TECHNICAL SPECIFICATION

ISO/IEC TS 22924

First edition
2021-05

Identification cards — Transport layer topologies — Configuration for HCI/HCP interchange

Cartes d'identification — Topologies de la couche transport — Configuration pour les échanges HCI/HCP

Reference number
ISO/IEC TS 22924:2021(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see patents.iec.ch).

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

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 17, *Cards and security devices for personal identification*.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

Introduction

This document is laid on the ground of ISO/IEC 7816 (all parts) specifying integrated circuit cards and the use of such cards for interchange, and on ETSI TS 102 622 defining the HCI core that is an application independent logical interface.

ETSI TS 102 622 is referenced in this document as a well-known HCI specification, however it should be noted ETSI TS 102 622 describes another host network with the host controller implemented by the CLF/NFC controller and with hosts residing on UICCs/SEs all connected to the host controller. ETSI TS 102 622 allows for other interfaces than SWP for data link layer of HCI, and does not mandate using the SWP but just describes the condition if the SWP is used.

Identification cards — Transport layer topologies — Configuration for HCI/HCP interchange

1 Scope

This document specifies the requirements for a protocol derived from HCI/HCP (see ETSI TS 102 622) enabling communication for devices regardless of data link and physical layers. This document covers the following:

a) outline of a system comprised of one or more hosts and one controller;

b) extension of connection topology between hosts and host controller (i.e. star topology and additional other topologies);

c) segregation between existing system using ETSI TS 102 613 and new system compliant to this document (this document refers ETSI TS 102 613, but does not change its specification and does not use RFU).

For ETSI TS 102 622, data link layer and physical layer like SWP specified in ETSI TS 102 613 is out of the scope.

Albeit questioned in this document, the duplication of OSI transport layer by e.g. enforcing encapsulation of HCP into T=1 or the reverse, is out of the scope.

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 7816-3, *Identification cards — Integrated circuit cards — Part 3: Cards with contacts — Electrical interface and transmission protocols*

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:

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

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

3.1
APDU gate
entry point to a service processing command APDU inside a *host* (3.6) or returning response APDU

3.2
APDU application gate
entry point to a service sending command APDU and retrieving correspondent response APDU

3.3
gate
entry point to a service that is operated inside a *host* (3.6)

[SOURCE: ETSI TS 102 622]

3.4
HCI network
star-topology network comprised of a *host network* (3.8) where *hosts* (3.6) are interconnected with a *host controller* (3.7) through HCI

3.5
HCP stack
layout comprised of a routing layer, a messaging layer and a collection of *gates* (3.3)

3.6
host
logical entity that operates one or more service(s)

[SOURCE: ETSI TS 102 622]

3.7
host controller
host (3.6) that is also responsible for managing a *host network* (3.8)

[SOURCE: ETSI TS 102 622]

3.8
host network
network of two or more *hosts* (3.6)

[SOURCE: ETSI TS 102 622]

3.9
managing host
host (3.6) which is in charge of resolving conflicts and interoperability issues between different contactless applications provided by different hosts

[SOURCE: ETSI TS 102 622]

3.10
pipe
logical communication channel between two *gates* (3.3) from different *hosts* (3.6)

[SOURCE: ETSI TS 102 622]

3.11
terminal host
host (3.6) allocated a static identifier HID '01'

4 Symbols and abbreviated terms

ADM_x	arbitrary command for administration gate, see ETSI TS 102 622 clause 6.1, e.g. ADM_CREATE_PIPE
APDU	application protocol data unit
API	application programming interface

ANY_x	arbitrary command for all gates, see ETSI TS 102 622 clause 6.1, e.g. ANY_OPEN_PIPE
CB	chaining bit
CLF	contactless front end
COS	card operating system
CPU	central processing unit
CRC	cyclic redundancy code
DF	dedicated file
EVT_x	arbitrary event, see ETSI TS 102 622 clause 6.3, e.g. EVT_HOT_PLUG
GID	gate identifier
HCI	host controller interface
HCP	host controller protocol
HID	host identifier
I^2C	inter-integrated circuit
ICC	integrated circuit card
IFD	interface device
IRQ	interrupt request
LRC	longitudinal redundancy code
NAD	node address
NFC	near field communication
N(S)	send sequence number
OSI	Open System Interconnection
PCB	protocol control byte
PID	pipe identifier
PPS	protocol and parameter selection
RF	radio frequency
RFU	reserved for future use
SCL	smart secure platform common layer
SE	secure element
SS	SPI slave select wire
SSP	smart secure platform
SWP	single wired protocol

TPDU	transmission protocol data unit
UART	universal asynchronous receiver and transmitter
UICC	Universal Integrated Circuit Card
USB	universal serial bus
eSE	(embedded) secure element

5 Architecture

5.1 System architecture view

5.1.1 General

This subclause describes the reference use case architecture where APDU gate fits. This architecture is based on a star topology where one or more hosts (e.g. secure element, ICC-managed device) physically connect to a component (e.g. IFD, device controller, contactless frontend) acting as a host controller. In this topology, the HCI defines the interface between hosts.

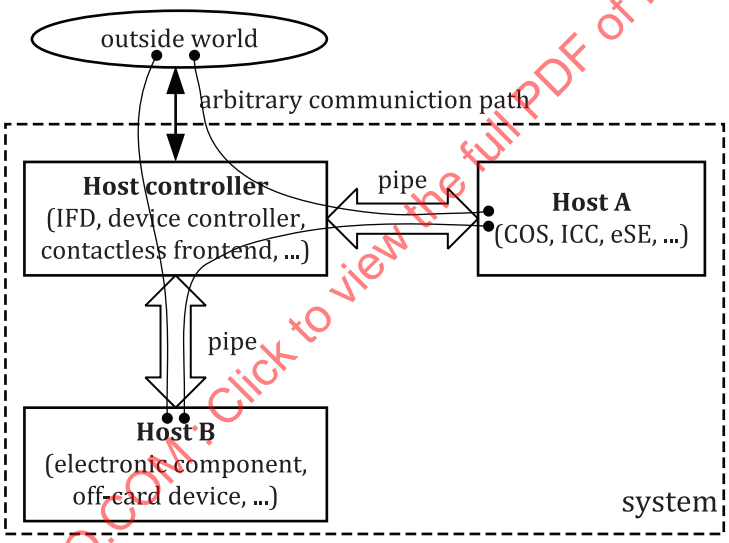


Figure 1 — System architecture for reference use case

ICC-managed devices may also make use of off-card devices (see ISO/IEC 18328-1 for use cases and ISO/IEC 18328-3:2016, Clause 7, for architecture description). The usage of ICC-managed off-card devices needs a communication with an ICC (or a secure element) through an IFD. The prerequisite for such communication is a COS or application which can handle additional devices and a host controller providing the suitable bi-directional communication means. Figure 1 describes this architecture.

