| Policy | |
|---|---|
| ELECTRONIC IDENTIFICATION SCHEME POLICY<br>OID: [1.3.6.1.4.1.62466.87.1.1.3.1.0] | |
| **Purpose/Summary** | ELECTRONIC IDENTIFICATION SCHEME POLICY |

| | |
|---|---|
| **Level of dissemination** | D3 – Free distribution |
| **Distribution list** | Audience |
| **Location** | BE YS TRUSTED SOLUTIONS FRANCE |

| Version | Date | Modifications | Author |
|---|---|---|---|
| 1.0 | 04/14/2025 | Creation | Gergina Kyoseva |
| 1.1 | 06/03/2025 | Addition of OID | Lidiya Ivanova |
| 1.2 | 07/04/2025 | Addition of legal entity registration data | Lidiya Ivanova |
| 1.3 | 10/16/2025 | Addition of commonly used name | Lidiya Ivanova |
| 1.4 | 11/11/2025 | Suspension not available | Mihael Stoyanov |
| **Expiration date** | | 2 years | |

**Reference Documents**

| Label | Location or insertion of the document |
|---|---|
| | |

**Glossary**

| Term/Acronym | Definition |
|---|---|
| ANSSI | National Agency for Information Systems Security |
| C2SC | Trusted Services Monitoring Committee |
| GTC | General Terms and Conditions |
| CSPN | First Level Security Certification |
| CNIL | French Data Protection Authority |
| EIMP | Electronic Identification Means Provider |
| EIM | Electronic Identification Means |
| OID | Object Identifier |
| RIVP | Remote Identity Verification Provider |

**Definitions**

| Term | Definition |
|---|---|
| KIPMI application | KIPMI is a mobile application that is part of BE YS TRUSTED SOLUTIONS FRANCE's digital trust services, enabling access to various services and the issuance of an electronic mean of identification. |
| User application | Application service, online or offline, requiring the electronic identification of its users via an electronic mean of identification issued by an EIMP. |
| Authentication | The act of verifying the identity of a natural or legal person or the origin of communication. |
| Client | Client entity that has decided to subscribe to the Service, which it uses for its own needs or makes available to users. |
| Electronic Identification Means (EIM) | A physical and/or intangible element containing personal identification data and used to authenticate oneself to an online service. The EIM issued by BE YS TRUSTED SOLUTIONS FRANCE is integrated into a mobile application called "KIPMI".<br>The Electronic Identification Mean is issued after an initial identity verification and its lifetime is as defined in this Policy. |
| Electronic Identification Scheme Policy | A set of rules, identified by a name and an identifier (OID), defining the requirements with which an FIE complies in the implementation and provision of its services. A policy may also, if necessary, identify the |

| | |
|---|---|
| | obligations and requirements relating to other parties, in particular Users and User Applications. |
| Service | The service for issuing and managing Electronic Identification Means issued by BE YS TRUSTED SOLUTIONS FRANCE as an FIE. |
| User | A natural person who uses the certified EIM issuance service offered by the FIE. |
| Stakeholders | Person, machine, or service involved in the EIM issuance process. |
| Trusted role | Formally identified trusted persons who participate in the performance of sensitive actions related to the certified service. |

**Validation**

| **Proofreader** | **Function (in relation to the document)** |
|---|---|
| Lidiya Ivanova | Service manager |
| **Approver** | **Function (in relation to the document)** |
| Younes El Gui | President |

## Summary

# 1 INTRODUCTION

## 1.1 General overview

As part of its dematerialization and trust services, BE YS TRUSTED SOLUTIONS FRANCE provides its Service to its Clients. BE YS TRUSTED SOLUTIONS FRANCE acts as an Electronic Identification Means Provider (EIMP) on behalf of the Users of its Clients' services.

This document constitutes the Electronic Identification Scheme Policy (EISP) of BE YS TRUSTED SOLUTIONS FRANCE as an EIMP for the issuance to Users of Electronic identification means (EIM) with a substantial assurance level under the eIDAS Regulation.

The purpose of this Policy is to define the requirements for Electronic Identification Means throughout all phases of their life cycle, as well as to set out the commitments expected from the various Service Stakeholders.

The electronic identification scheme implemented complies with the technical specifications and minimum procedures defined for the substantial level by:

- Regulation (EU) No. 910/2014 of the European Parliament and of the Council of July 23, 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, amended by Regulation (EU) 2024/1183 of the European Parliament and of the Council of April 11, 2024, amending Regulation (EU) No. 910/2014 as regards the establishment of the European Digital Identity Framework;
- Commission Implementing Regulation (EU) 2015/1501 of September 8, 2015;
- Commission Implementing Regulation (EU) 2015/1502 of September 8, 2015;
- Security requirements reference framework for electronic identification means, version 1.2, dated August 11, 2022, issued by ANSSI;
- ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers;
- ETSI EN 319 411-1 General requirements;

Electronic Identification Means enable, among other things, the User to identify and authenticate themselves to an EIMP partner user application that delegates this electronic identification to the Service. Electronic Identification Means are intended for natural persons acting in a private capacity.

## 1.2 Identification of the EIMP

The Electronic Identification Means Provider, responsible for the Service and the Electronic Identification Means, is the following company:

BE YS TRUSTED SOLUTIONS FRANCE
10 Boulevard Haussmann 75009 PARIS
Contact address: kipmi.customer.service@be-ys.com
Website: https://www.kipmi.com/

## 1.3 Electronic Identification Scheme Policy

This document represents the EIMP's Electronic Identification Scheme Policy (Policy). It sets out rules defining the requirements with which the EIMP complies, as well as the standards it applies in setting up and providing the Service.

The Policy also specifies the security measures, obligations, and requirements applicable to other parties, in particular Users and Clients, and forms an integral part of the GTC.

## 1.4 This document has been prepared in accordance with Regulation (EU) 2016/679 (GDPR) and applicable French legislation. The Policy is public and may be amended by the EIMP at any time.Document identification

This Policy is identified by the following object identification number (OID): [1.3.6.1.4.1.62466.87.1.1.3.1.0]

## 1.5 Effective date

The Policy shall enter into force after approval by the EIMP's C2SC and on the date set by that Committee. The Policy shall be published on the website https://www.kipmi.com/ at least 72 hours before its effective date.

