TECHNICAL SPECIFICATION

ISO/IEC TS 23465-3

First edition
2023-05

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

Part 3: Proxy

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

Partie 3: Proxy

Reference number
ISO/IEC TS 23465-3:2023(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 outlined in the ISO/IEC 7816 series is becoming, in some cases, a hindrance to the integration of integrated circuits (ICs) in environments such as mobile phones, handheld devices, connected devices (e.g. M2M, IoT) or other application using security devices.

Stakeholders often request an abstraction layer hiding IC specifics to avoid the complexity of APDU protocols. 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 aims to overcome or mitigate those issues by proposing a new approach that would preserve ICC functionality and allow for a seamless ICC portability onto new systems.

The ISO/IEC 23465 series focuses on a solution by designing an application programming interface (API) and a system with these characteristics:

— It offers a subset, from the ISO/IEC 7816 series, of mostly used multi-sectorial ICC functions.

— It results in no further middleware or very little middleware memory footprint (i.e. simplified drivers).

— It requires a simplified ICC capability discoverability (i.e. with significantly less complexity than ISO/IEC 24727-1). [3]

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

— ISO/IEC 23465-1: 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 (this document): describes the software (SW) called "proxy" which provides different services, e.g. to convert the API calls into serialized messages to be sent to the security device.

The ISO/IEC 23465 series is intended to be used by any sector relying on the interchange defined, but not limited to, the ISO/IEC 7816 series.

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

Part 3: Proxy

1 Scope

This document describes the software (SW) layer called "proxy". It supports the programming interface to security devices and the application using this API to access the application related security devices defined in ISO/IEC TS 23465-2.

This document is applicable to:

— proxy requirements, functionality and layers;

— resolving mechanisms for API functions;

— data structures related to security device handling;

— translation for security device communication;

— serialization/de-serialization syntax and methods.

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, *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
access rule
data element containing an access mode referring to an action and security conditions to be fulfilled before acting

3.2
client application
implemented application using the ISO/IEC 23465-API requesting services from a security device

3.3
security attribute
condition of use of objects in the card including stored data and data processing functions, expressed as a data element containing one or more *access rules* (3.1)

4 Symbols and abbreviated terms

APDU	application protocol data unit
API	application programming interface
ATR	answer to reset
CBOR	consise binary object representation
DO	data object
ICC	integrated circuit card
JSON	JavaScript open notation
MSE	manage security environment
OMAPI	open mobile API
OSI	open systems interconnection
PACE	password authenticated connection establishment
SM	secure messaging
SW	software
SD	security device, see terms and definitions

5 Proxy related requirements

5.1 Link between client application and security device

The proxy is the piece of software (SW) between the programming interface used by a client application dealing with security devices and the related security device(s). The functionality of the proxy and its APIs deal with communication, connectivity, provisioning of confidentiality and authenticity of the connection to the security device and its security device applications.

The general concept of client applications dealing with a set of security device is outlined in ISO/IEC 23465-1 and is depicted in Figure 1 (see also ISO/IEC 23465-1:2023, Figure. 2). The applications or clients use abstractions of access methods to the security devices, which are outlined as the ISO/IEC 23465-API in ISO/IEC TS 23465-2. Details of low-level security device addressing and accessing methods are kept hidden to these clients. The translation of the abstract API-functions into low-level commands and protocols shall be performed by the proxy, possibly supported by additional libraries and internal APIs.

The clients only have access to the physical security devices by the proxy which acts as a dispatcher for the direct access to the security devices and the related security device applications. In some use cases the proxy may handle as a multiplexer, especially in multitasking environments with parallel running clients.