NOTE For simplification, drivers and interfaces are not represented on Figure 1.

The reference use case on Figure 1 is deployed on Figure 2 over a general HCP stack. The route conveying instructions over a pipe created between the two gates is represented.

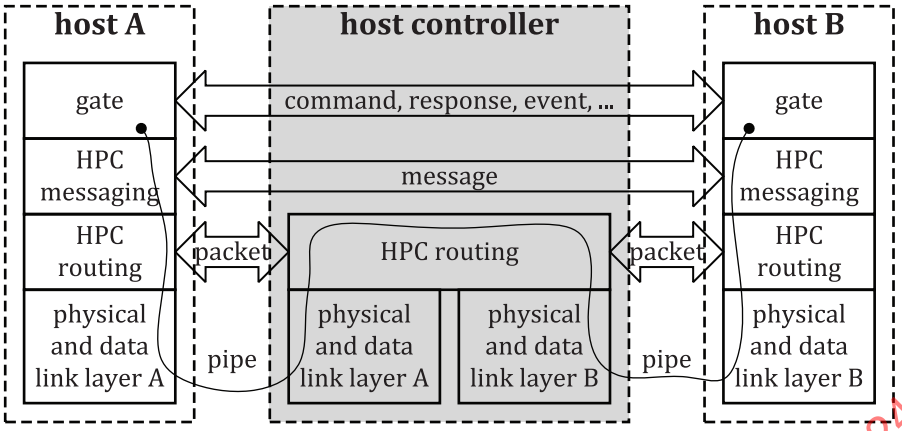


Figure 2 — HCI general stack representation

5.1.2 Hosts

This subclause contains a subset of information from ETSI TS 102 622 about hosts.

The identity of a host is coded in a byte named HID. Table 1 lists the reserved values for the HID.

Table 1 — Host identifiers

host	HID
host controller	'00'
terminal host	'01'
RFU	'02' to ''7F'[a]
dynamically allocated	'80' to 'BF'
proprietary	'C0' to 'FE'
not allowed	'FF'[b]
[a] In this table the value '02' is RFU whereas in ETSI TS 102 622 it is used for UICC host.	
[b] In this table the value 'FF' is not allowed whereas in ETSI TS 102 622 it is proprietary.	

The generic term "host" is used to refer to any host (e.g. terminal host, UICC host) excluding the host controller.

The dynamically allocated range of values shall be used by the host controller to assign a HID to any host not identified in Table 1. The host controller shall always assign the same HID to a given host throughout different sessions as long as there is no modification in the hardware configuration of the device.

NOTE 1 In ETSI TS 102 622, there is no statement that a HID has to be unique.

NOTE 2 ETSI TS 102 622 does not describe how a host controller assigns an HID to a host.

5.1.3 Gates

This subclause contains a subset of information from ETSI TS 102 622 about gates.

A gate provides an entry point to a service that is operated inside a host. The HCP enables gates from different hosts to exchange messages. There are two types of gates:

— management gates that are needed for the management of the host network;

— generic gates that are not related to the management of the host network.

The type of a gate is identified by a GID. GIDs are listed in Table 2 and are either unique within the scope of a host ('10' to 'FF'), or their values refer to the same gate type for every host ('00' to '0F').

Table 2 — Gate identifiers

gate	GID
reserved for proprietary use	'00' to '03'
loop back gate	'04'
identity management gate	'05'
RFU	'06' to '0F'
host specific	'10' to 'EF'
reserved for proprietary use	'F0' to 'FF'

The GID for the application gates are dynamically assigned by the host running the application gate.

The following rules apply to hosts and gates.

a) All hosts and the host controller shall have one administration gate.

b) All hosts may have one link management gate and the host controller shall have one link management gate.

c) All hosts and the host controller shall have one identity management gate.

d) All hosts and the host controller shall have one loop back gate.

e) All hosts and the host controller may have one or more generic gates.

5.1.4 Pipes

This subclause contains a subset of information from ETSI TS 102 622 about pipes.

A pipe is a logical communication channel between two gates. There are two types of pipes:

— static pipes that are always available, i.e. they do not need to be created and cannot be deleted;

— dynamic pipes that can be created and deleted.

The state of a pipe is either open or closed. The state shall remain persistent if the hosts are powered down and up again. It shall also remain persistent if a host is temporarily removed from the host network and is not replaced by a different device in the meantime. The state of a dynamic pipe after creation and the initial state of a static pipe shall be closed.

The PID is 7 bits long. The value of PID is used in the header of HCP packets as routing information (see B.6). For static pipes the PIDs are predefined with values as defined in Table 3. For dynamic pipes, PIDs are dynamically allocated by the host controller.

Table 3 — Pipe identifiers

PID	pipe ending at:	pipe type
'00'	link management gate	static
'01'	administration gate	
'02' to '6F'	other gate	dynamic
'70' to '7F'	RFU	

The following rules apply to gates and pipes.

a) A static pipe always connects a gate of a host to a gate of the host controller.

b) A dynamic pipe connects two gates from different hosts.

c) Static and dynamic gates connect to different types of gates; see Table 3 for the mapping.

d) Dynamic PIDs shall be unique in the host network.

5.1.5 Host controller

The host controller can be a dedicated physical device or a software component on a device exposing the host controller and zero, one or more hosts in the HCI network. The host controller can provide more than one physical interface. The host controller allocates dynamic HIDs and PIDs as applicable. A host can request the host controller to create a new dynamic pipe between two gates. The host requesting the pipe is the source host. If successful, then a pipe is created between the source host and a destination host. The host controller uses the WHITELIST defined by the destination host in order to verify that the source host is authorized to create a pipe.

Once a pipe is open between the gates of two hosts, the host controller handles packets of data between the two hosts based on the routing information provided by the PID in the network field of the HCP header. In case a packet length exceeds the physical buffers sizes present on the host and on the host controller, data are transferred in multiple subsequent fragments of the packet, with fragments in chaining mode specified by the CHAINING field in the HCP header. As the physical buffer size present on each host interface may vary with each implementation, the host controller may need to perform data re-assembly and re-segmentation before forwarding it, according to each interface specification.

Data integrity checking and flow control for communications with each host according to specific data link layer rules applicable for each physical interface is performed on each connection between a host and the host controller. The host controller should have the ability to set a host into a power saving mode and resume a host for access with a sequence specific to each physical interface and host architecture. These elements of the OSI physical layer and data link layer are not defined in this document.

5.1.6 General aspects on APDU gate

According to ETSI TS 102 622, the host sending the APDU command is called the "client APDU host"; and the host receiving and processing the APDU commands is called the "server APDU host". The server APDU host has an APDU gate with GID='30'. The client APDU host has an APDU application gate.

