e.g. to convert the API calls into serialized messages to be sent to the security device.

[1] Under preparation. Stage at the time of publication: ISO/IEC DTS 23465-3.

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

Part 1: Introduction and architecture description

1 Scope

This document introduces and describes the concept of the application programming interface (API) to security devices with the intention to simplify the usage of commands and mechanisms defined by the ISO/IEC 7816 series.

This document gives guidelines on:

- the system overview and description of the system of the programming interface;
- the architecture description;
- the data model in general, used by the API;
- the use cases and the usage model of the API.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the following terms and definitions 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
client
any type of entity requesting services from a *security device* (3.7)

3.2
ISO/IEC 23465 API
software interface defined in ISO/IEC TS 23465-2

3.3
middleware
software (SW) component allowing two systems from different or similar operating systems interconnection (OSI) layers to communicate with each other

3.4
operating systems interconnection model
OSI model
conceptual model that characterizes and standardizes the communication functions of a network or computing system without regard to its underlying internal structure and technology