INTERNATIONAL STANDARD

ISO/IEC 18328-1

First edition
2015-12-15

Identification cards — ICC-managed devices —

Part 1: General framework

Cartes d'identification — Dispositifs contrôlés par carte à circuit intégré (ICC) —

Partie 1: Cadre général

Reference number
ISO/IEC 18328-1:2015(E)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

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

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).

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).

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

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, Subcommittee SC 17, *Cards and personal identification*.

ISO/IEC 18328 consists of the following parts, under the general title *Identification Cards — ICC-managed Devices*:

— *Part 1: General framework*

— *Part 2: Physical characteristics and test methods for cards with devices*

— *Part 3: Organisation, security and commands for interchange*

Introduction

New upcoming technologies are providing flexible and suitable devices for input and output operations on ICCs and open a wide area of applications and use cases. Interoperability in current developments of new projects underlines the need of standardisation.

Integrated Circuit Card (ICC) consists of a card body with an embedded integrated circuit (or several integrated circuits). International Standards such as ISO/IEC 7816 and ISO/IEC 14443 define the physical and logical requirements of the ICC, e.g. location of the contacts, size of the card, electrical signals and communication protocols, security mechanisms, etc.

A lot of new requirements have to be considered when ICC-managed devices are on an ICC. This also incorporates physical aspects, as well as logical view on this type of card. The needs of useful applications and their environments have to be also taken into account for the ICC-managed devices on or in a card body. The nature of the device type leads to different definitions in physical and logical aspects. The intention of this part of ISO/IEC 18328 is to minimize the technology-dependent differences and to increase interchange.

This part of ISO/IEC 18328 offers a basic framework of different aspects which allows interoperability for application of ICC-managed devices on a card or possibly external off the card.

The International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) draws attention to the fact that it is claimed that compliance with this part of ISO/IEC 18328 may involve the use of a patent and their foreign counterparts.

— FR99/09818: Smart card architecture incorporating peripherals

— PCT/EP2011/058914: Bank card with display screen

— PCT/EP2011/059021: Bank card with display screen

— EP2001949522A: Contact-free display peripheral device for contact-free portable object

— WO2009077398, US20100263034, EP2225703, JP2010-538574, KR10-1162443: A method for authorizing a communication with a portable electronic device, such as an access to an electronic memory zone corresponding device and system.

ISO and IEC take no position concerning the evidence, validity and scope of this patent right.

The holder of this patent right has assured the ISO and IEC that he/she is willing to negotiate licenses under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statement of the holder of this patent right is registered with ISO and IEC. Information may be obtained from:

Gemalto
Intellectual Property and Licensing Department,
6, Rue de la Verrerie,
92197 Meudon Cedex, France

Gemplus
Avenue Pic de Bertagne,
Parc d'Activités de Gémenos BP 100
FR-13881 Gémenos Cedex

ASK SA
Les Boullides,
15, Traverse des Brucs, Sophia Antipolis,
06560 Valbonne, France

Attention is drawn to the possibility that some of the elements of this part of ISO/IEC 18328 may be the subject of patent rights other than those identified above. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO (www.iso.org/patents) and IEC (http://patents.iec.ch) maintain on-line databases of patents relevant to their standards. Users are encouraged to consult the databases for the most up to date information concerning patents.

Identification cards — ICC-managed devices —

Part 1:
General framework

1 Scope

This part of ISO/IEC 18328 describes the general architecture of an ICC with ICC-managed devices. This part of ISO/IEC 18328 is one of a series of International Standards which outlines the content and the boundaries covered and standardised by the other parts of ISO/IEC 18328. The general principle of this part of ISO/IEC 18328 is that all activities regarding the ICC-managed devices are controlled by the card-IC. This principle also applies when ICC-managed devices are outside the card. This part of ISO/IEC 18328 is applicable for all kind of cards independent from interface technology for communication.

2 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

2.1
button
tactile device used as a single input key

2.2
card-IC
integrated circuit with COS

2.3
ICC-managed devices
device or devices whose activities are controlled only by ICC

2.4
keypad
array of several *buttons* (2.1) organized as one entity

2.5
biometric capture device
sensor whose purpose is to acquire biometric data

Note 1 to entry: See also ISO/IEC 17839.

2.6
electronic display
electronic device to show information

3 Symbols and abbreviated terms

CLF	contactless frontend
COS	card operating system

NOTE COS is a logical element for implementation of functionalities defined in ISO/IEC 7816-4.

eID	electronic identification
eSE	embedded secure element
HCI	host controller interface
IC	integrated circuit
ICC	integrated circuit card NOTE An ICC consists of card body (or document, e.g. travel document) and one IC (or several ICs) with implementation of functionalities defined in ISO/IEC 7816-4. This ICC is independent from the physical interface technology.
I^{2}C	inter-integrated circuit
IFD	interface device
LED	light emitting diode
NFC	near field communication
OTP	one-time password
PIN	personal identification number
SPI	serial peripheral interface
SWP	single wire protocol
TEE	trusted execution environment
UICC	universal integrated circuit card

4 Framework for ICC-managed devices

4.1 Device categories of ICC-managed devices

Devices on an ICC mentioned here as ICC-managed devices extend the usage and definitions of a card. First implementations have shown ICCs using extensions, e.g. keypad, electronic displays, etc. Annex A outlines a motivation for having a standard for ICC-managed devices.

In general, an ICC-managed device is defined as an electronic device supplementary to the electronic system on a card, which allows internal transactions and/or transactions with the external world. The following is a general categorisation in groups seen from the perspective of the ICC:

— devices for input purposes, e.g. button, keypad, microphone, and biometric input sensor;

— devices for output purposes, e.g. display and loudspeaker;

— devices for input/output purposes, e.g. touch-screen;

— devices for communication purposes, e.g. LED, optical sensor, loudspeaker, microphone;

— support devices, e.g. power supplying device.