APDUs shall be as defined in ISO/IEC 7816-4. Usage of both the basic logical channel and further logical channel(s) is allowed.

Assume a secure element with a physical interface receives command APDU and sends corresponding response APDU. Its physical interface has a data link layer and a transport protocol for communication. If such a secure element acts as a server APDU host in an HCI network, then this secure element also has an APDU gate. The physical interface of such a secure element acts as a pipe to APDU application gates of other hosts. The APDU gate within such a secure element is the APDU handler of its COS.

A client APDU host shall not create more than one pipe to the APDU gate of a server APDU host. The APDU gate may accept only an implementation specific maximum concurrent number of pipes from other client APDU hosts.

The general rules are as follows.

a) A pipe bridges between two gates from two hosts.

b) A pipe identifier in a host shall address a unique gate within the other host.

c) A gate shall only accept a command or an event on a pipe when the state of that pipe is open unless determined otherwise by the application.

d) A gate shall not send a command or event on a pipe when it is waiting for a response to a previous command on that pipe.

HCI interface operates as an abstraction layer regardless of the underlying data link and physical layers, which leaves to the implementation a wide range of possibilities fitting the eSE with the context.

Interface activation, presence of power saving modes, entering and exiting a power saving mode, electrical parameters for a certain interface and handling of communication errors are outside the scope of this document and dedicated to physical layer and data link layer.

The underlying data link layer may vary depending on the ecosystem. As a general rule it is expected that a data link layer definition should meet the following properties.

— The data link layer ensures data is error free and the order of the received/sent data is respected.

— The data link layer provides its own data flow control.

— The data link layer delivers packets of the upper layer up to a maximum size specific to the data link layer.

— The data link layer reports the size of each received packet to its upper layer.

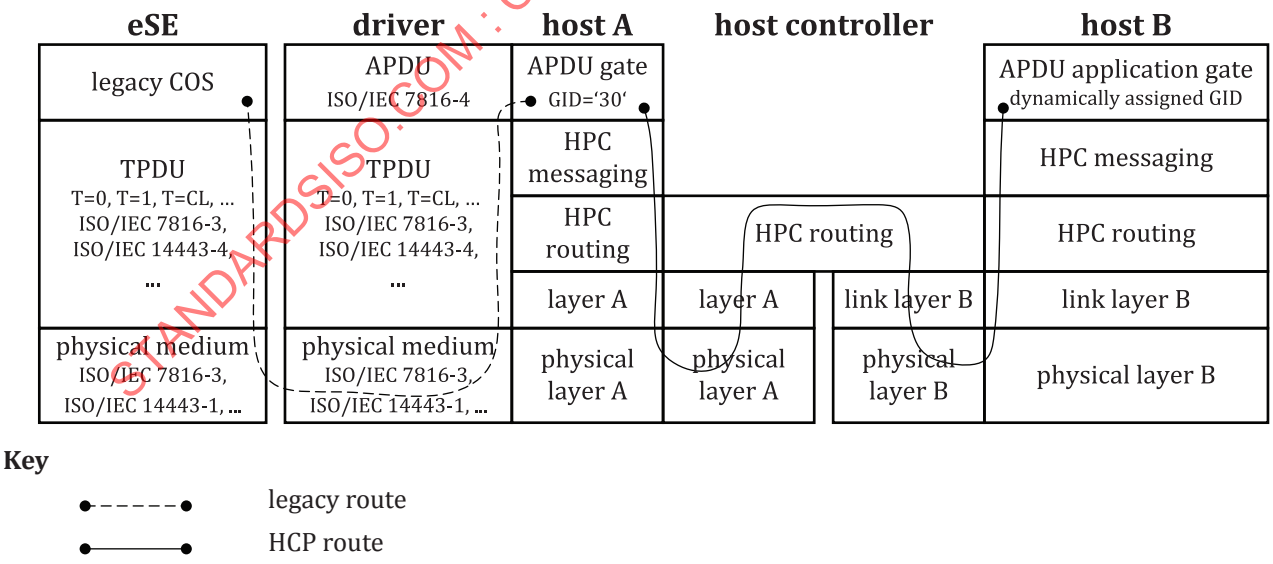
5.2 System architecture with legacy COS

In this subclause it is assumed that an eSE is connected to an HCI network, but the physical interface of the eSE is not compatible with the HCI (legacy COS). In that case the implementation of the server APDU host (host A in Figure 3) connects to the eSE using a specific driver. Figure 3 shows the complete communication path from a client APDU host (host B in Figure 3), via the host controller, through host A and driver to the eSE. Please note, that the communication path between host A and host B in Figure 3 is identical to Figure 2, although Figure 3 does not show any detail from Figure 2.

Figure 3 shows how HCI is an abstraction layer to the eSE, and how the route through an HCI pipe stretches from the APDU application gate to the legacy COS of the eSE. This pipe is logical and does not require necessarily a wired connection.

NOTE 1 Host A in Figure 3 can run on the same hardware as the host controller e.g. as an embedded software that emulates the eSE.

NOTE 2 Host B can run on the same hardware as the host controller e.g. a mobile controller.



Key

legacy route

HCP route

Figure 3 — HCI stack representation with legacy COS support

Further architecture variants with legacy secure element are described in Annex A.

6 Configuration requirements

6.1 General

This clause describes the required configuration for a host providing APDU gate service.

6.2 Logical components of an APDU-enabled host

A host supporting the present HCI/HCP specification and able to handle APDUs shall be implemented with, in addition to the APDU gate, the following other gates:

a) one (mandatory)administration gate allowing:

   1) to create and delete dynamic pipes (access to services that manage the network of pipes in HCI);

   2) the management of permissions through WHITELISTS (each host informs the host controller with its WHITELIST about which other hosts are allowed to communicate with it);

   3) the discovery of hosts at the first start-up or when configuration has changed;

   4) the management of sessions (session ID changes whenever the host configuration changes);

b) one link management gate allowing:

   1) the management of the underlying transport layer (i.e. number of invalid or lost frames due to communication error);

   2) EVT_HCI_END_OF_OPERATION to be sent by a host to the host controller over the pipe connecting the host and host controller link management gate to announce host entry into a power saving mode and requiring a resume sequence before a next access (the resume sequence is expected to be defined in other specifications describing the lower OSI layers).

c) one (mandatory) loopback gate allowing to verify pipe connectivity (for tests purposes);

d) one (mandatory) identity management gate allowing the discovery of software and hardware information about the APDU-enabled host;

e) generic (optional) gate(s) allowing various service(s) supported by the host.

