Politique	
POLITIQUE DE SCHEMA D'IDENTIFICATION ELECTRONIQUE OID : [1.3.6.1.4.1.62466.87.1.1.3.1.0]	
Objet / Synthèse	POLITIQUE DE SCHEMA D'IDENTIFICATION ELECTRONIQUE

Niveau de diffusion	D3 – Diffusion libre
Liste de diffusion	Public
Localisation	BE YS TRUSTED SOLUTIONS FRANCE

Version	Date	Modifications	Rédacteur
1.0	14/04/2025	Création	Gergynia Kyoseva
1.1	03/06/2025	Ajout d'OID	Lidiya Ivanova
1.2	04/07/2025	Ajout de données d'immatrculation entité juridique	Lidiya Ivanova
1.3	16/10/2025	Ajout de Nom d'usage	Lidiya Ivanova
1.4	11/11/2025	Suspension non disponible sur Kipmi	Mihael Stoyanov
Date de péremption		2 ans	

Documents de Références

Libellé	Localisation ou insertion du document

Glossaire

Terme / Acronyme	Définition
ANSSI	Agence nationale de la sécurité des systèmes d'information
C2SC	Comité de suivi des services de confiance
CGU	Conditions générales d'utilisation
CSPN	Certification de Sécurité de Premier Niveau
CNIL	Commission nationale de l'informatique et des libertés
FIE	Fournisseur de Moyens d'identification électroniques
MIE	Moyen d'Identification Electronique
OID	Object Identifier
PVID	Prestataire de vérification d'identité à distance

Définitions

Terme	Définition
Application KIPMI	KIPMI est une application mobile faisant partie des services de confiance numérique de BE YS TRUSTED SOLUTIONS FRANCE, permettant d'accéder à différents services et de délivrer un Moyen d'identification électronique.
Application utilisatrice	Service applicatif, en ligne ou non, demandant l'identification électronique de ses utilisateurs via un Moyen d'identification électronique délivré par un FIE.
Authentification	Action de s'assurer de l'identité d'une personne physique ou morale ou de l'origine d'une communication.
Client	Entité cliente ayant décidé de souscrire au Service, qu'elle utilise pour ses propres besoins ou qu'elle met à disposition des utilisateurs.

Moyen d'identification électronique (MIE)	Elément matériel, et/ou immatériel, contenant des données d'identification personnelle et utilisé pour s'authentifier à un service en ligne. Le MIE délivré par BE YS TRUSTED SOLUTIONS FRANCE est intégré dans une application mobile nommée « KIPMI ». Le Moyen d'identification électronique est émis après une vérification initiale d'identité et sa durée de vie est comme définit dans cette Politique.
Politique de Schéma d'Identification Electronique	Ensemble de règles, identifié par un nom et un identifiant (OID), définissant les exigences auxquelles un FIE se conforme dans la mise en place et la fourniture de ses prestations. Une politique peut également, si nécessaire, identifier les obligations et exigences portant sur les autres intervenants, notamment les Utilisateurs et les Applications utilisatrices.
Service	Le service de délivrance et de gestion des Moyens d'identification électronique émis par BE YS TRUSTED SOLUTIONS FRANCE en tant que FIE.
Utilisateur	Personne physique, qui utilise le service certifié de délivrance de MIE offert par le FIE
Parties prenantes	Personne, machine ou service participant au processus de délivrance de MIE
Rôle de confiance	Personnes de confiance, formellement identifiées, qui participent à la réalisation des actions sensibles du service certifié

Validation

Relecteur	**Fonction (par rapport au document)**
Lidiya Ivanova	Responsable du service
Approbateur	**Fonction (par rapport au document)**
Younes El Gui	Président

Sommaire

1 INTRODUCTION

1.1 Présentation générale

Dans le cadre de ses offres de services de dématérialisation et de confiance, BE YS TRUSTED SOLUTIONS FRANCE met à disposition de ses Clients son Service. BE YS TRUSTED SOLUTIONS FRANCE agit en tant que Fournisseur de moyens d'identification électronique (FIE) pour le compte des Utilisateurs des services de ses Clients.

Le présent document constitue la Politique de Schéma d'Identification Electronique (PSIE) de BE YS TRUSTED SOLUTIONS FRANCE en tant que FIE pour la délivrance aux Utilisateurs de Moyens d'identification électronique (MIE) de niveau de garantie substantiel au titre du règlement eIDAS.

