INTERNATIONAL STANDARD

ISO/IEC 18328-3

First edition
2016-10-15

Identification cards — ICC-managed devices —

Part 3: **Organization, security and commands for interchange**

Cartes d'identification — Dispositifs contrôlés par carte —

Partie 3: Organisation, sécurité et commandes pour les échanges

Reference number
ISO/IEC 18328-3:2016(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

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. 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*.

A list of all parts in the ISO 18328-series can be found on the ISO website.

Introduction

The purpose of this document is to establish a normative basis for ICCs with at least an additional device.

Many new developments of electronic displays and keypads offer the technical opportunity to integrate such devices on an ICC. First products are already available and the technical progress driven by mobile devices also enforces the definition of basic standards for these technologies. Upcoming projects require several different standardized aspects.

These different aspects are in the focus of the standardization related to electronic devices on ICC, primarily the physical and electrical aspects, but also in addition the logical, organizational and security definitions.

Physical characteristics for devices on an ICC are handled in ISO/IEC 18328-2. ISO/IEC 18328-3 deals with the logical and security aspects and covers all relevant definitions and mechanisms to logical interfaces, command sets, data structures and security aspects.

Many aspects in this document refer to ISO/IEC 7816 (all parts).

ISO and IEC draw attention to the fact that it is claimed that compliance with this document may involve the usage of the following patents and the 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 these patent rights.

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 document 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.

Identification cards — ICC-managed devices —

Part 3: Organization, security and commands for interchange

1 Scope

This document specifies the logical interface of an application supporting the necessary security features in a card-IC which communicates with the external world by a physical interface supporting APDUs. This application supports the usage of electronic devices.

This involves the design of commands, data structures and security mechanisms which are required to handle the data and handling the additional devices itself. The handling of the additional devices is always controlled by the card-IC. External inputs or outputs shall be managed by the existing interfaces. This document deals not with physical characteristics of the card and interface technology, but only with the logical aspects. Management of data for additional devices that is not subdued by the COS or application control is out of the scope of this document.

Definitions of coding requirement for "trust assessment" of the managed data like warning, font, colour etc. is in the scope of this document. A description of the logical internal interface functionality used by the COS or by device drivers, if any, is also part of this document.

Due to the fact that relevant technologies may evolve or be adopted very fast, this document defines commands and structures supporting extensions and adaptations.

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 7816-4, *Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange*

3 Terms and definitions

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

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

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

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

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

3.2
application
structures, data elements and program modules needed for performing a specific functionality

3.3
button
tactile device used for a singular input

3.4
card-IC
integrated circuit with COS

3.5
command-response pair
set of two messages at the interface

EXAMPLE A command APDU followed by a response APDU in the opposite direction.

3.6
data element
item of information seen at the interface for which are specified a name, a description of logical content, a format and a coding

3.7
data object
information seen at the interface consisting of the concatenation of a mandatory tag field, a mandatory length field and a conditional value field

3.8
device
additional electronic feature used as an extension of the ICC

3.9
device driver
part of the operating system which provides the required functionality and interfaces to the additional devices on ICC

3.10
device identifier
data element used to reference a device

3.11
device handle
logic data element used to work with a selected device

3.12
device manager
entity in an ICC which controls the device operation

3.13
device unit
electronic system providing all relevant entities to work with the device on the card

EXAMPLE Connections, driver-microcontroller, etc.

3.14
EF.ATR/INFO
optional EF indicating operating characteristics of the card, also known as Information file

3.15
electronic display
electronic device transporting optical information

3.16
file
structure for application and/or data in the card, as seen at the interface when processing commands

3.17
identification card
card identifying its holder and issuer, which may carry data required as input for the intended use of the card and for transactions based thereon

3.18
interindustry
occurring, existing or using between two or more industries

3.19
key
sequence of symbols controlling a cryptographic operation

EXAMPLE Encipherment, decipherment, a private or a public operation in a dynamic authentication, signature generation production, signature verification.

3.20
keypad
array of several buttons organized as one entity

3.21
payload
data of arbitrary length, to be sent to the card or by the card, in order to be processed together

3.22
record
string of bytes stored within EF, referenced and handled as a unit

3.23
secure messaging
set of means for cryptographic protection of (parts of) command-response pairs

3.24
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

3.25
secure element
tamper-resistant ICC in a different form factor securely hosting applications and their confidential and cryptographic data

3.26
security environment
set of components required by an application in the card for secure messaging or for security operations

3.27
structure
DF, EF, record, Data String or DO

3.28
template
concatenation of BER-TLV data objects, forming the value field of a constructed BER-TLV data object

4 Symbols and abbreviated terms

ACD	application capability description
ADM	additional device management
APDU	application protocol data unit
ATR	answer-to-reset
ATS	answer-to-select
BER	basic encoding rules of ASN.1 (see ISO/IEC 8825-1)
CCD	card capability description
CLA	class byte
COS	card operating system
NOTE	COS is a logical element for implementation of functionalities defined in ISO/IEC 7816-4.
CRT	control reference template
C-RP	command-response-pair
DF	dedicated file
DHN	device handle number
DO	BER-TLV data object
DO'...'	BER-TLV data object, the tag of which is a hexadecimal value given between simple quotes
DVCP	device control parameter
EF	elementary file
EF.ATR/INFO	answer-to-reset file, or information file
FMD	file management data
FCI	file control information
IC	integrated circuit
ICC	integrated circuit card
IFD	interface device
INS	instruction byte
I^2C	inter-integrated circuit
LCD	liquid crystal display
LED	light emitting diode
Le field	length field for coding the number N_e
N_c	number of bytes in the command data field

N_e	maximum number of bytes expected in the response data field
Nr	number of bytes in the response data field
OID	object identifier, as defined by ISO/IEC 8825-1
OLED	organic light emitting diode
RF	radio frequency
RFU	reserved for future use by ISO/IEC JTC 1/SC 17
SPT	security parameter template
SW1-SW2	status bytes (inserted for clarity, the dash is not significant)
TEE	trusted execution environment
TLV	tag length value
UTF	universal character set transformation format

5 Architectural aspects

5.1 General architecture

An ICC comprising additional devices connected to the card IC extends the functionality of existing implementations and applications. The new components require different new physical aspects to the card and the electronic system as well as some new approaches in logical perspective. Architecture, activities, commands and security are aspects which have to be covered in addition to existing standards. The definitions shall be easily extensible for new developments in the future.

An ICC with additional devices consists of an ICC with

- an interface to the external world, e.g. a contact module or an antenna,
- at least an electronic device connected physically to the card IC, or
- logically linked additional off-card devices.

The COS may support the usage of an additional device with an extension or an internal interface to an additional driver which may allow unidirectional or bi-directional information flow.

NOTE Devices referred in this document may consist of additional electronic equipment which allows delivering activity state information or internal device information even in the case of an output device. The ability is defined in the administration data of such devices.

This document deals with the interfaces between the external world and the ICC, and the ICC with the electronic device. A physical interface between the ICC and any input/output device on the card may use different technologies and transmission protocols. This is out of scope of this document. The COS should always enable communication via the implemented interfaces with any device.

An ICC with input/output devices is controlled by means of the COS. The general principle is kept, that the card is the slave, steered by commands of the IFD as the master. The initiative of any operation performed with an additional device shall be caused by the external world or IFD, by the COS or the active ICC application. A direct connection of the outside world to any input/output device on the card is not covered by this document and is finally forbidden.

The principles of access control to any additional devices shall be compliant with the access control syntax to files and data objects defined and described in ISO/IEC 7816-4.

The communication of the external world with the ICC dealing with an additional device consists of APDUs with C-RP according to the definition in ISO/IEC 7816-4. The handling of the APDU is always in the responsibility of the COS and uses the security means defined in ISO/IEC 7816-4.

The physical interfaces to different additional electronical input/output devices use a large variety of electronic protocols, e.g. I^{2}C, SPI, etc. The definition of a physical interface and related security requirements, e.g. integrity and confidentiality of transferred data to any input/output device and vice versa, is not in the scope of this document. Nevertheless, it is recommended to define generic abstract activities/instructions on a logical level to these interfaces to ease the description of any required activities.

This concept considers additional devices on a card, but also sets a general framework applicable to card or secure element implementing interchanges according to this document and using interfaces to off-card devices, e.g. display, LED and/or button in a handset.

For an informative description of the general system, see D.1.