4.2 Targeted subjects in the ISO/IEC 18328 series

Many card-IC of ICC used today have already ICC-managed devices on the card-IC itself. Examples are random number generators (RNG) or crypto coprocessors, etc. These on-board devices support the card-IC and the COS in dedicated use cases. Usually, today, they are proprietarily connected and linked in each implementation. In this part ISO/IEC 18328, they are out of scope, but it is not excluded in the future to apply the mechanisms, defined in this series of International Standards also to such on-board devices.

Devices in this part ISO/IEC 18328 are always electronic devices linked to the card-IC. Any information from or to the device shall be channelled through and controlled by the ICC operating system.

Physical and logical protocols from the physical interfaces of the card-IC of the ICC to the devices are not covered by this part ISO/IEC 18328. Currently, there are different physical interfaces in ICC in use, e.g. SPI or I^{2}C interfaces; the definitions applied in this part ISO/IEC 18328shall be independent from any existing or future interfaces. Concrete implementations of the physical and electrical interfaces from ICC to any device or buses to the physical device are also out of the scope of this part ISO/IEC 18328.

The wide range of devices with different purposes and the large number of manufactures offering devices in different technologies and new fast developing technologies require a generic approach which allows easy adapting of new devices, new manufactures and new technologies in the future. The definitions in this part ISO/IEC 18328 shall be as flexible as possible to allow the adaptation of new devices in the future.

This part ISO/IEC 18328 covers all devices connectable to the card-IC including, but not limited to, power supplying devices, displays, all kind of sensors, microphones, loudspeaker, buttons, keypads, etc. The list can be extended due to the fact that future developments and needs will arise. Mechanisms to use electronic devices located outside of the ICC are covered also by this part ISO/IEC 18328. Figure 1 outlines the list of characteristics and mechanisms which shall be standardised within this series of International Standards.

This part ISO/IEC 18328 defines the required functionality of card operating system and other parts of software. It covers physical characteristics and test methods and also aspects of coexistence of technologies for ICC-managed devices.

Definitions of coding required for "trust assessment" of managed data, e.g. warning, font, colour, etc. is also in the scope of this part ISO/IEC 18328.

The mechanisms described in this part ISO/IEC 18328 are independent from internal capabilities of the devices.

NOTE Complex devices may have a separate controller or driver to enable its functionality. For example, an electronic display may have a specific electrical driver which provides and controls the physical signals to the display.