## 1.6 Duration and early termination of the Policy

This document remains in force until a new version is published.

## 1.7 Policy Management

### *1.7.1 Entity managing the Policy*

This Policy is managed by the members of the EIMP's C2SC.

### *1.7.2 Point of contact*

The contact point for any questions about the Policy is:

- Mailing address: BE YS TRUSTED SOLUTIONS FRANCE
  VID Department
- 10 Boulevard Haussmann75009 PARIS Email address: [kipmi.customer.service@be-ys.com ]

### *1.7.3 Policy Approval Procedure*

The Policy is approved by the C2SC after review and proofreading of the document by the members of the Committee and by the persons designated by it.

The purpose of this review is to ensure that:

- The Policy complies with regulatory and normative requirements relating to the provision of the certified service;
- The consistency of the Policy with other documents published in connection with the service, such as the General Terms and Conditions;
- The commitments expressed in the Policy are consistent with the technical and organizational resources implemented by the EIMP and its partners;
- The supervisory body is effectively notified of any significant changes in the provision of the Service in accordance with the procedures described in the certification procedures. This includes, but is not limited to:
  - Changes resulting from a modification of the Service Policy or the associated General Terms and Conditions;
  - Changes to the hosting conditions;
  - Changes to cryptographic equipment;
  - Changes to the technical architecture;
  - Changes to procedures for issuing, re-issuing, revoking, suspending, or reactivating EIM;
  - Changes in the governance of the Service.

The C2SC shall ensure that the effective date of the new Policy allows, as far as possible, sufficient time for Clients to familiarize themselves with the new provisions and adapt their practices if necessary.

## 1.8 Published information

### *1.8.1 Entities responsible for providing information*

The EIMP shall publish information for Clients and Users on its website: https://www.kipmi.com/

### *1.8.2 Information to be published*

The EIMP undertakes to publish at least the following information:

- This document, describing the Electronic Identification Scheme Policy;
- The General Terms and Conditions of the Service;
- The points of publication of information associated with partner services.

### *1.8.3 Publication deadlines and frequency*

Information relating to the Service (changes, new versions of the Policy, etc.) is published as soon as needed to ensure continuous consistency between the published information and the EIMP's actual commitments, resources, and procedures.

The information publication point is available 24/7/365.

### *1.8.4 Control of access to published information*

All published information is freely accessible for reading and can be consulted here: https://www.kipmi.com/

Modification access to the publication systems for other information is strictly limited to the authorized internal functions of the EIMP. These individuals are defined in trusted roles and have a strong authentication method for logging into the publication systems.

## 1.9 Document amendment

### *1.9.1 Update procedure*

The EIMP ensures that any proposed amendments to its Policy remain compliant with applicable regulatory and normative requirements. The C2SC is always involved in the validation of any amendments. Any request for change is therefore placed on the agenda of a future committee meeting and the decision is recorded in the corresponding minutes.

Any proposed changes to the Service are subject to an impact analysis to determine their potential impact on:

- The quality or security of the Service;
- The compliance of the certified offer with ANSSI requirements;
- The need to update other published documents;
- The internal practices of the EIMP or its partners and suppliers.

### *1.9.2 Circumstances under which the Policy must be changed*

Amendments to this Policy may be made during the lifetime of the Service, for example for:

- Minor corrections (errors, additional clarifications, etc.);

- Developments or extensions to the service;
- The acceptance or implementation of new Means of Electronic Identification;
- Technical changes (implementation, partners, suppliers, etc.);
- Corrections resulting from audits of the Service.

### *1.9.3 Circumstances under which the OID must be changed*

In the event of a major impact, a change to the Policy OID is planned, and the change and its impact analysis are submitted to the supervisory body and the conformity assessment body for their opinion or comments.

The impact analysis is reviewed by the C2SC, which decides whether or not to approve the change. If approved, the new Policy will be submitted to the C2SC for approval.

### *1.9.4 Entry into force of the amended Policy*

The date of entry into force of the new version of the document is determined by the C2SC in its validation decision, taking into account the nature and complexity of the changes and, where applicable, the time needed for Stakeholders in the Service to implement the related adjustments.

### *1.9.5 Mechanism and period for providing information on amendments*

Once the change to the Service has been validated by the C2SC, the new Policy is communicated:

- Without delay to the EIMP's staff and all Stakeholders in the provision of the Service - by email. The time allowed for them to familiarize themselves with the new provisions and adapt (if necessary) their practices and procedures, as well as the date of entry into force, are explicitly indicated.
- At least 72 hours (seventy-two hours) before its effective date - to Clients and Users - by publication on the website: https://www.kipmi.com/

The EIMP sends the supervisory body an annual summary of all changes made to the provision of its Service.

# 2 RELATED DOCUMENTS

## 2.1 General Terms and Conditions

The applicable GTC (and their previous versions) are available on the EIMPwebsite: https://www.kipmi.com/ and on the KIPMI application

## 2.2 Normative documents

| | |
|---|---|
| [EIDAS] | Regulation (EU) No. 910/2014 of the European Parliament and of the Council of July 23, 2014 on electronic identification and trust services for electronic transactions in the internal markethttps://www.eur-lex.europa.eu |
| [ANSSI_MIE] | Requirements framework for electronic identification means General Security Frameworkhttps://cyber.gouv.fr/sites/default/files/document/20220811_np_anssi_eidas_eid-referentielexigences_v1.2.pdf |
| [HYGIENE] | IT hygiene guide<br>https://cyber.gouv.fr/publications/guide-dhygiene-informatique |
| [CERT_SERV_PROC ESS] | Service certification process<br>https://www.ssi.gouv.fr/ |
| [GDPR] | https://www.cnil.fr/fr/reglement-europeen-protection-donnees |
| [EN_319_401] | ETSI EN 319 401<br>Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers<br>https://www.etsi.org/ |
| [EN_319_411-1] | ETSI EN 319 411-1<br>Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates;<br>https://www.etsi.org/ |
| [2015/1501] | Commission Implementing Regulation (EU) 2015/1501 of September 8,<br>September 2015 on the interoperability framework referred to in Article 12 |

Paragraph 8, of Regulation (EU) No 910/2014.
https://eur-lex.europa.eu/

[2015/1502] Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 laying down technical specifications and minimum procedures relating to the assurance levels of electronic identification means referred to in Article 8(3) of Regulation (EU) No 910/2014 https://eur-lex.europa.eu/

# 3 STAKEHOLDERS AND OBLIGATIONS

## 3.1 EIM provider

The EIMP is responsible for the Service and performs the EIM management function. It ensures the implementation and oversight of the various functions necessary for the provision of the Service.