6.3 Gates registry

6.3.1 General

This subclause describes the required entries of the registry respective to each gate present in a host and in the host controller. General rules related to registries are as follows:

a) A registry template defining parameters related to the gate may be associated with such a gate.

b) Within a registry, parameters are identified by identifiers consisting of one byte; parameter identifiers are unique within the scope of the gate; a new instance of the registry is created for every pipe that connects to the gate.

c) Upon pipe creation all registry parameters shall be set to their default values. A host is responsible for managing its associated registries. When a pipe is deleted, its registry instance is also deleted.

6.3.2 Administration gate registry

6.3.2.1 Host controller administration gate

This subclause contains a subset of information from ETSI TS 102 622 about host controller administration gate.

The administration gate in the host controller provides access to services that manage the network of pipes in the HCI network. In addition, this gate provides access to services that allow the discovery of hosts at the first startup and when the configuration of the host network has changed. The registry shall be persistent.

Table 4 lists the entries in the gate registry. The values of HOST_LIST and HOST_TYPE_LIST shall be updated if a host is connected to or disconnected from the host controller. The value of MH_AVAILABILITY_STATE shall be updated to reflect current managing host availability.

Table 4 — Entries in the host controller administration gate registry

Type[a]	ID[b]	Parameter	AR[c]	Comment	Len/ byte	Default
M	'01'	SESSION_IDENTITY	RW	Session identifier that is used to detect if the connected host configuration changed.	8	'FFFF FFFF FFFF FFFF'
M	'02'	MAX_PIPE	RO	Maximum number of created dynamic pipes supported by the host controller per host.	1	'10'
M	'03'	WHITELIST	RW	List of hosts that may communicate with the host connected to this administration gate. Each entry in this list is a HID.	N_0	empty
M	'04'	HOST_LIST	RO	The list of the hosts that are accessible from this host controller including the host controller itself. Each entry in this list is a HID.	N_1	'00'
M	'05'	HOST_ID	RO	HID of the host connected on this pipe either statically or dynamically assigned.	1	no default value
M	'06'	HOST_TYPE	RW	Type of host connected on this pipe. The first byte defines the host type family and the second byte defines variant of this type and is defined by the respective organizations.	2	'FFFF'
M	'07'	HOST_TYPE_LIST	RO	The list of the host types that are accessible from this host controller including the host controller itself. Each entry in this list is a HOST_TYPE. This list follows the same order as the HOST_LIST.	2 x N_1	'0000'
M	'08'	MANAGING_HOST_ID	RO	HID of the host acting as the managing host.	0 or 1	empty
M	'09'	MH_CAPABILITY	WO	Indicates if the host writing this to this registry entry has the managing host capability.	1	'00'
M	'0A'	MH_AVAILABILITY_STATE	RO	Indicates the current availability state of the managing host.	1	'FF'
M	'0B'	HOST_VERSION	RW	HCI_VERSION of the host connected on this pipe.	1	'FF'

[a] Column Type: M = mandatory.

[b] Column ID indicates the identifier.

[c] Column AR indicates access rights: RW = read/write, RO = read only.

The SESSION_IDENTITY shall be modified by the host whenever a modification of the configuration is performed by the host. The default value of the SESSION_IDENTITY shall never be written by a host. The SESSION_IDENTITY shall use random values.

Every host writes its WHITELIST into the host controller administration gate in order to inform the host controller which hosts are allowed to communicate with it. The host controller shall reject create pipe requests if the source host is not listed in the WHITELIST of the destination host unless otherwise specified (e.g. for the managing host).

The WHITELIST shall not contain neither the HID of the host controller identifier nor the HID of the host accessing the WHITELIST.

The WHITELIST is an array containing a list of host identifiers as defined in Table 1.

Coding of the HOST_TYPE is defined as follow:

a) '0000' = host controller;

b) '0100' = terminal host;

c) '0200' = UICC;

d) '0300' = eSE;

e) '04XX' = secure digital cards (SD cards) as defined by SD Association;

f) 'FFFF' = Unknown host type;

g) all other values are RFU.

The second byte of HOST_TYPE for SD cards is defined by SD Association.

HOST_TYPE and HOST_VERSION shall be written by the host into the host controller administration gate registry during the session initialization, prior to any pipe creation, and shall not be further modified.

6.3.2.2 Host administration gate

The administration gate at a host provides access to services involved in the management of the pipes towards that host.

The administration gate at a host has no registry entries defined.

For support of TODO A.1.4 use case, the host may need to expose on the static pipe some of the information in the host controller administration gate registry.

6.3.3 Link management gate

The link management gate of host controller (always present) and host (if present) provides information about the underlying layer. The registry may not be persistent.

Table 5 lists the entries in the registry.

Table 5 — Entries in the link management gate registry

ID[a]	Parameter	AR[b]	Description	Len/ byte	Default
'01'	RC_ERROR	RW	Number of invalid or lost frames previously sent by an entity[c, d] due to communication errors at the data link layer. This parameter can only be set to 0 in order to restart an error rate measure. When 'FFFF' is reached, the counter stops.	2	'0000'

[a] Column ID indicates the identifier.

[b] Column AR indicates access rights: RW = read/write.

[c] From the perspective of the link management gate registry of the host controller, the sending entity is a host.

[d] From the perspective of the link management gate registry of a host, the sending entity is the host controller.

6.3.4 Identity management gate

This subclause contains a subset of information from ETSI TS 102 622 about identity management gate.

The identity management gate provides software and hardware information about the host. The registry shall be persistent.

This gate shall be provided by all hosts and the host controller. As destination gate, the identity management gate shall accept at least one pipe from each host in its WHITELIST.

Table 6 lists the entries in the registry. The values of VERSION_SW and MODEL_ID may change if the identity management gate host or host controller is updated.

Table 6 — Entries of identity management gate registry

Type[a]	ID[b]	Parameter	AR[c]	Description	Len/ byte	Default
O	'01'	VERSION_SW	RO	Version of the software defined by the vendor.	3	'000000'
M	'02'	HCI_VERSION	RO	Version of HCI supported by the host.	1	'03'
O	'03'	VERSION_HARD	RO	Version of the hardware defined by the vendor.	3	'000000'
O	'04'	VENDOR_NAME	RO	Vendor name UTF-8 coding. The maximum value for N_0 shall be 20.	N_0	$N_0 = 0$
O	'05'	MODEL_ID	RO	Model identifier assigned by the vendor.	1	'00'
M	'06'	GATE_LIST	RO	The list of all gates that accept dynamic pipes as a list of GID.	N_1	'0405'
O	'08'	MAX_CURRENT	RO	The maximum current provided / required by the host controller / host during operation / [mA].	1	10='0A'

[a] Column Type: M = mandatory, O = optional.

[b] Column ID indicates the identifier.

[c] Column AR indicates access rights: RO = read only.

6.3.5 Loop back gate

The loop back gate provides access to services for testing the HCI network. As destination gate, the loop back gate shall accept at least one pipe from each host in its WHITELIST.

