


**CSPN Security Target  
INWallet Mobile Middleware  
iOS version 1.1  
Android version 2.1.3**

Document identification	
Program reference	/IDNUM/INWALLET/CNIe
Date of creation	30/10/2020
Last update date	23/09/2021
Status	Release
Version	1.6
Classification	 <b>Public document</b> Property of IN Groupe - Reproduction and disclosure subject to IN Groupe's agreement
Number of page	20

**Version history:**

Version	Date	Autor	Nature of the revision Modified paragraphs
0.1	10/2020	Red Alert Labs	Document creation
1.0	19/11/2020	IN Groupe & Red Alert Labs	Release version 1.0
1.1	07/12/2020	Red Alert Labs	Adjustment of the content of the security target following latest internal feedback related to the scope of evaluation.
1.2	12/01/2021	Red Alert Labs	Adjustment of the content of the security target following latest internal feedback related to the scope of evaluation.
1.3	27/01/2021	Red Alert Labs	Adjustment of the content of the security target following latest internal feedback related to the scope of evaluation.
1.4	24/03/2021	IN Groupe	Adjustment of the document title.
1.5	30/03/2021	IN Groupe	Adjustment of the content of the specifications following latest external feedback.
1.6	23/09/2021	IN Groupe	Adjustment of the application version numbers

## Table of contents

<b>I.</b>	<b>INTRODUCTION.....</b>	<b>3</b>
I.1.	DOCUMENT PURPOSE.....	3
I.2.	PRODUCT IDENTIFICATION.....	3
I.3.	REFERENCE DOCUMENTS.....	3
I.4.	GLOSSARY.....	4
I.5.	DEFINITIONS.....	5
<b>II.</b>	<b>PRODUCT DESCRIPTION.....</b>	<b>6</b>
II.1.	GENERAL DESCRIPTION.....	6
II.2.	PRODUCT USAGE.....	7
II.3.	DEPENDENCIES DESCRIPTION.....	9
II.4.	DESCRIPTION OF THE EXECUTION ENVIRONMENT.....	9
	II.4.1. Compatible or Dedicated Hardware.....	9
	II.4.2. Operating System Precision.....	10
II.5.	PRODUCT EVALUATION PERIMETER.....	10
<b>III.</b>	<b>SECURITY ELEMENTS.....</b>	<b>12</b>
III.1.	TYPICAL USERS DESCRIPTION.....	12
III.2.	SENSITIVE ASSETS.....	13
III.3.	ENVIRONMENT ASSUMPTIONS.....	15
III.4.	THREATS DESCRIPTION.....	17
III.5.	SECURITY FUNCTIONS DESCRIPTION.....	19
III.6.	COVERAGE MATRIX.....	20

## I. Introduction

### I.1. DOCUMENT PURPOSE

This document is produced as part of an assessment according to the CSPN methodology of ANSSI on the product INWallet Mobile Middleware.

The document is structured following the description of section 4.2 of the [ANSSI\_CSPN\_CER\_P\_02] referential. For the sake of organization, some part of the structure were amended in a way to be adapted to the product's scope and functioning.

### I.2. PRODUCT IDENTIFICATION

Editor	IN Groupe
Editor's Website	<a href="https://www.ingroupe.com/">https://www.ingroupe.com/</a>
Commercial name of the product	<b>INWallet Mobile Middleware</b>
Versions for evaluation	Product shall be evaluated at least for the following versions: <ul style="list-style-type: none"> <li>• Android: Version 6.0 and upper with Middleware Version 2.1.3</li> <li>• iOS: Version 13 and upper with Middleware Version 1.1</li> </ul>
Product Category	Identification, authentication, and access control.

### I.3. REFERENCE DOCUMENTS

Reference	Document Name
[ANSSI_CSPN_CER_P_02]	CRITERES POUR L'EVALUATION EN VUE D'UNE CERTIFICATION DESECURITE DE PREMIER NIVEAU <a href="https://www.ssi.gouv.fr/uploads/2015/01/anssi-cspn-cer-p-02-criteres_pour_evaluation_en_vue_d_une_cspn_v4.0.pdf">https://www.ssi.gouv.fr/uploads/2015/01/anssi-cspn-cer-p-02-criteres_pour_evaluation_en_vue_d_une_cspn_v4.0.pdf</a> Version: 4.0
[CNle_SPEC]	Electronic National Identity Card – Technical Specifications Version: A031
[BSI_TR_03110]	Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token <ul style="list-style-type: none"> <li>-1. Part 1 – eMRTDs with BAC/PACEv2 and EACv1 Version: 2.20</li> <li>-2. Part 2 – Authentication and trust Services (eIDAS) Version: 2.21</li> <li>-3. Part 3 – Common Specifications Version: 2.21</li> <li>-4. Part 4 – Applications and Document Profiles Version: 2.21</li> </ul>