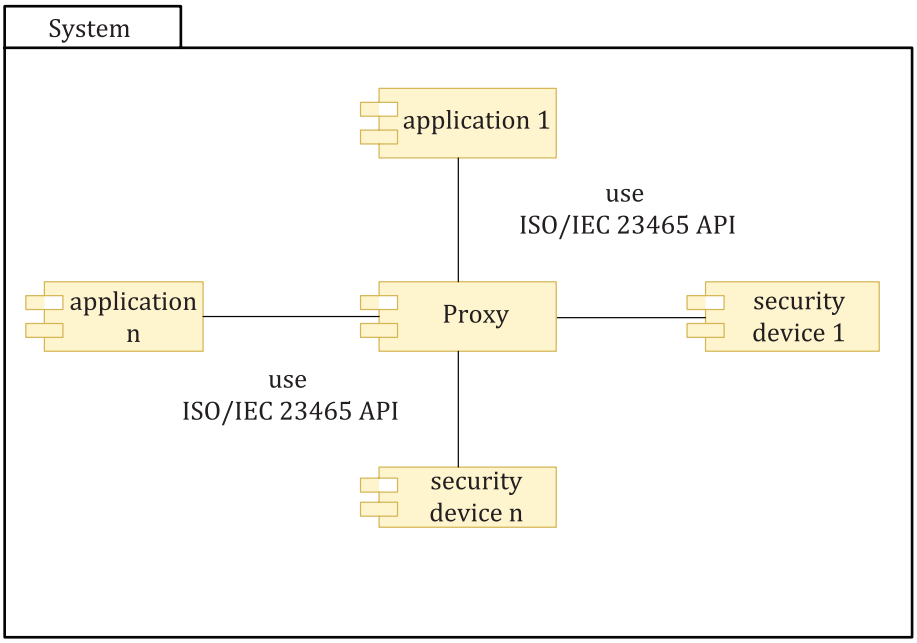

Figure 1 — Components of the system with distributing proxy

5.2 Proxy layers

5.2.1 Proxy layer model

Figure 2 depicts the layers and components of the proxy to perform the client application requests by the defined API. The proxy as a SW component requires some additional SW parts in a real implementation. These are not outlined here, but are mentioned separately.

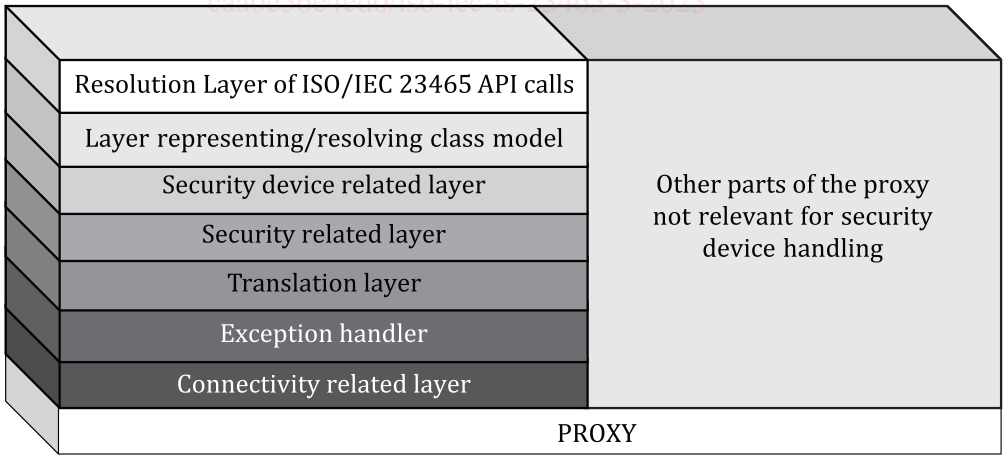

Figure 2 — Components of a proxy

5.2.2 Resolution layer of ISO/IEC 23465-API calls

Any API call needs a piece of programming code, called glue code, which has no functional relevance but is essentially to adhere to the different code parts. Any real implementation resolves, with this additional glue SW, the requirements of the applied programming language.

When several client applications are allowed to act in parallel, this layer shall be able to handle several tasks independently.

5.2.3 Layer representing/resolving class model

The class model, outlined in ISO/IEC TS 23465-2, represents the view of the client and part of the proxy to the object-oriented definition of a security device and its components. The client uses the references and methods of the classes provided by the instantiated objects. The instantiation of the objects is done in this layer. The proxy provides the object references to the client, administrates the objects in accordance to the resources of the systems, e.g. the available or addressed security devices and its related data.

5.2.4 Administration layer for security devices

All relevant data of the administrated and addressable security devices are handled in this layer. The layer tallies the security devices, identifies the access methods, administrates the security device individually and stores all relevant information of the available security devices.

Means for such administration is an internal registry holding all the information of available security devices. In case of removable security devices, this layer shall register when mounting and de-register when detaching the security devices. The registry entries for such devices has to be updated accordingly.