The EIMP has established an organization that is fully operational in all aspects relevant to the provision of the Service. In particular, the EIMP maintains an effective information security management system to manage and control information security risks. The EIMP remains responsible for the performance of any tasks outsourced to third parties, as well as for compliance with the scheme policy, as if those tasks had been performed internally.

The EIMP complies with all legal requirements incumbent upon it in connection with the operation and performance of the Service, including the categories of information that may be collected, the procedures for establishing proof of identity, the types of data that may be retained, and the duration of their retention.

## 3.2 Remote Identity Verification Provider

The RIVP is an entity that provides a service for verifying Users' identification data through a remote face-to-face meeting (as opposed to a physical face-to-face meeting).

The Service uses only RIVPs certified at the substantial or high assurance level by ANSSI, depending on the reference framework, for its User registration function. As such, the RIVP guarantees the reliability of its service, creates and keeps a record of evidence for each verification carried out, and regularly reports metrics relating to the operation of its service to the EIMP.

## 3.3 Users

The User, holder or applicant for an EIM, can only be a natural person, who is issued with an EIM after verification of their identity. The Service does not manage any link between the User and legal entities in the context of EIM identification data. The User declares that they have read and accept the GTC of the KIPMI Application.

The User uses their EIM to identify and authenticate themselves to the User Parties that delegate this electronic identification to the Service.

## 3.4 User Applications

User Applications are digital services, whether online or offline, managed by User Parties, which must identify (know the identity attributes such as first and last name, etc.) and authenticate (ensure that the user is actually the person designated by the identity attributes) their users in a reliable manner, and which delegate this electronic identification to the Service.

To do this, the user application asks the Service's electronic identification function to perform electronic identification using the EIM that its user must have obtained beforehand.

The person responsible for a User Application must ensure that the level of assurance provided by the Service is appropriate for the requirements of their application.

### 3.5 User Parties

A User Party is a natural or legal person who relies on electronic identification. Within the KIPMI Application, the User has the option of sharing documents and attributes with User Parties who request them. User Parties may include the User's employer, banks, insurance companies, government organizations, mobile phone operators, etc. The User Parties are Clients of the EIMP and rely on the Service to establish commercial, professional, administrative, and other relationships or to carry out various operations or transactions.

# 4 OPERATIONAL REQUIREMENTS FOR THE MIE LIFECYCLE

## 4.1 Functional breakdown of the Service and characteristics

The functional breakdown of the Service used in this document is as follows:

- **EIM management function**: This function ensures the overall management of the MIE lifecycle. It relies on the functions of registering Users, issuing and revoking EIM, and also manages the re-issuance and expiration of EIM, as well as the use of EIM by the electronic identification function.
- **User registration function**: This function verifies the identity information of a prospective EIM User before they can obtain an EIM. It is used during the initial issuance of an EIM to a new User, as well as during the reactivation of an EIM or after the expiration of a User's previous EIM.
- **EIM issuance function**: This function initializes and issues an EIM to a User who has been successfully registered. This phase includes the generation of User cryptographic elements and their secure implementation in the User's EIM. The User chooses their personal PIN code and creates their account;
- **EIM revocation function**: This function processes MIE revocation requests in order to determine the actions to be taken and, where applicable, terminate the validity of the MIE;
- **Electronic identification function**: This function disseminates and shares a User's identity information with User Parties that have requested it, after identifying and authenticating the User through their EIM and verifying the EIM's validity.

The EIM is designed so that it can only be used under the control or in the possession of the person to whom it belongs.

The cryptographic means constituting the EIM must, as a minimum, be qualified at the basic level of the [RGS] based on a First Level Security Certification (CSPN), on the basis of a security target validated by ANSSI.

## 4.2 Registration and application for an EIM

To use the Service, the User must download the KIPMI Application to their smartphone. When the User opens the KIPMI Application for the first time, they go through the registration process, which consists of several steps:

- Account creation
- Identity verification

- Issuance of EIM

To create an account, the User provides:

- Their email address
- Their first name and last name
- Their phone number

The User must then accept the KIPMI Application's general terms and conditions and click on the "*Register*" button. In order to create their account, the User must set up a PIN code during registration. The PIN code consists of 6 digits and is advised to follow with the recommendations below:

- Do not include repeated digits (e.g., 111111)
- Do not include sequential numbers (e.g., 123456 or 654321)

Once the PIN code has been created, the User must validate their email address and phone number.
The User verifies their email address using the 6-digit code sent to their email address. The phone number is verified using a 6-digit code sent by SMS to the phone number provided by the User.

### 4.3 Proof and verification of identity for individuals

Before being issued with an EIM, the User must have their identity verified by a remote identity verification service certified by a remote identity verification provider (RIVP) with a minimum substantial level of assurance. The User must present a valid official ID, and their face will be compared to the photo on the ID. Following a positive verdict from this verification service, the following identity attributes are associated with the account created and considered reliable with a substantial level of assurance:

- Last name;
- First names;
- Date of birth;
- Place of birth (city or country when the person was not born in France);
- Gender.

A request for the issuance of an EIM to the User is then automatically initiated.

### 4.4 Issuance of the EIM

Once identity verification has been successfully completed, the User will have 72 hours to activate their account by validating the verified credentials extracted from the identity document used for verification.

If an account is not activated by accepting the credentials within 72 hours, the User is required to go through the identity verification process again.

If identity verification fails, the User is notified and asked to restart the process. There is no limit to the number of times a user can attempt to verify their identity.

An EIM is issued when the account is activated, after a previous EIM has been revoked.

A notification in the KIPMI Application informs the User that their EIM has been successfully issued on the phone used.

An EIM is valid for the duration of validity of the identity document used for its issuance, but may not exceed five years. It must be re-issued before this expiry date, otherwise it will expire.