Reference	Document Name
[ICAO_9303]	ICAO 9303 : ICAO doc 9303 Edition 7 - 2015
[DigitalIdentity]	Electronic National Identity Card – Digital Identity Application Logical Data Structure (LDS) Version: L005
[A_PP0056]	Module: Annexe PP0056v2 eDigitalIdentity document using Remote Access Control with PACE v2
[RGS_B1]	GUIDE DES MÉCANISMES CRYPTOGRAPHIQUES (ex RGS Annexe B1) Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques. <a href="https://www.ssi.gouv.fr/uploads/2021/03/anssi-guide-mecanismes_crypto-2.04.pdf">https://www.ssi.gouv.fr/uploads/2021/03/anssi-guide-mecanismes_crypto-2.04.pdf</a> Version: 2.04
[RGS_B2]	Référentiel Général de Sécurité, Annexe B2 Règles et recommandations concernant la gestion des clés utilisées dans les mécanismes cryptographiques. <a href="https://www.ssi.gouv.fr/uploads/2014/11/RGS_v-2-0_B2.pdf">https://www.ssi.gouv.fr/uploads/2014/11/RGS_v-2-0_B2.pdf</a> Version: 2.0
[RGS_B3]	Référentiel Général de Sécurité, Annexe B3 Règles et recommandations concernant les mécanismes d'authentification <a href="https://www.ssi.gouv.fr/uploads/2015/01/RGS_B_3.pdf">https://www.ssi.gouv.fr/uploads/2015/01/RGS_B_3.pdf</a> Version: 1.0
[ANSSI_RSR_TLS]	Recommandations de sécurité relatives à TLS. <a href="https://www.ssi.gouv.fr/uploads/2017/07/anssi-guide-recommandations_de_securite_relatives_a_tls-v1.2.pdf">https://www.ssi.gouv.fr/uploads/2017/07/anssi-guide-recommandations_de_securite_relatives_a_tls-v1.2.pdf</a> Version: 1.2
[ANSSI_HSM]	Décision de qualification d'un produit – N° 905/ANSSI/SDE HSM TrustWay Proteccio

#### I.4. GLOSSARY

ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
APDU	Application Protocol Data Unit
CA	Chip Authentication
CNle	Carte Nationale d'Identité électronique
CSPN	Certification de Sécurité de Premier Niveau
CSCA	Country Signature Certification Authority
HSM	Hardware Security Module
NFC	Near Field Contact
PACE	Password Authenticated Connection Establishment
SM	Secure Messaging
SOD	Security Object Data

## I.5. DEFINITIONS

### TLS Pinning

Certificate pinning is the process of associating a host with their expected X.509 certificate or public key. Once a certificate or public key is known or seen for a host, the certificate or its issuing CA certificate, is associated or 'pinned' to the host. Pinning leverages knowledge of the pre-existing relationship between the user and an organization or service to help make better security related decisions. Because the application already has information on the server or service, it does not need to rely on generalized mechanisms meant to solve the key distribution problem. That is, it does not need to turn to DNS for name/address mappings or trusted CAs for bindings and status.

## II. Product Description

### II.1. GENERAL DESCRIPTION

The INWallet Mobile Middleware solution is designed to enable customers to develop applications with the capacity and authority to read identity data located on the CNle (The French National Electronic Identity Card) and to verify it by querying a database.

The Smartphone hosting the application, will communicate with the CNle of the user through NFC (Near Field Contact) Technology. The NFC allows data exchange between two object in contact (with a maximum distance of 3cm). Moreover, with the choice of NFC, the CNle won't be relying on any battery knowing that the chip will be powered with magnetic field generated by the reader (the Smartphone).

The solution is a middleware partly composed of librairies and a set of programming assistance tools to design mobile applications for a specific terminal and / or an Operating System. In order to operate, the middleware need to be used inside a mobile application that communicates with a mobile backend server at least composed of a client server.

The solution also includes a middleware backend communicating with the device hosting the application. The middleware backend include a middleware server which manage communication and data processing and a HSM which provide random data.

Both backends, the one of the middleware and the one of the mobile application communicate with each other.

The Figure 1 below illustrates the global architecture of the environment necessary to the functioning of the solution.

