FRANCE IDENTITE

SERVICE DE GARANTIE DE L'IDENTITÉ NUMÉRIQUE

NOVEMBER 16TH 2022, RENNES

Table of contents

1 – Introducing France Identité

Ensuring Trust in a Decentralized World

It has been the **role of the French State** for decades, through the **provisionning of identity documents**:

1. The State endorses the identity and emits the corresponding identity document to its legitimate holder;

2. The holder owns it and « stores » it;

3. He or she can freely reuse it in his/her daily life;

4. The State holds records indicating if the document if still valid or has been revoked.

How to provide the same service and trust in a digital environment ?

France Identité : a new public service and eID means

We aim to create **the root of trust** for a digital identity and wallet **user-friendly, secure,** performant et sovereign,

for French citizens and foreign residents, in partnership with them and with the service providers,

in order to prolong identity in the digital world, present identity related attributes and prove ownership of those attributes to third parties, either online (over the internet), et offline (physical presentation).

We promote and ensure a user-centric approach

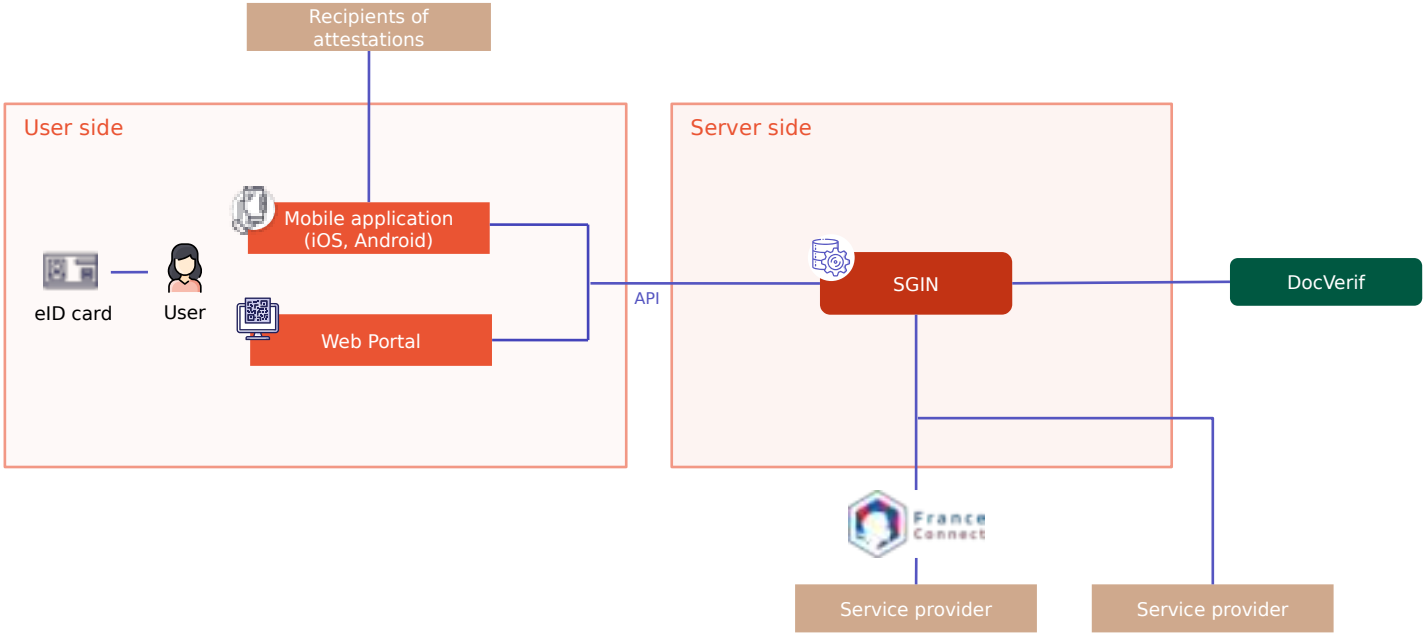
The electronic ID card at the core of the digital identity

The model is kept unchanged but extended to digital uses

In practice:

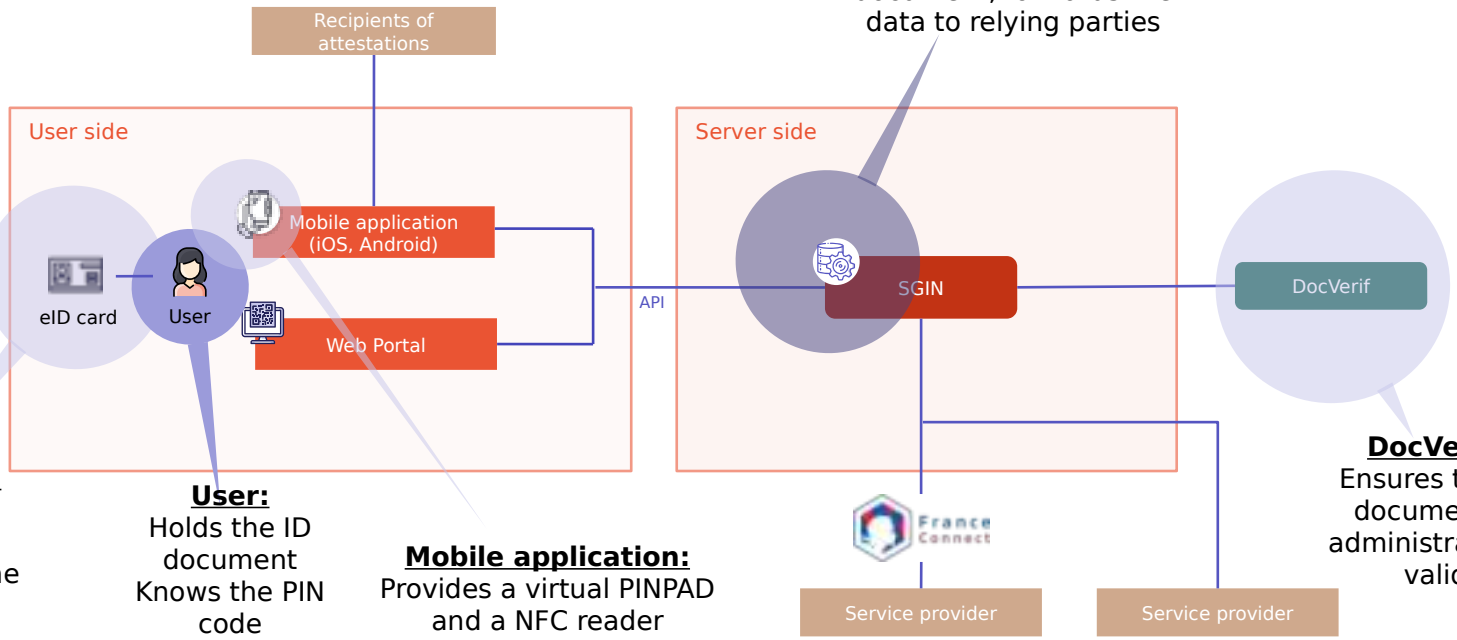
- The **ID card holds the data** and its user can present it to third parties, in digital format
- The **ID card authenticates the user** (proves its ownership over the ID document), **physically and remotely** (over the internet), using digital means (a PIN code, the digital photograph stored in the ID document)
- The **ID card implements security mechanisms** providing protection and trust, both physically and digitally

Global architecture of the service



Global architecture of the service

Backend server (SGIN):
Reads an verifies the authenticity of the ID document, forwards the data to relying parties



ID document :
Factor of possession and mean to verify the user's PIN code

User:
Holds the ID document
Knows the PIN code

Mobile application:
Provides a virtual PINPAD and a NFC reader
Secures connections to the backend

DocVerif:
Ensures the ID document is administratively valid

2 – Focus on the new French eID card

The French eID card (1/3)

There has been no evolution of the French ID card since 1995. **After several abandoned projects (2008, 2012), France complies with the European directive 2019/1157 that requires all Member States to deploy an electronic ID card.**

CNIe

CEV (visible digital seal)
- 2DDOC format (signed data)
- Alphanumerical data only

Addresses
- Main address
- Secondary address (for children in separated couples)

Transparent and secure edge

DOVID
Holographic mechanism

MLI
Visual security

OACI/ICAO
Norm 9303

MRZ
- Type of ID
- Nationality
- ID Card number
- Birth date
- Expiration date
- Names

The French eID card (2/3)

The PACE + PIN approach relies on **a distinct second dedicated application that stores the digital identity data**, in addition to the ICAO application required by the European legislation.

