Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
AGENCE NATIONALE DES TITRES SÉCURISÉS

Electronic National Identity Card
Technical Specifications

Document Owner: ANTS
Version: A031
Date: 14/05/2020

Contents of this document

1. Introduction to the French Digital Identity Application specifications

The European Commission, the Council and the European Parliament have agreed on the European regulation on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members exercising their right of free movement (Regulation (EU) 2019/1157 of 20 June 2019). The main objective is to harmonize the security features of the identity cards within the European Union. The Member States shall introduce an ICAO[1] compliant[2] chip into their national identity card within 24 months after the entry into force of this regulation. This ICAO compliant chip is used as travel document within the European Union.

The French administration is taking the opportunity of this European Regulation to introduce in parallel of the ICAO application a National Digital Identity application in the same chip in order to provide an inclusive means to all French citizen with a high level of assurance digital Identity.

This trusted Digital Identity can be used within the France Connect infrastructure and be also an enabler to new trusted on-line services for innovative use case to develop the French Tech initiative while respecting the Privacy by Design concept.

The Digital Identity application is designed with the following concepts:

- Full logical separation between the ICAO compliant application and the Digital Identity application
- Electronic identification and electronic authentication with two levels of assurance as per the eIDAS regulation:
  - High
  - Substantial
- Mandatory user-consent to disclose the Citizen Digital Identity relying on a user PIN
- Compliant to:
  - eIDAS regulation
  - French RGS requirements
- Contact & Contactless interfaces
- Re-use of standards protocols: PACE and EAC v1
- Possibility to load new applications in the future on existing already deployed identity cards.

To be in capacity to deploy these concepts within the time frame given by the European regulation on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members exercising their right of free movement, the French administration prepared a set of two technical contributions that are complementing the well-known BSI TR-03110 set of documents[3].
These two technical contributions are presented at the chapters 2 and 3 of this document.

1 ICAO : International Civil Aviation Organization

2 ICAO 9303 : ICAO doc 9303 Edition 7 - 2015

3 BSI TR-03110 1 to 4

2. French National Identity Application Profile (ICAO & Digital Identity)

2.1. ePassport Application

See Regulation (EU) 2019/1157 of 20 June 2019.

2.2. Digital Identity Application

This section specifies the Digital Identity application, which is an application for electronic identification. The Digital Identity application contains data groups with personal data of the holder.

2.2.1. Application Identifier

The Digital Identity application SHALL be identified by an application identifier. The RID of the Digital Identity application is D250 000010, the PIX is defined in [DigitalIdentity].

2.2.2. Authentication

The Digital Identity application requires the user consent prior to (1) being selected and (2) reading the data groups of the Digital Identity application.

2.2.3. Data Groups

The Digital Identity application consists of several data groups containing personal data. The presence of each data group is at the discretion of the issuer. An overview on the data groups is given in the table below.

DG	Content	FID	SFID	R/W	Access
EF.COM	Set at personalization	0x011E	0x1E	R	PACE
DG1	Set at personalization	0x0101	0x01	R	PACE + CA
DG2	Set at personalization	0x0102	0x02	R	PACE + CA
DG3	Set at personalization	0x0103	0x03	R	PACE + CA + TA
DG4	Set at personalization	0x0104	0x04	R	PACE + CA + TA
DG5	Set at personalization	0x0105	0x05	R	PACE + CA
DG6	Set at personalization	0x0106	0x06	R	PACE + CA
DG7	Set at personalization	0x0107	0x07	R	PACE + CA
DG8	Set at personalization	0x0108	0x08	R	PACE + CA
DG9	Set at personalization	0x0109	0x09	R	PACE + CA
DG10	Set at personalization	0x010A	0x0A	R	PACE + CA
DG11	Set at personalization	0x010B	0x0B	R	PACE + CA
DG12	Set at personalization	0x010C	0x0C	R	PACE + CA
DG13	Set at personalization	0x010D	0x0D	R	PACE + CA
DG14	ChipAuthentication public key	0x010E	0x0E	R	PACE
DG15	Set at personalization	0x010F	0x0F	R	PACE + CA
DG16	Set at personalization	0x0110	0x10	R	PACE + CA
SOD	Security Object	0x011D	0x1D	R	PACE + CA

Table 1: Data Groups of the Digital Identity Application

2.2.4. Data Structures

The structure of each elementary file content is defined in a separate specification document [DigitalIdentity].

2.2.5. Protocol support

2.2.5.1. User consent

The global PIN user credential is considered as the user consent.

2.2.5.1.1. User consent to access to the Digital Identity

The holder SHALL express his agreement for the physical use of the Digital Identity.

As such a successful PACE PIN authentication SHALL be performed prior to the selection of the Digital Identity Application.

2.2.5.1.2. User consent and operations

The table below indicates for each use case the user credential that is required to get access to the said service.