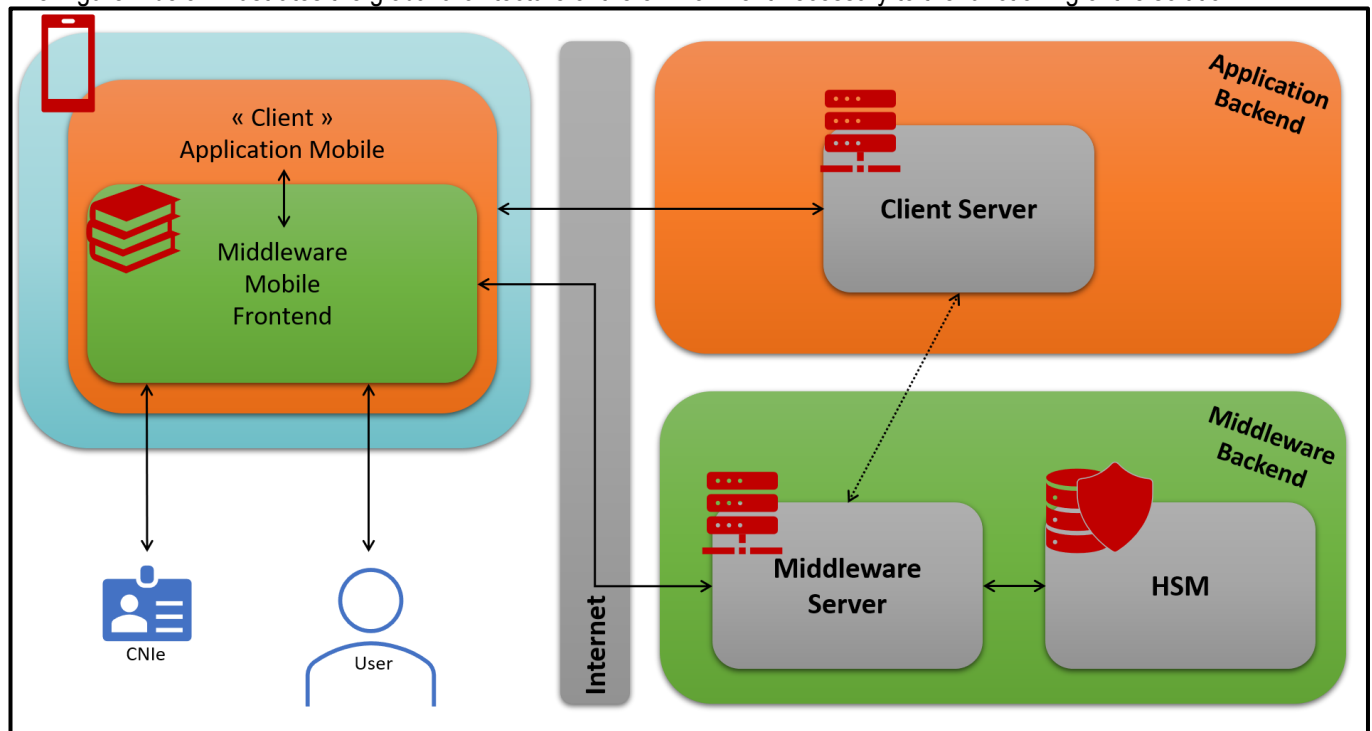


Figure 1 – Global Architecture

## II.2. PRODUCT USAGE

Each time the National Electronic Identity Card (CNle) is used to identify and authenticate its holder, the sequence of actions presented in Figure 2 below is carried out.

This process is summarized through the different steps described below :

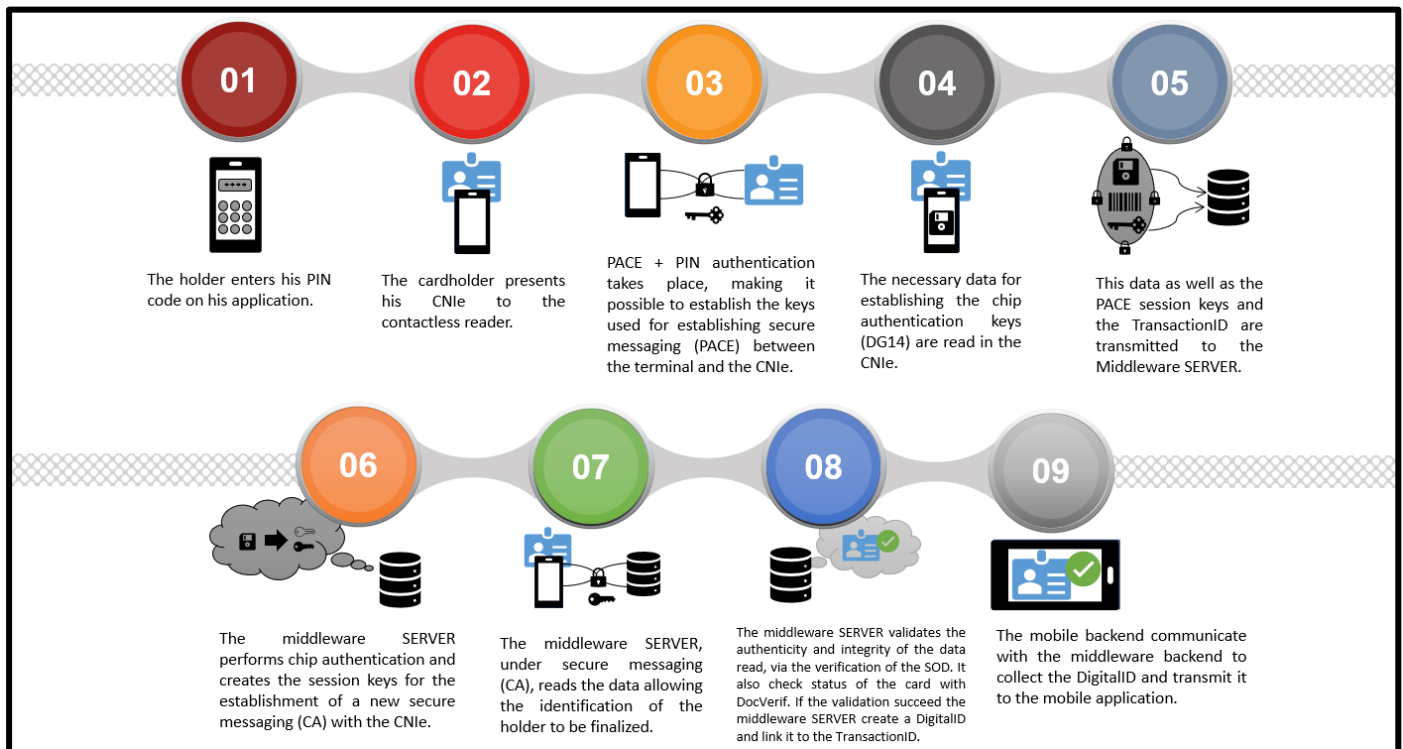


Figure 2 – Usage process of INWallet Mobile Middleware

0. The holder access the mobile application with a code. The mobile application communicate with its associated backend to launch the process.
1. The holder enters his PIN code (this code is the one linked to the CNle) through his mobile application. The virtual keyboard is provided by the middleware.
2. The cardholder presents his CNle to the contactless reader.
3. The PACE + PIN authentication takes place, making it possible to determine the keys used for establishing secure messaging (SM PACE) between the terminal and the CNle.
4. The necessary data for establishing the chip authentication keys (DG14) are read from the CNle.
5. This data as well as the PACE session keys and the TransactionID are transmitted to the Middleware SERVER. These data are sent through TLS protocol and encrypted with an AES-128 key. The middleware backend server and the middleware frontend are the only ones capable of using this key and therefore to decrypt these data. This step allows the authentication of the middleware front-end to the middleware backend.