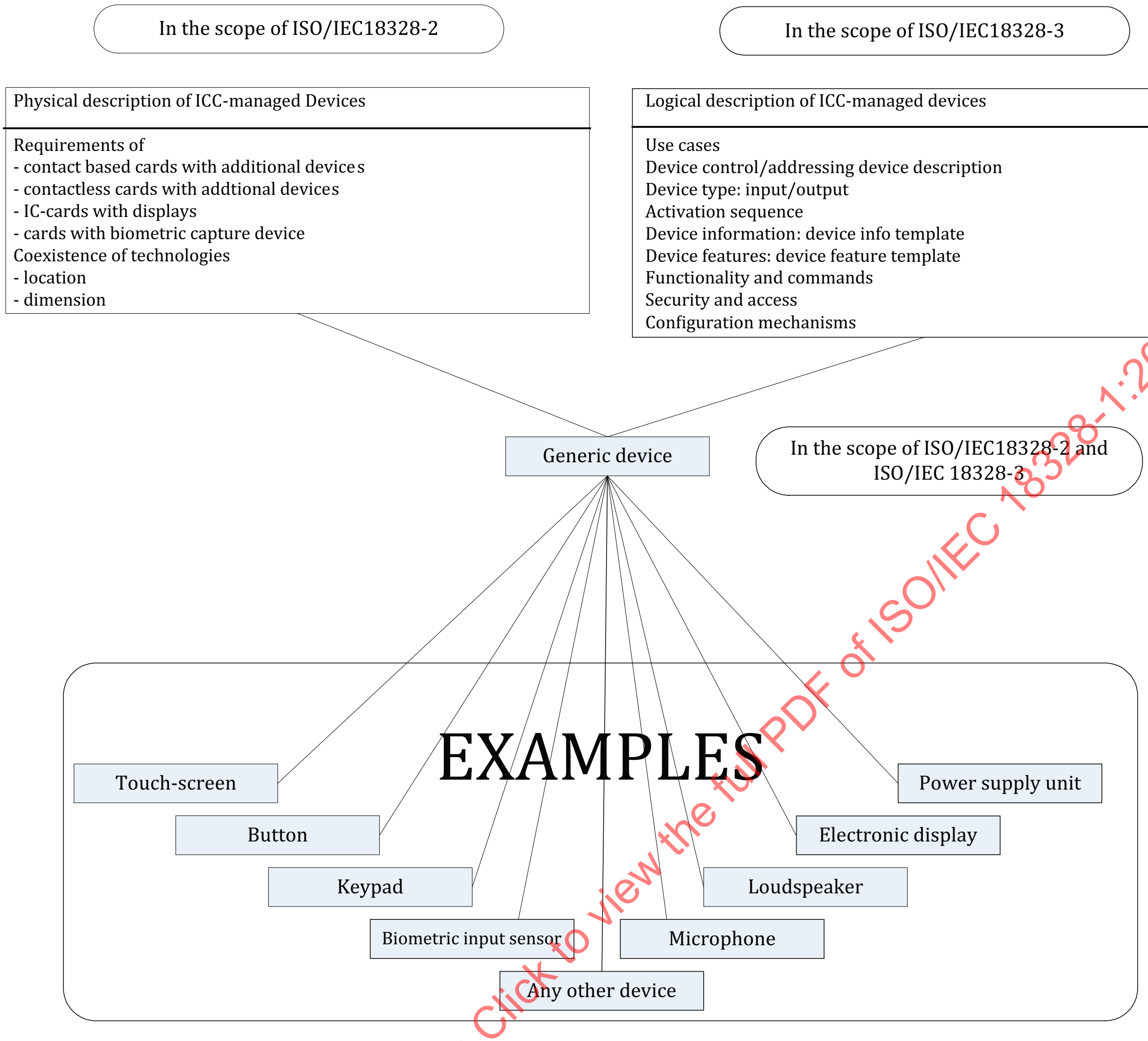

In the scope of ISO/IEC18328-2
In the scope of ISO/IEC18328-3
Physical description of ICC-managed Devices
Requirements of
- contact based cards with additional devices
- contactless cards with addtional devices
- IC-cards with displays
- cards with biometric capture device
Coexistence of technologies
- location
- dimension
Logical description of ICC-managed devices
Use cases
Device control/addressing device description
Device type: input/output
Activation sequence
Device information: device info template
Device features: device feature template
Functionality and commands
Security and access
Configuration mechanisms
Generic device
In the scope of ISO/IEC18328-2 and ISO/IEC 18328-3
EXAMPLES
Touch-screen
Button
Keypad
Biometric input sensor
Any other device
Microphone
Loudspeaker
Electronic display
Power supply unit

Figure 1 — Subjects in the ISO/IEC 18328 series

4.3 System architecture overview

The integration of devices into the ICC shall not reduce the functionality of the ICC, especially the functionality of proximity cards. Possible impacts are in the scope of the other parts of this part ISO/IEC 18328.

Devices located on different positions on the ICC are always electrically connected to the card-IC. Logical access to any device on the ICC is entirely under the responsibility of the COS. Figure 2 highlights the general architecture of ICC with ICC-managed devices.

Locations, physical and logical access, mechanical and electrical requirements, security-related definitions, etc. are subjects of the other parts of this part ISO/IEC 18328. Some optional features are outlined in Figure 2, e.g. a piece of software in the COS, so called driver, may handle the electrical access and bus activities from and to the device units on the ICC. An alternative for legacy systems to the system architecture on Figure 2 is described in Annex C.

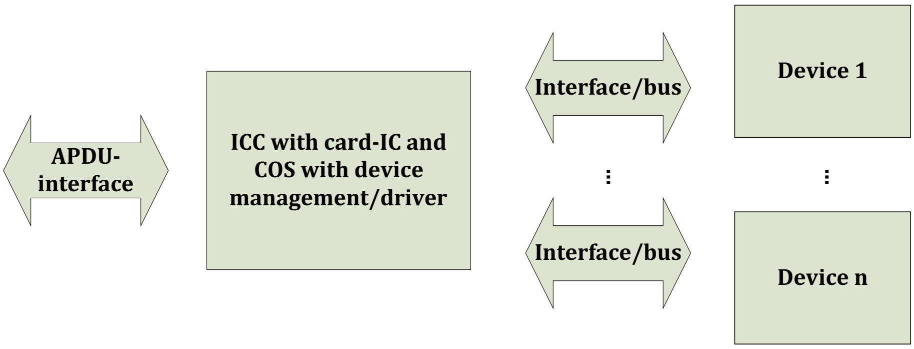


Figure 2 — System architecture of a card-IC with ICC-managed devices

4.4 Logical architecture

The logical framework shall support any ICC-managed devices used by existing or future applications. Mechanisms and templates of the framework shall embed the basic operations and data elements/objects of these applications without restricting their usage or enforcing a redefinition.

Figure 1 outlines some of the projected data templates and mechanisms provided by the operating system with the purpose to use the expanded functionality within the operating system/applications.

The logical architecture shall also include the usage of electrical devices located outside of the card. The interchange and security measures for such are the same as for devices on the card. Any access shall be under the control of the ICC; in case of external devices, an additional functionality for the external world shall be defined. Security is achieved by application of authenticity and confidentiality to transported data.

Logical system architecture is detailed in ISO/IEC 18328-3.

Annex B outlines examples of use cases with ICC-managed devices.

Annex A
(informative)

Device application context

A.1 General

Identity-related crimes have spread significantly with the increasing use of cyberspace, where the process of verification and authentication is less transparent than in an off-line environment. Criminals and other adversaries often exploit poor identification, authentication and authorization practices, as well as the infrastructure that the Internet utilizes. Thus, secure identification and authentication has arguably become the most important single security mechanism.

The classic paradigm for establishing confidence in an identity identifies the following three factors as the cornerstone of authentication:

- something you know, e.g. a password;
- something you have, e.g. an ICC or a cryptographic key;
- something you are , e.g. a fingerprint or other biometric data.

The strength of authentication mechanisms is largely determined by the number of factors incorporated. This part ISO/IEC 18328 focuses on multi-factor authentication with one of the factors being a physical token, such as an ICC or eID document.

For multi-factor authentication, there are two optional inputs to the token known as token activation *data* and token input data.

- Token activation data, such as a PIN or biometric data, may be required to activate the token and permit generation of an authenticator. Token activation data is needed when the token is controlled through something you know or something you are.
- Token input data, for example, a challenge or a nonce, may be required to generate a token authenticator. It may be supplied by the user or be a feature of the token itself (e.g. the clock in an OTP device).

A.2 Motivation for biometric capture devices on cards

The use of biometric characteristics for local authentication has many benefits. Example use cases include “unlocking” conventional authentication tokens, preventing repudiation of registration, or verifying that the same individual participates in all phases of a registration process. In order to improve the binding of an authentication token to the token owner, it is beneficial to integrate biometric capture device in ICC. Typical are fingerprint sensors, combined with on-card fingerprint storage and fingerprint verification.

- On-card biometrics allow for different modes for card authentication: PIN only, biometrics only, PIN or biometrics, PIN and biometrics.
- On-card biometrics allow for different modes for user authentication, from one-factor (card only) over various two-factor combinations up to three-factor authentication: token, PIN and biometrics.
- Biometric credentials are securely stored and processed on the ICC and therefore not susceptible to service outages or man-in-the-middle attacks.
- Enhanced convenience: biometrics are easier to use and there are no forgotten PIN issues.