The loop back gate has no registry entries defined.

6.3.6 APDU gate

This subclause contains a subset of information from ETSI TS 102 622 about APDU gate registry.

The APDU gate provides the registry shown in Table 7. The registry shall be persistent.

Table 7 — Entries in the APDU gate registry

ID[a]	Parameter	AR[b]	Description	Len/ byte	Default
'01'	MAX_C_APDU_SIZE	RO	Maximum acceptable total length of a command APDU in EVT_C-APDU event.	2	'0105' = 261
'02'	MAX_WAIT_TIME	RO	Maximum wait time for the execution of a command APDU / [ms].	2	'03E8' = 1000

[a] Column ID indicates the identifier.

[b] Column AR indicates access rights: RO = read only.

6.3.7 APDU application gate registry

An APDU gate has no registry.

6.4 Example of exchanging APDU via HCI/HCP

Figure 4 shows an example of exchanging one command-response pair between two hosts. That exchange starts with pipe creation, opening the newly created pipe and using that pipe.

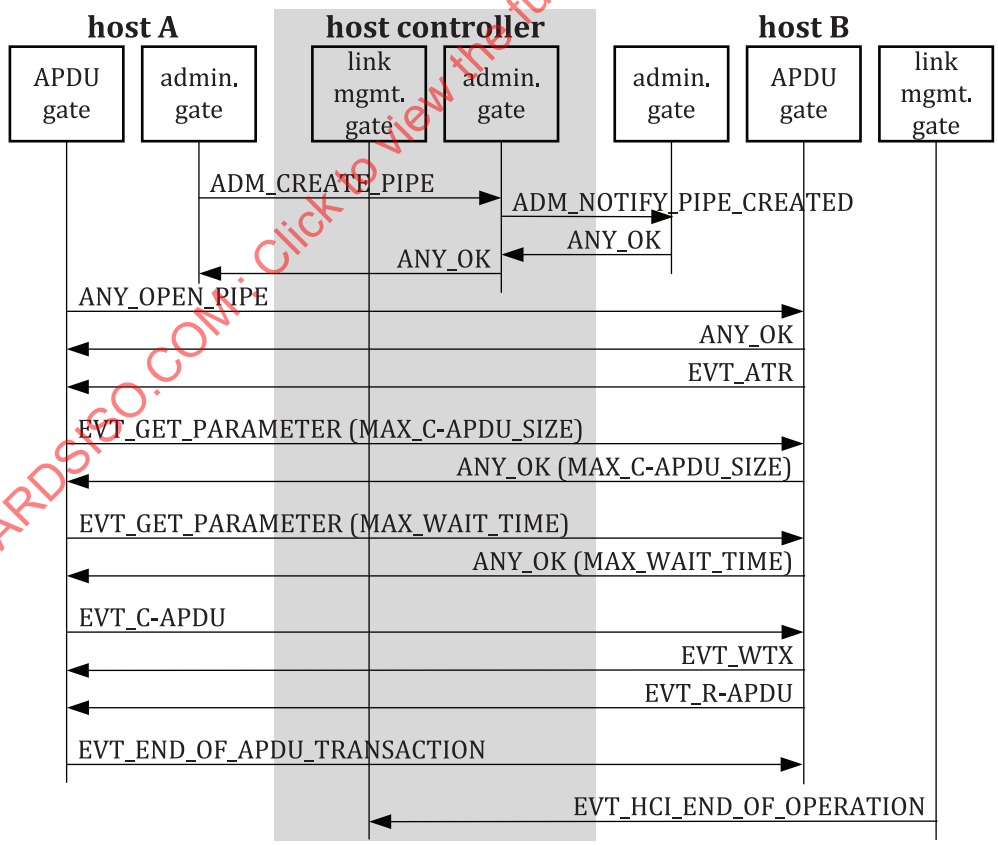


Figure 4 — Use of client and server APDU gates

6.5 APDU transport versus HCP frames

6.5.1 General

Encapsulation of HCP frames into T=1 blocks is definitely not an optimal option because of its restrictive aspects with regard to HCI/HCP. Definitions of client APDU hosts and server APDU hosts are provided by ETSI TS 102 622 (see also 5.1.6) for the purposes of client/server APDU legacy. See Annex B for ICC and HCI/HCP communication within OSI model (B.1 and B.2) and for detailed comparison of T=1 versus HCI/HCP (B.3).

Figure 5 describes from left to right respectively:

— the OSI layout for ICC featuring T=1 protocol as per ISO/IEC 7816-3 (with specific layers, white background);

— the HCI/HCP layout according ETSI TS 102 622 (with specific layers, grey background);

— the merge of ISO/IEC 7816-3 with HCI/HCP showing how the layers are interspersed (note the colour coding). Note, that the transport layers (messaging, routing, chaining) from ISO/IEC 7816-3 and HCI/HCP are fused, whereas data link and underlying half-duplex protocol framing are fully re-used according to the ISO/IEC 7816-3 T=1 protocol.

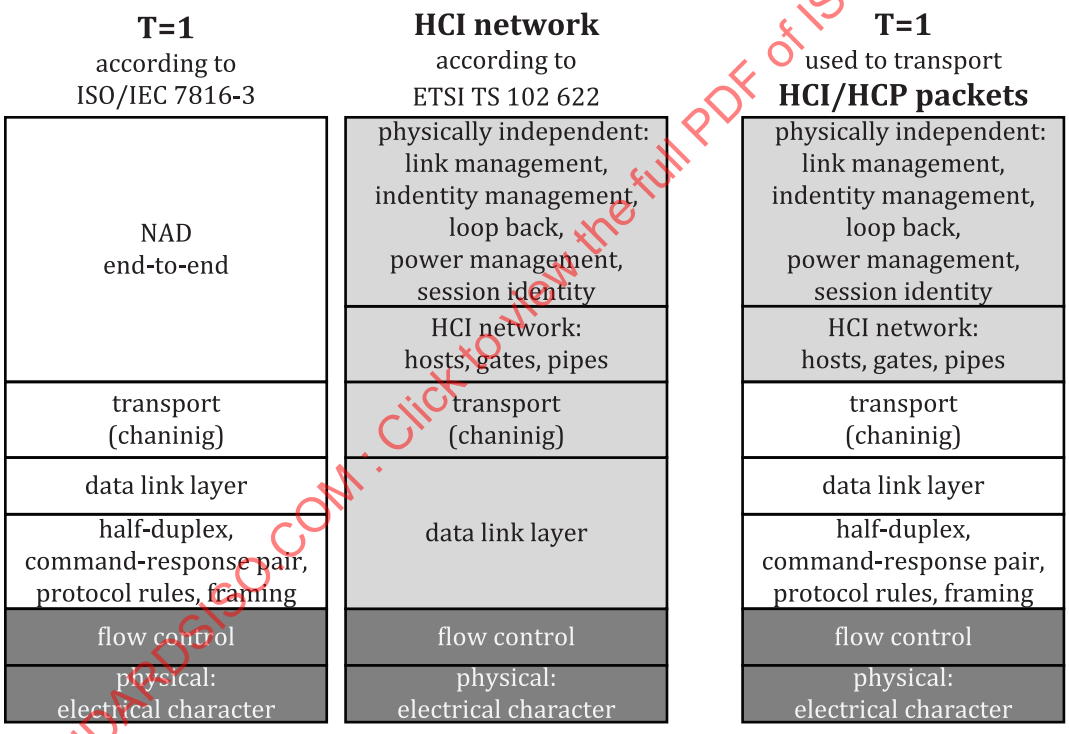


Figure 5 — T=1 protocol fit with HCI/HCP

The physical-independent layer properties and features are:

a) Identification: SESSION_IDENTITY (host controller administration gate) for HCI pipes persistency.