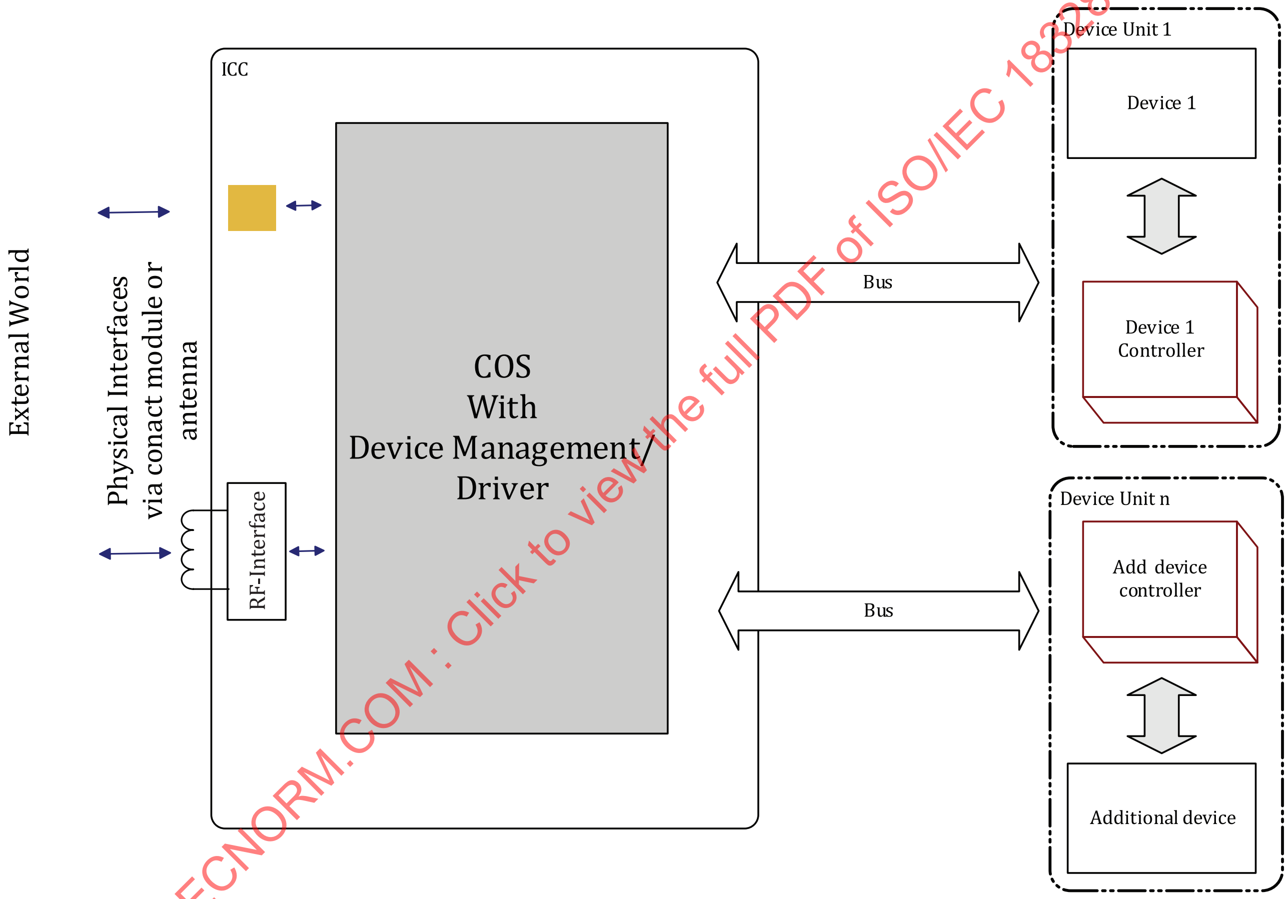


Figure 1 — Schematic ICC system with electronic devices

5.2 Operational conditions

5.2.1 Interfaces

Any transport protocols and interfaces are possible (e.g. according ISO/IEC 7816-3, ISO/IEC 7816-12, ISO/IEC 14443) as far as they allow the transmission of APDU-command-response pairs as defined in ISO/IEC 7816-4.

5.2.2 Identification of additional devices

The external world is able to get the information about the card capabilities. The external world may use different ways to retrieve this information, for example, with the following:

- an analysis of the General Feature Management DO’7F74’ in EF.ATR/INFO;
- analysis of the FCI of a selected application to retrieve a general feature management DO’7F74’;
- an OID referring the data set of capability description out of the general device information template (see Table 10);
- other identification means of the card, e.g. information according to ISO/IEC 24727 (ACD, CCD, card info file).

5.2.3 Device discovery mechanism

If used for device identification, the general feature management DO’7F74’ (see ISO/IEC 7816-4) in EF.ATR/INFO or in the FCI of the selected application shall contain the on-card service DO’81’. This data object contains a bitmap defining the on-card services. An additional DO’83’ may denote a device identifiers list in the same order as denoted in the bitmap of on-card services. Multi-occurrences of the same type of devices are represented with a prefixed occurrence number (one byte) followed by the concatenation of device identifier (two bytes each). Each entry of occurrence number and concatenated list of device identifier corresponds to the related bit in the bitmap of DO’81’ of the on-card services.

Table 1 — Device identifier list DO’83’

Tag	Length	Value
‘83’	var.	Occurrence number byte **n** of on-card service type A || Device identifier A1 || ... || Device identifier An
		Occurrence number byte **m** of on-card service type B || Device identifier B1 || ... || Device identifier Bm
		...

Table 2 defines further entries in the DO’81’ of the General Feature Management DO’7F74’. If there is a need to add new devices, the feature list has to be extended.

Table 2 — Extension of feature-list-entries in general feature management DO’7F74’

Tag	Length	Meaning																
‘81’	var.	Sub-template identifier for on-card services																
		Feature-List [0..n], expandable																
		Byte 1								Byte 2								
		b8	b7	b6	b5	b4	b3	b2	b1	b8	b7	b6	b5	b4	b3	b2	b1	**Meaning of bits**
		1	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	Display (defined by ISO/IEC 7816-4)
		—	1	—	—	—	—	—	—	—	—	—	—	—	—	—	—	Biometric input sensor (defined by ISO/IEC 7816-4)
		—	—	1	-	—	—	—	—	—	—	—	—	—	—	—	—	Button
		—	—	—	1	—	—	—	—	—	—	—	—	—	—	—	—	Keypad
		—	—	—	—	1	—	—	—	—	—	—	—	—	—	—	—	LED
		—	—	—	—	—	1	—	—	—	—	—	—	—	—	—	—	Loudspeaker
		—	—	—	—	—	—	1	—	—	—	—	—	—	—	—	—	Microphone
		—	—	—	—	—	—	—	1	—	—	—	—	—	—	—	—	Touchscreen
		—	—	—	—	—	—	—	—	1	—	—	—	—	—	—	—	Battery

5.2.4 Logical activation of additional devices

After retrieval of the information about the capabilities of the card, a logical activation of an additional device starts with the opening process by an ADM command (see Clause 6). The identification of the device is achieved by application of the device identifier (see 5.4.2) in the command.

The COS/device management returns a device handle number (see 5.4.3). With the positive acknowledgement in the response by the card, the device is ready for further usage in the course of the application. Table 3 denotes the states of the activation of a device.

5.2.5 Activation sequence

After enabling the physical interface between the ICC and the external world, all devices on the card which are covered by this document are selectable with an ADM command. The IFD activates a device in IDLE/WAIT state with the following steps:

- retrieval of the device identifier by the device discovery mechanisms, e.g. described in 5.2.3 or device identifier is implicitly known;
- application of the relevant device identifier in an ADM OPEN DEVICE command;
- the successful selection of the device returns a device handle number;
- all subsequent activities are applicable with this device handle number (see Clause 6).

Logical channels other than the basic channel shall start an activation sequence independently if support of additional devices is requested. Annex A describes activation sequences.

5.2.6 Activity states of additional devices

The activity states of an additional device depend on the characteristics of the device itself. Table 3 defines the general activity states of additional devices. Possible actions within the states are listed and may be performed by the COS, the devices driver or the external world. These actions may take place even the device is in DEVICE OPERATION state.

Table 3 — Logical device states

State	Definition	Possible actions (or functions for ADM command)
INACTIVE	Device is not available, e.g. power is off	power-on/off
IDLE/WAIT	Device is selectable	open device, power-off
READY	Device is selected	reactivate/deactivate device, general/exclusive device usage, get device information, device input/output, general/logical reset device, physical device reset, power-off
DEVICE OPERATION	Device is actively in usage, e.g. wait for input on a button, visible information on a display, lighting instruction to an LED	deactivate device, get device information, erase device content, device input/output, general/logical reset device, physical device reset, power-off
DEACTIVATED	Device is temporarily not in usage	activate device, get device information, general/logical reset device, physical device reset, power-off

The state DEACTIVATED can be achieved with an ADM DEACTIVATION function at any state after an open device function.

Transitions between the states of an additional device and their entailing activities are described in Figure 2.

When in its activity state READY, DEVICE OPERATION or DEACTIVATED, an additional device is said in OPERATIONAL state.

NOTE The support of physical or logical power-on/off depends on each device. After power-on and enabling of the interfaces to the ICC, an additional device shall be in the activity state IDLE/WAIT waiting for the activation sequence. The activation starts with a selection of the device by the function ADM OPEN DEVICE and passes the state into READY. The active usage of the device switches this state into DEVICE OPERATION. In this state, an input device requests actively for the input data, e.g. a button is waiting to be pressed, an output device offers the information to the external world, e.g. a LED emits light. Most of these activities may be controlled by timer (see 5.2.9). Two conditions may occur by this timer control. The first is an end of time frame for successful input/output execution and the activity status of a device returns from DEVICE OPERATION to READY. The second is a timeout for unsuccessful input/output execution, a state transition of device activity does not occur and SW1-SW2 = '6483' is provided for this process. Defect devices are outside of the scope, handled by the application and are not reflected in the diagram.