L'objectif de la présente Politique est de définir les exigences concernant les Moyens d'identification électronique dans toutes les phases de leur cycle de vie, ainsi que d'exposer les engagements attendus de la part des différentes Parties prenantes du Service.

Le schéma d'identification électronique mis en œuvre est conforme aux spécifications techniques et procédures minimales définies, pour le niveau substantiel, par :

- Règlement (UE) no 910/2014 du Parlement Européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, modifié par Règlement (UE) 2024/1183 du Parlement européen et du Conseil du 11 avril 2024 modifiant le règlement (UE) n° 910/2014 en ce qui concerne l'établissement du cadre européen relatif à une identité numérique ;
- Règlement d'exécution (UE) 2015/1501 de la Commission du 8 septembre 2015 ;
- Règlement d'exécution (UE) 2015/1502 de la Commission du 8 septembre 2015 ;
- Référentiel d'exigences de sécurité pour les moyens d'identification électronique version 1.2. du 11 août 2022 de l'ANSSI ;
- ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers;
- ETSI EN 319 411-1 General requirements ;

Les Moyens d'identification électronique permettent, entre autres, à l'Utilisateur de s'identifier et de s'authentifier auprès d'une Application utilisatrice partenaire du FIE qui délègue au Service cette identification électronique. Les Moyens d'identification électronique sont destinés à des personnes physiques agissant à titre particulier.

1.2 Identification du Fournisseur des MIE

Le Fournisseur des Moyens d'Identification Electronique, responsable du Service et des Moyens d'Identification Electronique, est la société suivante :

BE YS TRUSTED SOLUTIONS FRANCE
10 Boulevard Haussmann 75009 PARIS
Adresse de contact : kipmi.customer.service@be-ys.com
Site Web : https://www.kipmi.com/

1.3 Politique de schema d'identification electronique

Ce document représente la Politique de schéma d'identification électronique (Politique) du FIE. Il décrit l'ensemble de règles définissant les exigences auxquelles le FIE se conforme, ainsi que les normes qu'il applique dans la mise en place et la fourniture du Service.

La Politique identifie également les mesures de sécurité, les obligations et les exigences portant sur les autres intervenants, notamment les Utilisateurs et les Clients et fait partie indissociable des CGU.

Ce document a été élaboré en conformité avec le Règlement (UE) 2016/679 (RGPD), ainsi que la législation française applicable. La Politique est publique et peut être modifiée par le FIE à tout moment.

1.4 Identification du document

La présente Politique est identifiée par le numéro d'identification d'objet (OID) suivant : [1.3.6.1.4.1.62466.87.1.1.3.1.0]

1.5 Date d'entrée en vigueur

La Politique entre en vigueur après approbation par le C2SC du FIE et à la date fixée par ce Comité. La Politique est publiée sur le site web https://www.kipmi.com/ au moins 72h avant sa date d'entrée en vigueur.

1.6 Durée et fin anticipée de validité de la Politique

Le présent document reste en vigueur jusqu'à la publication d'une nouvelle version.

1.7 Gestion de la Politique

1.7.1 Entité gérant la Politique

La présente Politique est gérée par les membres du C2SC du FIE.

1.7.2 Point de contact

Le point de contact pour toute question à propos de la Politique est :

- Adresse postale : BE YS TRUSTED SOLUTIONS FRANCE
  Service VID
- 10 Boulevard Haussmann75009 PARIS Adresse électronique : [kipmi.customer.service@be-ys.com]

1.7.3 Procédure d'approbation de la Politique

La Politique est approuvée par le C2SC après examen et relecture du document par les membres du Comité, et par les personnes désignées par celui-ci.

Cette relecture a pour objectif d'assurer :

- La conformité de la Politique avec les exigences réglementaires et normatives portant sur la fourniture du service certifié ;
- La cohérence de la Politique avec les autres documents publiés dans le cadre du service, tels par exemple que les Conditions Générales d'Utilisation ;
- La concordance entre les engagements exprimés dans la Politique et les moyens techniques et organisationnels mis en œuvre par le Prestataire et ses partenaires ;
- L'information effective de l'organe de contrôle pour toute modification importante dans la fourniture du Service selon les modalités décrites dans les procédures de certification. Cela comprend notamment, sans s'y limiter :
  - Les changements induits par une modification de la Politique de service ou des Conditions Générales d'Utilisation associées ;
  - Les modifications des conditions d'hébergement ;
  - Les changements de matériels cryptographiques ;
  - Les modifications d'architecture technique ;
  - Les changements de procédures de délivrance, réémission, révocation, suspension ou réactivation des MIE ;
  - Les changements dans la gouvernance du Service.