- Enhanced privacy and compliance: biometric credentials never leave the card (no need to store biometric data in central repositories).
- No infrastructure required for enrolment and verification.

A.3 Motivation for token on ICC

Token is a popular application for ICC with on-card input/output devices. By combination of such devices, the following use cases are implemented.

- Single-factor one-time password (OTP) Token: Hardware device that generates one-time passwords based on an embedded secret used as the seed for generation and that does not require activation through a second factor. Typically, the OTP (e.g. six characters) is displayed permanently on the device and no user input is required.
- Multi-factor one-time password (OTP) token: Hardware device that generates one-time passwords which requires activation through a second authentication factor, i.e. something you know or something you are. The second factor can, for example, be realized via some entry pad or an integral biometric capture device (e.g. fingerprint). The one-time password is typically displayed on the device for a short period of time.
- Multi-factor cryptographic token: Hardware device that contains a protected cryptographic key that requires activation through a second authentication factor, i.e. something you know or something you are. The second factor can be realized, for example, via some entry pad or an integral biometric capture device (e.g. fingerprint). Authentication is accomplished by proving possession of the device and control of the key, which typically results in a cryptographically signed message. Details depend on the specific cryptographic token and protocol.

Table A.1 characterizes the different popular tokens.

Table A.1 — Key characteristics for these use cases

Device	Display	Input Elements	Remarks
Single-factor OTP token	segmented display	none	on-board power source required
Multi-factor OTP token	segmented display	keypad and/or biometric capture device	no on-board power source required
Multi-factor crypto token	LED	keypad and/or biometric capture device	no on-board power source required

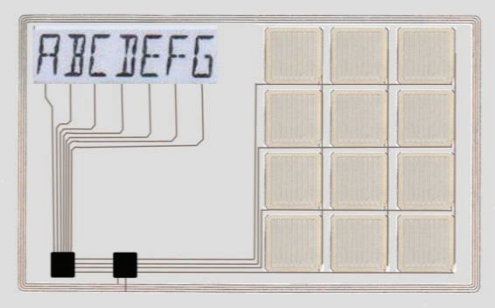


Figure A.1 — Example of a multi-factor OTP token with integrated display and keypad

Annex B
(informative)

Use cases

B.1 PIN verification or PIN input on the ICC

B.1.1 Display user control information

Some applications using ICC as a security element, e.g. signature cards run in unprotected environments with terminals which may be corrupted. The user of the application is not able to identify the correctness of the session and the reliability of the terminal. A display on the card may allow the user to control the authentic input on the terminal keypad when the ICC is able to display the input on the display of the ICC, because the communication of the terminal with the ICC is normally secured by a secure channel. The secured and authentic communication channel between IFD and ICC can be checked in this way by the user and a man-in-the-middle-attack may be avoided.

Same check may be performed by reading of internal information which is stored encrypted on the card in secured channel. If the card is able to show the plain text on its own display, the user is convinced that the terminal is trustworthy.

B.1.2 PIN verification on the ICC

Applications on an ICC protect the access to specific functionality or data after a successful verification of a user PIN or password. Normally, the input is performed on the keypad of the terminal. In addition, a secure channel is necessary to perform a VERIFY command. High secured applications, e.g. signature applications, are obliged to use expensive IFD or terminals to allow an authentic input via a special secured keypad.

All these measures are redundant when an ICC allows the authentic input of a PIN on a keypad located on the ICC. The terminal has to trigger the application to perform the input of the information on the ICC's keypad and perform a verification of the data internally of the ICC without involvement of the terminal.

Both use cases may be combined, e.g. with a touch-screen.

B.1.3 Reference data changing with on-card display and keypad

An ICC with an electronic display and a keypad offers new possibilities for PIN or password change. This password change is separated in several steps with interactive usage of display and keypad.

The request for the Verification Data and New Reference Data starts with a display message "ENTER YOUR PIN". The current value is entered on the keypad and may be temporarily stored in the ICC for later verification. A process of re-entering this value may be necessary for security reason. For getting the new reference data, the message "ENTER NEW PIN" is displayed and the new value is entered on the keypad. The value may be stored in the ICC. The procedure may be also repeated again for security reasons.

After having all information available, the ICC operates the CHANGE REFERENCE DATA command.