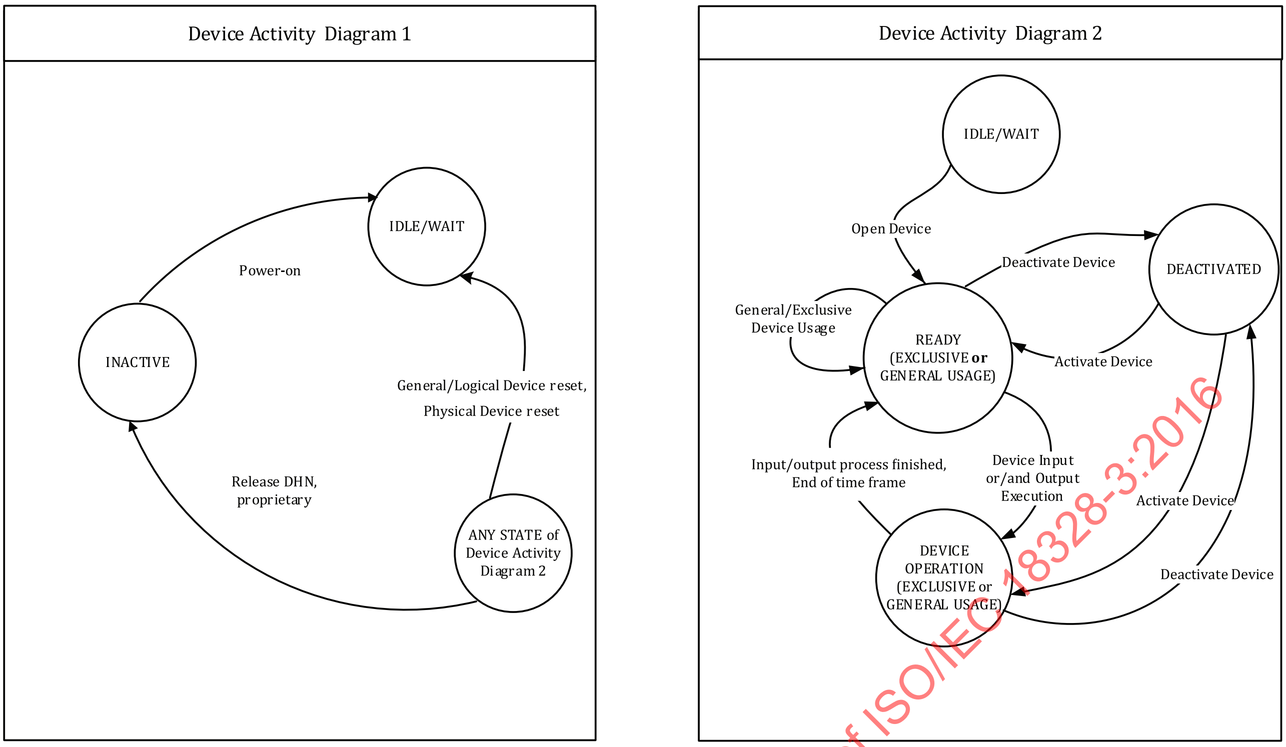

Device Activity Diagram 1
IDLE/WAIT
Power-on
INACTIVE
General/Logical Device reset,
Physical Device reset
Release DHN,
proprietary
ANY STATE of Device Activity Diagram 2
Device Activity Diagram 2
IDLE/WAIT
Open Device
Deactivate Device
DEACTIVATED
General/Exclusive Device Usage
READY (EXCLUSIVE or GENERAL USAGE)
Activate Device
Input/output process finished,
End of time frame
Device Input or/and Output Execution
Activate Device
Deactivate Device
DEVICE OPERATION (EXCLUSIVE or GENERAL USAGE)

Figure 2 — State diagram of electronic device activities

The external world may get the current activity state of any additional device by applying an ADM GET DEVICE INFORMATION command (see 6.3.11).

Table 4 shows meanings of this byte.

Table 4 — Activity status byte

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
—	—	—	—	—	x	x	x	**Activity State**
—	—	—	—	—	0	0	0	No information given
—	—	—	—	—	0	0	1	IDLE/WAIT
—	—	—	—	—	0	1	0	READY
—	—	—	—	—	0	1	1	DEVICE OPERATION
—	—	—	—	—	1	0	0	DEACTIVATED
—	—	—	—	—	x	x	x	any other values are RFU
—	x	x	x	x	—	—	—	0000, any other values are RFU
x	—	—	—	—	—	—	—	**Usage Attribute**
1	—	—	—	—	—	—	—	EXCLUSIVE DEVICE USAGE
0	—	—	—	—	—	—	—	GENERAL DEVICE USAGE

5.2.7 Exclusive usage attribute

Beside the activity states a specific usage attribute shall be applicable. This attribute reserves in case of EXCLUSIVE DEVICE USAGE the usage of the device for a single application only. The attribute can be set by a specific operation for all those devices which are allowed to be used by all applications (see

6.3.7). The general shareability of a device is denoted in the DVCP of the device (see 5.5.2.1). The usage attribute can be unset by an opposite operation to allow an unreserved usage again (see 6.3.8).

NOTE The unreserved mechanisms may be activated in some critical situations by COS or device management. This is outside of scope and depends on the policy for such situation. The process is responsible to restore the original settings.

5.2.8 General functionality

Independent from implemented internal interfaces between card IC and any input/out device, the COS shall be able to establish a stable physical and logical connection to the additional device. The COS serves and administrates the device handling internally or as an extension by specific driver functionality. The set of functions of the ADM command (see Clause 6) allows the external world to have also access to the device handling functionality.

To fulfil all required activities to an additional device, a set of internal abstract instructions or functionality shall be available in the COS to support the basic device handling. The following list describes the minimal set of functionality which may have a corresponding function in the ADM command. These functions may be used by the application internally whenever necessary, regardless of any ADM command.

- **Logical device reset**

  The device is logically set to the state IDLE/WAIT. All internal data structures are cleared, a device handle is released. See also 6.3.3.

- **Logical device selection**

  The device is opened and registered by assignment of a device handle. The state is switched to READY. See also 6.3.4.

- **Logical device activation**

  The device is switched from DEACTIVATED to READY or DEVICE OPERATION. See also 6.3.6.

- **Logical device deactivation**

  The device is switched from READY or DEVICE OPERATION to DEACTIVATED. The device is temporarily un-usable. See also 6.3.5.

- **Output of data on the device**

  The process to handover to a device can be only achieved in the state DEVICE OPERATION. A functionality performing such device output has to switch the internal state (temporarily) from READY to DEVICE OPERATION. Output data is handed on to the device. See also 6.3.10.

- **Input of data from the device**

  The process to receive data from a device can only be achieved in the state DEVICE OPERATION. A functionality performing such device input has to switch the internal state (temporarily) from READY to DEVICE OPERATION. Input data is requested from the device. See also 6.3.9.

- **Get state of activity of additional device**

  The internal status of the device is requested. This functionality is available at any state after open device operation. See also 6.3.11.

- **Set state of activity of additional device**

  The internal status of the device is set by the application. This internal functionality may be available at any state after open device operation.

— **Reserve device**

The device is exclusively usable by a single application. See also 6.3.7.

— **Un-reserve device**

The exclusive usage of a device is unset. See also 6.3.8.

— **Get device information**

General device information is requested and returned. This functionality is available at any state after OPEN device operation. See also 6.3.11.

— **Erase device content**

The content of the device is deleted or overwritten with a pattern. This functionality may be available in all states after OPEN device operation. See also 6.3.12.

— **Manage device configuration**

The predefined configuration values for a device are changed or set. See also 6.3.13.

This general functionality can be provided either by the COS or additional device control methods.

5.2.9 Timer control

In the course of the usage of an additional device on an ICC, the active conveyance of information to and from the device switches the device state from READY to DEVICE OPERATION. The process to output the data information or waiting for input depends on the system configuration and can be controlled by timer. Device configuration templates (see 10.1) enable a device management to use timer control for handling the input/output process. At the end of time frame, the process is stopped, the state switches from DEVICE OPERATION to READY and the result of the function is available.

5.3 Energy depending activation

Additional electronic devices on an ICC show specific power consumption requirements. Depending on the interface and the ability of the IFD, it may occur that not enough energy for additional devices on an ICC is available.

If this is the reason for a failure of an activation of such additional device, the ICC shall return a specific error code. Table 14 shows the additional device related SW1-SW2 values.

In case of energy deficits, an application dealing normally with additional devices may work without device usage in the course of the application.

5.4 Addressing of an additional device

5.4.1 General

The different entities managing or having access to any additional device administrated by the ICC shall address or reference these devices on a logical level. The physical mapping and access to a dedicated additional device is internally known by the COS or the additional device control methods.

5.4.2 Device identifier

The device identifier is the logical identifier to address an additional device on the card. It is the internal reference which is reserved for device oriented commands and is used by the COS to address the device unambiguously (see 5.2.3). The device identifier shall be a two-byte value.

5.4.3 Device handle

The device handle is a logical structure identified by a unique number which is defined by the COS for each additional device within a session. This number may be static or dynamic and shall be available or usable after the selection/open of the additional device.

Device identifiers are static values and internal references to the card and do not correlate directly to the device handle number (DHN). The COS shall maintain a logical link between uniquely attributed device identifier value and corresponding device handle number. A given DHN generated by the COS or statically assigned shall relate to a unique additional device identified by its unique device identifier. Once a DHN is available, it shall be employed by the external world instead of the device identifier from the device identifier list.

The device handles are used in the device related commands (see Clause 6). The DHN shall be returned by the card in the response to device selection. When a device turns INACTIVE, its current DHN shall be released. Table 5 shows the predefined static device handle numbers, which shall be used to address the related additional device.

Table 5 — Interindustry device handle numbers

Device handle number	Additional device
‘01’	Electronic display (static)
‘02’	Keypad (static)
‘03’-’7F’	Dynamic assignment
‘00’,’80’-’FF’	RFU

5.5 Device control information

5.5.1 Administration of additional devices

Device control information is a byte string available in the response of an ADM GET DEVICE INFORMATION command (see Clause 6) of an additional device. It offers internal information about the device to the COS or to the external world.

Table 6 — Interindustry templates for device control information

Tag	Value
‘62’	Set of device control parameters (DVCP DOs) (see Table 7)

5.5.2 Device control parameter DVCP

The control parameter DO’62’ provides information to handle or administrate a device by the COS, related entities and the external world.

Table 7 lists a set of DOs in the DVCP which are useful to gain information about the additional device and support the ICC to administrate the device internally. Some of the DOs are mandatory; others are optional, depending on the application and the device type.

NOTE This document does not define neither storage nor administration of device CP data, e.g. creating or modifying of CP data for devices.