Operation	Type of data required	Mode of operation
User credential management (Change)	PUK	PACE
User credential management (Unblock)	PUK	PACE
User credential management (Resume)	CAN	PACE
Digital Identity DGs and Chip Authentication	PIN	PACE

2.2.6. Open Digital Identity Application

The opening procedure consists of the following steps:

1. **Read CardAccess** **(REQUIRED)**

The terminal SHOULD try to read CardAccess to determine the parameters (i.e. symmetric ciphers, key agreement algorithms, domain parameters, and mappings) supported by the chip. The terminal may select any of those parameters.

2. **PACE** **(REQUIRED)**

The chip SHALL accept the following password for PACE:

	MRZ	CAN	PIN	PUK
ePassport application	X	X	N/A	N/A
Digital Identity application	N/A	X	X	X

The PACE management is described in detail at section 3.2.1.1.

3. **Open Digital Identity Application** **(REQUIRED)**

The selection of the Digital Identity Application SHALL only be granted after successful PACE PIN.

4. **Chip Authentication Version 1** **(REQUIRED)**

The terminal SHALL read DG14 and perform Chip Authentication. The Digital Identity Application performs the following:

- It SHALL restart Secure Messaging.
- It SHALL grant access to less-sensitive data (see table 1).
- It SHALL restrict access rights to require Secure Messaging established by Chip Authentication.

Notes:

1) Chip authentication shall use chip authentication keys that are unique for each Digital Identity Application.
2) The chip authentication keys used for Digital Identity Application SHALL be different from the ones used by the ePassport Application.

5. **Passive Authentication (started)** **(REQUIRED)**

The terminal performs the following:

- It SHALL read and verify the Document Security Object.

- It SHALL verify DG14. If CardAccess was read, the terminal SHALL compare the unsecured SecurityInfos read from CardAccess to the secured contents of DG14.

6. Terminal Authentication Version 1 (CONDITIONAL)

This step is REQUIRED to access sensitive Digital Identity application data (DG3 and/or DG4). If successful, the Digital Identity application performs the following:

- It SHALL additionally grant access to data groups according the terminal's access rights.

7. Read and authenticate data

The terminal MAY read and verify the Digital Identity application data groups according to the terminal's access right.

2.3. References and Glossary

2.3.1. References

[TR-03110-1]	BSI Technical Guideline TR-03110 - Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token – Part 1 – eMRTDs with BAC/PACEv2 and EACv1 – v2.20
[TR-03110-2]	BSI Technical Guideline TR-03110 - Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token – Part 2: Protocols for electronic IDentification, Authentication and trust Services (eIDAS) - v2.21
[TR-03110-3]	BSI Technical Guideline TR-03110 - Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token – Part 3: Common Specifications - v2.21
[TR-03110-4]	BSI Technical Guideline TR-03110 - Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token – Part 4: Applications and Document Profiles - v2.21
[ICAO 9303]	ICAO doc 9303 Edition 7 – 2015
[DigitalIdentity]	National Personalization specification

2.3.2. Glossary

ASN.1	Abstract Syntax Notation One
CA	Chip authentication
CAN	Card Access Number
DG	Data Group
EAC	Extended Access Control
FID	File Identifier
MF	Master File
MRTD	Machine Readable Travel Document
OID	Object IDentifier
PACE	Password Authenticated Connection Establishment
PIN	Personal Identification Number
PUK	PIN Unblocking Key
RFU	Reserved for Future Use
SFI	Short File Identifier
SOD	Security Object Data
TA	Terminal Authentication

3. French National Identity Document Profile (ICAO, Digital Identity & Embedded Software)

3.1. Introduction

This Part specifies profiles of applications and profiles of documents compliant with the eIDAS regulation. It relies on the different schemes and algorithm specified in the TR-03110 part1,2 and 3. This specification supports two applications: ePassport and Digital Identity. Both applications are selectable in contact (ISO/IEC 7816) and contactless (ISO/IEC 14443).

3.2. Documents profiles

This section defines Document Profiles based on the Application Profiles from the preceding section.

3.2.1. eID Card

3.2.1.1. Passwords

This Document Profile requires support for the following Passwords:

•MRZ (see TR-03110-1) **(REQUIRED)**

•CAN (see TR-03110-1) **(REQUIRED)**

•PIN (see TR-03110-2 §2.2.1) **(REQUIRED)**

The Personal Identification Number (PIN) is a blocking secret password of 6 digits ASCII that SHALL be only known to the legitimate holder of the document. The PIN is associated with a retry counter sets at 3 (RC) that is decreased for every failed authentication (see Part 2 §2.2.3)

•PUK (see TR-03110-2 §2.2.2) **(REQUIRED)**

The PIN Unblock Key (PUK) is a blocking secret password of 12 digits in ASCII that SHALL be only known to the legitimate holder of the document. The PUK is associated with a retry counter sets at 5 (RC) that is decreased for every failed authentication (see TR-03110-2§2.2.3).
Password Verification and user consent SHALL be based on PACE:

- PACE MRZ is used to only access the ePassport application.
- PACE CAN is used to access the ePassport application or to resume the PIN or PUK required with Digital Identity application
- PACE PIN is used to only access the Digital Identity application.
- PACE PUK is used to unblock or to change the PIN

The PIN is the only password that may be changed.