## 4.5 Use of the EIM

The use of an EIM is restricted to the electronic identification of its User on the Service's electronic identification function. **Any other use is prohibited.**

### *4.5.1 Use of EIM for electronic identification requested by a User Application*

The User's electronic identification is requested by a User Application (including the Service itself). This User Application displays a QR code which requests the information necessary to authenticate the User. The User opens their KIPMI mobile application. The User authenticates themselves on their mobile application using their PIN code. The User scans the QR code. The KIPMI mobile application asks the User to confirm the sharing of personal data requested by the User Application. The User agrees (or refuses) to provide the data. Upon acceptance, KIPMI shares the User's data with the User Application. This allows the User, for example, to access the services of this application or to validate an operation on it.

The User must ensure that authentication is requested by a legitimate application, and if this is not the case, must not enter their PIN code and must report this incident to the Service.

### *4.5.2 Use of EIM for electronic identification requested by company systems that are directly integrated with the KIPMI application*

The User's electronic identification may also be requested by User Parties that have direct integration with the KIPMI Application. In this case, the User receives a notification in the application containing information about the legal entity requesting their electronic identification.

The User has the option to accept or decline the request. To accept or decline the request, the User must authenticate themselves using their PIN.

#### *4.5.3 Use of EIM for document sharing*

EIM can be used for document sharing between Users and User Parties. The KIPMI Application has a feature that allows Users who are also members of the organization's space to receive document sharing requests from the organizations of which they are members. The User has the option to accept or reject the request. To accept or reject the request, the User must authenticate themselves using their PIN code.

#### *4.5.4 Use of EIM for sharing attributes*

The KIPMI Application offers the functionality of sharing identity attributes as defined by the eIDAS 2 regulation between Users and User Parties. The User has the option to decide whether to accept or refuse the request to share attributes. To accept or refuse the request, the user must authenticate themselves using their PIN code.

### 4.6 Revocation or suspension of the EIM

The revocation of an EIM may be requested by the User themselves (after the loss or theft of their phone or ID card, for example) on the KIPMI Application or directly by the EIMP via email to kipmi.customer.service@be-ys.com.

The KIPMI Application does not support Suspension of the MIE.

#### *4.6.1 Request for revocation by the User from the KIPMI application*

The User may request the revocation of their EIM from the KIPMI mobile application, after authentication with their PIN code.

The revocation management function on the KIPMI application is available 24 hours a day, 7 days a week. Any request for revocation of an EIM is processed within 24 hours. This period begins upon receipt of the request and ends when information about the revocation is made available to third parties.

Revocation prohibits any further use of the EIM. The User may request a new EIM following revocation, under the same conditions as for an initial request.

#### *4.6.2 Request for revocation by the EIMP*

The revocation of an EIM may be decided by the EIMP in the following cases:

- The User does not meet or no longer complies with the general terms and conditions of use;
- An error (intentional or unintentional) has been detected in the registration file;
- The EIM or associated activation data is suspected of being compromised, is compromised, lost, or stolen;
- The User has died;
- The User has filed a complaint for identity theft.

Based on a validated decision, an administrator logs into the service, searches for the EIM of the User concerned, and revokes it.

#### *4.6.3 Re-Issuance of EIM*

In order to re-issue the EIM, the User must go through identity verification procedure.

### 4.7 EIM re-issuance

EIM re-issuance consists of requesting an EIM when the User already has a valid EIM that has not expired or been revoked. Otherwise, it is considered a new request and is treated as an initial request.

Re-issuance may be requested by the User or proposed by the Service.

The Service automatically sends a notification to Users whose EIM is about to expire. When they wish, and before their EIM expires, Users open the KIPMI application on their mobile phone and authenticate themselves by entering their confidential PIN code.

If the ID document registered when the EIM was previously issued is no longer valid, the User must complete the RIVP process as the first step in the re-issuance process.

After the User has been authenticated and their identity has been verified, the KIPMI application initiates the EIM re-issuance process. It generates new cryptographic elements and asks the User to set a confidential PIN code.

The application informs the User that the re-issuance has been successful.

The previous EIM on the same device is revoked.

# 5 NON-TECHNICAL SECURITY MEASURES

## 5.1 Physical security measures

The EIMP undertakes to implement and maintain the level of physical security required for the premises where the Service components are operated.

### *5.1.1 Geographical location and construction of sites*

Depending on the sensitivity of the Service components, the sites are defined at level 1 of the security policy: vital impact (major for the company). As such, the security of the building site complies with level 1 physical security measures for peripheral, perimeter, and interior protection, in particular measures relating to:

- Power supply and air conditioning;
- Vulnerability to water damage;
- Fire prevention and protection.

The measures also enable compliance with the commitments made in the policy or in contractual commitments with Service Clients regarding service availability.

### *5.1.2 Physical access*

In order to prevent any loss, damage, or compromise of EIMP's resources, access to the premises is controlled in accordance with the Level 1 zoning of the premises: "very restricted access."

For the User's EIM delivery functions, access is strictly limited to persons specifically authorized to enter the premises, and access is traceable. Outside business hours, security is reinforced by the implementation of physical and logical intrusion detection measures. In addition, entry and exit control is permanent during non-business hours (NBH).

Each entry and exit to the secure area is subject to independent monitoring and traceability. All unauthorized personnel must be accompanied by an authorized person.

In order to ensure systems availability, access to machines is restricted to persons authorized to perform operations requiring physical access. For this purpose, the relevant Service components establish a physical security perimeter in which these machines are installed. Any premises shared between the component concerned and another component (within or outside the Service) are considered outside this security perimeter.

The door is opened by an access control system.

#### 5.1.3 Power supply and air conditioning

The characteristics of the power supply and air conditioning equipment enable compliance with the conditions of use of the EIMP equipment as specified by their suppliers.

They also comply with the requirements of the specifications provided by the EIMP in terms of the availability of its functions, in particular the revocation management function.

#### 5.1.4 Vulnerability to water damage

The protective measures put in place by the EIMP protect its infrastructure against water damage.

#### 5.1.5 Fire prevention and protection

The EIMP implements fire protection and firefighting measures.

#### 5.1.6 Media storage

Media (paper, hard drives, floppy disks, CDs, etc.) used within the EIMP are processed and stored in accordance with the security requirements defined for sensitive assets (in terms of confidentiality, integrity, and availability). In particular, media are subject to measures against damage, theft, unauthorized access, and obsolescence. These measures apply throughout the retention period for the content of these media.