Le C2SC s'assure que la date d'entrée en vigueur de la nouvelle Politique laisse, dans la mesure du possible, un délai suffisant aux Clients pour prendre connaissance des nouvelles dispositions et adapter si besoin leurs pratiques.

1.8 Informations publiées

1.8.1 Entités chargés de la mise à disposition des informations

Le Prestataire assure la publication d'informations à destination des Clients et des Utilisateurs sur son site web : https://www.kipmi.com/

1.8.2 Informations devant être publiées

Le Prestataire s'engage à publier au minimum les informations suivantes :

- Le présent document, décrivant la Politique de schéma d'identification électronique ;
- Les CGU du Service ;
- Les points de publication des informations associées aux services des partenaires.

1.8.3 Délais et fréquences de publication

Les informations liées au Service (évolutions, nouvelle version de la Politique, etc.) sont publiées dès que nécessaire, afin que soit assurée à tout moment la cohérence entre les informations publiées et les engagements, moyens et procédures effectifs du Prestataire.

Le point de publication des informations est disponible 24h/7/365(6).

1.8.4 Contrôle d'accès aux informations publiées

L'ensemble des informations publiées est en accès libre en lecture et est consultable ici : https://www.kipmi.com/

L'accès en modification aux systèmes de publication des autres informations est strictement limité aux fonctions internes habilitées du FIE. Ces personnes sont définies dans des rôles de confiance et disposent d'un moyen d'authentification forte pour se connecter sur les systèmes de publication.

1.9 Amendement du document

1.9.1 Procédure de mise à jour

Le FIE contrôle que tout projet de modification de sa Politique reste conforme aux exigences réglementaires et normatives applicables. Le C2SC intervient toujours en validation des éventuels amendements. Toute demande de changement est donc mise à l'ordre du jour d'un comité futur et la prise de décision est attestée dans le compte rendu correspondant.

Toute proposition d'évolution du Service fait l'objet d'une analyse d'impact afin de déterminer son éventuelle incidence, sur :

- La qualité ou la sécurité du Service ;
- La conformité de l'offre certifiée aux exigences de l'ANSSI ;
- La nécessité de mise à jour des autres documents publiés ;

- Les pratiques internes du FIE ou de ses partenaires et fournisseurs.

1.9.2 Circonstances selon lesquelles la Politique doit être changée

Des amendements à la présente Politique peuvent être prévus au cours de la durée de vie du Service, par exemple pour :

- Des corrections mineures (erreurs, précisions supplémentaires…) ;
- Des évolutions ou extensions du service ;
- L'acceptation ou la mise en œuvre de nouveaux moyens d'identification électronique ;
- Des changements d'ordre technique (mise en œuvre, partenaires, fournisseurs, etc…) ;
- Des corrections induites par les audits du Service.

1.9.3 Circonstances selon lesquelles l'OID doit être changé

En cas d'impact majeur, un changement d'OID de Politique est prévu, et l'évolution et son analyse d'impact sont soumises à l'organe de contrôle et à l'organisme d'évaluation de la conformité pour avis ou commentaire.

L'analyse d'impact est étudiée par le C2SC qui valide ou non le lancement d'une évolution. Le cas échéant, la nouvelle Politique sera soumise à l'approbation du C2SC.

1.9.4 Entrée en vigueur de la Politique amendée

La date d'entrée en vigueur de la nouvelle version du document est déterminée par le C2SC dans sa décision de validation tenant compte de la nature et de la complexité des modifications et, le cas échéant, du temps nécessaire aux parties prenantes dans le Service de mettre en œuvre les adaptations y liées.

1.9.5 Mécanisme et période d'information sur les amendements

Une fois l'évolution du Service validée par le C2SC, la nouvelle Politique est communiquée :

- Sans délai au personnel du Prestataire et à toutes les parties prenantes dans la fourniture du Service - par envoi par messagerie. Le délai leur permettant de prendre connaissance des nouvelles dispositions et d'adapter (si besoin) leurs pratiques et procédures, ainsi que la date d'entrée en vigueur, sont explicitement indiqués.
- Au moins 72h (soixante-douze heures) avant sa date d'entrée en vigueur - aux Clients et Utilisateurs - par publication sur le site web : https://www.kipmi.com/

Le FIE adresse annuellement à l'organe de contrôle une synthèse de l'ensemble des modifications apportées à la fourniture de son Service.