CNIe

FRONT

BACK

Travel application (ICAO)

- Alphanumerical data: identity
- Biometric data: photo, fingerprints
- Access management: MRZ or CAN

Digital ID application (eID)

- Alphanumerical data, minimized
- No biometric data
- Access management: user's PIN

CAN (Card Access Number)

The CAN gives access to the content of the chip without scanning the MRZ:

- Allows access to the ICAO data
- Allows the last PIN entry to eID app

MRZ

Machine-readable zone

The French eID card (3/3)

Physical interfaces, security requirements, specifications and personalization.

Contact and **contactless** interfaces

Chip **Qualified by ANSSI** (reenforced level)

Security certification :
BSI-CC PP 068 - EAL 5+ (PACE) + addendum on PIN (V11)

BSI-CC PP 056V2 – EAL 5+ (EACv1 with PACE)

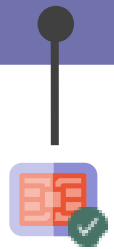
eID application based on othe TR Electronic National Identity Card Technical Specifications V32

User authentication : the PACE + PIN approach to access the eID application

Card reading (eID application)

VERIFYING USER'S CONSENT : PIN CODE ENTRY

- Verifying user's **knowledge** of the PIN code
- Verifying user's **consent** to give access to their ID data.



VERIFYING THE AUTHENTICITY OF THE CHIP : CHIP AUTHENTICATION

- Checking that the chip is **authentic** : it is not a clone, it has been personalized by the French State.

READ PERMISSION FOR THE ID DATA STORED IN THE EID APPLICATION

VERIFYING THE INTEGRITY OF THE DATA : PASSIVE AUTHENTICATION

- Checking the hash and **digital signature** of the ID data, signed by the French State

Authentic chip

User authentication : the PACE + PIN approach

Card reading (eID application)

VERIFYING USER'S CONSENT : PIN CODE ENTRY

VERIFYING THE AUTHENTICITY OF THE CHIP : CHIP AUTHENTICATION

READ PERMISSION FOR THE ID DATA STORED IN THE EID APPLICATION

VERIFYING THE INTEGRITY OF THE DATA : PASSIVE AUTHENTICATION

Authentic chip

Mobile application

Backend server

To sum up : key functions of the eID card

AUTHENTIC SOURCE OF IDENTIFICATION DATA

Each eID card has been personalized with identity data, endorsed by the French State

- **Removes the need for a centralized database** for the digital identity, each holder can present trustworthy identification data
- **Checking the hash and digital signature** of the identification data by the French State **proves the integrity and authenticity of the data**

VERIFY THE USER'S IDENTITY AND CONSENT

Access to the eID application in the eID card is **conditioned by the knowledge of a PIN code**

- Through this PIN code, **the user has sole control** over his or her ID card
- Protects the identification data and **allows the holder's authentication** on remote services
- **PIN trials are limited** by the card using a retry counter, providing security with a PIN code of low entropy

POSSESSION FACTOR

When the eID card is personalized, its identification data is bound to its chip

- A **public key** is part of the data **signed by the French State**
- The corresponding **private key cannot be extracted** from the chip
- The combination of the two **allows the reader to ensure that it is interacting with the authentic ID document**, preventing any cloning attempt.

PIN verification and user consent

The data stored in the eID application is **accessible once the user's PIN code is entered**.

The PIN entry allows to

- **Verify that the user knows the PIN** code
- **Confirm the consent** of the user to the reading of the identification data stored in the eID application
- Access and read the public key (DG14) which will later to used to **verify the authenticity of the chip**
- The **PACE+PIN** (Password Authenticated Channel Establishment) is opened **between the mobile device and the ID card**

Data stored in the eID application of the ID card:

	Eléments de données
DG1	Type of document, issuing country, nationality
...	
DG12	Issuing date
DG13	Identity data, hash of the document number
DG14	Chip Authentication public key
	Security object document (SOD)

Access conditioned by Chip Authentication

Access conditioned by PACE+PIN

3 – The mobile application

The role of the mobile application

The **mobile application provides the user with all the necessary interfaces** to interact with his or her digital identity, while securing the exchanges between the user, the ID card and the backend server.