#### 5.1.7 Decommissioning of media

At the end of their life, media will either be destroyed or reset for reuse, depending on the level of confidentiality of the information they contain.

The procedures and means of destruction and reset comply with EIMP's Security Policy.

#### 5.1.8 Off-site backup

In addition to on-site backups, the Service components implement off-site backups of their applications and information. These backups are organized to ensure the fastest possible recovery of services after an incident.

Backups are tested regularly.

### 5.2 Procedural security measures

The following procedural security measures supplement those defined in the Key Ceremony, during which the dual key used by EIMP is created.

Security procedures and policies are communicated to employees on a need-to-know basis.

Procedures are established and enforced for all operations performed by personnel in positions of trust that may impact service delivery.

### *5.2.1 Trusted Roles*

The trusted roles defined below are those required for the components of the Service, independently of the trusted roles defined as part of the Key Ceremony.

- **Service Security Officer**: The Security Officer is responsible for implementing the Service's security policy. He or she manages physical access controls to the entity's system equipment. He or she is responsible for analyzing event logs to detect any incidents, anomalies, attempts at compromise, etc.
- **Application Manager**: The Application Manager is responsible for implementing the various EIMP policies within the relevant Service component. Their responsibility covers all the functions provided by the applications and the corresponding performance.
- **Compliance Manager**: The Compliance Manager is responsible for ensuring compliance with the functional and technical requirements of the ANSSI regulations and European digital wallet regulations (eIDAS and eIDAS2).
- **Systems Engineer**: Responsible for the start-up, configuration, and technical maintenance of the entity's IT equipment. Ensures the technical administration of the entity's systems and networks. Also responsible for restoration operations.
- **Operator**: An operator within the relevant Service component carries out, as part of their duties, the operation of the applications used to deliver the services provided by that Service component.
- **Controller**: A person appointed by the head of the Service component whose role is to regularly check that the services provided by the Service component comply with EIMP policies.
- **Revocation operator**: Person responsible for applying the EIM revocation procedure.

### *5.2.2 Number of people required per task*

Internal documentation specifies which operations require the involvement of several persons and which constraints these persons must comply with (positions in the organization, hierarchical links, etc.), in particular, the persons required for the key ceremony.

#### 5.2.3 *Identification and authentication for each role*

Each entity operating a component of the Service verifies the identity and authorizations of all members of its staff before assigning them a role and the corresponding rights, in particular:

- That their name is added to the access control lists for the premises of the entity hosting the systems concerned by the role;
- That their name is added to the list of persons authorized to physically access these systems;
- That an account is opened in their name in these systems;
- Where applicable, that cryptographic keys and/or a certificate are issued to them to perform their assigned role in the Service.

These controls are described in internal documentation and comply with EIMP's Security Policy.

#### 5.2.4 *Roles requiring separation of duties*

Several roles may be assigned to the same person, provided that this does not compromise the security of the services offered.

The responsibilities associated with each role are described in EIMP's internal documentation and comply with the Security Policy.

For the various trusted roles, it is recommended that no individual hold multiple roles, and the following combinations are prohibited:

- Security officer and system engineer/operator;
- System engineer and operator.

### 5.3 Security measures for the personnel

The following procedural security measures supplement those defined in the Key Ceremony, during which the EIMP's Bi-key is created.

#### 5.3.1 *Required qualifications, skills, and authorizations*

All personnel assigned to work within the Service components are subject to a confidentiality agreement.

The EIMP manager must ensure that the duties assigned to personnel working within the Service correspond to their professional competencies.

Management personnel must have the appropriate expertise for their role and be familiar with the security procedures in force within the Service, as well as personal data protection measures.

The EIMP must inform anyone involved in trusted roles within the Service:

- Of their responsibilities relating to the Service's services,
- The procedures related to system security and personnel control, with which they must comply.

This appointment is made formally by the EIMP's security officer and is accepted in writing by the person appointed to a trusted role.

The qualifications, skills, and authorizations required for the key ceremony are defined in a specific procedure.

The responsibilities of personnel in trusted roles are assigned in such a way as to separate roles and responsibilities, avoid conflicts of interest, and reduce opportunities for intentional or unintentional modification or misuse of the Service's systems.

Access rights and authorizations are granted and configured in accordance with the principle of least privilege.

### *5.3.2 Background check procedures*

Personnel working within a component of the Service, depending on the applicable context, are required to submit a sworn statement of no criminal convictions, a criminal record extract, or a confidentiality agreement.

Persons in trusted roles must not have any conflicts of interest that could compromise the impartiality of their duties.

### *5.3.3 Initial training requirements*

Personnel receive prior training on the software, hardware, and internal operational and security procedures that they implement and are required to comply with within the component of the Service in which they operate.

Personnel are aware of and understand the implications of the operations for which they are responsible.

### *5.3.4 Continuing training requirements and frequency*

The personnel concerned shall receive adequate information and training prior to any changes in systems, procedures, organization, etc., depending on the nature of these changes.

In addition, continuing training includes annual training on new threats and security procedures.

#### *5.3.5 Penalties for unauthorized actions*

Appropriate sanctions shall be applied to personnel who fail to comply with applicable security procedures and policies.

This policy does not set out specific requirements in this regard. Further details may be provided in internal documentation.

#### *5.3.6 Requirements for external service provider personnel*

External service provider personnel working on EIMP premises and/or on Service components shall also comply with the requirements of this Policy and the Security Policy.

This must be reflected in appropriate clauses in the relevant contracts with service providers.

#### *5.3.7 Documentation provided to staff*

All staff shall have access to at least the relevant documentation concerning the operational procedures and specific tools they use, as well as the general policies and practices of the component within which they work, more specifically the Security Policy that affects them.

### 5.4 Audit data collection procedures

Event logging consists of recording events electronically by manual entry or automatic generation.

The resulting files, in electronic form, must enable the traceability and accountability of the operations performed.

#### *5.4.1 Types of events to be recorded*

Each entity operating a component of the Service logs at least the following events automatically upon system startup and in electronic form:

- Creation/modification/deletion of user accounts (access rights) and corresponding authentication data (passwords, certificates, etc.);
- Startup and shutdown of computer systems and applications;
- Events related to logging: start-up and shutdown of the logging function, modification of logging settings, actions taken following a failure of the logging function;
- Logging in/out of users with trusted roles, and corresponding unsuccessful attempts.