2 DOCUMENTS ASSOCIES

2.1 Conditions générales d'utilisation

Les CGU applicables (et leurs version antérieures) sont disponibles sur le site du FIE : https://www.kipmi.com/ et sur l'application KIPMI

2.2 Documents normatifs

Renvoi	Document
[EIDAS]	Règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur https://www.eur-lex.europa.eu
[ANSSI_MIE]	Référentiel d'exigences pour les moyens d'identification électroniques Référentiel Général de Sécuritéhttps://cyber.gouv.fr/sites/default/files/document/20220811_np_anssi_eidas_eid-referentielexigences_v1.2.pdf
[HYGIENE]	Guide d'hygiène informatique https://cyber.gouv.fr/publications/guide-dhygiene-informatique
[CERT_SERV_PROC ESS]	Processus de certification d'un service https://www.ssi.gouv.fr/
[RGPD]	https://www.cnil.fr/fr/reglement-europeen-protection-donnees
[EN_319_401]	ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers https://www.etsi.org/
[EN_319_411-1]	ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; https://www.etsi.org/
[2015/1501]	Règlement d'exécution (UE) 2015/1501 de la commission du 8

	septembre 2015 sur le cadre d'interopérabilité visé à l'article 12, paragraphe 8, du règlement (UE) no 910/2014. https://eur-lex.europa.eu/
[2015/1502]	Règlement d'exécution (UE) 2015/1502 de la commission du 8 septembre 2015 fixant les spécifications techniques et procédures minimales relatives aux niveaux de garantie des moyens d'identification électronique visés à l'article 8, paragraphe 3, du règlement (UE) no 910/2014 https://eur-lex.europa.eu/

3 PARTIES PRENANTES ET OBLIGATIONS

3.1 Fournisseur des MIE

Le FIE est le responsable du Service et assure la fonction de gestion des MIE. Il garantit la mise en œuvre et le contrôle des différentes fonctions nécessaires à la fourniture du Service.

Le FIE a mis en place une organisation établie et pleinement opérationnelle à tous les égards pertinents pour la fourniture du Service. Le FIE maintient en particulier un système de gestion de la sécurité de l'information efficace pour la gestion et le contrôle des risques de sécurité de l'information. Le FIE est responsable de l'exécution de toute tâche sous-traitée à une autre entité, ainsi que du respect de la politique du schéma, comme s'ils s'étaient acquittés eux-mêmes de leur mission.

Le FIE respecte toute exigence légale qui lui incombe dans le cadre du fonctionnement et de l'exécution du Service, y compris les types d'informations pouvant être recherchés, la façon dont la preuve d'identité est établie, le type d'informations pouvant être conservées et leur durée de conservation.

3.2 Prestataire de vérification d'identité à distance

Le PVID est une entité qui fournit un service de vérification des données d'identification des Utilisateurs par un face-à-face à distance (par opposition à un face-à-face physique).

Le Service recourt exclusivement, dans le cadre de sa fonction d'enregistrement des Utilisateurs, à des PVID certifiés au niveau de garantie substantiel ou élevé par l'ANSSI, selon le référentiel. A ce titre, le PVID garantit la fiabilité de son service, constitue et conserve un dossier de preuve pour chaque vérification effectuée, et rapporte de façon régulière au FIE des métriques relatives au fonctionnement de son service.

3.3 Utilisateurs

L'Utilisateur, porteur ou demandeur d'un MIE, ne peut être qu'une personne physique, à laquelle est remis un MIE après contrôle de son identité. Le Service ne gère pas de lien entre l'Utilisateur et des personnes morales dans le cadre des données d'identification du MIE. L'Utilisateur déclare avoir pris connaissance et accepte les CGU de l'Application KIPMI.

L'Utilisateur utilise son MIE pour s'identifier et s'authentifier auprès des Parties utilisatrices qui délèguent au Service cette identification électronique.

3.4 Applications utilisatrices

Les Applications utilisatrices sont des services numériques, en ligne ou non, gérées par des Parties Utilisatrices, qui doivent identifier (connaître les attributs d'identité tels que nom et prénom etc.) et authentifier (s'assurer que l'utilisateur est réellement celui désigné par les attributs d'identité) leurs utilisateurs de manière fiable, et qui délèguent cette identification électronique au Service.

