ISO/IEC DTS 23465-3

ISO/IEC JTC 1/SC 17

Secretariat: BSI

Date: 2022-12-21

Deleted: TC /SC N ¶
Date: ¶
¶
/SC /WG

Deleted: ¶
Copyright notice¶
This ISO document is a working draft

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

FDIS stage

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.

Deleted: In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.…

Deleted: on

Deleted: following URL:

Field Code Changed

Deleted: iso.org/iso/foreword.html

Deleted: The committee responsible for

Deleted: is

Deleted: ISO/IEC 23465 consists of the following parts, under the general title *Card and security devices for personal identification — Programming interface for security devices¶*
¶
— Part 1:

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.

Several stakeholders are not familiar with, or not very fond of APDU protocol because of its complexity. They will often circumvent its constraints by requesting an abstraction layer hiding IC specifics.

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[1]: provides an introduction to the series and a short overview of the architecture;

— ISO/IEC TS 23465-2[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.

—

Deleted: *and architecture description*

Deleted: — *Part 2: API definition¶*
— *Part 3: Proxy¶*
¶
Introduction¶

Deleted: the system

Deleted: is

Deleted: like

Deleted: secure elements

Deleted: for

Deleted: would

Deleted: ¶
But

Deleted: standard

Deleted: allows

Deleted: ¶
This

Deleted: of standards

Deleted: ¶
—

Deleted: —

Deleted: finally

Deleted: —

Deleted: capabilities

Deleted:).

Deleted: — Part 1 (IS):

Deleted: — Part 2 (

Deleted:):

Deleted: — Part

Deleted: Proxy

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

[2] Under preparation. Stage at the time of publication: ISO/IEC PRF TS 23465-2.

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

Part 3: Proxy

1 Scope

Deleted: (Part3)

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.

Deleted: part of ISO/IEC 23465

Deleted: " supporting

Deleted: ,

Deleted: part

Deleted: of this series of standards

Deleted: This series of standards is intended to be used by any sectors relying on the interchange defined by the ISO/IEC 7816 series but no limited.¶
¶
This is the third part of the series dealing with ¶

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.

Deleted: ,

Deleted: ,

Deleted: ,

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/

Deleted: —

Deleted: —

3.1
access rule
data element containing an access mode referring to an action and security conditions to be fulfilled before acting

Deleted: .

3.2
bus
communication system transferring data between electronic components

[SOURCE: ISO/IEC/IEEE 24765:2017, 3.441]

Deleted: .

3.3
client
any type of entity requesting services from a *security device* (3.9)

Deleted: .

Deleted: (3.9)

3.4
client application
implemented application using the *ISO/IEC 23465-API* (3.5) requesting services from a *security device* (3.9)

Deleted: .

Deleted: (3.5)

Deleted: (3.9)

3.5
ISO/IEC 23465-API
software (SW) interface defined in ISO/IEC TS 23465-2[5]

3.6
middleware
software (SW) component allowing two systems from different or similar open systems interconnection (OSI) layers to communicate with each other

3.7
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)

3.8
proxy
sub-system to perform conversion from the application programming interface (API) function to the interface of the *security device* (3.9)

3.9
security device
tamper-resistant secure hardware component which is used in a device to provide the security, confidentiality and multiple application environment required to support various business models

Note 1 to entry: Can exist in any form factor, e.g. universal integrated circuit card (UICC), embedded SE, smartSD, smart microSD.

EXAMPLE A SIM, an UICC, an eSIM, an eSE or a secure memory card

[SOURCE: GlobalPlatform Device Technology] [8]

3.10
serialization
process of translating data structures or object states into a format that can be transmitted

3.11
use case
list of actions or event steps typically defining the interactions between a role (known in the Unified Modeling Language as an actor) and a system to achieve a goal

Note 1 to entry: A role is known as an actor in the Unified Modelling Language.

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

Deleted: .

Deleted: [5]

Deleted: .

Deleted: .

Deleted: (3.1)

Deleted: .

Deleted: (3.9)

Deleted: .

Deleted: ,

Deleted: ¶
[SOURCE: Global Platform Inc.: "GlobalPlatform Device Technology - TEE System Architecture", Version¶

Deleted: .2, Public Release, December 2018]¶
¶
NOTE

Deleted: such as

Deleted: ,

Deleted: serve as security device

Deleted: .

Deleted: .

Deleted: a

PACE	password authenticated connection establishment
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;20—, 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 have to be performed by the proxy, possibly supported by additional libraries and internal APIs.

Deleted: , Fig.

Deleted: device's

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 pplications. In some use cases the proxy may handle as a multiplexer, especially in multitasking environments with parallel running clients.