Other events are also collected, either electronically or manually. These are security-related events that are not automatically generated by computer systems, including:

- Physical access;
- Maintenance actions and changes to systems configuration;
- Changes to personnel;
- Destruction and reset actions on media containing confidential information (keys, activation data, personal information about Users, etc.);
- Receipt of an MIE request (initial and re-issuance);
- Approval or rejection of an MIE request;
- Events related to the management of sensitive cryptographic materials and the keys they implement (generation (key ceremony), backup/recovery, revocation, re-issuance, destruction, etc.);
- Where applicable, the generation of secret user elements (dual keys, activation codes, etc.) or public elements (certificates, etc.);
- Transmission of MIEs to Users and, where applicable, explicit acceptance or rejection by Users;
- Where applicable, the delivery of the MIE to the User;
- Publication and updating of the GTC or other documents published by the entity responsible for the electronic identification scheme;
- Receipt of a revocation request;
- The validation or rejection of a revocation request;
- The generation and publication of LCRs (and possibly deltaLCRs) or OCSP queries/responses.

Each event log entry contains, where applicable, the following fields:

- Event type,
- Name of the executor or reference of the system triggering the event,
- Date and time of the event,
- Result of the event (failure or success).

Responsibility for an action lies with the person, organization, or system that performed it. The name or identifier of the executor is explicitly included in one of the fields in the event log. In addition, depending on the type of event, each record also contains the following fields:

- Requester and recipient of the operation (where possible),
- The operation or reference of the system making the request,
- Names of persons present (if the operation requires several persons),
- Cause of the event,
- Any information characterizing the event (for example, for the generation of a Certificate, the serial number of that Certificate).

Logging operations are performed during the process. In the case of manual entry, the entry is made, with some exceptions, on the same business day as the event.

#### *5.4.2 Frequency of event log processing*

The Service's event logs are analyzed on average 2 to 3 times each week.

In addition, event logs are automatically analyzed to identify abnormal activity and alert staff to the potential occurrence of critical security events.

#### *5.4.3 Event log retention period*

Event logs are retained on site for at least one month. Logs are retained and archived for the period required by applicable law, even if the Service ceases to operate.

#### *5.4.4 Backup protection of event logs*

The EIMP implements protection for event logs that is appropriate to the level of sensitivity of the information contained in these logs. This level of sensitivity is determined by a risk analysis.

#### *5.4.5 Event log backup procedure*

The EIMP implements an event log backup process appropriate to the level of sensitivity of the information contained in these logs. This level of sensitivity is based on a risk analysis.

#### *5.4.6 Event log collection system*

The EIMP implements an event logging system that includes date stamping.

#### *5.4.7 Notification of event recording to the event manager*

This policy does not set out any specific requirements in this regard. Further details may be provided in the EIMP's internal documentation.

#### *5.4.8 Vulnerability assessment*

The EIMP implements vulnerability management for EIMP systems in accordance with the EIMP Security Policy.

Event logs are checked regularly in accordance with the procedures defined in paragraph 3.4.2.

Logs are analyzed as soon as an anomaly is detected. This analysis results in a summary in which the important elements are identified, analyzed, and explained. The summary highlights any

anomalies and falsifications that have been detected. Any critical vulnerabilities are addressed by the EIMP within 48 hours of their discovery. Depending on the results of its analysis, the EIMP will:

- Implement a plan to correct the vulnerability;
- Document the reasons why no correction will be applied.

## 5.5 Data archiving

### *5.5.1 Types of data to be archived*

This archiving ensures the longevity of the logs created by the various components of the Service. It also allows for the preservation of paper documents related to certification operations, as well as their availability in case of need.

The data to be archived includes at least the following:

- Software (executables) and configuration files for IT equipment;
- Policies;
- Internal documentation;
- Receipts or notifications (for information purposes).

The EIMP has put in place the necessary measures to ensure that these archives are kept for the specified periods, even in the event of cessation of activity.

### *5.5.2 Archive retention period*

Information such as:

- Personnel;
- Traffic;
- Connection;
- Billing;

and resulting from an automatic data processing process is not archived for more than one year.

The archiving periods are as follows:

- Policy: lifetime of the EIMP;
- Organizational documents for key ceremonies: EIMP lifetime;
- Internal documentation: lifetime of the EIMP;

Other information such as:

- EIM application files;
- Event logs after they are generated;

are retained by the EIMP for five years after the expiration of the EIM.

### *5.5.3 Protection of archives*

Throughout their retention period, archives and their backups must:

- Be protected in terms of integrity;
- Be accessible to authorized persons;
- Be able to be read and used.

Internal documentation specifies the means used to archive documents securely.

### *5.5.4 Archive backup procedure*

The procedure is specified in the internal documentation.

The level of protection for backups must be at least equivalent to the level of protection for archives.

#### *5.5.5 Archive collection system*

Internal documentation specifies the means used to collect archives securely.

#### *5.5.6 Archive recovery and verification procedures*

Archives (paper and electronic) can be retrieved within two business days, provided that only the EIMP can access all archives (as opposed to an entity operating a component of the Service, which can only retrieve and consult the archives of the component in question).

The conditions for retrieving archives are specified in internal documentation.

### 5.6 Recovery following a compromise and/or disaster

#### *5.6.1 Incident and compromise reporting and handling procedures*

Each component of the Service implements procedures and means for reporting and handling incidents in accordance with the requirements of the EIMP Security Policy.

In the event of a major security incident or loss of integrity having a significant impact on its trusted service operations or personal data, the EIMP will notify the parties concerned, in particular the supervisory body and the CNIL, within 24 hours of identifying the incident, in accordance with the requirements of the eIDAS Regulation and, where applicable, the Clients affected.

#### *5.6.2 Recovery procedures in the event of corruption of IT resources (hardware, software, and/or data)*

In accordance with the Security Policy, the EIMP has implemented a business continuity plan to meet the availability requirements of its various functions, based on:

- This policy;
- Commitments in terms of service quality for the various components of the Service, particularly with regard to functions related to the publication and/or revocation of Certificates.

This plan is tested at least once every three (3) years.

