Technical report

Physical Authentication

Version 1.0 Release Candidate

Date: 2014/12/18

Foreword

This technical report specifies physical user authentication mechanisms that may be embedded on an eIDAS token. Unless explicitly mentioned, this specification is compliant with all referenced standards.

This document has been written by ACSIEL (www.acsiel.fr) in close relation with ANSSI (www.ssi.gouv.fr) and ANTS (www.ants.interieur.gouv.fr).

TABLE OF CONTENT

Glossary

APDU	Application Protocol Data Unit
BIO	BIOmetric data
BIT	Biometric Information Template
BITg	Biometric Information Template Group
LCS	Life Cycle State
MF	Master File
PACE	Password Authenticated Connection Establishment
PIN	Personal Identification Number
PUK	PIN Unlocking Key

1. Introduction

The user consent performed with user authentication shall be done in a secure way, to ensure protection of the authentication data. User authentication via physical user data ensures authentication of the given agreement;

Physical authentication features may be supported byan application embedded in an eIDAS token (smartcard, SIM, µSD…).

2. Physical user credentials

Physical user credential allow authentication of the user. Depending on the configuration of the application, it MAY unlock the access to some function of the application or unlock the usage of the signature creation function;

2.1. User credentials

A Physical user credential may be used to:

a. Authenticate the user;

b. Express the consent of user before access any operation;

When delivered, the data container dedicated to store the user credential SHALL be in one of the following state:

c. Initialized. The physical user credential is already loaded.

d. Uninitialized. The user SHALL initialize the physical user credential prior any usage.

The current technical report does not limit the number of physical user credential. Depending on the configuration, one or several physical user credential may be present, and each of them may protect the access to one or several operations.

2.1.1. Available operations

The following operations may be performed on a physical user credential:

a. **Verification**: this operation submits a candidate physical user credential and compares it against the reference physical user credential. Upon success the following actions are performed

- the physical user credential verification status is set;
- the corresponding access rights are granted;
- the retry counter is restored to its initial value;

Upon failure, the following actions are performed:

- the physical user credential verification status is reset;
- the corresponding access rights are denied;
- the retry counter is decremented by one;

b. **Change**: this operation changes the reference physical user credential values stored. If successful, the physical user credential verification status is reset.

c. **Devalidation**: this operation resets the physical user credential verification status.

d. **Unblocking**: this operation consists in unblocking the physical user credential, namely restoring its retry counter to the initial value (described below), resetting its verification status, and changing its reference value.

2.1.2. Life cycle state

Physical user credentials have a life cycle compliant with [ISO/IEC 7816-9] and support the four following states:

a. **Initialization state**: in this state the data container is created, but the data has not been initialized yet. The physical user credential usage is restricted.

b. **Operational state – activated** : in this state the data container is created, filled with a physical user data, and usable;

c. **Operational state – deactivated**: in this state the data container is created, filled with a physical user data, and its usage is restricted;

d. **Termination state**: in this state, the data container is irreversibly unusable;

The transitions and the command used to perform these transitions are compliant with [ISO/IEC 7816-9].

2.1.3. Attributes

Physical user credentials SHALL contain the two following attributes:

a. **Retry counter**: counter indicating the number of remaining tries for the verification of the physical user credential. This counter is persistent, meaning it is not reset upon reset or application selection. It is decremented on a wrong verification, and restored to its initial value (described below) upon successful verification of the physical user credential. When this counter has reached ’00’, the physical user credential becomes unusable. Prior any other use, it SHALL be unblocked.

b. **Initial value of retry counter**: value indicating the maximum number of incorrect verification allowed by the physical user credential. The retry counter is reset to the initial value in case of successful verification/unblock/change. The initial value may take any value between ’1’ (decimal) and ‘15’ (decimal) and its value is indicated in the [ISO/IEC 7816-15] structure. No modification SHALL be possible once this value is set.