The passwords (CAN and MRZ) are static and non-blocking.

The password (PUK) is static and blocking.

The password (PIN) MAY be changed and is blocking.

The passwords (PIN and PUK) SHALL support the state suspended via contact and contactless interfaces.

3.2.2. Authentication Procedure

This Document Profile requires implementation of the following Authentication Procedure.

•Advanced Inspection Procedure ONLY (see TR-03110-1§2.4.3) **(REQUIRED)** *To select ePassport application and Digital Identity application*

The optional step 4, Active Authentication is not requested.

3.2.3. Applications

This Document Profile requires implementation of the following Applications:

•ePassport Application **(REQUIRED)**

•Digital Identity Application **(REQUIRED)**

3.2.4. Protocols

This Document Profile requires implementation of the following Protocols:

• PACE (see TR-03110-2) **(REQUIRED)**

• Terminal Authentication Version 1 (see TR-03110-1) **(REQUIRED)**

• Chip Authentication Version 1 (see TR03110-1) **(REQUIRED)**

• Passive Authentication (see TR03110-1) **(REQUIRED)**

3.2.5. Javacard Open Platform

The document shall be made up with a javacard open platform meeting the requirements listed in the following chapters.

3.2.5.1. Compliance

The javacard open platform shall comply at least with the following standards:

- Javacard v3.0.4 – Classic edition;
- Global Platform v2.2.1

3.2.5.2. Data Authentication Pattern (DAP)

The Data Authentication Pattern (DAP) mechanism shall support both algorithms:

- PKCS#1 v2.1 PSS 2048 bits
- AES 128 bits

3.2.5.3. Secure Channel Protocol

The secure channel protocol SCP03 as defined in "-Amendment D, Secure Channel Protocol 03"SHALL be supported at least. The following configuration SHALL be used:

- "Random Card Challenge" ("i" ='00')

Furthermore, after issuance to the final holder, the document SHALL enforce the following security level (AUTHENTICATED | C_MAC | C_DECRYPTION).

3.2.5.4. Security requirements

The underlying javacard platform SHALL be certified at least at level EAL5+AVA_VAN.5+ALC_DVS.2 according to common criteria with one of the following protection profile: PP « Java Card System Open Configuration » referenced under PP-2010/03, ormore recent.

4. Certification and Qualification requirements:

items	Certification	Qualification
Chip	BSI-CC-PP 0084 – EAL5+	Reinforced Qualification from the French ANSSI[4]
Embedded Software	ANSSI-CC-PP-2010/03 – EAL5+ or more recent	
ICAO Application	BSI-CC PP 068 - EAL 5+ (PACE) BSI-CC PP 056V2 – EAL 5+ (EACv1 with PACE)	
Digital Identity Application	BSI-CC PP 068 - EAL 5+ (PACE) BSI-CC PP 056V2 – EAL 5+ (EACv1 with PACE)	

5. Functional Conformity

5.1. Embedded Software

The Embedded Software SHALL be functionally tested by using the Global Platform compliance testing suite

5.2. ICAO Compliant application

The ICAO Compliant application SHALL be functionality tested against the ICAO testing plan (ISO/IEC 18745-2). The defined tests are focus radio frequency and therefore not limited to the operating system (OS) alone but to a complete physical smartcard including chip, OS and the antennas.

5.3. Digital Identity

A testing plan is currently under preparation by the French ANTS agency, these conformity specifications will be finalized after the results of this public consultation.

4 More information on the ANSSI Reinforce qualification is available at https://www.ssi.gouv.fr/en/security-visa/

6. Supported Algorithms

6.1. PACE

	Algorithms	Domain parameters
Minimum implementation	id-PACE-ECDH-GM-AES-CBC-CMAC-256	BrainpoolP256r1
Preferred complementary implementation	id-PACE-ECDH-IM-AES-CBC-CMAC-256	BrainpoolP256r1
Allowed complementary implementation	id-PACE-DH-GM-AES-CBC-CMAC-256	2048-bit MODP Group with 256-bit Prime Order Subgroup

6.2. Chip Authentication

	Algorithms	Domain parameters
Minimum implementation	id-CA-ECDH-AES-CBC-CMAC-256	BrainpoolP256r1
Allowed complementary implementation	id-CA-DH-AES-CBC-CMAC-256	2048-bit MODP Group with 256-bit Prime Order Subgroup

6.3. Terminal Authentication

	Algorithms	Domain parameters
Minimum implementation	id-TA-ECDSA-SHA-256	BrainpoolP256r1
Allowed complementary implementation	id-TA-RSA-PSS-SHA-256	RSA 3K

6.4. Embedded Software

Data Authentication Pattern (DAP)	PKCS#1 v2.1 PSS 2048 bits **AND** AES 128 bits
SCP	SCP03 with “Random Card Challenge” (i = '00')

6.5. Note on cryptographic algorithms and key length

The above algorithms and key length shall be used according to this document only for Digital Identity application and shall be compliant with the French RGS appendix B1.