Pour ce faire, l'application utilisatrice demande à la fonction d'identification électronique du Service d'effectuer une identification électronique en recourant au MIE que son utilisateur doit avoir obtenu au préalable.

Le responsable d'une Application utilisatrice doit s'assurer que le niveau de garantie apporté par le Service convient aux exigences portant sur son application.

3.5 Parties utilisatrices

Partie utilisatrice est une personne physique ou morale qui se fie à une identification électronique. Dans le cadre de l'Application KIPMI l'Utilisateur a la possibilité partager des documents et des attributs avec des Parties Utilisatrice qui le demandent. Des Parties utilisatrices peuvent être l'employeur de l'Utilisateur, des banques, des sociétés d'assurance, organisations gouvernementales, opérateurs de téléphonie mobile, etc. Les Parties Utilisatrices sont des Clients du FIE et font confiance au Service pour établir des relations commerciales, professionnelles, administratives et autres ou pour effectuer diverses opérations ou transactions.

4 EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES MIE

4.1 Décomposition fonctionnelle du Service et caracteristiques

La décomposition fonctionnelle du Service retenue dans ce document est la suivante :

- **Fonction de gestion des MIE** : Cette fonction assure la gestion globale du cycle de vie du MIE. Elle s'appuie sur les fonctions d'enregistrement des Utilisateurs, de délivrance et révocation des MIE et gère aussi le réémission et l'expiration des MIE, ainsi que l'utilisation du MIE par la fonction d'identification électronique ;
- **Fonction d'enregistrement des Utilisateurs** : Cette fonction vérifie les informations d'identité du futur Utilisateur d'un MIE avant que celui-ci ne puisse obtenir un MIE. Elle est sollicitée dans le cadre de la délivrance initiale d'un MIE à un nouvel Utilisateur, mais aussi dans le cadre de réactivation du MIE ou après la fin de vie du précédent MIE d'un Utilisateur ;
- **Fonction de délivrance des MIE** : Cette fonction initialise et délivre un MIE à un Utilisateur qui a été auparavant enregistré avec succès. Cette phase intègre la génération d'éléments de cryptographie de l'Utilisateur et leur mise en œuvre sécurisée dans le MIE de l'Utilisateur. L'Utilisateur choisit son d'activation PIN et crée son compte ;
- **Fonction de révocation des MIE** : Cette fonction traite les demandes de révocation des MIE, afin de déterminer les actions à mener et le cas échéant mettre fin à la validité du MIE ;
- **Fonction d'identification électronique** : Cette fonction diffuse et partage les informations d'identité d'un Utilisateur à des Parties Utilisatrices qui l'ont sollicitée, après identification et authentification de l'Utilisateur par usage de son MIE, et vérification de validité du MIE.

Le MIE est conçu de sorte qu'il est utilisé uniquement sous le contrôle de la personne à laquelle il appartient ou en sa possession.

Les moyens de cryptologie constitutifs du MIE doivent au minimum faire l'objet d'une qualification au niveau élémentaire du [RGS] reposant sur une Certification de Sécurité de Premier Niveau (CSPN), sur la base d'une cible de sécurité validée par l'ANSSI.

4.2 Enregistrement et demande de MIE

Pour utiliser le Service l'Utilisateur doit télécharger l'Application KIPMI sur son smartphone. Lors de la première ouverture de l'Application KIPMI par l'Utilisateur, l'Utilisateur passe par le processus d'enregistrement qui se compose de plusieurs étapes :

- Création de compte
- Vérification d'identité
- Délivrance de MIE

Pour création de compte l'Utilisateur indique :

- Son adresse e-mail
- Son prénom, son nom
- Numéro de téléphone

Par la suite l'Utilisateur doit accepter les conditions générales d'utilisation de l'Application KIPMI, et cliquer sur le bouton « *S'inscrire*». Afin de créer son compte, l'Utilisateur doit configurer un code PIN lors de son inscription. Le code PIN est composé de 6 chiffres et est conseillé de suivre les recommandations ci-dessous :

- Ne pas inclure de chiffres répétés (par exemple, 111111)
- Ne pas inclure de chiffres séquentiels (par exemple, 123456 ou 654321)

Une fois le code PIN créé, l'Utilisateur doit valider son adresse e-mail et son numéro de téléphone. L'Utilisateur vérifie l'adresse e-mail à l'aide du code à 6 chiffres envoyé à son adresse e-mail. Le numéro de téléphone est vérifié au moyen d'un code à 6 chiffres envoyé par SMS au numéro de téléphone fourni par l'Utilisateur.