6. The Middleware SERVER performs a chip authentication and creates the session keys used for the establishment of a new secure messaging (SM CA) with the CNle.
7. The Middleware SERVER, under secure messaging (SM CA), reads the data allowing the identification of the holder to be finalized (DG1, DG13, SOD).
8. The Middleware SERVER validates the authenticity and integrity of the data read, via the verification of the SOD (Security Object Data). If the validation succeed the middleware SERVER create a DigitalID and link it to the TransactionID.
9. The mobile backend communicate with the middleware backend to collect the DigitalID and transmit it to the mobile application.

### Precisions & Remarks

*PACE is a password authenticated Diffie-Hellman key agreement protocol that provides secure communication and password-based authentication of the chip and the inspection system (i.e. chip and inspection system share the same password  $\pi$ ). PACE establishes Secure Messaging between a chip and an inspection system based on weak (short) passwords. The protocol enables the chip to verify that the inspection system is authorized to access stored data. The protocol produced securely an encryption key (ENC\_PACE\_KEY) and a hashing key (HASH\_PACE\_KEY).*

*The Chip Authentication Protocol is an ephemeral-static Diffie-Hellman key agreement protocol that provides secure communication and unilateral authentication of the chip. The protocol provides implicit authentication of both the chip itself and the stored data by performing Secure Messaging using the new session keys. This protocol also produced securely an encryption key (ENC\_CA\_KEY) and a hashing key (HASH\_CA\_KEY).*

*More information and details could be found in the following specifications : [\[CNle\\_SPEC\]](#) and [\[BSI\\_TR\\_03110\]](#).*

*The INWALLET MOBILE MIDDLEWARE solution support only mandatory algorithms specified in the [\[CNle\\_SPEC\]](#).*



All the communications are briefly summarized in the Figure 3 below:

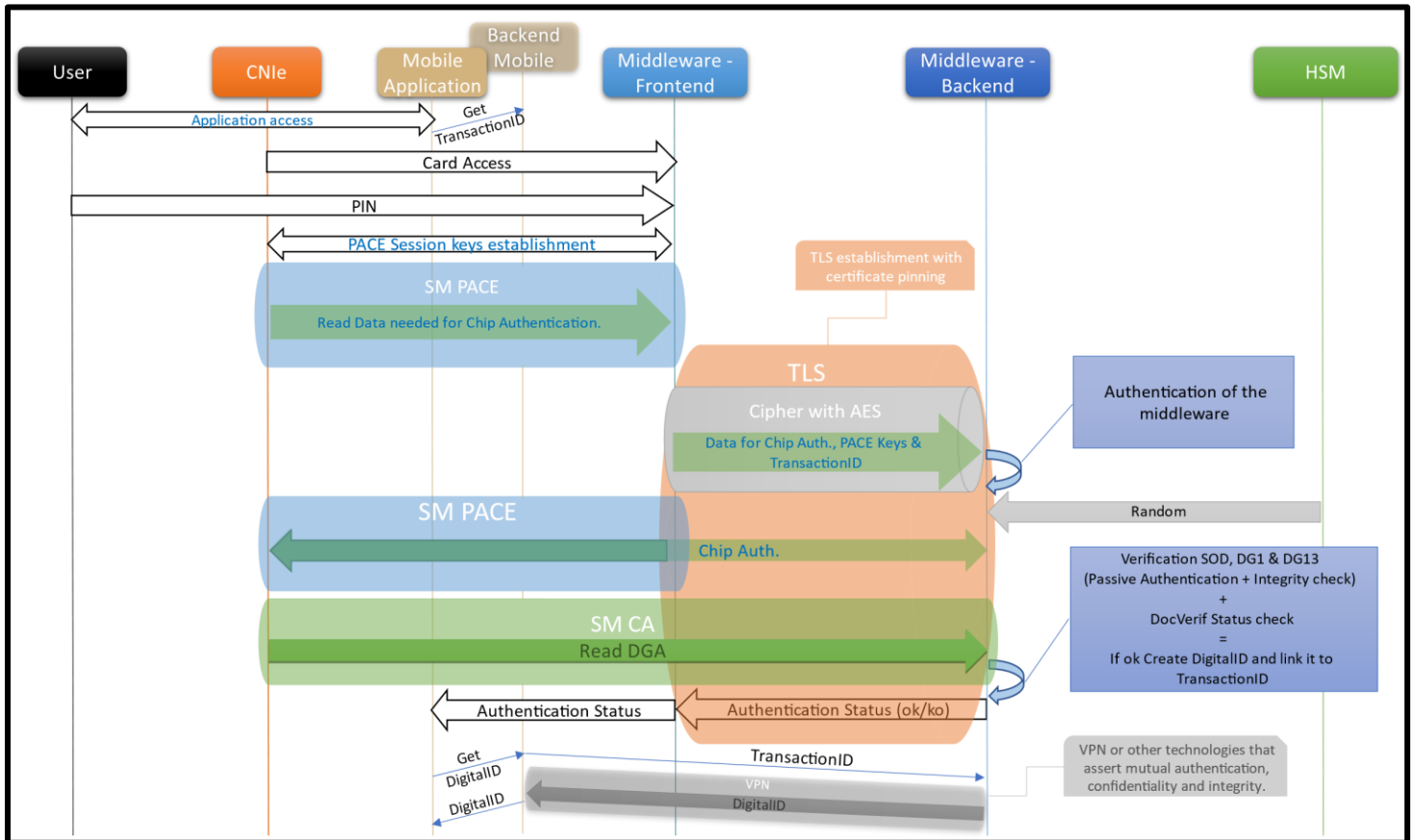


Figure 3 - Exchanges overview

### II.3. DEPENDENCIES DESCRIPTION

A mobile with IP networking is needed to use the solution. The middleware must also be invoked by a mobile application in order to run. Depending on the mobile operating system that is used for the application execution, at least Android version 6.0 or iOS version 13 are required for the INWallet Mobile Middleware to run.

### II.4. DESCRIPTION OF THE EXECUTION ENVIRONMENT

#### II.4.1. COMPATIBLE OR DEDICATED HARDWARE

The middleware is designed to be used by a mobile application running on Android Operating System or iOS. The minimum versions required for the functioning of the middleware are versions are 6.0 for Android and iOS13. The middleware version is 2.1.3 for Android and version 1.1 for iOS.

The middleware will be manipulated and used by a mobile application developed by potentially different clients. These mobile applications are out of the scope of the CSPN evaluation but are necessary to the functioning.

The technical environment necessary for the operation of the application, developed with INWallet Mobile Middleware, requires a physical handset (Smartphone or tablet) supporting mobile application execution environment and IP networking (through SIM card with data subscription or through WIFI).

The middleware frontend which is a part of the Smartphone, also communicate with a backend-server. The middleware backend server is manage by IN Groupe .

This back-end server has specific roles that are defined below :

- Creating session keys.
- Verifying the authenticity of the middleware front-end and the CNle chip.
- Verifying CNle status in DocVerif Database.
- Verifying integrity and consistency of data received.
- Transmitting the digital ID to the mobile server

The middleware backend and frontend communicate through an encrypted application link (TLS).

The INWALLET MOBILE MIDDLEWARE also embedded mechanisms which allow :

- The middleware frontend to authenticate itself to the middleware backend through a mechanism described more in details in [step 5 \(section 0 p. 7\)](#) of the product usage process description.
- To protect sent data.

#### **II.4.2. OPERATING SYSTEM PRECISION**

This security target covers the specificities of both intended Operating systems (Android and iOS) that could be used in the context of the product.

For the evaluation purpose the application playing the role of the mobile application is "INWallet Mobile Middleware Démo".

The middleware backend server for both operating systems will run on an updated Linux Red Hat Server comprising the latest security patches.

##### **1. Android Specificities:**

NFC communications are directly managed by the middleware.

##### **2. iOS Specificities:**

NFC communications are managed directly by the operating system. The iOS implementation of the middleware relies on iOS system functions to manage the NFC module.

#### **II.5. PRODUCT EVALUATION PERIMETER**

The evaluation scope covers the:

- Middleware frontend. And his 3 modules :
  - Communication module
  - APDU module (This module is used to format messages send to the CNle and read those received)
  - The software layer that uses the NFC module of the phone and the OS.
- Communication between the middleware and the CNle.
- Communication with the middleware backend

- Configuration of the communication protocols implemented by the middleware Backend server.

The following elements/parties/processes are considered as out of the scope of the CSPN evaluation. The:

- Mobile application which is hosting the middleware
- Mobile application backend.
- HSM
- Communication between the middleware backend and the HSM
- Communication between the middleware backend and the mobile application backend.
- Communication between the mobile application and the mobile application backend.
- Enrolment phase of the user to the mobile application backend

The assessment scope is summarized in Figure 4 below.