2.2. PIN unblocking keys (PUK)

PIN unblocking key (PUK) aims at unblocking user credentials once their retry counter has reached zero. A PUK may be a physical user object instead of a PIN value and SHALL be located in the MF. The PUK may be a blocking or unblocking physical user credential.

Its usage MAY be limited thanks to a usage counter.

2.3. Format of biometric data

This chapter provides information about the format and structure of biometric data associated with the physical user credential.

2.3.1. Format

Biometric data may be of any type (fingerprint, iris...). The type of biometric data, as well as its format SHALL be described in the [ISO/IEC 7816-15] structure.

> ***Notes***
>
> The FAR value is out of the scope of the current technical report. It is up to the issuer to set up its own recommendations.
>
> The technical report is neutral and does not consider any specific biometry technology. As such, any type of biometry can be used.

2.3.2. Specific interoperability concerns for biometric

Biometric data data SHALL be handled in compliance with [ISO/IEC 7816-11].

The BIT/BITg corresponding to the biometric data MAY be made available in a file declared in the [ISO/IEC 7816-15] structure. These data structure MAY be protected in a manner ensuring privacy protection.

2.3.3. Physical user credential initialization

A physical user credential SHALL be initialized according to the process flow and following the access rights of the application supporting the physical user authentication features.

2.3.4. Physical user credential update

A physical user credential MAY be updated according to the process flow and following the access rights of the application supporting the physical user authentication features.

The old value of the physical user credential SHALL be submitted first with VERIFY command, and then new value of the physical user credential SHALL be sent with CHANGE REFERENCE DATA command with P1='01' and reference indicated in P2. The update is effective only if first step of verification with the indicated current value succeeded. Previous validation status is lost.

The update of the physical user credentials SHALL be performed using two APDU commands.

1. The old template SHALL be submitted first with VERIFY command
2. The new template SHALL be sent with CHANGE REFERENCE DATA command with P1='01' and reference data qualifier indicated in P2.

110 The update is effective only if first step of verification with the indicated current value succeeded. Previous validation status is lost.

2.3.5. Physical user credential unblocking

Once the retry counter of the physical user credential has reached zero, it is locked and does not allow further usage.

115 A physical user credential MAY be unblocked according to the process flow and following the access rights of the application supporting the physical user authentication features.

2.3.6. Physical user authentication devalidation

The physical user authentication can be devalidated.

3. ISO/IEC 7816 mapping

3.1. VERIFY of physical user credential

Biometric based physical user verification requires a user to provide a biometric template.

Note: If the biometric data is absent from the data field, the verification status of the physical user credential is returned through the status word. If status word is 0x9000, the physical user credential verification status is still set. This command has no impact on the status and associated rights.

COMMAND PARAMETER	MEANING
CLA	ISO
INS	'21'
P1	'00'
P2	reference data qualifier
L_c field	Data Length or absent
Data field	If Lc present, < candidate biometric template> If Lc absent, absent
Le field	Absent

RESPONSE PARAMETER	MEANING
Data field	Absent
SW1-SW2	See [ISO/IEC 7816-4], Tables 5 and 6 where relevant

3.2. DEVALIDATION of physical user credential

The command resets the physical user authentication status.

COMMAND PARAMETER	MEANING
CLA	ISO
INS	'21'
P1	'FF'
P2	reference data qualifier
L_c field	Absent
Data field	Absent
Le field	Absent

RESPONSE PARAMETER	MEANING
Data field	Absent
SW1-SW2	See [ISO/IEC 7816-4], Tables 5 and 6 where relevant

3.3. CHANGE REFERENCE DATA of physical user credential initialization

The command initializes the new physical user credential template sent from the interface device. It can be performed only if the security status satisfies the security attributes for this command.

This command SHALL be used to activate the physical user credential object when it is in created state. It SHALL be used to change the current physical user credential object with the new biometric template if it is already activated.