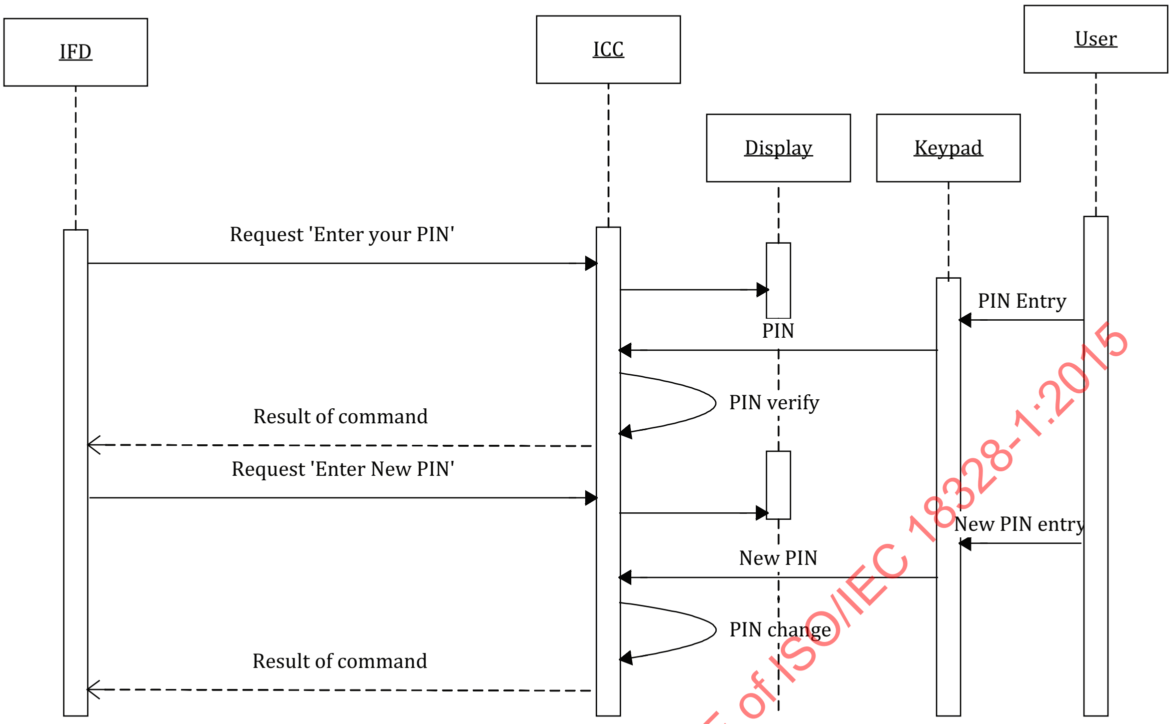


Figure B.1 — Reference data changing with on-card display and keypad on ICC

B.2 Temporary numbers

B.2.1 One-time password

An authentication of a user by a remote entity may use PIN or password verification to identify that the user is in possession of the ICC, e.g. on contactless applications or in applications running over a remote interface. Most of the applications today are using static passwords/PINs. To increase the security, the card may use session-related PINs or passwords instead, which are generated within the session on the ICC. This one-time password may be generated on the card-IC according a specific algorithm and can be checked on the remote counterpart which has the same knowledge.

The PIN or password is notified temporarily on the display of the ICC and may be used in the course of the application. Entering the PIN or passwords may be done on the keypad of the IFD or ICC.

B.2.2 Transaction numbers

Instead of a one-time password, some applications use transaction numbers which authenticates the cardholder. The dynamic transaction numbers notified on the display of the ICC are only available if the security state allows the access to this functionality. The expected transaction number can be checked by the remote application.

B.2.3 Card access numbers

A Card Access Number is used to identify the acknowledgement of the user to perform an application, especially in the contactless case. This number is used to establish the secure channel between the card and the terminal (see Reference [10]). To prevent misuse (eavesdropping and skimming) and to enhance the entropy of the secrets a display and/or a keypad on the ICC allow in combination both intentions. The on-card application generates a random/dynamic Card Access Number, e.g. after enabling the physical interface or selection of an application, and notifies it on the display of the ICC. This information may be optically scanned, e.g. by an optical reader or keyed in by an operator or cardholder (e.g. on a keypad on the computer or on the ICC) to setup the key establishment of the security protocol and the security channel. The displayed information in the display may be presented in many different ways, e.g. alpha-numeric, optical signal-based, or in combination with static information, etc.

B.3 Display of internal stored data

Applications on an ICC store data which may be interesting or relevant for the user/cardholder, e.g. in a banking application the amount of a balance or a purse might be interesting for the cardholder or in ID-applications the home address of the cardholder is shown. The application may read the internal stored data and can notify it on the display of the ICC. In case of a bi-stable display, this information is shown always and will be only changed if internal stored value has changed.

The display of internal stored data only known to the cardholder might be also an additional security feature to notify the user a secure channel has been established. This internal data might be notified on the display of the ICC. The user or cardholder can check the authenticity of the IFD or middleware by comparing the displayed information.

B.4 Display of received external data

A banking application needs the authorisation of an amount by the cardholder. Normally, this amount is displayed by the terminal at POS or ATM. Today the cardholder has to trust the terminal and a receipt is necessary to check the transaction amount. With a display on an ICC the cardholder is enabled to check the amount independently from the terminal when the amount is notified at the display of the ICC. If the display activity is combined with the use case in B.4, with an established secure channel the user can identify the authenticity of the terminal as well.

B.5 Trust assessment with display or LED

This feature may be generally used to enhance trust in the course of any application by using a simple display techniques, e.g. LED. This LED is controlled by the card-IC and tells the cardholder that the transaction is correctly running and trustable.

B.6 User consent with additional ICC-managed devices

If a service provider requires user information (e.g. attributes like name, home address, etc.) to grant access to an electronic service, user consent prior to user information delivery is preferable. To prevent user profiling or tracing, user consent is of utmost importance to ensure that only attributes necessary to access the electronic service are disclosed to the service provider.

This use case illustrates a solution for such selective disclosure by relying on non-cryptographic means with an ICC managing an on-board electronic display and input devices (e.g. buttons, touch-screen).

The service provider either

— exposes on the electronic display on the card the list of attributes for selection along with their respective applicable conditions required for the access to the service, and ask for selection and acceptance of the attributes to be disclosed, or

— exposes on a monitor (e.g. on a html form) the list of attributes for selection along with their respective applicable conditions required for the access to the service and user gives confirmation on the keypad on the card for the selection of the attributes to be disclosed.