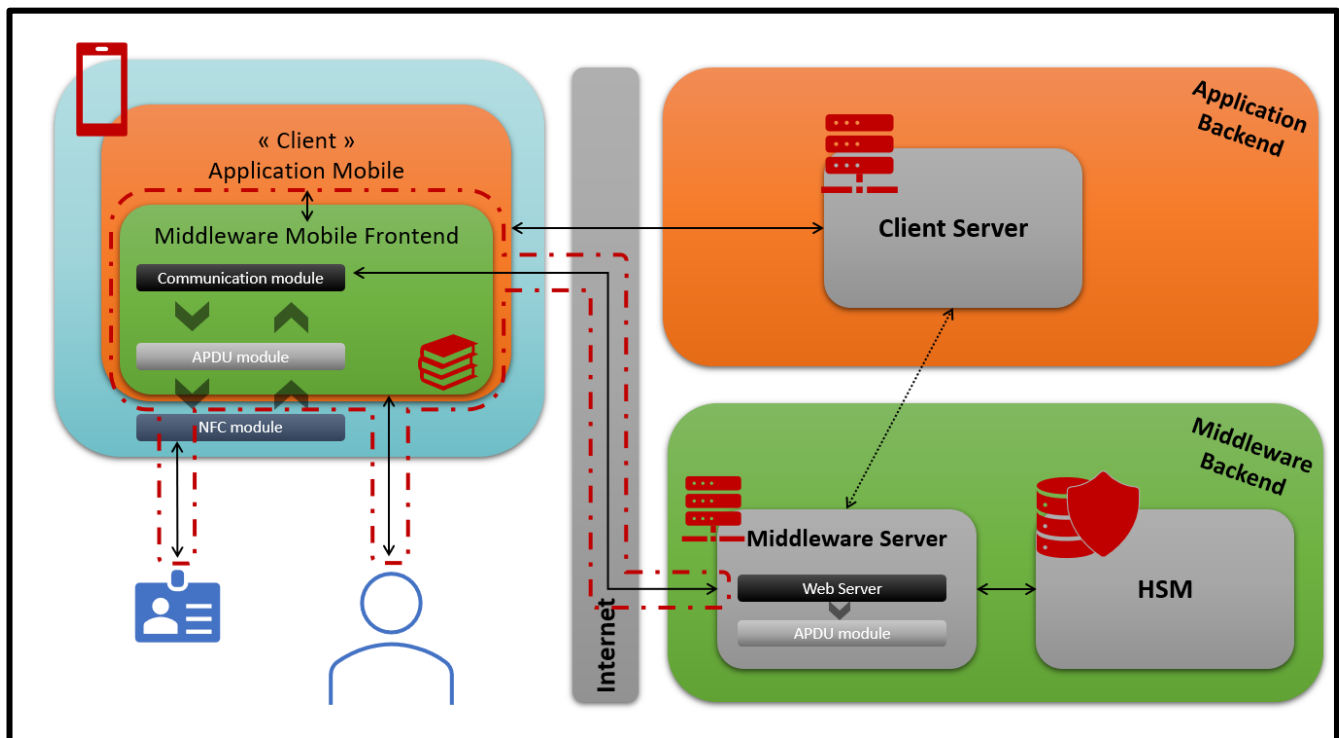


Figure 4 - Scope of the evaluation

## III. Security Elements

---

### III.1. TYPICAL USERS DESCRIPTION

Typical users to be considered are final users of the mobile application that is developed on top of the INWALLET MOBILE MIDDLEWARE.

Final users are typically holder of a CNle and clients of the service that need to authenticate themselves to a remote service.

**For the sake of comprehension, it is important to note that other indirect users/actors are implicated in the environment of the solution:**

#### **Service Providers**

A website that uses the result of authentications on the Platform to authenticate end users.

#### **Administrators of the Platform**

The manager of the backend platform.

### III.2. SENSITIVE ASSETS

The sensitive assets to be protected are the ones involved in the usage process of the CNle. This list covers both identification and authentication phases of the process and could be found below.

Each of these assets is mapped to a security criteria (also called security need): availability, integrity, authenticity and confidentiality.

**- A1. PIN Code :**

The PIN code is provided by the user through the mobile application in order to generate shared keys between the card and the Smartphone through the PACE protocol.

Security needs : Confidentiality, Integrity

**- A2. Secure Messaging Keys (PACE):**

Are the keys used to communicate through the PACE Secure Messaging and to perform a mutual authentication between the CNle and the middleware front-end.

Security needs : Confidentiality, Integrity

**- A3. Chip Authentication public key (include in DG14):**

The key used to perform Chip authentication between the CNle and the middleware back-end.

Security needs : Integrity

**- A4. TLS pinning certificate**

The CA certificate issuing the server certificate of the backend middleware, is used by the middleware frontend to established the TLS secure channel.

Security needs : Integrity.

**- A5. Identity Data (DG1, DG13):**

Identity data that are stored inside the CNle chip

Security needs : Integrity, Authenticity

**- A6. DG1, DG13, DG14 (SOD) signatures:**

Signatures used during the passive authentication to verify the integrity of the Identity Data and the consistency with DG14.

Security needs : Integrity, Authenticity

#### Note related to A5 and A6

The following assets do not directly fall in the target scope. They are related to the CNle card and the middleware back-end server. However, these assets transit through the application, and can be indirectly impacted by its functioning. Some threats and environment assumptions are directly related to them. Even though these assets are not directly related to the scope of the assessment, it is important to verify that they are never stored by the application during the evaluation.

The Table 1 below summarize the different assets to take into account in the context of the CSPN assessment phase considering their security needs.

		Availability	Integrity	Authenticity	Confidentiality
A1	PIN Code		✓		✓
A2	PACE Keys		✓		✓
A3	Chip Authentication public Key (DG 14)		✓	✓	
A4	TLS pinning certificate		✓		
A5	Identity Data (DG1, DG13)		✓	✓	
A6	DG1, DG13, DG14 (SOD) signatures		✓	✓	

*Table 1 - Matrix Assets / Security needs*

### Precisions & Remarks

*PACE and CA protocol is implemented in the CNle according to the [CNle\_SPEC]. The middleware interacts with the CNle, so the implementation of those protocols in the middleware is also compliant with the [BSI\_TR\_03110].*

*The CNle is compliant to the Protection Profile [(BSI\_TR\_03110)-1] and French RGS requirements ([RGS\_B1],[RGS\_B2] and [RGS\_B3]).*

*Specification about the properties of cryptographic keys (type, length, etc..) and supported versions of algorithms supported can be found in [CNle\_SPEC]. The above algorithms and keys length are compliant with the French RGS appendix B1 [RGS\_B1].*

*Information relative to DG1, DG13, DG14, SOD can be found in the [CNle\_SPEC], [DigitalIdentity] and [ICAO\_9303].*

*Public CA key (the one include in DG14) and the correspondent private key are BrainpoolP256r1 type keys.*