b) Identity management gate contains information according to Table 6.

c) Visibility of other hosts present in the HCI network, and host type information, with the possibility to condition creating and opening of dynamic pipes between the gates of two hosts on the WHITELIST configured by the target host.

d) Routing of messages between hosts over opened pipes between the gates of two hosts handled in the HCI network layer in Figure 5.

e) APDU transport capability using the pre-defined gates/pipes, events, registry.

f) Possibility to define generic gates and pipes with dedicated registry for specific data transfers.

g) Link management gate for evaluation of error rates, power management and a loop back gate both independent of the physical layer.

ISO/IEC 7816-3 T=1 protocol enables a half-duplex communication that can be adapted for various physical interfaces following the same data link layer rules and framing definitions; and it makes possible transport of HCI frames containing APDU or other types of data.

6.5.2 Chaining of T=1 message blocks wrapping HCP packets

ISO/IEC 7816-3 T=1 protocol defines the data link layer. The ISO/IEC 7816-3 T=1 frames shall wrap the HCI/HCP frames. Both, the ISO/IEC 7816-3 T=1 and ETSI TS 102 622 define chaining support. As the ISO/IEC 7816-3 integrates the chaining in the data link layer rules for frames and errors handling, T=1 chaining should be actually used whenever necessary while the HCI/HCP chaining information remains redundant, unused.

6.5.3 Handling of error recovery with T=1 features

ISO/IEC 7816-3 T=1 defines a half-duplex communication protocol which includes documenting the data link layer rules.

In accordance with the error handling rules defined by ISO/IEC 7816-3, data link layer can be re-used independent of the physical interface over which this protocol is running, assuming specified frames structure is maintained.

6.6 APDU fragmentation

In accordance with ISO/IEC 7816-4 for command and response chaining and payload fragmentation rules, HCP messaging layer can handle APDU command/response and encapsulate fragmented APDU within HCP packets (see Figure B.1). The HCP routing layer conveys HCP packets towards the pipe denoted by its identifier. The size of the message contained in a packet is application specific.

The source gate is responsible for fragmenting messages. The host controller may need to re-assemble data from the source host and perform data fragmentation according to maximum fragments size specific to capabilities of the interface module of the destination host.

When transmitting oversize APDU command/response payloads, the HCP packet (according to ETSI TS 102 622, 5.3) applies the following rules.

a) Packet header is mandatory in all message fragments.

b) Message header shall only be in the first message fragment.

c) Chaining bit = 0 in all packet headers except the last one.

6.7 Supported set of commands and events

The type of an instruction can be: command, event, response to a command (see ETSI TS 102 622, clause 6).

The type of an instruction is indicated by the TYPE field of the HCP message header, see B.7.

Annex A
(informative)

Examples of architecture variants

A.1 Architecture variants

A.1.1 Variant with full legacy secure element

Descriptions of the main features (see Figure A.1) are as follows.

a) eSE is a full legacy secure element e.g. compliant with ISO/IEC 7816 (all parts) and supporting T=1.

b) Host A, host B and host controller perform communication with HCI/HCP i.e. they handle routine and packing according HCI/HCP standard requirements.

c) Host B may be a software hosted on a microcontroller on board the device; host B is called "client APDU host". Host B has an APDU application gate. Host B acts as a host calling a service on the APDU gate of another host (here host A). Host B does not necessarily generate and process APDUs on its own; it may instead hand on back and forth APDU exchanged with a remote server e.g. through the device baseband radio processor and over the air (OTA) operator network (not shown in Figure A.1). Host B may exchange back and forth with host A command/response APDU pairs.

d) Host A and driver may be software components either

   1) running as application on host controller, or

   2) built in the host controller's operating system (more efficient).

Driver component carries out the mapping of de-encapsulated payload, passed on from APDU gate, into APDUs transported over a transmission protocol supported by the eSE application T=1 in case of Figure A.1.