Deleted: only

Deleted: an

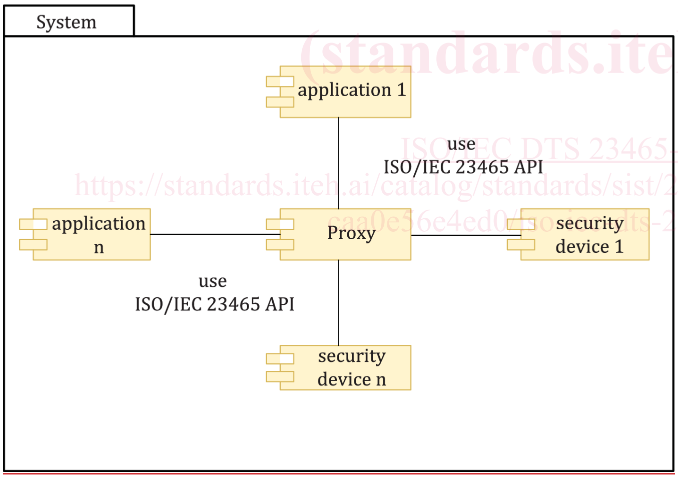


Figure 1 — Components of the system with distributing proxy

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.

Deleted: Figure 2

Deleted: software

Deleted: ,

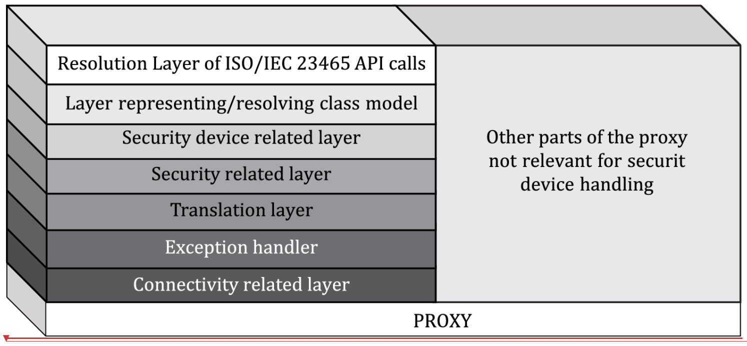
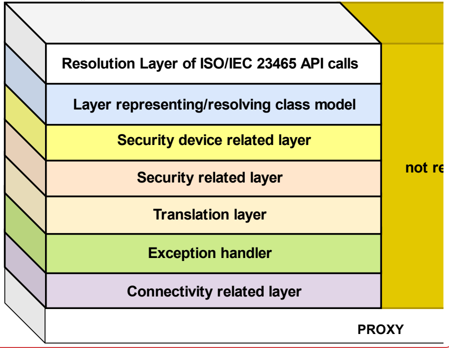

Resolution Layer of ISO/IEC 23465 API calls
Layer representing/resolving class model
Security device related layer
Security related layer
Translation layer
Exception handler
Connectivity related layer
Other parts of the proxy not relevant for securit device handling
PROXY

Figure 2 — Components of a proxy

Deleted: ¶


Resolution Layer of ISO/IEC 23465 API calls
Layer representing/resolving class model
Security device related layer
Security related layer
Translation layer
Exception handler
Connectivity related layer
not re
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 the different code parts. Any real implementation resolves, with this additional glue SW, the requirements of the applied programming language.

Deleted: software

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 ressources 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.

Deleted: indivually

Means for such administration is an internal registry holding all the information of available security devices. In case of removable security devices, this layer has to 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 have to be performed by this proxy layer.

Deleted: has

Deleted: has

Relevant information of fulfilled security features has to 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 has to be done in this layer.

Deleted: may

Deleted: as

Deleted: be

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.

Deleted: finally

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.

Deleted: Vice versa

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.

Deleted: the software

Deleted: is

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.

Deleted: might

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, have to 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.

Deleted: might

Deleted: may

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[7].

Deleted: devices/readers

Deleted: could

Deleted: .

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.

Deleted: behavior

According to the needs of the latter situation, the proxy has to be designed as a SW running in a multitasking environment. When several clients interact with one security device simultaneously, the proxy has to obey the ability of the security devices. 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.

Deleted: software

Deleted: today

Deleted: also

The security device's behaviour has to 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.

Deleted: could

5.3.2 Crypto functionality

Many API functions defined in ISO/IEC 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

Deleted: A lot ot

Deleted: part

Deleted: of this series of standard are dealing 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.

Deleted: usually

The proposed API calls for crypto operations to cover algorithms and mechanisms which are 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 sequene of APIs has to 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) 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 has to be done by the proxy.

5.3.3 Discovery functionality

ISO/IEC TS 23465-2 offers the API call **isoIec23465_getSDList** which provides the security device attributes of the accessible security devices. This set of information shall be collected and distributed by the proxy. The discovery service is responsible for the collection and distribution of the relevant attributes.

This can be performed by specific discovery mechanisms related to the security devices known by additional interfaces, middlewares or other means. A possible registration service (see 5.3.4) with a persistent registry can be an additional source of information to be filled in the list of security device attributes.

Deleted: clause

Deleted: could

5.3.4 Registration functionality

This service may be established to administrate the connected security devices. It allows the storage of security device related information in a registry of the proxy. The service periodically polls the existence and the identification of security devices in the system and updates the registry accordingly. This behaviour is also important for removable devices.

Deleted: periodically

The registration and discovery functionality services are normally handled in conjunction with each other.