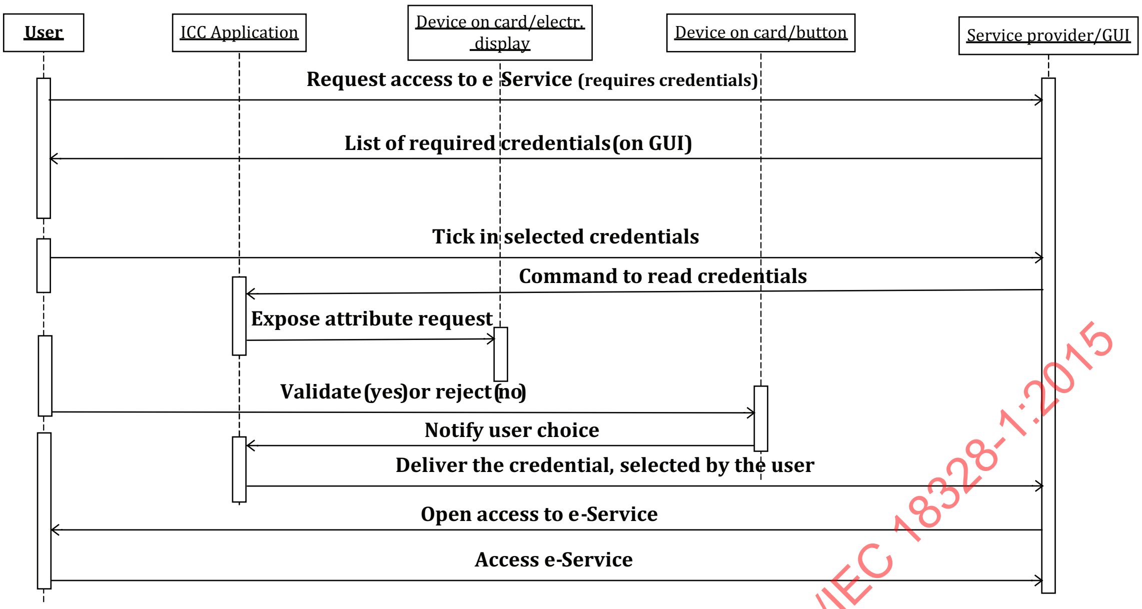

User
ICC Application
Device on card/electr. display
Device on card/button
Service provider/GUI
Request access to e Service (requires credentials)
List of required credentials (on GUI)
Tick in selected credentials
Command to read credentials
Expose attribute request
Validate (yes) or reject (no)
Notify user choice
Deliver the credential, selected by the user
Open access to e-Service
Access e-Service

Figure B.2 — ISO/IEC 18328 usage in combination with User Consent

B.7 Usage of ISO/IEC 18328 in handsets

B.7.1 eSE-managed devices

Trusted Execution Environment (TEE) is a special secure environment running on the main handset chipset and providing hardware-based isolation from rich operating systems. This kind of secure extension of the mobile hardware is used by several Mobile Operating Systems.

A Secure Element (eSE) embedded on a handset, e.g. mobile with a TEE, may host additional functionality, data structures and access rules along with cryptographic secrets according to this part of ISO/IEC 18328. Such eSE may exclusively control the access to an additional device off-card (e.g. LED, buttons, loudspeaker, etc.) by application of ISO/IEC 18328 mechanisms. In combination with a TEE, extended with functionality related to this part of ISO/IEC 18328, this usage enhances security and trust, e.g. loudspeaker, LED or display may be active, during transactions held by TEE application running on-board the handset.

Figure B.3 incorporates this use case as an example of ISO 18328-compliant Secure Element controlling off-card devices in a handset environment. When a TEE transaction starts, the TEE initiates the activation of the device handling in the eSE. The eSE activates e.g. a LED or start a tone on a loudspeaker to signal the external world, that a secure TEE transaction take place. Before finishing the TEE transaction, the signal has to be stopped.

It is not the role of such ISO/IEC 18328-compliant eSE to substitute to the TEE control of hardware secure resources by relying on secure drivers piloting the handset usual devices; TEE has privileged access to handset resources as user interface (e.g. keypad, screen), crypto accelerators, secure elements, etc. Besides the secure drivers' path, TEE can establish a secure channel with the eSE and addresses instructions from TEE application to application hosted by the eSE and implementing ISO/IEC 18328 interchange.