#### *5.6.3 Recovery procedures in the event of compromise of a component's private key*

In the event of compromise of an algorithm, the EIMP will apply the above measures with the exception of the immediate revocation of all compromised EIM. The EIMP will schedule a planned revocation in accordance with the state of the art regarding the weaknesses of the compromised algorithm.

### *5.6.4 Business continuity capabilities following a disaster*

The various components of the Service have the reasonably necessary means to ensure the continuity of their activities in accordance with the requirements of this Policy.

The EIMP has an up-to-date business continuity plan in order to respond effectively in the event of a disaster and restore the system within the time frame specified in this plan.

## 5.7 End of life of the scheme

One or more components of the Service may be required to cease all or part of its activities, or to transfer them to another entity. In such cases, the EIMP has allocated the necessary resources. These are detailed in an up-to-date business cessation plan.

In the event of a cessation of activity, the EIMP or, if this is not possible, any entity that replaces it by virtue of a law, regulation, court decision, or agreement previously concluded with that entity, shall ensure the revocation of the EIM in accordance with the commitments made in its policy.

Before terminating its services, the EIMP must:

- inform the following persons: all Users and other entities with whom the EIMP has entered into contracts or has established other form of relationship, including the User Parties, competent authorities, and other Stakeholders;
- terminate the authorization of all subcontractors to act on behalf of the EIMP in the performance of any function related to the token issuance process;
- transfer obligations to a reliable party to maintain all information necessary to provide evidence of the EIMP's operation for a reasonable period of time, unless it can be demonstrated that the EIMP does not hold such information;
- destroy or withdraw from use the private keys, including backup copies, in such a way that the private keys cannot be recovered;
- to the extent possible, make arrangements to transfer the provision of trust services for its existing Users and Clients to another trust service provider.

The EIMP has made arrangements to cover the costs associated with meeting these minimum requirements if the EIMP goes bankrupt or, for other reasons, is unable to cover the costs itself, to the extent possible and within the limits of applicable bankruptcy law.

The EIMP must maintain or transfer to a reliable party its obligations to make its key or trusted service tokens available to the User Parties for a reasonable period of time.

# 6 TECHNICAL SECURITY MEASURES

## 6.1 Authentication function security

The authentication mechanism of the electronic identification means uses two factors from distinct categories:

- Possession of the phone on which the KIPMI mobile application instance is installed, initialized with user-specific secrets;
- Knowledge of the User's PIN code.

The authentication protocol uses a challenge generated by the authentication service, which is then sent to the user's phone for signing. The validation happens by signing and validating the signed challenge with the FIDO2 keypair generated on registration – first the user unlocks the FIDO2 private key with his PIN, then the challenge is signed with the private key and sent back to the authentication service. The authentication service has the FIDO2 public key (obtained during the registration process) and it uses it to validate the signed challenge. The necessary security controls are implemented so that it is highly unlikely that activities such as decryption attempts, eavesdropping, replay attacks, or communication manipulation by an attacker with moderate attack potential could compromise the authentication mechanisms.

The mobile application incorporates several security features, particularly against threats such as phone theft, compromise of encryption keys, secrets or brute force attacks:

- Secure PIN code management, including, for example, a secure virtual keyboard and a secure function for users to change their PIN code;
- Confidentiality of encryption keys and secrets used by the application throughout their entire lifecycle (generation, storage, use, destruction);

## 6.2 Security of distribution of identity attributes

Authentication of customer digital services

Signing of tokens

Token lifetime

Security level of components

## 6.3 IT system security measures

A minimum level of security assurance provided on the Service's IT systems is defined in the EIMP's internal documentation. In particular, it meets the following security objectives:

- Strong user identification and authentication for system access (two-factor authentication, physical and/or logical);
- Management of user rights (enabling the implementation of the access control policy defined by the EIMP, in particular to implement the principles of least privilege, multiple controls, and separation of roles);
- Management of user sessions (logout after a period of inactivity, access to files controlled by role and username);
- Protection against computer viruses and all forms of compromising or unauthorized software, and software updates;
- User account management, including rapid modification and deletion of access rights;
- Network protection against intrusion by unauthorized persons;
- Network protection to ensure the confidentiality and integrity of data transmitted over the network;
- Audit functions (non-repudiation and nature of actions performed);
- Possibly, error recovery management.

The protection of the confidentiality and integrity of private or secret infrastructure and control keys must be consistent with the Security Policy.

To achieve these security objectives, the EIMP uses reliable systems and products that enable the various Service processes to be implemented securely. Systems and products are selected and/or developed taking security requirements into account.

Monitoring devices (with automatic alarms) and procedures for auditing system settings are put in place. These devices enable:

- Detect, record, and respond as quickly as possible to unauthorized access or attempted access to Service resources;
- Monitor service usage and requests;
- Trigger alarms in the event of potential security breaches being detected;
- Monitor the activation or deactivation of trace generation functions;
- Monitor network availability and traffic.

Monitoring devices take into account the sensitivity of the information collected and analyzed. Monitoring of alerts related to critical security events is carried out by personnel in trusted roles. They ensure that incidents are analyzed and handled in accordance with established procedures.

## 6.4 System security measures during their lifecycle

### *6.4.1 Security measures related to system development*

The implementation of a system enabling a Service function to be carried out shall be documented.

The configuration of the Service components and any modifications and upgrades shall be documented. Change control procedures are implemented and applied to each modification (planned or urgent) to the information system or its configuration.

All development shall be consistent with the Security Policy and with the requirements contained in this policy.

### *6.4.2 Security management measures*

6.6.2.1. Components updates

Any significant change to a system of a Service component must be reported to the EIMP for validation. It must be documented.

In particular, the EIMP has specified and implemented procedures for managing security updates so that they are applied as soon as possible. In the event of the potential introduction of new vulnerabilities or a threat to the stability of the system, the EIMP will document the reasons for not applying a security update.

6.6.2.2. Risk analysis

The EIMP has carried out a risk analysis to identify, analyze, and assess the risks to l'IGC, taking into account technical and business risks. Following this risk analysis, the EIMP has selected and implemented risk treatment measures and associated operational procedures to ensure that the level of security is appropriate to the degree of risk.

The risk analysis is approved by the Service Manager, who thereby accepts the identified residual risk.