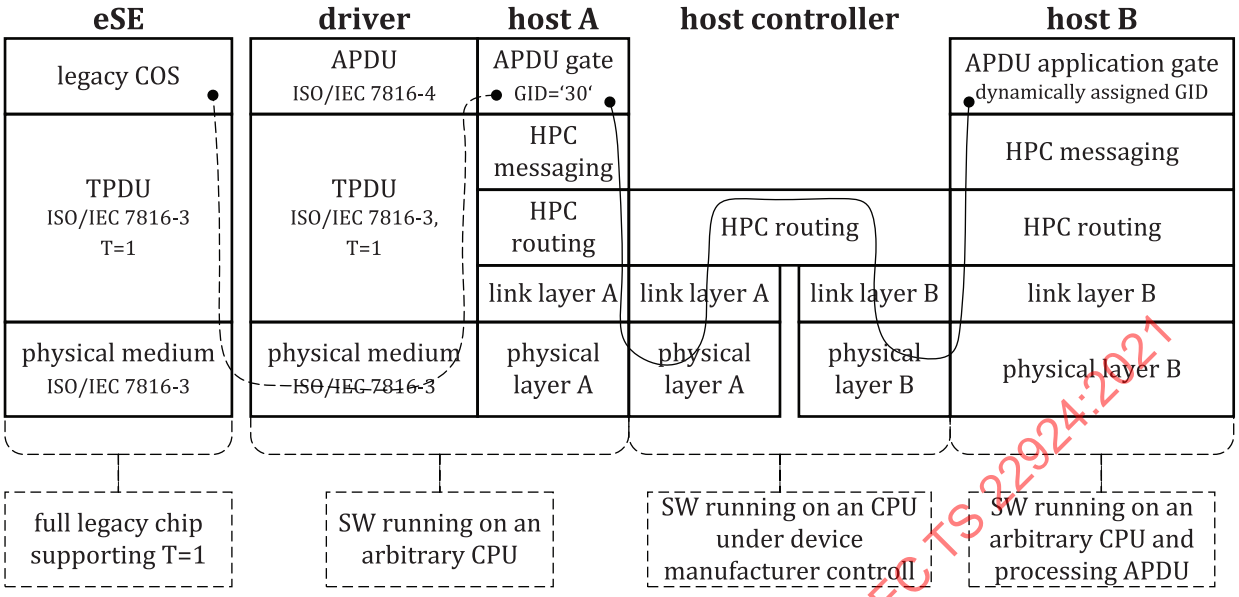


Figure A.1 — Architecture variant with full legacy eSE

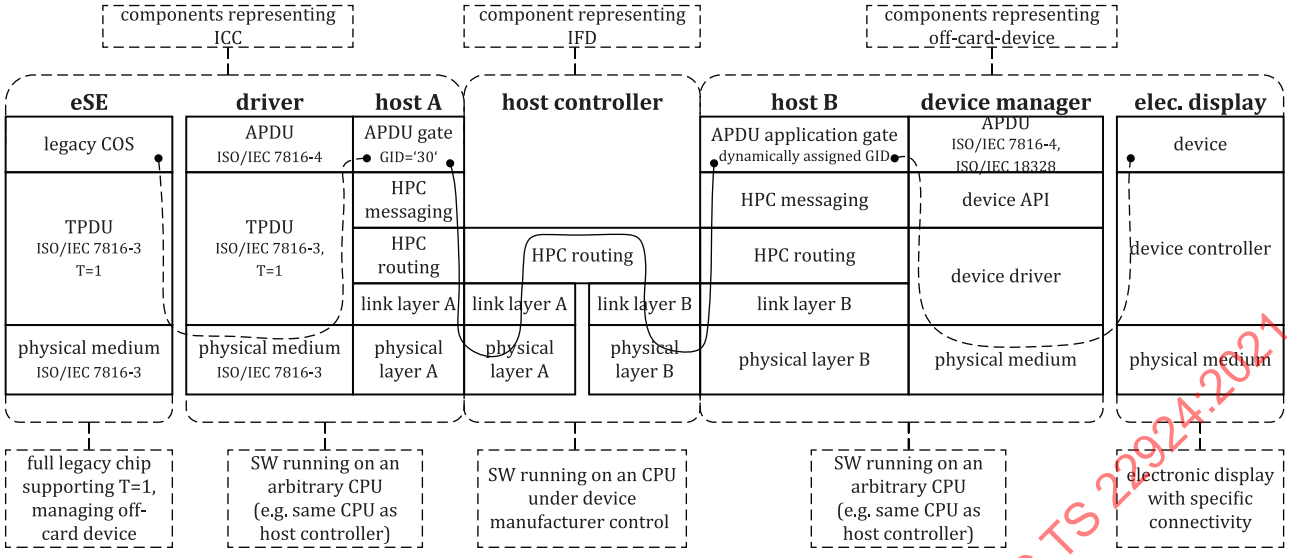
A.1.2 Variant with ICC-managed device

The architecture on Figure A.2 can be applied to off-card ICC-managed devices. Figure A.2 is mapped for clarity onto ISO/IEC 18328-3:2016, Figure 5.

— An application (either rich operating system (rich OS) or trusted execution environment (TEE) application) running on the same CPU as the host controller, or on another host, acts as IFD.

— Host A stands for APDU gate offering APDU protocol service and acting as a proxy to the legacy eSE.

— c Host B provides an abstraction of the device manager piloting the off-card device (i.e. electronic display); instructions addressed to this device are controlled by the eSE acting behind host A.



Key

specific route

HCP route

Figure A.2 — Architecture variant with ICC-managed device

The sequence of operations may comprise the following main steps:

a) IFD, host A and host B write their respective WHITELIST into the host controller administration gate in order to inform the host controller which hosts are allowed to communicate with them. As example, IFD will put in its WHITELIST the HID of host B and HID of host A. The host B will put on its WHITELIST the HID of host A and HID of IFD.

b) IFD opens a pipe with host A.

c) The host A opens a pipe with host B.

d) IFD sends to host A an HCP command packet encapsulating an APDU with ADM function (see ISO/IEC 18328-3:2016, 7.2), this command being intended to the ICC-managed device.

e) The host A conveys to the driver the APDU payload to the attention of eSE.

f) The eSE returns to host A a device related command to the attention of host B.

g) Then host A sends to host B an HCP command packet encapsulating the device related command.

h) Device manager component handles the electronic display instruction i.e. implements the electronic display API.

i) The response from the off-card device is returned by host B to host A, then conveyed to IFD.

Whereas outside HCI/HCP enabled environment, the card-originated byte string (see ISO/IEC 18328-3:2016, 7.1 and 7.2) can be used for the communication between the eSE and an off-card device, when HCI/HCP is supported, there is no need for the IFD component to:

— retrieve information from the ICC dedicated to an off-card device using the card-originated byte string mechanism;

— dispatch the received byte string to the off-card device for the purposes of processing and retrieving information;

— send to the ICC the result after processing of the device related information by the off-card device. Consequently, off-card device management by eSE with HCI/HCP does not require card-originated byte string and can take place directly between two hosts over a dedicated pipe. The IFD intervening only to deliver the ADM command received from the outside world or from an application running on a rich operating system (Rich OS) or a trusted execution environment (TEE).

A.1.3 Variant with application interface to secure element

The architecture described in Figure A.3 may be applied with legacy eSE hosting a data element exported as an API. That API is interpreted by host B which uses its entry points to request services from host A. The API can as well be interpreted by a remote server connected to host B.

a) It is possible that host A offers a generic gate (i.e. not necessarily APDU gate in this case).

b) It is possible that host B offers a generic gate (i.e. not necessarily APDU application gate in this case).

c) The host B opens a pipe with host A.

d) Then host B send a request to host A to read a dedicated data element from host A.

e) The eSE stores a data element (e.g. data object (DO)). That data element possibly encapsulates references to objects within the eSE, which can be used from the interface. Additionally, the data element possibly stores sequence of instructions along with their respective descriptor. Upon request from host B, the data element is read out of the eSE and interpreted by host B as an ordered set of inputs to be used as arguments for a generic application interface.

f) Then host B can call an application interface function, and the related message is encapsulated in HCP packets and conveyed to host A through the pipe.

g) The host A unwraps the application interface function call and passes it on to the driver component implementing the application interface, i.e. the application interface function call is serialized in an HCP packet.

h) The driver component translates the incoming data of each function call into a command APDU and sends it to the eSE.

i) The driver component processes the response APDU returned by eSE and translates it into application interface function outgoing data and delivers it to host A.

j) The host A wraps the outgoing data payload in an HCP packet and returns it to host B over the pipe.