PROVIDE A SECURE VIRTUAL PINPAD

- Allows the user to enter its ID document's PIN code in order to consent and authenticate
- Protects the PIN code entry against eavesdropping

SECURE COMMUNICATIONS WITH THE BACKEND

- Provides protection in integrity, authenticity and confidentiality for the communication exchanges between the mobile application, the backend server and the ID card

ENABLE THE BACKEND TO INTERACT WITH THE CARD

- While the PACE channel establishment is handled by the mobile device, the Chip Authentication channel is build between the ID card and the backend server: the mobile application acts
  - as an APDU proxy
  - as an NFC reader

ALLOW THE USER TO INTERACT WITH THE SERVICE

- Enroll, provide contact information, revoke or delete the digital identity
- Handle the life cycle of the digital identity, in particular the ID card's PIN code
- Provide clear information about the required user actions
- Let the user consent to using his or her digital identity and identification data

User interactions with France Identité

ENROLMENT

When creating his or her digital identity, the **user enrolls with France Identité**

- **Contact information is provided** (email address) for OTPs and communication needs
- **The docnumber of the user is registered,** alongside with its status (blocked, valid, revoked etc.)

DAILY USE

Once enrolled and with a valid digital identity, **the user can use it** to generate electronic attestations and authenticate online and offline

- **Electronic attestations replace scans of ID documents** with a PDF document, electronically signed
- **Online authentication** relies on the presentation of the ID card and its associated PIN code
- **Offline authentication** will be provided in 2023

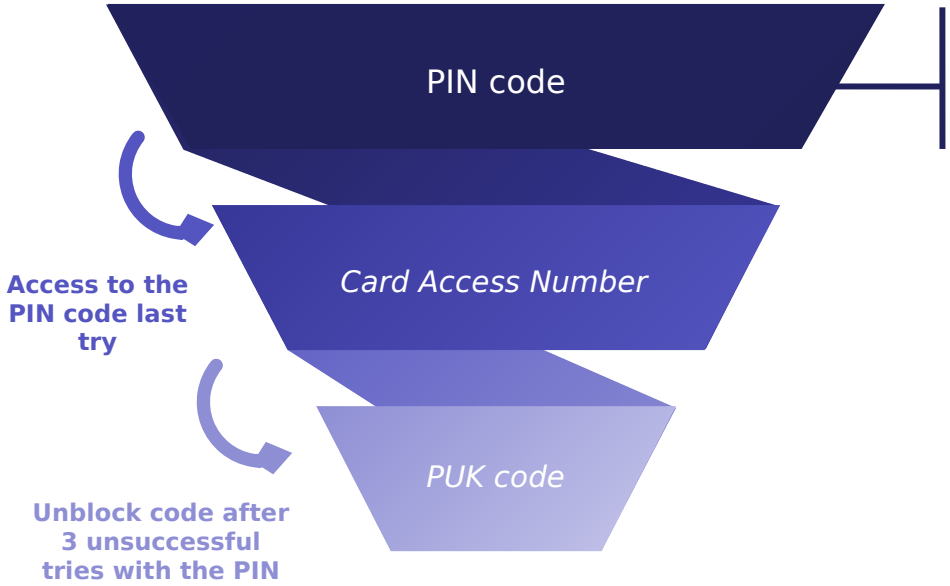
DIGITAL IDENTITY LIFE CYCLE MANAGEMENT

The digital identity is optional and **under the control of the user**, who can at any given time

- **Unblock the PIN code of the ID card** (requires an identity proofing)
- **Change the PIN code** of the ID card
- **Change the contact information**
- **Revoke or delete** his or her digital identity