Risk treatment measures are described in the EIMP's internal documentation as well as in its ISSP.

This risk analysis is reviewed regularly, at least annually and whenever there is a significant change to a system or component of the Service.

6.6.2.1. Vulnerability scan

The EIMP regularly performs vulnerability scans on its public and private IP addresses. Each scan is performed by a qualified and independent person or entity.

6.6.2.1. Penetration testing

The EIMP performs intrusion tests when new infrastructure is implemented or when significant changes are made to a component. The EIMP keeps evidence of the tester's qualifications and independence.

## 6.5 Network security measures

### *6.5.1 Zone segmentation*

Based on the results of the risk analysis, the EIMP has segmented its network into separate zones (functionally, logically, or physically). Similar control measures are implemented for all elements within the same zone. Each system of the Service is operated in a secure network zone and is installed according to procedures and a configuration that ensure secure operation.

The most critical systems, such as the Root CAs, are operated in the most secure zones.

The EIMP has also implemented a strict separation between production systems and other systems (testing, qualification, etc.).

### *6.5.2 Interconnections*

Interconnection to public networks and interconnection between each network zone is protected by security gateways configured to accept only the protocols necessary for the component to function within the Service.

The EIMP ensures that local network components (e.g., routers) are maintained in a physically and logically secure environment.

In addition, exchanges between components within the Service are subject to the implementation of logically distinct secure channels that ensure the authentication of the data destination and the integrity and confidentiality of the data exchanged.

### *6.5.3 Connections*

Only personnel in trusted roles have access to secure network areas.

Any connection to an account that allows a certificate to be created directly is only possible after multi-factor authentication. The networks used to operate and administer the IGC are separate. The administration network is dedicated to this use.

All EIMP systems are configured to delete or disable accounts, applications, services, and ports that are not used for Service operations.

### *6.5.4 Availability*

In order to meet the availability requirements of its components, the EIMP has implemented redundancy measures to ensure high availability of critical services.

### 6.6 Time Stamping/Dating System

The dating systems are synchronized with a reliable source of universal time (UTC) and a time synchronization system (NTP) with an accuracy of at least one minute.

### 6.7 Personal data protection

The provision of EIM involves the processing of personal data within the meaning of Article 4-2 of the GDPR. As such, from the design of the electronic identification scheme onwards and by default, the EIMP complies with the essential principles of personal data protection set out in the requirements of the GDPR and Law No. 78-17 of January 6, 1978 on information technology, files, and civil liberties.

The minimum identity data that will be transmitted for each electronic identification of the person (as defined in the implementing regulation [2015/1501], in particular surname as it appears on the birth certificate, preferred name, if applicable, first names, sex, date and place of birth) are collected.

The processing of personal data, and more specifically of so-called "sensitive" data, is carried out in accordance with the GDPR. The applicant is informed of the processing carried out on the data collected in accordance with Articles 13 and 14 of the GDPR.

The collection of data other than that mentioned in this document is limited to what is strictly necessary for the purpose of processing for the issuance of the EIM.

The EIMP has implemented a Privacy Policy which can be consulted on the Service's website and on the mobile application.

# 7 OPERATIONAL REQUIREMENTS

To obtain and use EIM, the User must have a smartphone with an Internet connection, a valid email address, a phone number, and an identity document.

# 8 RISK MANAGEMENT

## 8.1 Risk analysis

Before launching the qualified service, the EIMP conducted a risk assessment to identify, analyze, and evaluate risks, taking into account technical, business, and commercial aspects. The risk analysis identifies, in particular, the "critical" systems of the service.

Security measures are taken based on the results of this analysis.

The EIMP sets out in its ISSP the security requirements and operational procedures necessary to implement the measures identified.

The risk analysis is reviewed and revised as necessary on an annual basis. It is also updated whenever there is a change that has a significant impact on the service, particularly in the event of a change in policies or practices relating to its provision.

The residual risks identified are explicitly accepted by the MIE service manager and submitted for approval by the C2SC and Management.

## 8.2 General information security policy

The EIMP has an information system security policy (ISSP) for the service, which defines the organization of information security. The ISSP covers the security measures and procedures applied to the service's physical and technical infrastructure and sensitive assets. The PSSI and all its developments are approved by BeYs management.

The ISSP is communicated to employees and any subcontractors, service providers, Clients of the Service, and assessment bodies.

The EIMP retains overall responsibility for compliance with the procedures set out in its ISSP, even when certain functions are performed by subcontractors. In particular, the EIMP ensures the effective implementation of the measures set out in the ISSP and includes audit clauses in its contractual relationships with third parties.

The ISSP establishes an inventory of information system assets. This inventory is reviewed regularly and whenever there is a significant change to the information system.

Any change that could have an impact on the level of security provided must be approved by the C2SC.

The information systems configuration is audited at least once a year to detect any changes that could lead to a breach of security policies.

## 8.3 Security Accreditation of the Service

Before being put into production, the EIMP carries out a security accreditation of its service. This accreditation enables the EIMP management to be informed of the security level of its service and that of its support systems and to explicitly accept the identified residual risks.

The accreditation decision is formally issued by the EIMP and reviewed prior to each renewal of its service qualification.

# 9 MANAGEMENT AND OPERATION

## 9.1 Internal organization

### *9.1.1 Reliability*

The EIMP shall establish a reliable organization structure for the delivery of the Service.

Responsibilities are defined within the organization to oversee the processes implemented for the provision and management of the Service, whether these are handled internally or by subcontractors. Subcontractors involved in the delivery of the Service are bound by contractual obligations that enable the EIMP to retain overall responsibility for the Service's compliance with this policy, in particular with regard to security and service quality requirements. The Service relies in particular on partners subject to obligations under the eIDAS Regulation, whose compliance with the requirements of the EIMP's Service is verified by the EIMP.

The practices implemented by the EIMP are non-discriminatory. The EIM service is accessible to any natural or legal person targeted by the service, provided that they comply with the obligations set out in this policy and in the declaration of practices. Support and dispute management procedures are defined in order to address requests or difficulties from Users or Stakeholders of the Service.

The EIMP has sufficient material, human, and financial resources to ensure the operation of the Service in accordance with this Policy, including the ability to cover the financial consequences of its liability resulting from damage that may be caused to Users.