COMMAND PARAMETER	MEANING
CLA INS P1 P2	ISO '25' '01' reference data qualifier
L_c field	Data Length
Data field	<new biometric template>
Le field	Absent

RESPONSE PARAMETER	MEANING
Data field	Absent
SW1-SW2	See [ISO/IEC 7816-4], Tables 5 and 6 where relevant

3.4. CHANGE REFERENCE DATA of physical user credential update

This command intends to replace the physical user credential template with a new one. A VERIFY command on the current physical user credential object template SHALL be performed beforehand in order to grant the access rights. This operation can only be performed only if the security status satisfies the security attributes for this command.

COMMAND PARAMETER	MEANING
CLA	ISO
INS	'25'
P1	'01'
P2	reference data qualifier
L_c field	Data Length
Data field	<new biometric template>
Le field	Absent

RESPONSE PARAMETER	MEANING
Data field	Absent
SW1-SW2	See [ISO/IEC 7816-4], Tables 5 and 6 where relevant

3.5. RESET RETRY COUNTER of physical user credential

After N (N as specified by application) wrong consecutive verification of a candidate physical user credential, the physical user credential is locked and does not allow any further verification. It can be performed only if the security status satisfies the security attributes for this command.

After successful completion of the command, the retry counter of the physical user credential is restored at its initial value N.

COMMAND PARAMETER	MEANING
CLA	ISO
INS	'2D'
P1	'02'
P2	reference data qualifier
L_c field	Data Length
Data field	<new biometric template>
L_e field	Absent

RESPONSE PARAMETER	MEANING
Data field	Absent
SW1-SW2	See [ISO/IEC 7816-4], Tables 5 and 6 where relevant

3.6. MANAGE DATA: OPERATIONAL CHANGE LCS Physical user credential

This command changes the LCS (see [ISO/IEC 7816-4] Table 14) of the physical user credential to
160 the value of LCS indicated in the P2 parameter. It can be performed only if the security status satisfies the security attributes for this command.

The LCS MAY be changed to operational-state activated, operational-state deactivated or terminated.

COMMAND PARAMETER	MEANING
CLA	ISO[1]
INS	'CF'
P1	'00'
P2	LCS to be set by the command (see [ISO/IEC 7816-4] Table 14)
L_c field	Data Length
Data field	'7F71'- L – { '7F70' – L – {'83' –L - <Physical user credential Id>}}
L_e field	Absent

RESPONSE PARAMETER	MEANING
Data field	Absent
SW1-SW2	See [ISO/IEC 7816-4], Tables 5 and 6 where relevant

[1] This command is currently under discussion in [ISO/IEC 7816-9]. In the meanwhile, a proprietary class byte is used waiting for the outcomes of the standardization process. Based on the outcomes, this command OR ACTIVATE/DEACTIVATE/TERMINATE commands should be used..

4. Example of [ISO/IEC 7816-15] structure

The mandatory features indicated below define the minimal set of functionality that must be supported by an application in order to guarantee interoperability. The Cryptographic Information application shall be designed according to [ISO/IEC 7816-15]; this chapter specifies the use of CIA for a Signature application, and a set of associated APDU commands. It describes the physical user objects.

- SignBio authentication object is defined through the following fields [OPTIONAL]