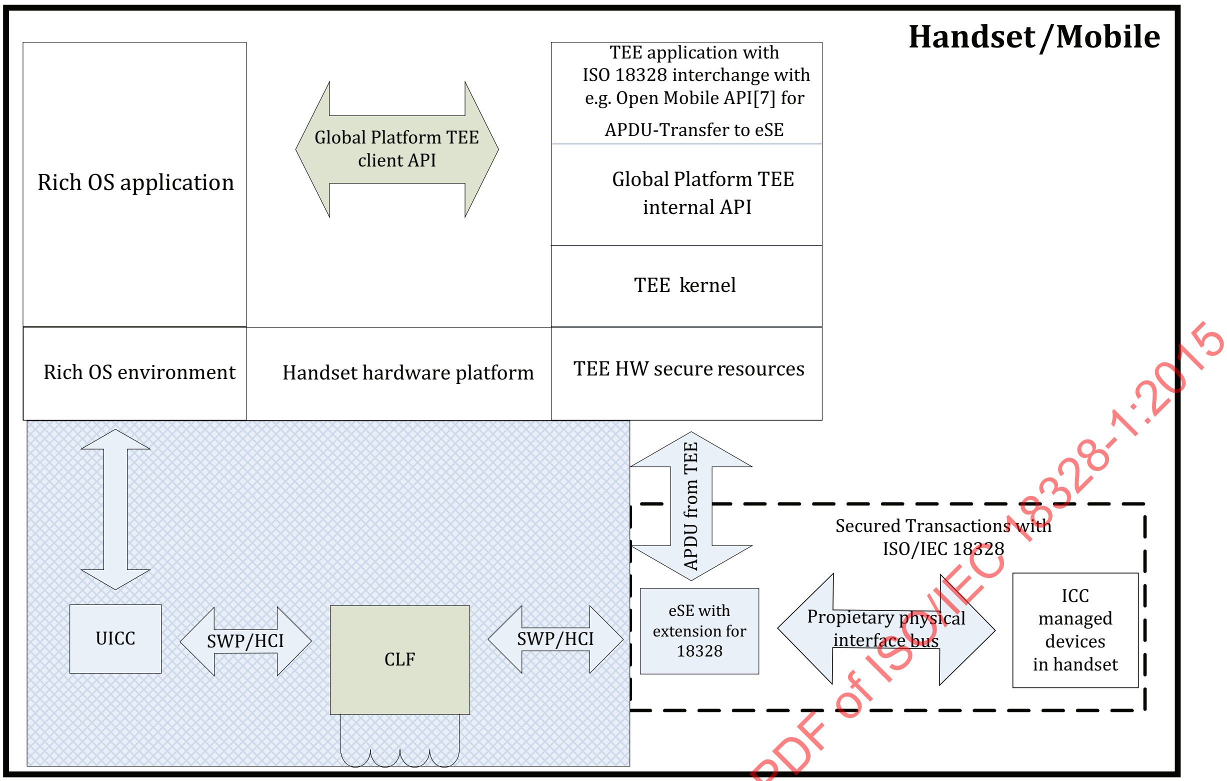

Handset/Mobile
Rich OS application
Global Platform TEE client API
TEE application with ISO 18328 interchange with e.g. Open Mobile API[7] for APDU-Transfer to eSE
Global Platform TEE internal API
TEE kernel
Rich OS environment
Handset hardware platform
TEE HW secure resources
APDU from TEE
Secured Transactions with ISO/IEC 18328
UICC
SWP/HCI
CLF
SWP/HCI
eSE with extension for 18328
Propietary physical interface bus
ICC managed devices in handset

Figure B.3 — ISO/IEC 18328 usage in a handset environment

B.7.2 Extension of TEE transaction via ICC

A contactless ICC supports ISO/IEC 18328 interchange and is equipped with a keypad, a LED or an electronic display, etc. This ICC is coupled with a NFC-enabled mobile. A TEE application running in the TEE environment starts a transaction and initiates the on-card device control via the NFC-Interface on the ICC.

Once the ICC and the related application has verified and checked the access rights of the TEE request, it activates the on-card device controller, e.g. to light or blink a LED or to sound a tone on a loudspeaker. The user notifies the available TEE application on the mobile.

The user may be prompted (may be through an optional on-card electronic display) to press a button to trigger purposely the digital signature validating the transaction. The cryptogram may be returned to the TEE.

Figure B.4 illustrates this use case.

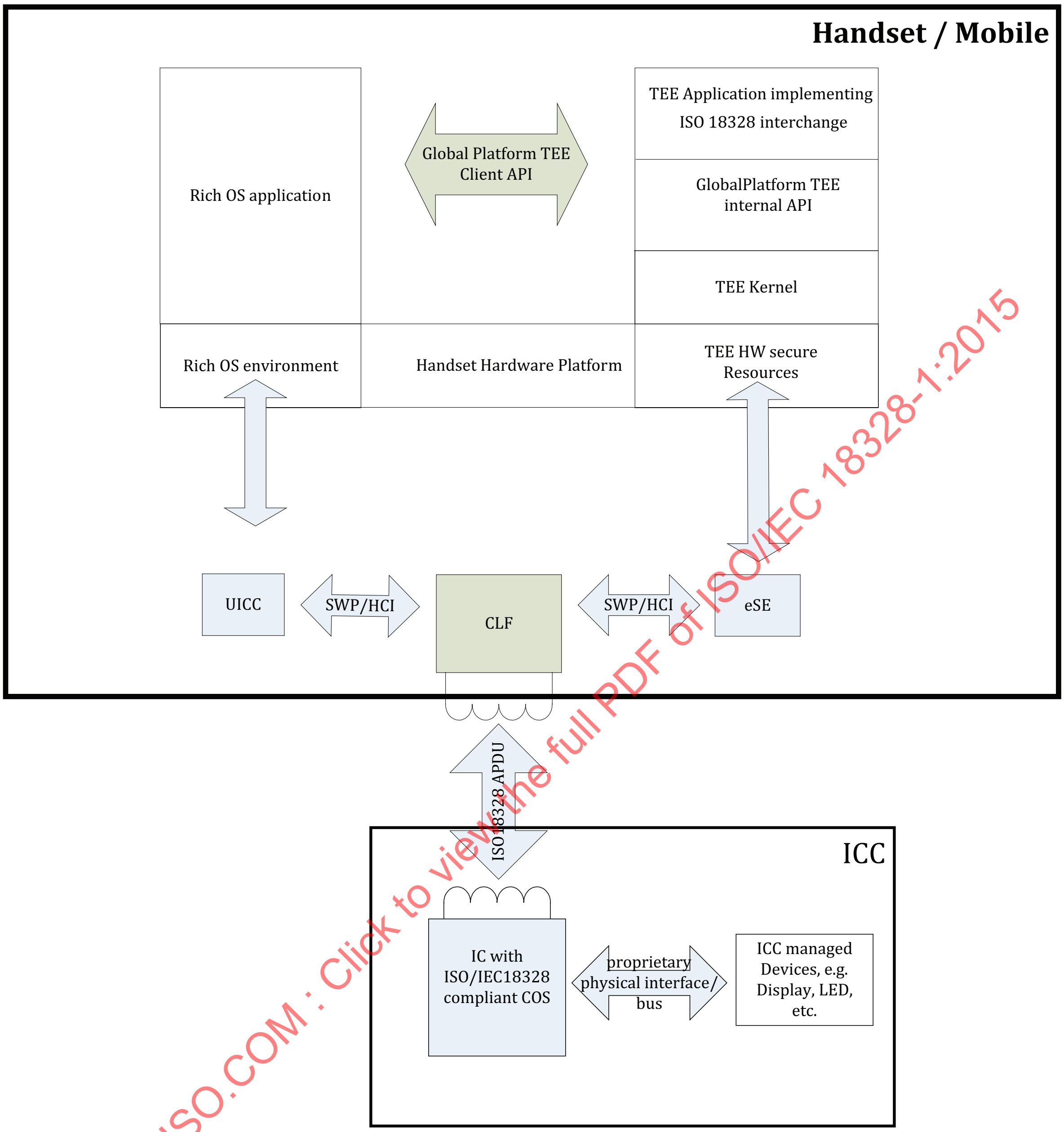

Handset / Mobile
Rich OS application
Global Platform TEE Client API
TEE Application implementing ISO 18328 interchange
GlobalPlatform TEE internal API
TEE Kernel
Rich OS environment
Handset Hardware Platform
TEE HW secure Resources
UICC
SWP/HCI
CLF
SWP/HCI
eSE
ISO18328 APDU
ICC
IC with ISO/IEC18328 compliant COS
proprietary physical interface/ bus
ICC managed Devices, e.g. Display, LED, etc.