4.3 Preuve et vérification d'identité pour des personnes physiques

Avant de se voir délivrer un MIE, l'Utilisateur doit faire vérifier son identité par un service de vérification d'identité à distance certifié par un prestataire de vérification d'identité à distance (PVID) de niveau de garantie substantiel a minima. L'Utilisateur doit présenter une pièce d'identité officielle et valide, et son visage sera comparé à la photo qui y figure. A l'issue d'un verdict positif de ce service de vérification, les attributs d'identité suivants sont associés au compte créé et considérés fiables avec un niveau de garantie substantiel :

- Nom ;
- Prénoms ;
- Date de naissance ;
- Lieu de naissance (ville ou pays lorsque la personne n'est pas née en France) ;
- Genre.

Une demande de délivrance d'un MIE à l'Utilisateur est alors automatiquement lancée.

4.4 Délivrance du MIE

Une fois la vérification d'identité réussie, l'Utilisateur disposera de 72 heures pour activer son compte en validant les informations d'identification vérifiées extraites de la pièce d'identité qui a été utilisée pour la vérification.

Si un compte n'est pas activé en acceptant les informations d'identification dans le délai de 72 heures, l'Utilisateur est tenu de repasser par le processus de vérification d'identité.

En cas d'échec de la vérification d'identité, l'Utilisateur est informé et invité à recommencer le processus. Il n'y a pas de limite au nombre de fois que l'utilisateur peut essayer de vérifier son identité.

La délivrance d'un MIE est réalisée à l'activation du compte, après révocation d'un précédent MIE.

Une notification dans l'Application KIPMI informe l'Utilisateur du succès de la délivrance de son MIE sur le téléphone utilisé.

Un MIE est valide pendant la durée de validité du document d'identité utilisé pour sa délivrance, sans toutefois pouvoir excéder cinq ans. Il doit être réémis avant cette échéance, faute de quoi il expirera.

4.5 Usage du MIE

L'usage d'un MIE est restreint à l'identification électronique de son Utilisateur sur la fonction d'identification électronique du Service. **Tout autre usage est interdit.**

4.5.1 Usage de MIE pour identification électronique demandée par une Application Utilisatrice

L'identification électronique de l'Utilisateur est demandée par une Application Utilisatrice (y compris le Service lui-même). Cette Application Utilisatrice affiche un QR code qui demande les informations nécessaires à l'authentification de l'Utilisateur. L'Utilisateur ouvre son application mobile KIPMI. L'Utilisateur s'authentifie sur son application mobile à l'aide de son code PIN. L'Utilisateur scanne le QR code. L'Application mobile KIPMI demande à l'Utilisateur de confirmer le partage des données personnelles demandées par l'Application Utilisateur. L'Utilisateur accepte (ou refuse) de fournir les données. Dès acceptation, KIPMI partage les données de l'Utilisateur avec l'Application Utilisatrice. Cela permet à l'Utilisateur, par exemple, d'accéder aux services de cette application ou de valider une opération sur celle-ci.

L'Utilisateur doit s'assurer que l'authentification est demandée par une application légitime, et si ce n'est pas le cas, ne pas saisir son code PIN et signaler cet incident au Service.

4.5.2 Usage de MIE pour l'identification électronique demandée par les systèmes de l'entreprise ayant une intégration directe avec l'application KIPMI

L'identification électronique de l'Utilisateur peut aussi être demandée par les Parties Utilisatrices qui ont une intégration directe avec l'Application KIPMI. Dans ce cas, l'Utilisateur reçoit une notification dans l'application contenant des informations sur la personne morale qui demande son identification électronique. L'Utilisateur a la possibilité de décider d'accepter ou de refuser la demande. Pour accepter ou refuser la demande, l'Utilisateur doit s'authentifier à l'aide de son code PIN.

4.5.3 Usage de MIE pour le partage de documents

MIE peut être utilisé pour le partage de documents entre les Utilisateurs et les Parties Utilisatrices. L'Application KIPMI a une fonctionnalité permettant aux Utilisateurs qui sont également membres de l'espace de l'organisation de recevoir des demandes de partage de documents de la part des organisations dont ils sont membres. L'Utilisateur a la possibilité de décider d'accepter ou de refuser la demande. Pour accepter ou refuser la demande, l'Utilisateur doit s'authentifier à l'aide de son code PIN.