Digital identity life-cycle management

PIN code
- ✓ Personalized on the ID card
- ✓ Modifiable

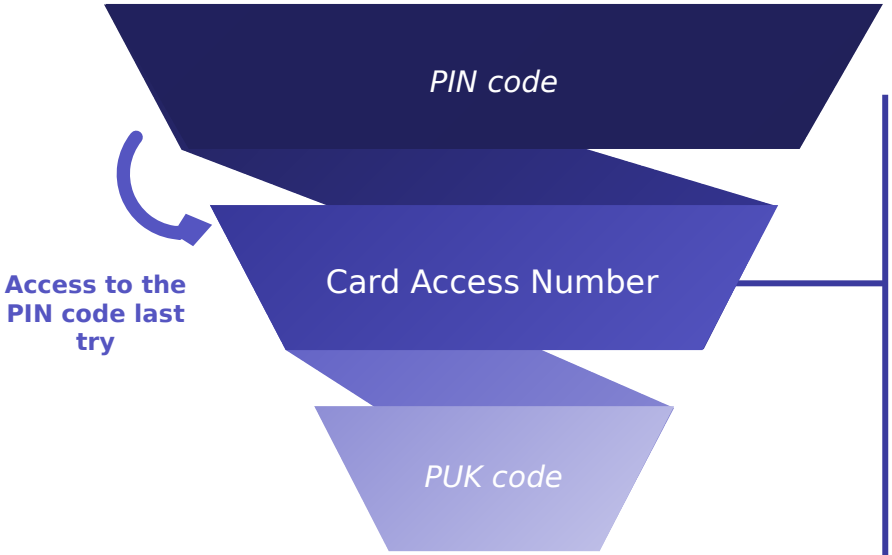


The **PIN code authenticates the user** and **materializes his or her consent** to provide the identification data.

Digital identity life-cycle management

CAN

- ✓ Protects the last try of the PIN code
- ✓ Random code, printed on the card, non-modifiable



The last try (third try) of the PIN code is **protected by the entry of the CAN** (6 figures printed on the ID card), followed by the PIN code, in order to ensure that the reader has physical access to the ID card (to read the CAN on it).

It covers the case when a malicious user would try several PIN codes via the contactless inferface to lock the ID card (sort of denial of service).

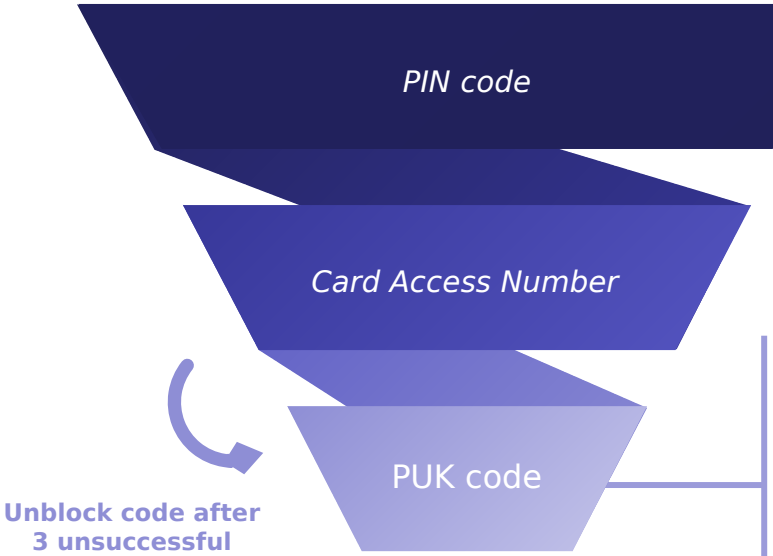
Imposing the entry of the CAN prior to the entry of the PIN guarantees that the user physically holds the ID card.

N.B. The CAN is also a mean to access the travel application of the eID card, without having to read the MRZ.

Digital identity life-cycle management

PUK code

✓ Unblock code personalized on the card



The PUK code is **an unblock code personalized** for the eID card. It the number of PIN code tries falls to 0, **the PUK code must to use to reset the PIN code and the retry counter.**

For interoperability reasons, it is also used when the user wants to change the PIN code of the eID card, even it the card is not blocked.

4 – The backend server

The role of the backend server

The backend server acts as a **trusted party** which issues digital identities, verifies their authenticities, and forwards the authentication to third parties.

READ AND VERIFY INTEGRITY, AUTHENTICITY AND VALIDITY OF THE CARD

- The backend server is responsible for **reading the data in the card, and verifying the authenticity** of the data and the card
- It also **ensures that the ID document is valid** (for instance, has not been declared lost or stolen)

KEEPS TRACK OF STATUSES, IN PARTICULAR REVOCATION

- The digital identity is under the control of the user: the user can **revoke it or delete it** at any given time
- Depending on the security level of the identity proofing process which lead to unblocking the ID card, the **eID means may have different levels of trust, which the backend keeps track off**