*The TLS pinning CA certificate reference can be the full certificate or a SHA256 hash.*

### III.3. ENVIRONMENT ASSUMPTIONS

#### 1. *User, Mobile equipment and hosting application*

- **EH1. The user is managing his mobile equipment in a way to minimize security risks. More specifically:**
  - o The mobile equipment operating system is always up-to-date and the latest security patches available are applied on a regular basis.
  - o Filesystem encryption is activated whenever available.
  - o A mobile lock screen authentication is active (i.e: password, biometric).
  - o The user doesn't record his PIN inside the mobile equipment or transmit it to a third party. The PIN is not used for any other usage than the authentication in the context of the product.
- **EH2. The mobile equipment enforces a first level of protection:**
  - o The root certificate authority of the mobile equipment is considered as trusted.
  - o The mobile equipment has the capacity to connect to the solution servers.
  - o The random number generator has a sufficient entropy.
  - o The cryptography primitives provided by the operating system are resistant to state-of-the-art "basic" attacks.
- **EH3. Enrolment of the mobile application to the mobile backend application.**

In order to unroll the mobile application, the user have to enter a code (this one has nothing in common with the PIN mentioned in this security target).  
This code is delivered securely to the user. Only the user of this application knows this code.
- **EH4. User PIN provisioning :**

PIN is provided through a secure channel in a manner that the holder of the CNle is the only one to know it.
- **EH5. TLS certificate protection:**

The TLS CA certificate (or its hash) is protected in integrity with obfuscation mechanism.

#### Note

*The obfuscation mechanism is outside the scope of this CSPN security target.*

#### 2. *Backends servers and related communications*

- **EH6. Operational Back-end server**

It is considered that Backend servers (hardware and software) are hardened and not corrupted (only authorized administrators and users can access it) .
- **EH7. HSM**

Random number generator of the solution shall have sufficient quality to be used as source of entropy and in compliance with [\[RGS\\_B1\]](#) rules.
- **EH8. Secure communications between the HSM and the backend server.**

In order to ensure a certain level of security, communications with the HSM are implemented as defined in accordance with the guide number 7 provided as an annex to the "Fiche 4 : Base documentaire" of the qualification decision of the HSM Proteccio ([\[ANSSI\\_HSM\]](#)).
- **EH9. TLS implementation on Middleware backend server.**

It is considered that the middleware backend server correctly implements TLS protocol in order to guarantee authentication, integrity and confidentiality of messages. Moreover, the server following the ANSSI recommendation guide [\[ANSSI\\_RSR\\_TLS\]](#) to set up TLS connections.
- **EH10. Secure communication between middleware Backend and mobile application backend.**

The web communications implemented between the two backend servers provide mutual authentication, confidentiality and integrity.

**- EH11. Integrity and Authenticity Protection of identity data.**

The signature verification of the SOD is based on the CSCA and therefore considered as ensured by a security function that is outside of the application.

The consistency check between SOD, DG1, DG13 and the DG14 previously transmitted is also ensured by components which are outside the scope of the target.

**3. CNle**

**- EH12. Secure CNle**

The electronic National Identity Card is certified CC EAL4+ and is augmented in compliance with the [\[A\\_PP0056\]](#) protection profile.



### III.4. THREATS DESCRIPTION

By definition, a threat is an action or event liable to prejudice the security of the deployed target.

The security model of the INWALLET MOBILE MIDDLEWARE has been designed to counter-act the following attack vectors:

- Attacks during session keys generation of the process
- Attacks on user authentication of the process
- Attacks impacting the integrity of data sent during the process
- Attacks on the cryptographic keys related to the process and that are stored

The following threats are identified:

- **T1. DG14 transmission without PACE SM Establishment**

Transmission of the DG14 of CNle by an attacker without the PACE SM establishment and without the PIN code knowledge.

**Goal:** Impersonation of the attacked person, via the data transmission of a CNle aimed at performing the Chip Authentication without having presented his PIN code.

- **T2. PIN code stealing during keypad entering**

Capture of the PIN code during keypad entering.

**Goal:** sensitive data theft.

- **T3. PACE Keys theft or cryptanalysis**

Capture or cryptanalysis of the keys implemented for Secure Messaging (PACE) during their establishment or their using.

**Goal:** Steal information which allow the attacker to perform identity theft.

- **T4. Second CA identification**

Identification with a second service, other than the one with which the CNle owner initially identified himself, without the owners' knowledge, by performing a new Chip Authentication.

**Goal:** Identity theft.

- **T5. Man in the Middle and Middleware backend server impersonation**

Information theft through passive network sniffing or backend server spoofing through for example certificate alteration that is used to establish the TLS connection between both part of the middleware.

**Goal:** Middleware backend server spoofing, information modification and theft.

- **T6. Transmission of identity data after CA SM establishment with another CNle**

After a legal establishment of a SM PACE and a SM CA with a CNle which is under the control of an attacker (known PIN code), the attacker succeed transmitting a SOD, DG1, DG13 from another CNle. This latter is possible without the knowledge of second PIN code by the attacker.

**Goal:** Impersonation of the attacked person.

- **T7. Alteration of Data after CA SM establishment**

After a legal establishment of a SM PACE and a SM CA with a CNle under the control of an attacker (known PIN code), the attacker succeed altering the sent data.