Table 7 — List of possible control parameter for additional devices

Tag	Length	Value	Comment
‘82’	1,2,3	Device descriptor (see 5.5.2.1)	Mandatory
‘83’	2	Device identifier (see 5.4.2)	Mandatory
‘85’	var.	Proprietary information not encoded in BER-TLV	Optional
‘86’	var.	Security attribute in proprietary format	Optional
‘8A’	1	Current Activity State	Mandatory
‘8B’	var.	Security attribute referencing the expanded format (see ISO/IEC 7816-4)	Optional
‘8C’	var.	Security attribute in compact format, SE oriented (see ISO/IEC 7816-4)	Optional
‘8D’	2	Identifier of an EF containing security environment templates (see ISO/IEC 7816-4)	Optional
‘8E’	1	Logical Channel security attribute (see ISO/IEC 7816-4)	Optional
‘9C’	var.	Security attribute in compact format, SPT oriented (see ISO/IEC 7816-4)	Optional
‘A1’	var.	Security attribute template in proprietary format	Optional
‘A3’	var.	Interface and Activity State dependent security attribute template	Optional
‘A4’	var.	General device information template (see 5.5.3)	Optional
‘A5’	var.	Proprietary information encoded in BER-TLV	Optional
‘AB’	var.	Security attribute template in expanded format (see ISO/IEC 7816-4)	Optional
‘AC’	var.	Cryptographic mechanism identifier template (see ISO/IEC 7816-4)	Optional
‘AD’	var.	Security parameters template (see ISO/IEC 7816-4)	Optional

5.5.2.1 Device descriptor

Any additional device is characterized by its device descriptor. Table 8 shows the definition of the DO.

Table 8 — Device descriptor data objects

Tag	Length	Value	Applies to
‘82’	1	Device descriptor byte (see Table 9)	Any device
	2 or 3	Device descriptor byte (see Table 9) || Max. length of input/output data	

If DO’82’ is present, it shall be coded according to Table 8.

- The first byte of the value is the device descriptor byte (see Table 9).
- If the value consists of two or three bytes, then the additional bytes indicate the maximum number of data bytes the device is working with.

Table 9 — Coding of the device descriptor byte

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
x	—	—	—	—	—	—	—	**Device location**
0	—	—	—	—	—	—	—	— Off-card device
1	—	—	—	—	—	—	—	— On-card device
—	X	—	—	—	—	—	—	**Device shareability**
—	0	—	—	—	—	—	—	— Not shareable
—	1	—	—	—	—	—	—	— Shareable
—	—	x	—	—	—	—	—	**Additional device security**
—	—	0	—	—	—	—	—	— No additional security features
NOTE “shareable” means that the device is accessible on different logical channels by different applications.								

Table 9 *(continued)*

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
—	—	1	—	—	—	—	—	— Additional security features, further information in the general device information template (see DO’A1’ in Table 10)
—	—	—	x	x	x	—	—	**Device category**
—	—	—	0	0	1	—	—	— Input device
—	—	—	0	1	0	—	—	— Output device
—	—	—	0	1	1	—	—	— Input and output device
—	—	—	1	0	0	—	—	— Device for communication purposes
—	—	—	1	0	1	—	—	— Device for support functions
—	—	—	x	x	x	—	—	— any other values are RFU
—	—	—	—	—	—	x	—	**Device structure**
—	—	—	—	—	—	0	—	— Transparent structure or implicitly known
—	—	—	—	—	—	1	—	— Structured, structure information in general device information template (see Table 10)
						—	x	**Configuration DO capability (see 6.3.13 and Clause 10)**
—	—	—	—	—	—	—	0	— Device is not configurable
—	—	—	—	—	—	—	1	— Device is configurable, when security attributes allow this
NOTE “shareable” means that the device is accessible on different logical channels by different applications.								

A card may use device handling applications which also act with additional logical channels. A selected and opened device in an application may be shared in a different other channel. This information about shareability is available in the device descriptor byte.

5.5.3 General device information template

5.5.3.1 General

The general device information template DO’A4’ may be present in the DVCP and contains DOs which describe the general characteristics and attributes of the additional device. The external world may retrieve this template in the response data of an ADM GET DEVICE INFORMATION command (see 6.3.11) or by reading information with the referenced profile OID.

NOTE The external world may retrieve additional information in the document referenced by the OID.

Annex B gives examples of coding for device info template DO’A0’ in a general device information template regarding different devices.

Table 10 — General device information template content

Device information template	Length	Value			
‘A4’	var.	**General device information template**			
		Tag	**Length**	**Value**	
		‘06’	var.	Profile OID	Optional
		‘A0’	var.	Device info	Optional
		‘91’	‘02’	Supported ADM functions	Mandatory
		‘92’	var.	Product serial number	Optional

Table 10 *(continued)*

Device information template	Length	Value			
		‘A1’	var.	Additional device security features in proprietary format, referenced in device descriptor byte (bit 6 in Table 9)	Optional
		‘A2’	var.	Device feature template	Optional
		‘A3’	var.	Definition template for trust assessment (see 9.4 and Table B.10)	Optional

5.5.3.2 Profile OID

If available, this DO defines an OID which references a document containing the general device information template and other additional information.

5.5.3.3 Device info

Device Info DO’A0’ is a container of different proprietary data object describing the device for internal and external purposes. The interpretations of such data objects are in the responsibility of the application and the application related entities. Such DOs may describe, e.g. device type technology, device data type, structure information for input and output operations, etc. Annex B gives examples for device info DOs.

5.5.3.4 Supported ADM functions

This DO’91’ offers a bit map which indicates the support of ADM functions defined in Clause 6 (see Table 10).

Table 11 — Supported ADM functions

First Byte								Second Byte								
b8	b7	b6	b5	b4	b3	b2	b1	b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	general device reset
—	1	—	—	—	—	—	—	—	—	—	—	—	—	—	—	logical device reset
—	—	1	—	—	—	—	—	—	—	—	—	—	—	—	—	open device
—	—	—	1	—	—	—	—	—	—	—	—	—	—	—	—	deactivate device
—	—	—	—	1	—	—	—	—	—	—	—	—	—	—	—	reactivate device
—	—	—	—	—	1	—	—	—	—	—	—	—	—	—	—	exclusive device usage
—	—	—	—	—	—	1	—	—	—	—	—	—	—	—	—	general device usage
—	—	—	—	—	—	—	1	—	—	—	—	—	—	—	—	get from device
—	—	—	—	—	—	—	—	1	—	—	—	—	—	—	—	put to device
—	—	—	—	—	—	—	—	—	1	—	—	—	—	—	—	get device information
—	—	—	—	—	—	—	—	—	—	1	—	—	—	—	—	erase device content
—	—	—	—	—	—	—	—	—	—	—	1	—	—	—	—	manage device configuration
—	—	—	—	—	—	—	—	—	—	—	—	x	x	x	x	0000, any other values are RFU

5.5.3.5 Product serial number

The DO’92’ provides the product serial number of the device which enables a fast identification of the device type by the COS or external world.

5.5.3.6 Device feature template

The device feature template DO’A2’ may contain definitions and extensions for the additional device defined by other standards or protocols, and may be used by the external world to hand on specific technology-dependent data to the device; such data will be supported by the application accessing the device or by a device driver e.g. display manager. This template incorporates the device configuration template (see Clause 10) if existing, but other definition of value field of device feature template is out of scope of this document. Content of the device feature template could be, for example,

- one or more device configuration template(s),
- extensions, related to applications or specific requirements of applications, and
- references to proprietary means of application, e.g. for scripting, etc.

Table 12 — Device feature template content (under DO’A4’ in DVCP DO’62’)

Tag	Length	Value
‘A2’	var.	Device configuration template(s), other device type related low level templates, proprietary, may be filled by other standards

6 Functions of the ADDITIONAL DEVICE MANAGEMENT command

6.1 General

The interindustry command ADDITIONAL DEVICE MANAGEMENT comprises a set of functions which are used to perform all activities of a COS dealing with any additional device independent from existing or future physical interfaces.

The set of functions may be either implemented in the COS directly to have access to the additional device or there might be an internal interface description to a device driver hiding the real physical interface from the card-IC to the device or, for example, a display manager as a specific entity dealing all activities with the additional device.

The ADM command uses INS code ‘16’ and ‘17’. P1 indicates the different functions of the ADM command according to Table 13.

NOTE INS ‘17’ is currently not used, but shall be reserved for future use.

Table 13 — Coding of P1 in the ADDITIONAL DEVICE MANAGEMENT command

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	0	0	0	0	0	0	1	GENERAL DEVICE RESET function
0	0	0	0	0	0	1	0	LOGICAL DEVICE RESET function
0	0	0	0	0	0	1	1	OPEN DEVICE function
0	0	0	0	0	1	0	0	DEACTIVATE DEVICE function
0	0	0	0	0	1	0	1	REACTIVATE DEVICE function
0	0	0	0	0	1	1	0	EXCLUSIVE DEVICE USAGE function
0	0	0	0	0	1	1	1	GENERAL DEVICE USAGE function
0	0	0	0	1	0	0	0	GET FROM DEVICE function
0	0	0	0	1	0	0	1	PUT TO DEVICE function
0	0	0	0	1	0	1	0	GET DEVICE INFORMATION function
0	0	0	0	1	0	1	1	ERASE DEVICE CONTENT function
0	0	0	0	1	1	0	0	MANAGE DEVICE CONFIGURATION function
others								RFU

Related to the device type and the implementation of the device capabilities, not all functions are necessarily supported.

6.2 Specific status bytes for ADDITIONAL DEVICE MANAGEMENT

The result of the command processing is indicated by SW1-SW2. Table 14 lists additional device specific SW1-SW2 values.