4.5.4 Usage de MIE pour le partage d'attributs

L'Application KIPMI offre la fonctionnalité de partage d'attributs d'identité tel que définis par le règlement eIDAS 2 entre les Utilisateurs et les Parties Utilisatrices. L'Utilisateur a la possibilité de décider d'accepter ou de refuser la demande de partage d'attributs. Pour accepter ou refuser la demande, l'utilisateur doit s'authentifier à l'aide de son code PIN.

4.6 Révocation ou suspension du MIE

La révocation d'un MIE peut être demandée par l'Utilisateur lui-même (après la perte ou le vol de son téléphone ou de sa carte d'identité par exemple) sur l'Application KIPMI ou bien directement par le FIE en adressant une demande via email à kipmi.customer.service@be-ys.com.

L'application KIPMI ne prend pas en charge la suspension du MIE.

4.6.1 Demande de révocation par l'Utilisateur depuis l'appication KIPMI

L'Utilisateur peut demander la révocation de son MIE depuis l'application mobile KIPMI, après authentification avec son code PIN.

La fonction de révocation sur l'application KIPMI est disponible 24h/24 et 7j/7. Toute demande de révocation d'un MIE est traitée dans un délai de 24 heures. Ce délai commence à la réception de la demande et se termine par la mise à disposition d'informations sur la révocation à des tiers.

La révocation interdit toute utilisation ultérieure de MIE. L'Utilisateur peut demander un nouvel MIE à la suite d'une révocation, dans les mêmes conditions que pour une demande initiale.

4.6.2 Demande de révocation par le FIE

La révocation d'un MIE peut être décidée par le FIE dans les cas suivants :

- L'Utilisateur n'a pas ou ne respecte plus les conditions générales d'utilisation ;
- Une erreur (intentionnelle ou non) a été détectée dans le dossier d'inscription ;
- Le MIE ou les données d'activation associées sont suspectées d'être compromises, sont compromises, sont perdues ou volées ;
- L'Utilisateur est décédé ;
- L'Utilisateur a déposé une plainte pour usurpation d'identité.

Sur la base d'une décision validée, un administrateur s'authentifie sur le service, recherche le MIE de l'Utilisateur concerné et le révoque.

4.6.3 Réémission du MIE

Afin de réémettre son MIE, l'Utilisateur doit passer par la procédure de vérification d'identité.

4.7 Réémission du MIE

La réémission du MIE consiste à demander un MIE lorsque l'Utilisateur dispose déjà d'un MIE valide qui n'est ni expiré ni révoqué. Dans le cas contraire, il s'agit d'une nouvelle demande et elle est traitée comme une demande initiale.

La réémission peut être demandé par l'Utilisateur ou proposé par le Service.

Le Service envoie automatiquement une notification aux Utilisateurs dont le MIE arrive prochainement à expiration. Lorsqu'il le souhaite, et avant l'expiration définitive de son MIE, l'Utilisateur ouvre l'application KIPMI sur son mobile et s'authentifie par la saisie de son code PIN confidentiel.

Si la pièce d'identité enregistrée lors de la précédente délivrance de MIE n'est plus valide, l'Utilisateur doit refaire le parcours PVID.

Après authentification de l'Utilisateur et potentielle préalable vérification d'identité, l'application KIPMI initie la réémission du MIE. Elle génère de nouveaux éléments cryptographiques et demande au à l'Utilisateur de définir un code PIN confidentiel.

L'application informe le client du succès de la réémission.

Le précédent MIE sur le même appareil, est révoqué.

5 MESURES DE SECURITE NON TECHNIQUES

5.1 Mesures de sécurité physique

Le FIE s'engage à mettre en œuvre et maintenir le niveau de sécurité physique exigé pour les locaux d'exploitation des composantes du Service.

5.1.1 Situation géographique et construction des sites

En fonction de la sensibilité des composants du Service, les sites sont définis au niveau 1 de la politique de sécurité : impact vital (majeur pour l'entreprise). A ce titre, la mise en sécurité du site du bâtiment respecte les mesures de sécurité physique de niveau 1 pour la protection périphérique, périmétrique et intérieure et notamment les mesures relatives à :

- L'alimentation électrique et la climatisation ;
- La vulnérabilité aux dégâts des eaux ;
- La prévention et la protection incendie.

Les mesures permettent également de respecter les engagements pris dans la politique ou dans les engagements contractuels avec les Clients du Service, en matière de disponibilité des services.