NOTE The entries of such a registry are used to inform the client about the details of the requested security devices.

5.2.5 Security related layer

This layer provides the means to perform all the security mechanisms related to the security devices.

Any security device supports or requires security features, directly or indirectly. Depending on the security attributes of the security device application, these security-related activities have to be provided or performed, sometimes in cooperation with the client application, sometimes hidden to the client application. In the latter case the security activities shall be performed by this proxy layer.

Relevant information of fulfilled security features shall be stored, in case this information is required for further security device access.

A security device requires sometimes an authentication procedure according to external specifications, to set-up a secure channel**,** which are be completely hidden to the client application. In this case a session management has to be considered in the security related layer.

5.2.6 Translation layer

The most important abstraction of the access methods to security devices is the concealment of the direct communication, offered by the API. As outlined in ISO/IEC 23465-1, the evolution of security device technologies can require different protocols and data formats than those currently being used. The conversion into protocols understood by the used security device shall be done in this layer.

The translation layer provides the means to perform the translation of the client application's initiated activity into security device related protocols and formats. An abstract API call from the client application finally results in at least one command understood by the addressed security device.

In contrast, responses of the security device after processing of the command(s) are returned in the format of the used security device protocol. This layer re-translates the replied data into the formats defined by the API which are finally expected and understood by the client application.

The translation process is understood as a serialisation/marshalling and de-serialisation/unmarshalling technique, which is well-known in SW technology and used by many computer languages.

NOTE The actual protocol dealing with security devices based on ICC technology uses APDU, defined by ISO/IEC 7816-4. Upcoming application specifications use, e.g. CBOR, JSON or other coded protocols which can be relevant in the future.

5.2.7 Exception handler

Most of the API functions defined in ISO/IEC TS 23465-2 expect exception messages. Dedicated return values of the security devices, e.g. defined in ISO/IEC 7816-4, shall be translated by the translation layer. In case of errors or unforeseeable situations, the program flow is interrupted by throwing an exception This is managed by this exception layer.

The service can be used in conjunction with the translation layer since a response of a security device can require exception handling.

5.2.8 Connectivity related layer

The physical connection of the security device in the system has to be used by the proxy. Depending on the runtime environment of the used system, security device/reader-related device drivers or middlewares are available. This layer uses existing APIs which may be manufacturer dependent and requires a system related implementation. Some systems offer standardized APIs which can facilitate the interaction between proxy and security devices, e.g. the Global Platform Open Mobile API[6].

5.3 Conditional proxy functionality

5.3.1 Multitasking/Multiplexing

ISO/IEC 23465-1 outlined different runtime environments in which client applications can use the ISO/IEC 23465-API. The behaviour of a proxy varies from either supporting only one security device by one client, or one client with access to several security devices (in a single task), or several clients with access to several security devices in parallel in a multitasking runtime environment.

According to the needs of the latter situation, the proxy shall be designed as a SW running in a multitasking environment. When several clients interact with one security device simultaneously, the proxy shall obey the ability of the security device. An existing solution for such simultaneous access on a single security device is possible today when logical channels are supported. The approach of multiple logical interfaces in addition to logical channels also allows the parallel processing of security device applications in a single physical security device.

The security device's behaviour shall be managed by the proxy. Logical channel or multiple logical interface support can be part of a discovery mechanism of the proxy or a specific information in the proxy's registry of security devices.

5.3.2 Crypto functionality

Many API functions defined in ISO/IEC TS 23465-2 deal with crypto-functionality related to the security device. Addressing means used by the client application and the internal management within the security device usually differs. The knowledge about the behaviour, the needs of crypto protocols and the translation into security device related formats is provided by this service.

The proposed API methods for crypto operations cover all algorithms and mechanisms which are currently in common usage. Since the calculation is performed on the security device, the proxy shall adopt and structure the data in a way that the addressed security device can use the data.

Some crypto API calls are separated into calls for initialization of the method followed by one or more subsequent calls of the crypto API for processing. The sequence of APIs shall be controlled by the proxy.

Existing crypto protocols performed on security devices need additional commands to set-up a crypto-functionality. ISO/IEC 7816-4 defines concepts and commands which are used to set-up the security environment (MSE command) with essential information, expected by the security devices in advance. These activities should be completely hidden to the client application. The application of such security device related commands shall be performed by the proxy.