Table 14 — ADM or device related values of SW1-SW2

SW1-SW2	Meaning
'6483'	Timeout occurred, no further information available
'6601'	Not enough power
'6981'	Device handle not retrievable /device is not suitable according to the command[a]
'6984'	Device identifier not valid (device identifier list DO'83' under DO'7F74' is not valid)
'6985'	Activity state not fit to command, condition of use is not satisfied
'6989	Format of command data field not fit
'6A81'	Activity status byte in DVCP forbids general device usage
'6A82'	DHN not available (P2 not valid)
'6A88'	DO is not available, requested information not available
'6F01'	Internal device error or device/device-driver not responding

[a] When ADM PUT TO DEVICE command is applied to an input device or ADM GET FROM DEVICE command is applied to an output device, device is not suitable for the command and = '6981' is appropriate.

When ADM GET FROM DEVICE or ADM PUT TO DEVICE command is not completed in a certain time defined by internal or external configuration, e.g. timing controls under DO'A3', timeout may occur.

6.3 Functions of ADDITIONAL DEVICE MANAGEMENT command

6.3.1 General command handling

The ADDITIONAL DEVICE MANAGEMENT command supports several functions outlined in detail in the next subclauses. All functions dedicated to devices handling in activity state OPERATIONAL addresses the device in P2 by a DHN. The function itself is defined as a number in P1 (see also Table 13).

The command is usable for on-card and off-card devices as well. When the off-card device is addressed by DHN in P2, further procedure defined in Clause 7 is required to complete this function indicated by ADM command.

6.3.2 GENERAL DEVICE RESET function

The function resets all devices which has been open and dealing with a DHN.

Any used DHN is released. This function addresses exclusively used or deactivated devices as well. As the result of this function, any device is in IDLE/WAIT state.

Table 15 — GENERAL DEVICE RESET function — Command response pair

CLA	As defined in ISO/IEC 7816-4
INS	'16'
P1	'01', (see Table 13)
P2	'00'
L_C field	Absent for encoding $N_C = 0$
Data field	Absent

Table 15 *(continued)*

L_e field	Absent for encoding $N_e = 0$

Data field	Absent
SW1-SW2	See ISO/IEC 7816-4 and Table 14

6.3.3 LOGICAL DEVICE RESET function

This function resets a single additional device which is in OPERATIONAL state. The device shall be addressed with DHN in P2. As the result of this function, this device will be in IDLE/WAIT state and its DHN is released.

Table 16 — LOGICAL DEVICE RESET function — Command response pair

CLA	As defined in ISO/IEC 7816-4
INS	‘16’
P1	‘02’, (see Table 13)
P2	Device handle number (see Table 5)
L_c field	Absent for encoding $N_c = 0$
Data field	Absent
L_e field	Absent for encoding $N_e = 0$

Data field	Absent
SW1-SW2	See ISO/IEC 7816-4 and Table 14

6.3.4 OPEN DEVICE function

Any access to an additional device is only allowed if the device is registered to the COS. The registration process shall be initiated by an OPEN DEVICE function. The device shall be addressed with a device identifier in command data field.

With this function, the device shall be initialized by COS means, e.g. initialization of a new device handle, get addressable by a device handle number and optionally set into a predefined condition. A device has to be in IDLE/WAIT state when this function is applied. When this function is performed successfully, the device is in READY state.

As the successful result of this function, a unique DHN for further addressing in this session is returned.

Table 17 — OPEN DEVICE function — Command response pair

CLA	As defined in ISO/IEC 7816-4
INS	‘16’
P1	‘03’, (see Table 13)
P2	‘00’
L_c field	Encoding $N_c = 2$
Data field	Device identifier
L_e field	Encoding $N_e = 1$

Data field	Device handle number
SW1-SW2	See ISO/IEC 7816-4 and Table 14

6.3.5 DEACTIVATE DEVICE function

An additional device shall be deactivated by applying this function. As a precondition for the command, the device has to be in the state READY or DEVICE OPERATION.

After a successful command processing, the device state is DEACTIVATED. In this state, GET FROM DEVICE and PUT TO DEVICE functions cannot be applied. In this state, REACTIVATE DEVICE, GET DEVICE INFORMATION and GENERAL/LOGICAL DEVICE RESET functions can be applied.

Table 18 — DEACTIVATE DEVICE function — Command response pair

CLA	As defined in ISO/IEC 7816-4
INS	‘16’
P1	‘04’, (see Table 13)
P2	Device handle number (see Table 5)
L_c field	Absent for encoding $N_c = 0$
Data field	Absent
L_e field	Absent for encoding $N_e = 0$

Data field	Absent
SW1-SW2	See ISO/IEC 7816-4 and Table 14

NOTE Activity state dependent security attribute setting on a device is recommended when this device supports DEACTIVATED state, i.e. to prevent logical device reset for reactivation or to restrict the unauthorized access to a device in DEACTIVATED state.

6.3.6 REACTIVATE DEVICE function

An additional device in DEACTIVATED state is activated into the state READY or DEVICE OPERATION by applying this function.

Table 19 — REACTIVATE DEVICE function — Command response pair

CLA	As defined in ISO/IEC 7816-4
INS	‘16’
P1	‘05’, (see Table 13)
P2	Device handle number (see Table 5)
L_c field	Absent for encoding $N_c = 0$
Data field	Absent
L_e field	Absent for encoding $N_e = 0$’

Data field	Absent
SW1-SW2	See ISO/IEC 7816-4 and Table 14

6.3.7 EXCLUSIVE DEVICE USAGE function

The exclusive access to an additional device may be obtained by bit 8 of activity status byte (see Table 4). A device in general usage is changed into exclusive usage by applying this function.

This function can be applied to a device supported usage attribute in OPERATIONAL state. This function does not change the activity state (bit 3 to 1) in the activity status byte but may change usage attribute (bit 8) in the activity status byte (see Table 4).

The data field of the command is absent and the current selected application exclusively uses the device addressed by DHN in P2.

Table 20 — EXCLUSIVE DEVICE USAGE function — Command response pair

CLA	As defined in ISO/IEC 7816-4	
INS	‘16’	
P1	‘06’, (see Table 13)	
P2	Device handle number (see Table 5)	
L_c field	Absent for encoding $N_c = 0$	
Data field	Absent	Application is internally known
L_e field	Absent for encoding $N_e = 0$	

Data field	Absent
SW1-SW2	See ISO/IEC 7816-4 and Table 14

6.3.8 GENERAL DEVICE USAGE function

This function turns back an additional device being set in exclusive usage by an EXCLUSIVE DEVICE USAGE function into general usage.

This function can be applied to a device in OPERATIONAL state. This function does not change the activity state (bit 3 to 1) in the activity status byte, but may change usage attribute (bit 8) in the activity status byte (see Table 4).

Table 21 — GENERAL DEVICE USAGE function — Command response pair

CLA	As defined in ISO/IEC 7816-4
INS	‘16’
P1	‘07’, (see Table 13)
P2	Device handle number (see Table 5)
L_c field	Absent for encoding $N_c = 0$
Data field	Absent
L_e field	Absent for encoding $N_e = 0$

Data field	Absent
SW1-SW2	See ISO/IEC 7816-4 and Table 14

6.3.9 GET FROM DEVICE function

This function enables input operation of an input device in READY state. While this function is being executed, the activity status of an input device is switched from READY to DEVICE OPERATION state. When an input device is in DEVICE OPERATION state, input operation is enabled. After input operation has finished or an end of time frame has occurred, the activity status of an input device is turned back from DEVICE OPERATION to READY state.

NOTE An input device means an input device or an input and output device.

The input data through an input device is returned as a response data field and/or stored in the ICC. The storage for the input data in the ICC is implicitly known by application or indicated by the object locator or general reference template in command data field.

The content of the response shall be structured according to the needs of the external world and the prescriptions for this may be found in the general device information template or is implicitly known.

Table 22 — GET FROM DEVICE function — Command response pair

CLA	As defined in ISO/IEC 7816-4	
INS	‘16’	
P1	‘08’, (see Table 13)	
P2	Device handle number (see Table 5)	
L_c field	Absent for encoding $N_c = 0$, present for encoding $N_c > 0$	
Data field	Absent	Input data through the device is not stored or the storage for this stored input data is implicitly known
	Reference to card internal object	Object locator DO’7F72’ or general reference template DO’60’ (see ISO/IEC 7816-4)
L_e field	Absent for encoding $N_e = 0$, present for encoding $N_e > 0$’	

Data field	Data possibly formatted according to general device information template (see 5.5.3)
	Absent, if input data through the device is not returned
SW1-SW2	See ISO/IEC 7816-4 and Table 14

6.3.10 PUT TO DEVICE function

This function enables output operation of an output device in READY state. While this function is being executed, the activity status of an output device is switched from READY to DEVICE OPERATION state. Then, the output data is put on an output device. After this process has finished or an end of time frame has occurred, the activity status of an output device is turned back from DEVICE OPERATION to READY state.

NOTE An output device means an output device or an input and output device.

The output data to an output device is presented in the command data field or shall be taken internally from the ICC. In this case, the data is implicitly known by application or indicated by the object locator or general reference template in command data field.

The output data shall be structured according to the needs of the device and the prescriptions for this may be found in the general device information template.

Table 23 — PUT TO DEVICE function — Command response pair

CLA	As defined in ISO/IEC 7816-4	
INS	‘16’	
P1	‘09’, (see Table 13)	
P2	Device handle number (see Table 5)	
L_c field	Absent for encoding $N_c = 0$, present for encoding $N_c > 0$	
Data field	Absent	Output data is in the ICC and its reference is implicitly known by application
	Output Data	Data possibly formatted according to general device information template (see 5.5.3)
	Reference to card internal object	Reference to card internal object, e.g. by object locator DO’7F72’ or general reference template DO’60’ (see ISO/IEC 7816-4)
L_e field	Absent for encoding $N_e = 0$	

Data field	Absent
SW1-SW2	See ISO/IEC 7816-4 and Table 14

6.3.11 GET DEVICE INFORMATION function

The function GET DEVICE INFORMATION allows retrieving all or parts of the DVCP of a device in OPERATIONAL state. This function does not change the activity state.