Attributes	**Item**	**Description**												
Common	label	**An ASCII descriptive string (e.g. "Sign BIO")**												
	accessControlRules	APDU	Accessmode										securityConditions	Communication Mode [OPTIONAL]
			Read(0)	Update(1)	Execute(2)	Delete(3)	Attribute(4)	Pso_cds(5)	Pso_verif(6)	Pso_dec(7)	Pso_enc(8)	Int_auth(9)	Ext_auth(10)	
		CHANGE REFERENCE DATA		1									SM and Role xxx And UserConsent	BIT STRING { contact (0), contactLess (1) }
		VERIFY			1								ALWAYS	
		RESET RETRY COUNTER					1						SM and Role xxx And UserConsent	
		MANAGE DATA			1		1						SM and Role xxx And UserConsent	
	currentLCS	ENUMERATED { init(1), op-activated(2), op-deactivated(3), termination(4)}												
Class	authId	Unique identifier of the object in the [ISO/IEC 7816-15] structure												
Type	bioFlags	**Flag**	**Value**											
		(1)Local	local PIN											
		(2)change-disabled	False = change is allowed											
		(3)unblock-disabled	False = unblock is allowed											
		(4)initialized	True											
		(8)disable-allowed	False											
		(9)integrity-protected	True											
		(10)confidentiality-protected	True											
	templateId	CHOICE { oid OBJECT IDENTIFIER, issuerId OCTET STRING, }												
	bioType	CHOICE { fingerPrint FingerPrintInformation, iris [0] IrisInformation, chained [1] SEQUENCE SIZE (2..cia-ub-biometricTypes) OF BiometricType, }												
	BioReference	Reference used in VERIFY command to reference the Bio in application												
	Bit	[APPLICATION 96] BiometricInformationTemplate												

Attributes	Item	Description
Commo	label	**An ASCII descriptive string (e.g. “Sign BIO”)**
	bitGroup	[APPLICATION 97] BiometricInformationTemplateGroup

175 • SignBio1Ton authentication object is defined through the following fields [OPTIONAL], on one container referencing many biometric.

Attributes	Item	Description												
Common	label	**An ASCII descriptive string (e.g. "Sign BIO 1ton")**												
	accessControlRules	APDU	Accessmode										securityConditions	CommunicationMode [OPTIONAL]
			Read(0)	Update(1)	Execute(2)	Delete(3)	Attribute(4)	Pso_cds(5)	Pso_verif(6)	Pso_dec(7)	Pso_enc(8)	Int_auth(9)	Ext_auth(10)	
		CHANGE REFERENCE DATA		1										SM and Role xxx And UserConsent	BIT STRING { contact (0), contactLess (1) }
		VERIFY			1									ALWAYS	
		RESET RETRY COUNTER					1							SM and Role xxx And UserConsent	
		MANAGE DATA			1		1							SM and Role xxx And UserConsent	
	currentLCS	ENUMERATED { init(1), op-activated(2), op-deactivated(3), termination(4)}													
Class	authId	Unique identifier of the object in the [ISO/IEC 7816-15] structure													
Type	bioFlags	**Flag**	**Value**												
		(1)Local	local PIN												
		(2)change-disabled	False = change is allowed												
		(3)unblock-disabled	False = unblock is allowed												
		(4)initialized	True												
		(8)disable-allowed	False												
		(9)integrity-protected	True												
		(10)confidentiality-protected	True												
	templateId	CHOICE { oid OBJECT IDENTIFIER, issuerId OCTET STRING, }													
	bioType	--many items CHOICE { fingerPrint FingerPrintInformation, iris [0] IrisInformation, chained [1] SEQUENCE SIZE (2..cia-ub-biometricTypes) OF BiometricType, }													
	BioReference	Reference used in VERIFY command to reference the Bio in application													
	Bit	[APPLICATION 96] BiometricInformationTemplate													
	bitGroup	[APPLICATION 97] BiometricInformationTemplateGroup													

5. Normative References

ISO/IEC 7816-4 - Identification cards -- Integrated circuit cards -- Part 4: Organization, security and commands for interchange

ISO/IEC 7816-6 - Identification cards -- Integrated circuit cards -- Part 6: Interindustry data elements for interchange

ISO/IEC 7816-8 - Identification cards -- Integrated circuit cards -- Part 8: Commands for security operations

ISO/IEC 7816-9 - Identification cards -- Integrated circuit cards -- Part 9: Commands for card management

ISO/IEC 7816-11 - Identification cards -- Integrated circuit cards -- Part 11: Personal verification through biometric methods

ISO/IEC 7816-15 - Identification cards -- Integrated circuit cards -- Part 15: Cryptographic information application

ISO/IEC 2382-37 - Information technology -- Vocabulary -- Part 37: Biometrics