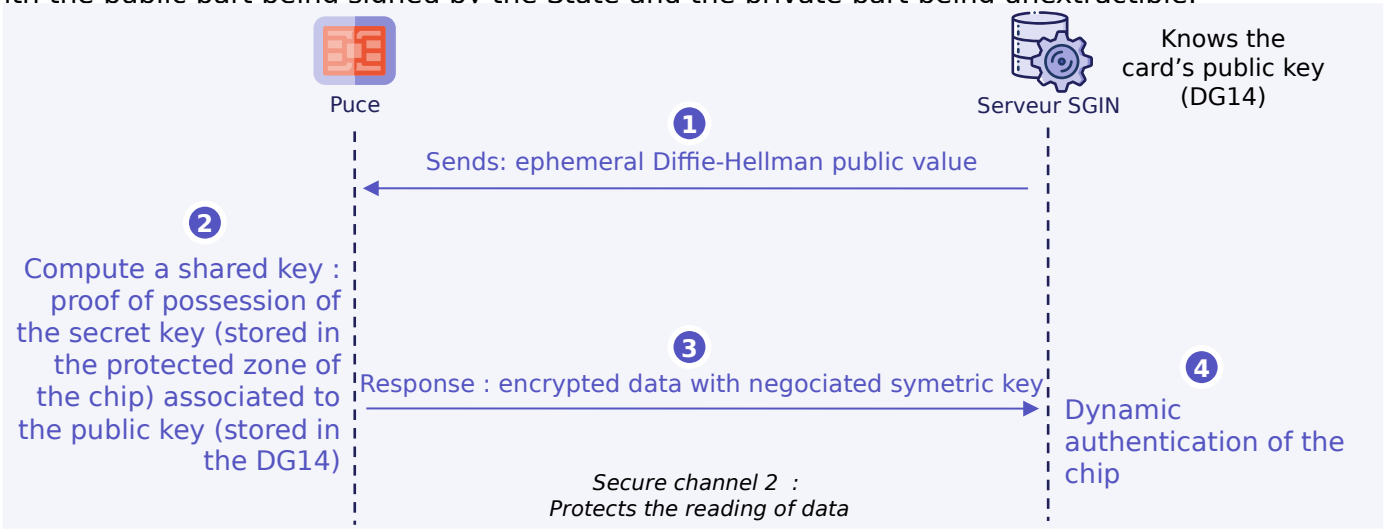
FORWARDS DATA TO RELYING PARTIES

- The backend server offers an **OpenID Connect interface** to relying parties
- After the user authentication using his or her ID card, the identity data is forwarded by the backend to the relying party
- It acts as **a trusted intermediary**

The Chip Authentication mechanism

The dynamic authentication mechanism of the chip allows for verification of the chip's authenticity, which means it is not a clone and the data it stores has been personalized by a State. **It guarantees the binding between the chip and the data it stores**.
This mechanism uses a static-ephemeral Diffie-Hellman key exchange, where the static public and private parts are on the chip's side, with the public part being signed by the State and the private part being unextractible.

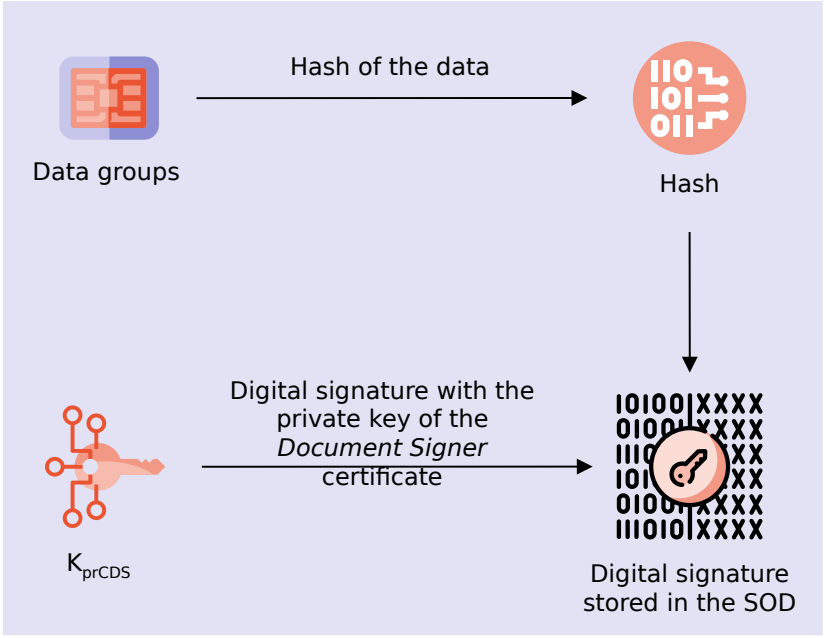
Prerequisite: the PIN entry grants access to the DG14



Once this process has gone through, all DGs in the eID application are readable

The Passive authentication mechanism

The chip's memory is **structured in datagroups (DG).** Each data group used is **hashed and then digitally signed** using the process indicated bellow. The result is stored in the Security Object Document (SOD).