Table 24 — GET DEVICE INFORMATION function — Command response pair

CLA	As defined in ISO/IEC 7816-4
INS	‘16’
P1	‘0A’, (see Table 13)
P2	Device handle number (see Table 5)
L_c field	Absent for encoding $N_c = 0$, present for encoding $N_c > 0$
Data field	Empty or tag list of DO(s) in DVCP
L_e field	Present for encoding $N_e > 0$

Data field	Complete DVCP DO’62’ if command data field is empty or the concatenated DO(s) according to the tag list
SW1-SW2	See ISO/IEC 7816-4 and Table 14

6.3.12 ERASE DEVICE CONTENT function

The function may overwrite any information with a predefined value or turns the condition of an additional device back into same as after OPEN DEVICE function has applied, except its activity state and the usage condition. This function can be applied to additional device in OPERATIONAL state.

Table 25 — ERASE DEVICE CONTENT function — Command response pair

CLA	As defined in ISO/IEC 7816-4
INS	‘16’
P1	‘0B’, (see Table 13)
P2	Device handle number (see Table 5)
L_c field	Absent for encoding $N_c = 0$, present for encoding $N_c > 0$
Data field	Absent
	Data possibly formatted according to general device information template (see 5.5.3)

Table 25 *(continued)*

L_e field	Absent for encoding $N_e = 0$

Data field	Absent
SW1-SW2	See ISO/IEC 7816-4 and Table 14

6.3.13 MANAGE DEVICE CONFIGURATION function

The function MANAGE DEVICE CONFIGURATION allows either to select a device configuration template for the device, or to set existing control DO(s) of a selected device configuration template DO'A3' temporarily (see also Clause 10 and Table 29). This function can be applied to additional devices in OPERATIONAL state.

When a device control template is selected with its identifier DO'80', its entire control DO(s) are applied with their existing values. In case of an already selected template, the value(s) of the referenced control DO(s) become valid temporarily if applicable. If set with identifier and control DO(s), the new value(s) thereof apply temporarily when applicable. The value(s) of the other control DO(s) will be kept unchanged.

The function allows also the combination of selection and/or setting of one or several control DO within a single command.

Table 26 — MANAGE DEVICE CONFIGURATION function — Command response pair

CLA	As defined in ISO/IEC 7816-4
INS	'16'
P1	'0C', (see Table 13)
P2	Device handle number (see Table 5)
L_c field	Present for encoding $N_c > 0$
Data field	DO'80' only: selection and setting of a DO'A3' and its control DO(s), referenced by configuration identifier
	DO'80' and a set of control DO(s): selection and setting of a DO'A3' with its control DO(s) and replace the referred control DO(s) with their new values temporarily.
	Set of control DO(s): replace the referred control DO(s) of a previous selected DO'A3' with new values temporarily
L_e field	Absent for encoding $N_e = 0$

Data field	Absent
SW1-SW2	See ISO/IEC 7816-4 and Table 14

7 Usage of off-card devices

7.1 General

ICC-managed devices may use off-card devices in the course of an application. ISO/IEC 18328-1 describes use cases with off-card-devices. The usage of off-card devices needs a communication between the external entity and the card-IC. The prerequisite for such communication is a COS or application which is able to handle additional devices and an IFD providing the suitable bi-directional communication means.

The general architecture for handling commands and access control shall be the same as for on-card devices:

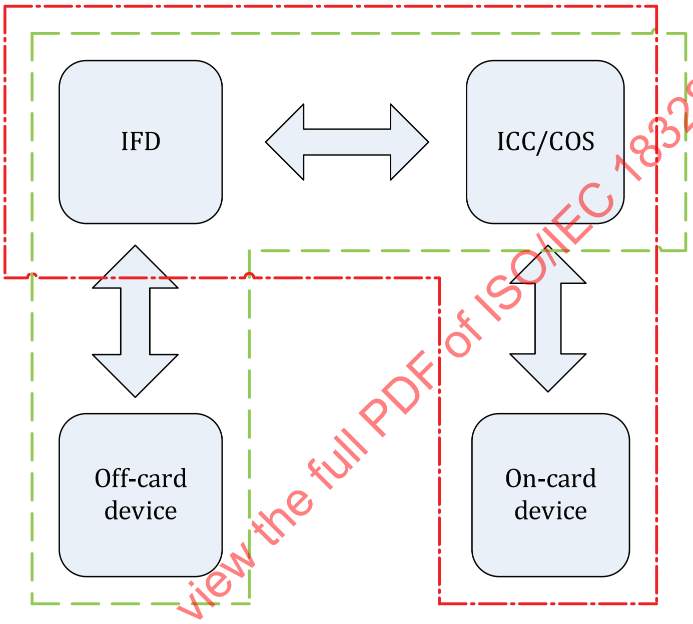
- commands are sent from IFD to the card, e.g. an ADM command;

— security and access condition is always checked by the ICC;

— the ICC communicates with an off-card device through an IFD. The card-originated byte string defined in ISO/IEC 7816-4 is used for this communication;

— when the IFD retrieves information from the ICC dedicated to an off-card device using the card-originated byte string mechanism, the IFD dispatches the received byte string to the off-card device for the purposes of processing and retrieving information. After processing the device related information by the off-card device, the IFD sends its result to the ICC using also the card-originated byte string mechanism.

Figure 4 shows the general architecture of a system with the usage of off-card devices and/or on-card devices.



Key

— — —	handling and information flow for off-card devices
—·—·	handling and information flow for on-card devices