Deleted: service is

6 Instantiation of class objects

6.1 Class model

The class model for the API was introduced in ISO/IEC TS 23465-2, together with the object handling and the resolution of the instances. Figure 3 (see also ISO/IEC 23465-1:20—, Figure 7) depicts the proposed way to handle the API calls in the proxy.

Deleted: , Fig.

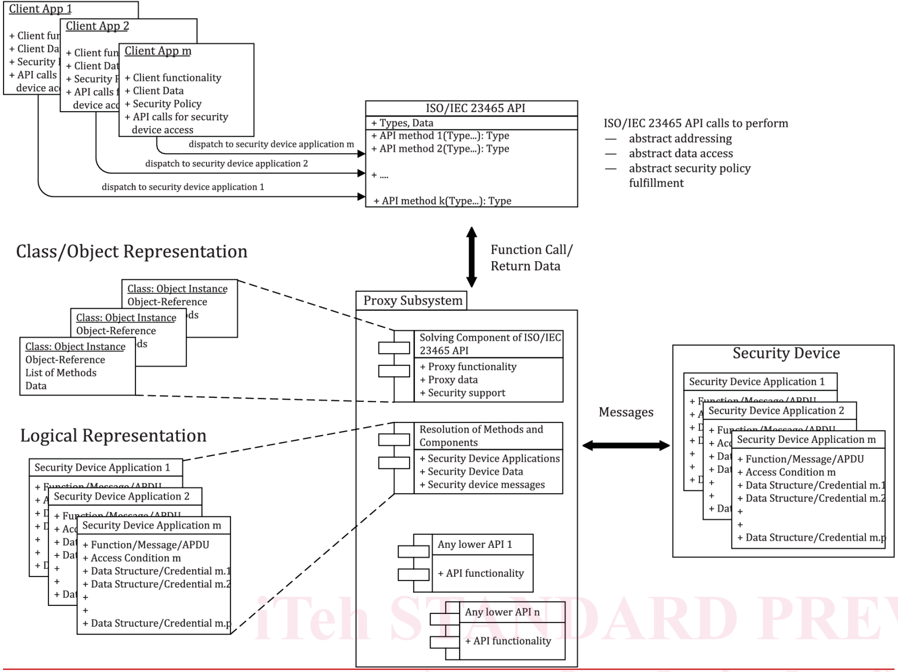

Client App 1
Client App 2
Client App m
+ Client functionality
+ Client Data
+ Security Policy
+ API calls for security device access
dispatch to security device application m
dispatch to security device application 2
dispatch to security device application 1
ISO/IEC 23465 API
+ Types, Data
+ API method 1(Type...): Type
+ API method 2(Type...): Type
+ ....
+ API method k(Type...): Type
ISO/IEC 23465 API calls to perform
— abstract addressing
— abstract data access
— abstract security policy fulfillment
Class/Object Representation
Function Call/ Return Data
Class: Object Instance
Object-Reference
List of Methods
Data
Proxy Subsystem
Solving Component of ISO/IEC 23465 API
+ Proxy functionality
+ Proxy data
+ Security support
Resolution of Methods and Components
+ Security Device Applications
+ Security Device Data
+ Security device messages
Messages
Logical Representation
Security Device Application 1
Security Device Application 2
Security Device Application m
+ Function/Message/APDU
+ Access Condition m
+ Data Structure/Credential m.1
+ Data Structure/Credential m.2
+ Data Structure/Credential m.p
Any lower API 1
+ API functionality
Any lower API n
+ API functionality
Security Device

Figure 3 — Class model in context of the API and the security device

The client applications use the ISO/IEC 23465-API to handle the user functionality. The application refers to the class definitions and establishes the access to the objects defined in the class model via the API calls to the proxy. The calls are handled in the proxy's resolving layer (see 5.2.2). Based on the references of the instantiated objects, subsequent API calls on these objects are applicable.

The proposed class model and its possible usage reflects the structure and the content on the security device. Any client application can only use objects and methods which are supported by the underlaying security device. The proxy is the entity which conveys the application request, e.g. addressing of objects/methods and finally transforming into adequate format to the security device.

Deleted: establish

Deleted: uses

Deleted: ,

Deleted: finally

The real objects on the security device have their counterparts in the proxy as objects defined in the class model. Usable methods reflect the set of commands of the security device. The proxy resolves the usage of methods into sequences of security device commands, at least into one command.

An example is provided in Annex A.

6.2 Process of instantiation

After identifying the corresponding security device (in case more than one are available) the client application starts to interact with the security device by instantiating the SdApplication related to the client application. The link and binding of the instance of this object to its physical counterpart on the security device shall be established by the proxy.

The underlaying resolution layer detects the application on the security device by the selection mechanism of ISO/IEC 7816-4. The proxy generates the reference of this object and links its methods to the command set of the client related application on the security device.

According to the results of this process the proxy collects all relevant information:

— The object reference becomes valid, when the security device application exists.

— Additionally, available information, e.g. data objects of the FCI, application related access conditions, are collected and assigned to the object/reference.