**Goal:** Alteration of attacker identity.

#### Note related to T6 and T7

The threats T6 and T7 are linked to both assets A5 and A6 that are out of the scope of the evaluation. Also, the security functions that are mapped to them are provided by components that are located outside the target of evaluation. However, these threats are mentioned in this security target for the sake of having the full context of the external environment. Also, the application remains a necessary vector for the implementation of attacks scenarios involving the mentioned threats.

The table below describes the impacts in availability (**A**v), integrity (**I**), confidentiality (**C**) and authenticity (**A**u) of threats on sensitive assets.

		DG14 transmission without PACE SM Establishment	PIN code stealing during keypad entering	PACE Keys theft or cryptanalysis	Second CA identification	MITM and Middleware backend server impersonation	Transmission of identity data after CA SM establishment with another CNle	Alteration of Data after CA SM establishment
		-T1	-T2	-T3	-T4	-T5	-T6	-T7
<b>A1</b>	PIN Code		<b>C I</b>					
<b>A2</b>	Secure Messaging Keys (PACE)			<b>C I</b>		<b>C I</b>		
<b>A3</b>	Chip Authentication public key (DG14)	<b>I Au</b>			<b>Au</b>	<b>I Au</b>		
<b>A4</b>	TLS pinning certificate					<b>I</b>		
<b>A5</b>	Identity Data (DG1, DG13)						<b>I Au</b>	<b>I</b>
<b>A6</b>	DG1, DG13, DG14 (SOD) signatures						<b>I Au</b>	<b>I</b>

Table 2 - Impacts of threats on sensitive assets

### III.5. SECURITY FUNCTIONS DESCRIPTION

#### - SF1. PIN Management

- PIN policy  
The PIN code has a size of six numeric characters.
- Secure PIN Pad  
Secure PIN Pad is a single visual view that provides security for data entries through a graphical keyboard. Mechanisms in place allow mitigating risks related to key loggers, screenshots and over shoulder attacks. The secure PIN pad is managed directly by the middleware.
- PIN Verification  
PACE Keys are generated basing on shared secrets which are derived from the PIN code. When a bad PIN is entered by the user, the mutual identification between the CNle Chip and the middleware frontend will not occur because the smartphone will generate different PACE Keys that are different from those generated by the CNle.

#### Note

According to the [\[CNle\\_SPEC\]](#), a counter limits the number of failed attempts to establish secure messaging (PACE) to protect against brute-force attacks. The PIN is associated with a retry counter sets at 3 that is decreased for every failed authentication.

- PIN Confidentiality  
PIN code:
  - Is only stored on the CNle and never store elsewhere.
  - Is never transmitted over a network.
  - Is never used directly without a preliminary calculation for PACE keys generation.These latter allow to mitigate the risks related to PIN code disclosure by an attacker.

#### - SF2. Protection of PACE keys

- PACE Protocols implementation  
The PACE protocol is implemented in compliance with the [\[CNle\\_SPEC\]](#) and [\[ICAO\\_9303\]](#), hence it is also compliant with the French [\[RGS\\_B1\]](#).
- SM PACE Keys storage  
PACE Keys are shared between the CNle and the middleware frontend. Confidentiality and integrity are ensured on one side by the CNle and relies on its properties to ensure those. However The CNle is certified CC EAL4+ and is augmented in compliance with the [\[A\\_PP0056\]](#) protection profile.

#### - SF3. Data transmission regulation

- DG14 Sending  
DG14 can be sent from the chip to the Smartphone only if a SM PACE is established between both parties.
- Identity Data  
The transmission of data (DG1, DG13, SOD) from the card to the middleware SERVER can only be done under a secure messaging (CA).
- CA data (DG14 from middleware frontend to backend)  
Prohibition to create a new secure messaging (CA) establishment without a new secure messaging establishment (PACE).

#### Note

Moreover communications between the middleware frontend and the middleware backend are considered as secure. In fact, in addition to the TLS communication, data sent from the frontend to the backend is encrypted with AES algorithm before the SM

CA establishment. The AES key used for this matter is stored obfuscated in the middleware and is only shared between the middleware backend and its frontend. Therefore, this process and the TLS CA certificate pinning ensure a mutual authentication between the middleware backend and the middleware frontend. However, this functionality and its associated key are outside the scope of this CSPN security target.

**- SF4. TLS implementation and CA Certificate verification**

- TLS Protocols implementation  
The INWALLET MOBILE MIDDLEWARE implements TLS protocol in compliance with the ANSSI recommendation guide [\[ANSSI\\_RSR\\_TLS\]](#).
- TLS certification pinning  
The INWALLET MOBILE MIDDLEWARE perform server authentication through TLS CA certificate pinning. Before the establishment of the TLS connection between the middleware frontend and the middleware backend, the middleware compares the certificate provided by the server with the stored reference. The establishment of the TLS connection occurs only if they match.

**III.6. COVERAGE MATRIX**

	T1: DG14 Transmitting without PACE SM Establishment	T2: Pin stealing during typing	T3: Stealing or cryptanalysis of the PACE Keys	T4: Second CA	T5: MITM and Middleware backend server impersonation	T6: Transmission of identity data after CA SM establishment with another CNle	T7: Alteration of Data after CA SM establishment
SF1 – Pin Management		✓	✓				
SF2 – Protection of PACE keys			✓		✓		
SF3 – Data transmission regulation	✓			✓		✓	
SF4 – TLS implementation and CA Certificate verification					✓		
EH5 – TLS certificate protection					✓		
EH11 – Integrity Protection of identity data						✓	✓

Table 3 - Matrix Threats / Security Functions & Environment Assumptions