Figure 3 — General architecture for usage of on- and off-card device

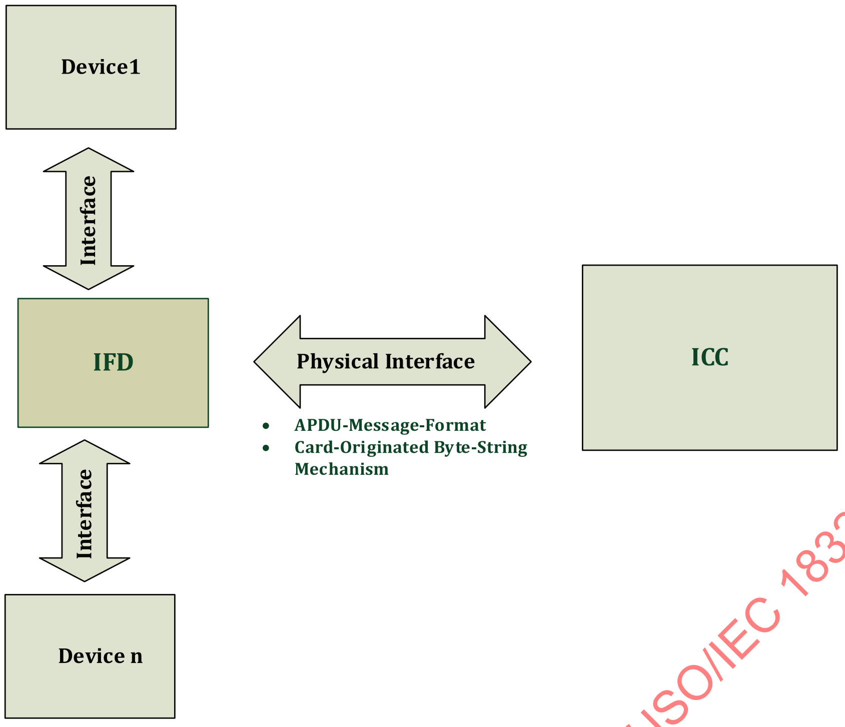


Figure 4 — System architecture for usage of off-card devices

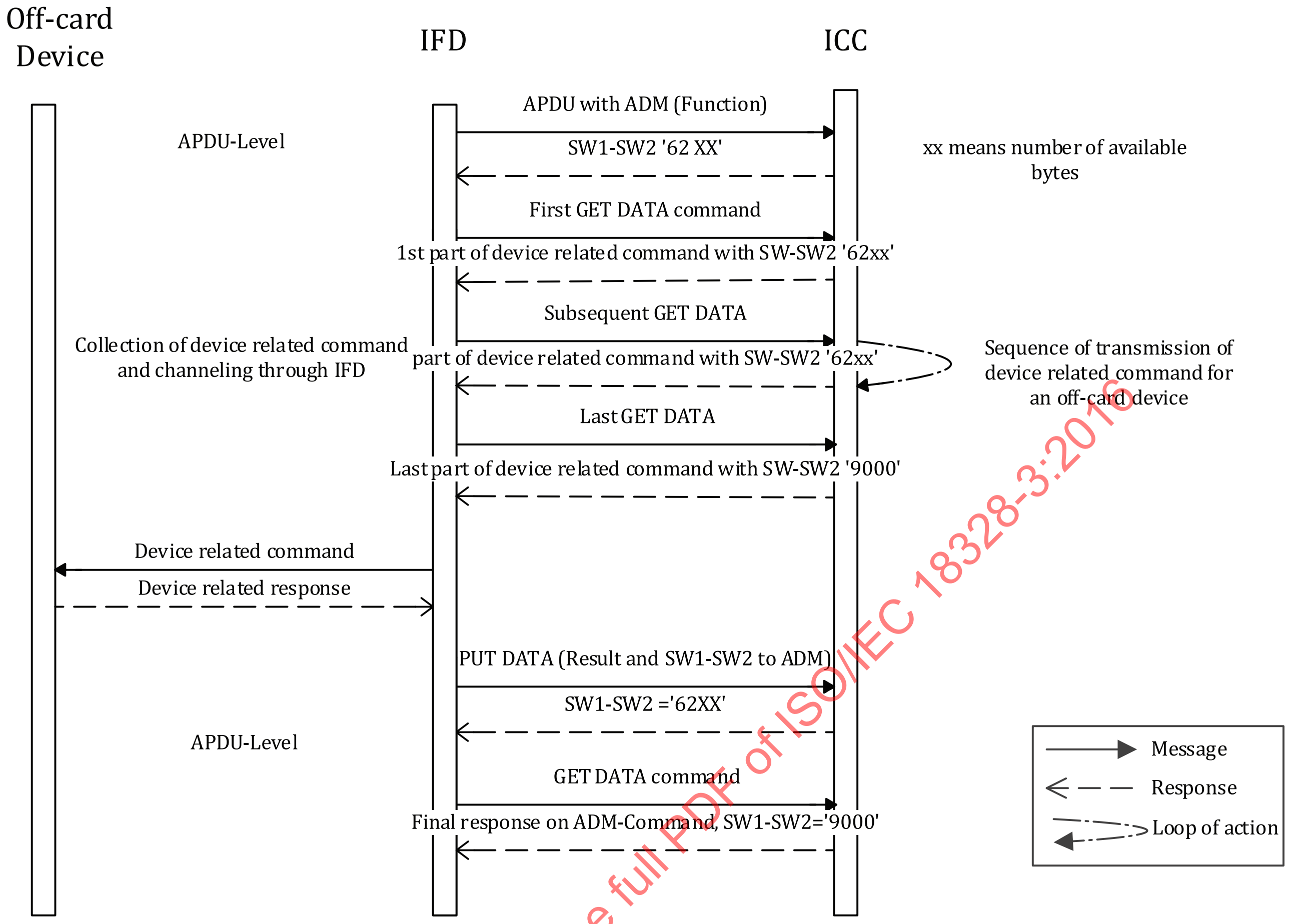
7.2 Transmission mechanism

ISO/IEC 7816-4:2013, 12.5 describes the mechanism of card-originated byte strings to allow the specific command-response transmission from the ICC to the IFD.

The IFD sends an ADM command to the ICC to address an off-card device. The ICC checks according to the general requirements the access rights and starts the initiation of the card-originated byte string mechanisms by responding with a SW1-SW2 '62XX' The IFD starts to collect all device related information from the ICC by subsequent GET DATA commands.

Within a trusted environment and its associated security policy, an IFD may interpret the information and dispatch it to the off-card device as a device related command. If the IFD is not trustworthy and has no ability to handle secured information, the device related command shall be forwarded to the off-card device without any interpretation. The information handling to or from the off-card device is out of scope of this document. The information is finally transmitted to the ICC as the controlling instance by using also the card-originated byte string mechanism. The handling of this command sequence needs normally several steps and therefore several commands-response pairs between ICC and IFD.

Figure 5 outlines the general command-response pairs.


Off-card Device
IFD
ICC
APDU-Level
APDU with ADM (Function)
SW1-SW2 '62 XX'
xx means number of available bytes
First GET DATA command
1st part of device related command with SW-SW2 '62xx'
Subsequent GET DATA
Collection of device related command and channeling through IFD
part of device related command with SW-SW2 '62xx'
Sequence of transmission of device related command for an off-card device
Last GET DATA
Last part of device related command with SW-SW2 '9000'
Device related command
Device related response
PUT DATA (Result and SW1-SW2 to ADM)
SW1-SW2 ='62XX'
APDU-Level
GET DATA command
Final response on ADM-Command, SW1-SW2='9000'
Message
Response
Loop of action

NOTE The communication between ICC and IFD may be performed with other protocols which are out of scope.

Figure 5 — Usage of card-originated bytes strings for command transmission for off-card devices

7.3 Device handle

Off-card devices shall be administrated by the COS in analogous way as on-card devices. A device handle is linked to the properties and activities of the off-card device. All commands to the ICC dealing with the devices reference an off-card device by its device handle number (except GENERAL RESET DEVICE and OPEN DEVICE function).

7.4 Secure channel

Figures 3 and 4 shows three different communication channels, such as between the ICC and the IFD, between the IFD and the off-card device and between the ICC and the off-card device through the IFD. Communication channel between ICC and IFD may be protected by applying secure messaging defined in ISO/IEC 7816-4.

The communication between ICC and the off-card device may be peer-to-peer secured on the top of the card-originated byte string protocol, e.g. between the ICC and a TEE or secure element. This communication channel may be protected by application. This security is outside of the scope of this document, but the document provides control DOs regarding information of this security. These control DOs are included in the device feature template DO'A2' in general device information template DO'A4' in DVCP DO'62.

The access conditions contain the appropriate security information to fulfil both requirements:

— security information for the security handling with the external world;

— security information for the security handling with the secure host applications, e.g. TEE, secure elements.

NOTE Access conditions may be a combination of established secured channel with an independent secure messaging stream with the external security system of the TEE or secure element.

The secure channel may be established with a specific protocol within the card-originated byte strings.

8 Command structures with ADM functions in applications

Command definition for ICC generally did not take additional devices into account. Since the ADM command allows separated additional input or output channels to handover information internally in the ICC or to the external world, application are now able to enhance command definitions to incorporate such new features. Commands may consist of additional steps since the interaction of the ICC with the device(s) is separated in different functions or the card holder (or IFD) may have to interact with the application by device activities with additional intermediate commands. Annex C shows examples, how a possible future command uses the ADM sub-functions or internal functionality to fulfil the requirement of the command.

9 Security aspects

9.1 Security attributes

The COS controls the access to any resources managed by the COS according to the security mechanism defined in ISO/IEC 7816-4. Additional devices as new extensions of the ICC are additional resources and shall be protected by the same mechanisms.

Device security attribute are comprised of access mode field with security condition byte for compact format or access mode DO with security condition DO for expanded format. These are defined in ISO/IEC 7816-4. See Tables 27 and 28 for access mode field for device security attribute. The coding of security attributes applying to an additional device is nested within the DVCP referenced by a device identifier.

Referenced by tags ‘86’, ‘8B’, ‘8C’, ‘8E’, ‘9C’, ‘A1’, ‘AB’, ‘AD’ security attributes may be present in the DVCP (see Table 7).

Data integrity and confidentiality from the card IC to the additional devices and vice versa may be implemented within the COS and/or in a dedicated device driver. An adaptation of the existing concept for ICCs may be used to secure the communication between ICC and the ICC-managed devices.

The execution of ADM command functions is determined by the verification of the security attributes in the DVCP.

CRT parameters as defined in ISO/IEC 7816-4 are not subject to any extension or change when applied to additional devices.

9.1.1 Access mode field for ADM command

Access mode bytes may be used in compact and expanded format as well. For the functions of the ADM command set, the access mode bytes are defined in Tables 27 and 28.

Table 27 — Coding of the access mode field (1st byte) for ADM command

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
x	—	—	—	—	—	—	—	Next byte for access mode field
0	—	—	—	—	—	—	—	Last byte of access mode field
1	—	—	—	—	—	—	—	Another byte follows in this access mode field

Table 27 *(continued)*

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
—	x	x	x	x	x	x	x	Function of ADM command
—	1	—	—	—	—	—	—	GET DEVICE INFORMATION
—	—	1	—	—	—	—	—	GENERAL DEVICE USAGE
—	—	—	1	—	—	—	—	EXCLUSIVE DEVICE USAGE
—	—	—	—	1	—	—	—	REACTIVATE DEVICE
—	—	—	—	—	1	—	—	DEACTIVATE DEVICE
—	—	—	—	—	—	1	—	LOGICAL DEVICE RESET
—	—	—	—	—	—	—	1	GENERAL DEVICE RESET

Table 28 — Coding of the access mode field (2nd byte) for ADM command

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
x	—	—	—	—	—	—	—	Next byte for access mode field
0	—	—	—	—	—	—	—	Last byte of access mode field
1	—	—	—	—	—	—	—	Another byte follows in this access mode field
—	x	x	x	x	x	x	x	Function of ADM command
—	1	—	—	—	—	—	—	GET FROM DEVICE
—	—	1	—	—	—	—	—	PUT TO DEVICE
—	—	—	1	—	—	—	—	GET DEVICE INFORMATION
—	—	—	—	1	—	—	—	ERASE DEVICE CONTENT
—	—	—	—	—	1	—	—	MANAGE DEVICE CONFIGURATION
—	—	—	—	—	—	x	x	‘00’, any other values are RFU

9.1.2 Security conditions

ISO/IEC 7816-4 defines the security conditions for the different formats. These definitions are also valid and applicable to control the access to any additional device in an ICC following this document. In compact format, the security condition is coded in a single security condition byte; in case of the expanded format, the security condition DO represents the requirements for device access. As defined in ISO/IEC 7816-4, the same security conditions means like secure messaging, authentications, etc. are applicable.

9.2 Data integrity and confidentiality

The security attributes (see 9.1.1 and 9.1.2) define access control, data integrity and data confidentiality on application protocol level. Some applications need also a protection of the data transfer between ICC and device. The ICC shall support data structures, e.g. CRT, SM-DO or proprietary means defined by the external world or application to enforce additional data protection to/from the device. If this feature is used, the ICC can always check the authenticity of the dedicated additional device.

NOTE The definition of the protocol for this internal data protection is outside of the scope of this document.

Bit 6 in the device descriptor (see Table 9) indicates if additional security for the device access within the ICC is needed. If bit 6 is set, the related security needs may be found in the general device information template (see Table 10). The DO’A1’ may contain further information regarding how to protect the data transfer between ICC and additional device should be managed.