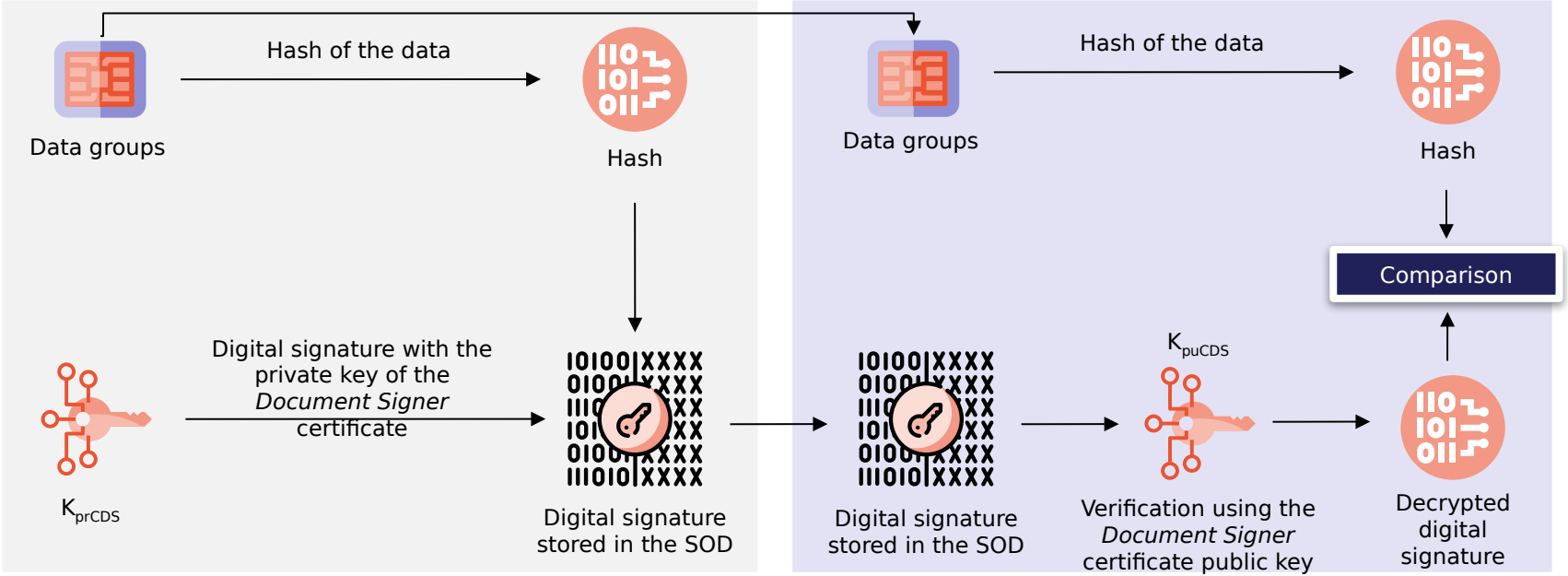
Data stored in the eID application of the ID card:

	Eléments de données
DG1	Type of document, issuing country, nationality
...	
DG1 2	Issuing date
DG1 3	Identity data, hash of the document number
DG1 4	Chip Authentication public key

Security object document (SOD)

The Passive authentication mechanism

The reader controls the **authenticity of the data groups** stored in the chip's memory. It verifies that the electronic signature is correct. The goal of the « Passive Authentication » is to ensure that the signed data in the SOD were **signed by a State certification authority**.



5 – Next steps

Extend the decentralized identity sources

In the current model, **everything relies on the eID card**: identification data and 2FA. The next steps consist of **integrating other electronic identity documents**, and **create new autonomous eID means**.

eID card

- Stores the identification data
- Provides the possession factor
- Verifies the PIN code

Passports

- Stores the identification data
- Provides a possession factor
- Requires a second factor, built in the application:
  - Local use of the mobile phone's biometry
  - User secret verified by the mobile device and/or the backend

Issuing "derived identities" in smartphones

Using the trusted identification of the eID card, **provision the user's smartphone** with:

- **The identification data**
- **Private keys** binding this data to the device (possession factor)
- **User control** over the data (local biometry / user secret)

Challenges:

- Provide better user experience
- While preserving security

Thank you !