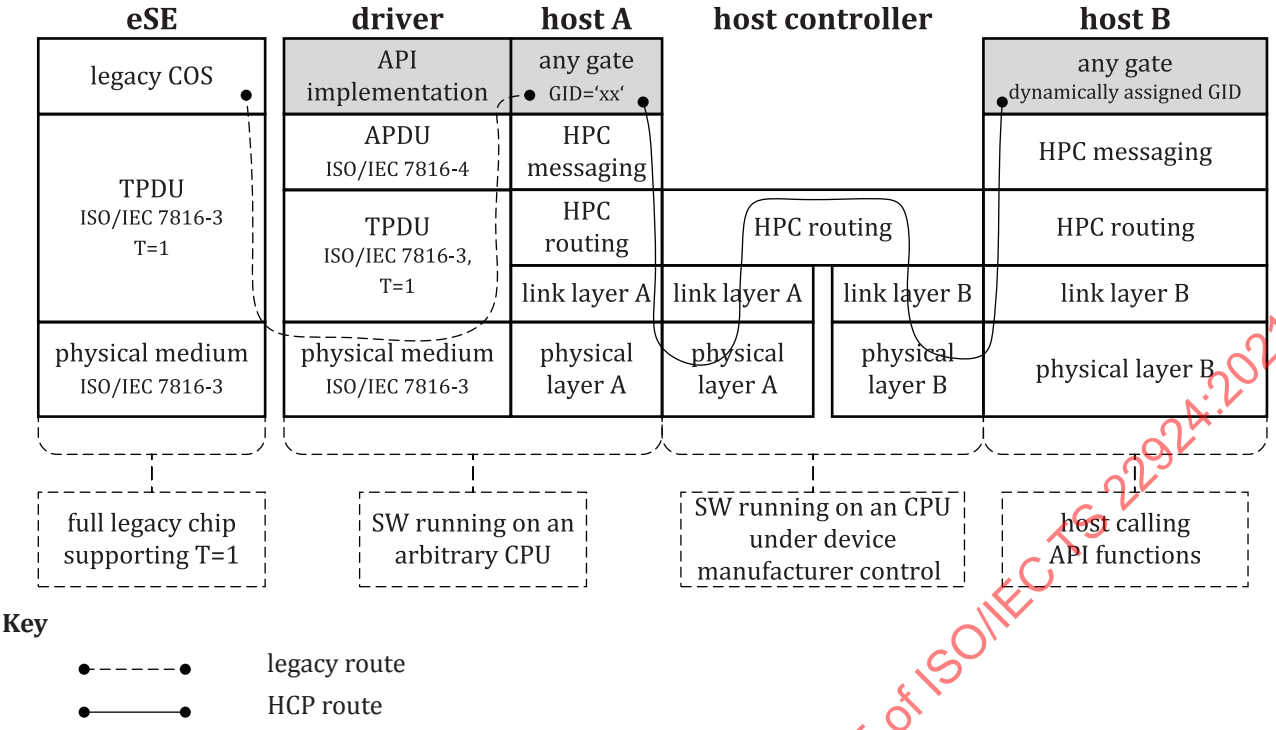


Figure A.3 — Architecture variant with application interface to eSE

NOTE Figure A.3 is similar to Figure 3 and Figure A.1. Boxes with grey background show differences.

Since different application interfaces can be used depending on the use case, it is recommended for host A to offer one gates per supported application interface. Upon selection of an application interface by host B (possibly identified by its unique identifier or its object identifier), host A is able to load the appropriate driver component.

For the architecture model of Figure A.3, host B can either interpret the data element, or just relay it to a remote server that will interpret it and call the application interface functions in order to access the eSE services through host B.

A.1.4 Variant in a simplified HCI architecture when only two hosts are present

In systems where only two hosts are present and can be connected through the same physical interface, usual host controller responsibilities are not necessary:

a) Provide information on the available hosts or regarding a host connection or disconnection.

b) Support the process of creating pipes between gates of the hosts according to the WHITELIST information of the destination host.

c) Route packets according to pipes information possibly for multiple instances of inter-hosts communication.

d) Receive EVT_HCI_END_OF_OP sent by a host on the link management gate signalling host entry into power saving mode and that an interface specific resume will be required for a subsequent access. The same can be handled by the other host.

For best usage of resources, performance and power efficiency, it can be considered that main necessary pipes are default created. Opening pipes is performed using only the gates available on the two hosts – as per the GATES_LIST available in the identity management gate of each host. CONNECTION_TYPE can indicate a direct host-to-host connection or through a host controller. The requirement for a host controller software component on one of the two hosts can be avoided.

Annex B
(informative)

Background information

B.1 ICC communication within the OSI model

From the OSI model comprised of seven layers, five layers are applied to ICC and to eSE, that are:

a) application layer, serving to business logic data i.e. based on APDU protocol (see ISO/IEC 7816-4, ISO/IEC 7816-7, ISO/IEC 7816-8, ISO/IEC 7816-9, ISO/IEC 7816-11, ISO/IEC 7816-13, ISO/IEC 7816-15, ISO/IEC 18328-3 and ETSI TS 102 622);

b) network layer for addressing as per ISO/IEC 7816-3 (i.e. with NAD byte), or performing routing of packets (see ETSI TS 102 622) based on HID, GID and PID;

c) transport layer (i.e. TPDU), building datagrams and performing segmentation and reassembly of data (see ISO/IEC 7816-3, ISO/IEC 14443-4 and ETSI TS 102 622);

d) data Link layer managing structure and exchange of blocks of asynchronous characters captured on the connection line (see ISO/IEC 7816-3, ISO/IEC 14443-2 and ETSI TS 102 613);

e) Physical layer transmitting signals organized in asynchronous characters (see ISO/IEC 7816-3, ISO/IEC 14443-1 and ETSI TS 102 613).

B.2 HCI/HCP communication within the OSI model

Table B.1 provides a mapping of OSI layers to HCI/HCP functionality and identifiers the functions that are addressed by this document.

Table B.1 — OSI layers based equivalence between ISO and ETSI

Corresponding features between OSI and HCI/HCP		Addressed in this document
OSI model	**HCI/HCP model**	
Application layer	Command/Response APDU	No
Network layer	PID information in HCP packets corresponding to the pipes created based on HID and GID	Yes
Data link layer	Link management gate provided for retrieving communication error rate from these layers and informing power saving mode	Yes, only exchanging information in these layers
Physical layer		

B.3 Comparison of HCI/HCP versus T=1

T=1 protocol defined in ISO/IEC 7816-3 is similar to HCI/HCP defined in ETSI TS 102 622. Both are derived from HDLC (high-level data link control, see ISO/IEC 13239). Table B.2 describes the common parts, similarities and differences of ETSI TS 102 622 HCI/HCP protocol and ISO/IEC 7816-3 T=1 protocol.