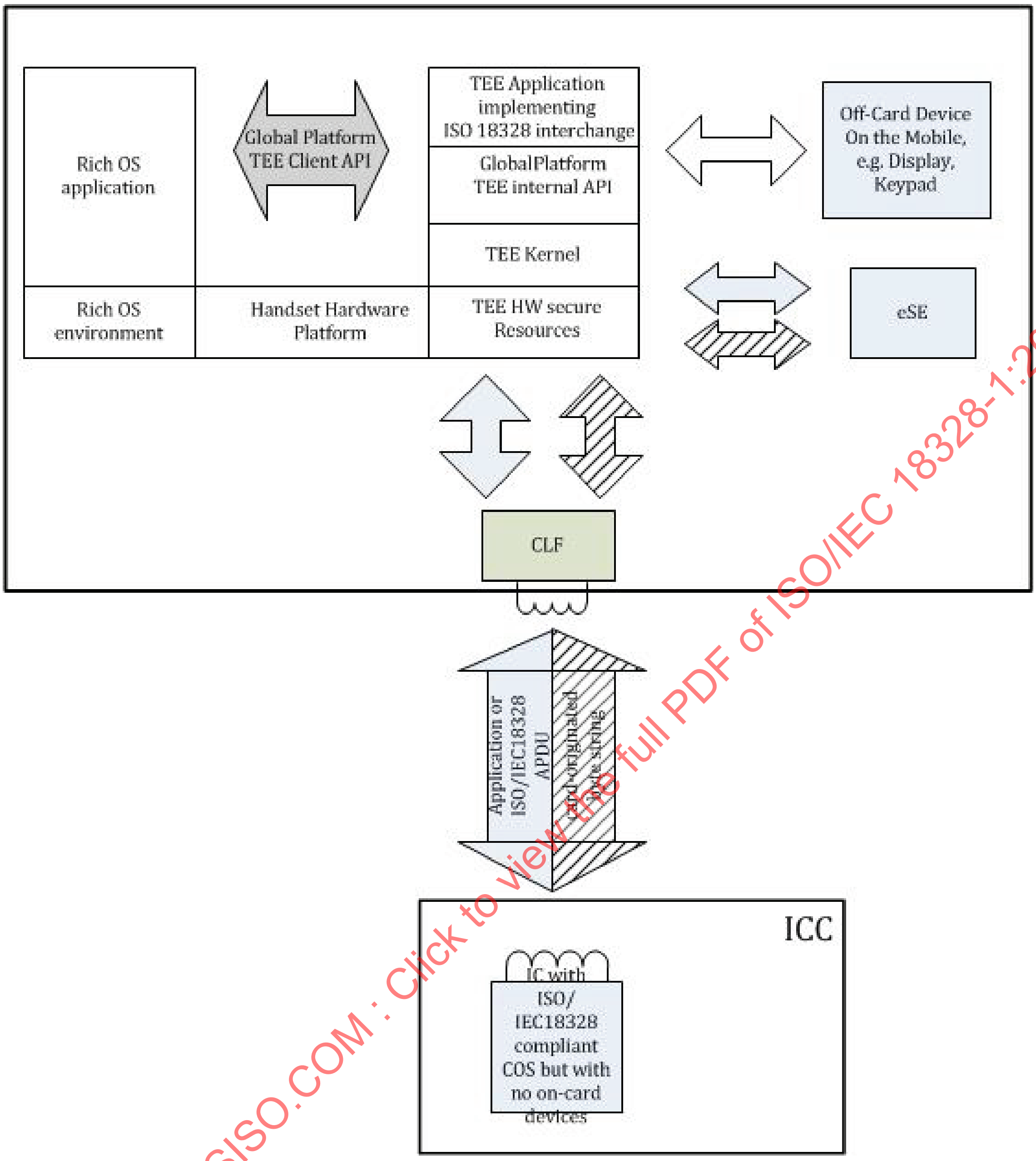
Figure B.4 — ISO/IEC 18328 usage with ICC and handset environment

B.7.3 Usage of off-card devices in a card application with TEE support

A supporting TEE application is running in a mobile. A contactless ISO/IEC 18328-enabled ICC without having any on-board devices is used to run an application, e.g. an ID-application, triggered by the mobile as IFD. In the course of the application, a user input, e.g. specific information or PIN, is requested which shall be entered.

Once the ICC and the related application on the ICC has verified and checked, the access rights of the request and the ICC supports ISO/IEC 18328 mechanisms, it activates a separate reverse command channel by using the card-originated byte string mechanism. With this channel, the ICC is able to handover command strings to the supporting TEE application, e.g. to get input from the keypad and/or to put information on display of the mobile. This channel may be protected with additional security means, e.g. using encryption of the byte strings, temporarily defined colours or fonts, etc.

The result of the card originated byte string command is returned to the card and can be used in the course of the application. Figure B.5 illustrates this use case.


Rich OS application
Global Platform TEE Client API
TEE Application implementing ISO 18328 interchange
GlobalPlatform TEE internal API
Off-Card Device On the Mobile, e.g. Display, Keypad
TEE Kernel
Rich OS environment
Handset Hardware Platform
TEE HW secure Resources
eSE
CLF
Application or ISO/IEC18328 APDU
Card originated byte string
ICC
IC with ISO/IEC18328 compliant COS but with no on-card devices

Key

▨ ISO/IEC 18328 card origined byte string

⇔ APDU based interface

Figure B.5 — Off-card device usage with ICC in a handset environment

B.8 Usage of ISO/IEC 18328 in security protocols

B.8.1 Facilitation of secure end-to-end communication

When performed peer-to-peer, a secure messaging (SM) between a server and an ICC uses session keys that are not shared with the middleware. This obvious security measure hinders the communication