Potential solutions to authenticate the additional device/controller may be, for example

— unilateral authentication,

— classical mutual authentication, and

- others solutions with delegation of some parts of the computations to the chip of the secure element connected to the additional device.

In any case, the choice of the technical solution to authenticate the additional device is linked to the performances required in the field, and a secret shall be stored in the controller of the additional device.

9.3 Security with off-card-devices

Off-card devices shall be addressed in the same way as on-card devices. The DVCP data for the off-card device denotes the security conditions for commands dealing with the off-card device. The ICC uses this information to check the access conditions for such a device handling. ‘86’, ‘8B’, ‘8C’, ‘8D’, ‘8E’, ‘9C’, ‘A1’, ‘A3’, ‘AB’, ‘AC’ and ‘AD’ in the DVCP may contain security conditions to be checked by the ICC.

9.4 Trust assessment

Additional devices on an ICC may support the confidence in the running course of a transaction. For example, after establishing a secure channel between IFD and ICC a display, a LED or a loudspeaker can be used to notify the user about the secured connection. Trust assessment may be achieved by using the additional devices. A “trusted” display, LED or loudspeaker may indicate managed data or activities as trustable in a specific way, defined by the application or card holder, for example,

- display text in a specific font,
- display letters in a specific colour,
- usage of a specific background colour,
- a tone, signal or a melody of a loudspeaker, and
- specific LED (blinking or changing colours).

Trust may be enhanced by the usage of combinations of additional devices, e.g. an additional LED may indicate a “trusted” input on keypad or output on a display, together with a tone of a loudspeaker. Means of trust assessment are defined in a definition template DO’A3’ in the general device information template (see Table 10). Such means may consist of a group of DO defining the behaviour of the trusted additional device. Table B.10 gives an example of applicable DOs within the template.

The activation of the trusted device(s) by application of the content of the definition template for trust assessment in the course of the transaction may be triggered by the device manager with usage of the additional device security feature DO’A1’ (see Table 10) or by the security management of the COS.

10 Device configuration template

10.1 Configuration template

A device configuration template DO’A3’ defines specific information for the device handling or the usage of the device in the course of the command itself. Templates are located in the device feature template. Such information for the ADM command is only available in the OPERATIONAL state.

An existing configuration template offers control DOs with predefined values as static information which remains valid until a new value is presented to the ICC which changes the value temporarily. For example, an IFD may change values of control DOs dynamically in the course of the application.

Table 29 contains a list of control DOs for any device configuration template and indicates for which configuration template they may be relevant. Different devices need different control references according to the structure and the character of the device.

Table 29 — Control DOs in device configuration template DO’A3’

Tag	Length	Value	Keypad	Display	Touch	Biometric Sensors	Other devices
	Identification						
‘80’	‘01’	Configuration identifier as hexa-decimal number	x	x	x	x	x
	Timing controls						
‘81’	var.	Activation time in seconds (general)	x	x	x	x	x
‘82’	var.	Keypad activation time in seconds	x		x		
‘83’	var.	Display activation time in seconds		x	x		
‘84’	‘01’	End of time frame indicator	x	x	x	x	x
‘94’	‘01’	Timeout indicator	x	x	x	x	x
	Additional security controls						
‘85’	var.	Reference to a key	x	x	x	x	x
‘86’	var.	Algorithm identifier	x	x	x	x	x
‘87’	var.	Internal usage counter value	x	x	x	x	x
	Other values RFU						

10.2 Usage of device configuration templates

After opening a device by an ADM OPEN DEVICE function, no device configuration template is in use. Values applied by applications in that phase are default values, known implicitly. Application may then select an appropriate configuration template DO’A3’ with an ADM MANAGE DEVICE CONFIGURATION function (see 6.3.13) to set the predefined values of the device configuration template. When a DO’A3’ template has been selected, an application is allowed to set new values of existing control DO within the selected configuration template temporarily. These new settings are valid until the values are changed by the described mechanism again, a new DO’A3’ is selected or the device is reset and the DHN is released. An application is responsible not to use settings which may open security issues.

Annex A
(informative)

Activity sequences

A.1 Activation sequences

A device becomes usable for an application by the following steps:

- identification;
- selection;
- retrieval of device related information;
- fulfilling of the security conditions.

For identification of usable devices, the IFD gets the first information after enabling of the physical interface. The ATR/ATS, the EF.ATR/INFO or the FMD/FCI of an application may offer the general feature management DO'7F74' (see ISO/IEC 7816-4). The DO'81 and DO'83' may contain device information, for example, the device identifier list.

For selection of a specific device, the IFD applies an ADM OPEN DEVICE command referencing the device with its device identifier. The DHN in the response will be used for further addressing of the device in the course of application.

Detailed information can be retrieved by applying the ADM GET DEVICE INFORMATION which may offer the DVCP-DO, the device information template, the device feature template or an OID as a reference to a document.

Security conditions may be available in the DVCP or in the device information template. The external world only gets access to the device if these security conditions are fulfilled. If this is the case, additional ADM commands may be successfully applied. Figure A.1 outlines the sequence of activity schematically.

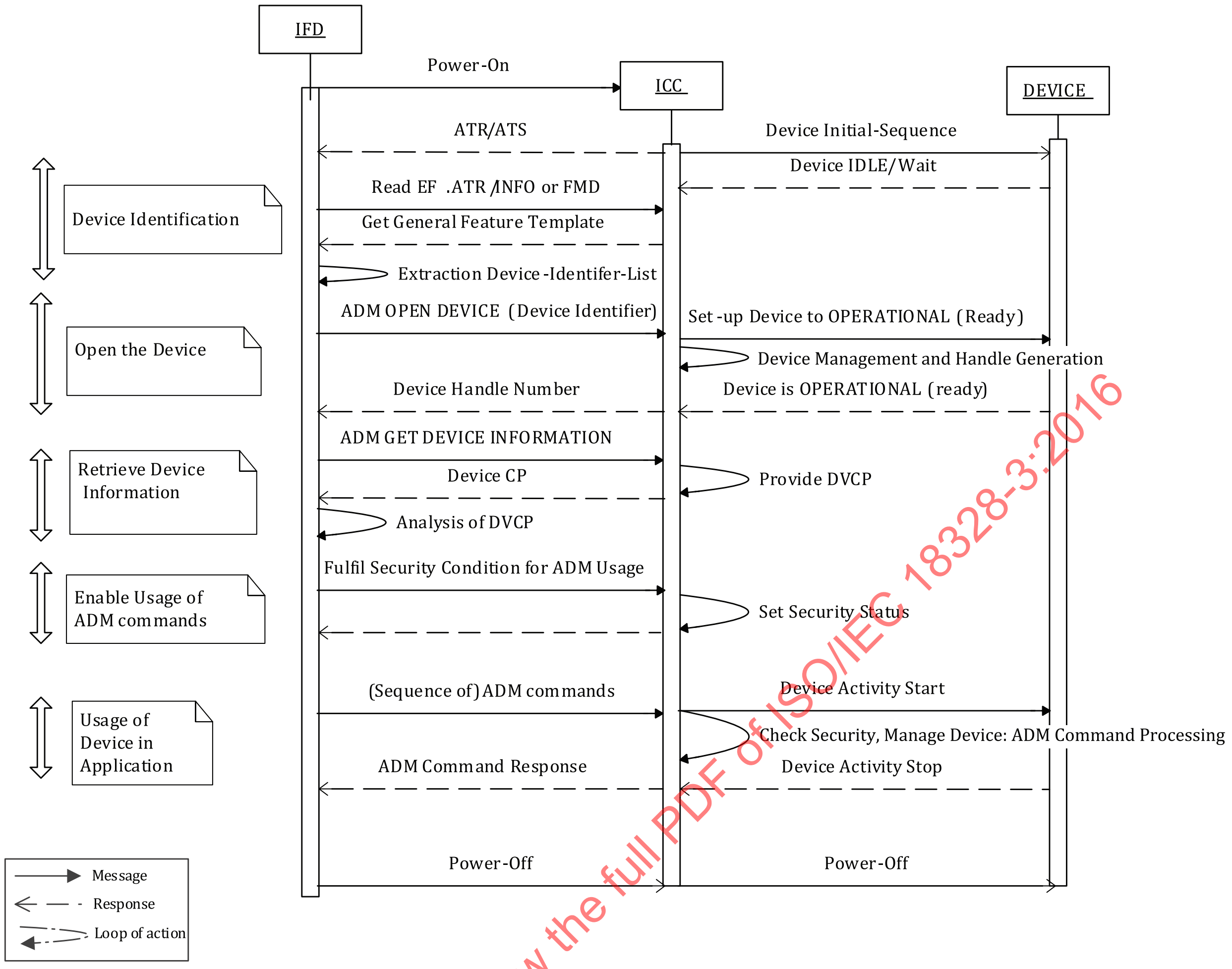

IFD
ICC
DEVICE
Power-On
ATR/ATS
Device Initial-Sequence
Device IDLE/Wait
Read EF .ATR /INFO or FMD
Get General Feature Template
Extraction Device -Identifer-List
Device Identification
ADM OPEN DEVICE (Device Identifier)
Set -up Device to OPERATIONAL (Ready)
Device Management and Handle Generation
Open the Device
Device Handle Number
Device is OPERATIONAL (ready)
ADM GET DEVICE INFORMATION
Device CP
Provide DVCP
Analysis of DVCP
Retrieve Device Information
Fulfil Security Condition for ADM Usage
Set Security Status
Enable Usage of ADM commands
(Sequence of) ADM commands
Device Activity Start
Check Security, Manage Device: ADM Command Processing
ADM Command Response
Device Activity Stop
Usage of Device in Application
Power-Off
Power-Off
Message
Response
Loop of action

Figure A.1 — Activity sequence for identification, selection and applications of devices