5.1.2 Accès physique

Afin d'éviter toute perte, dommage et compromission des ressources du FIE, les accès aux locaux sont contrôlés conformément au niveau de zonage des locaux de niveau 1 : « accès très restreint ».

Pour les fonctions de délivrance du MIE de l'Utilisateur, l'accès est strictement limité aux seules personnes nominativement autorisées à pénétrer dans les locaux et la traçabilité des accès est assurée. En dehors des heures ouvrables, la sécurité est renforcée par la mise en œuvre de moyens de détection d'intrusion physique et logique. De plus, le contrôle en entrée et en sortie est permanent en heures non ouvrées (HNO).

Chaque entrée et sortie dans la zone sécurisée fait l'objet d'une surveillance indépendante et d'une traçabilité. Tout personnel non-autorisé doit obligatoirement être accompagné d'une personne autorisée.

Afin d'assurer la disponibilité des systèmes, l'accès aux machines est limité aux seules personnes autorisées à effectuer des opérations nécessitant l'accès physique aux machines. Pour cela, les composantes concernées du Service définissent un périmètre de sécurité physique où sont

installées ces machines. Tout local utilisé en commun entre la composante concernée et une autre composante (de ou hors du Service) est en dehors de ce périmètre de sécurité.

L'ouverture de la porte est commandée par un système de contrôle d'accès.

5.1.3 Alimentation électrique et climatisation

Les caractéristiques des équipements d'alimentation électrique et de climatisation permettent de respecter les conditions d'usage des équipements du FIE telles que fixées par leurs fournisseurs.

Elles respectent également les exigences du cahier des charges fourni par le prestataire des services, en matière de disponibilité de ses fonctions, notamment la fonction de gestion des révocations.

5.1.4 Vulnérabilité aux dégâts des eaux

Les moyens de protection mis en place par le FIE permettent de protéger son infrastructure contre les dégâts des eaux.

5.1.5 Prévention et protection incendie

Le FIE met en places des moyens de protection et de lutte contre les incendies.

5.1.6 Conservation des supports

Les supports (papier, disque dur, disquette, CD, etc.) utilisés au sein du FIE sont traités et conservés conformément aux besoins de sécurité définis pour les actifs sensibles (en confidentialité, intégrité et disponibilité). En particulier, les supports font l'objet de mesures contre les dommages, le vol, les accès non autorisés et l'obsolescence. Ces mesures s'appliquent durant toute la période de rétention du contenu de ces supports.

5.1.7 Mise hors service des supports

En fin de vie, les supports seront, soit détruits, soit réinitialisés en vue d'une réutilisation, en fonction du niveau de confidentialité des informations correspondantes.

Les procédures et moyens de destruction et de réinitialisation sont conformes à la Politique de Sécurité de FIE.

5.1.8 Sauvegarde hors site

En complément de sauvegardes sur sites, les composantes du Service mettent en œuvre des sauvegardes hors sites de leurs applications et de leurs informations. Ces sauvegardes sont organisées de façon à assurer une reprise des services après incident la plus rapide possible.

Les sauvegardes sont testées régulièrement.

5.2 Mesures de sécurité procédurales

Les mesures de sécurité procédurales ci-après complètent celles définies dans le cadre de la Cérémonie des Clés, cérémonie au cours de laquelle est créée la biclé utilisée par FIE.

Les procédures et politiques de sécurité sont communiquées aux employés suivant le besoin d'en connaître.

Des procédures sont établies et appliquées pour toutes les opérations des personnels en rôle de confiance pouvant impacter la fourniture du service.

5.2.1 Rôles de confiance

Les rôles de confiance définis ci-dessous sont ceux requis pour les composantes du Service, indépendamment des rôles de confiance définis dans le cadre de la cérémonie des clés.

- **Officier de Sécurité du Service** : L'Officier de Sécurité est chargé de la mise en œuvre de la politique de sécurité du Service. Il gère les contrôles d'accès physiques aux équipements des systèmes de l'entité. Il est chargé de l'analyse des journaux d'événements afin de détecter tout incident, anomalie, tentative de compromission, etc.
- **Responsable applicatif** : Le responsable d'application est chargé, au sein de la composante du Service concernée, de la mise en œuvre des différentes politiques du FIE. Sa responsabilité couvre l'ensemble des fonctions rendues par les applications et des performances correspondantes.
- **Responsable compliance et conformité** : Le responsable compliance est la personne en charge d'assurer le bon respect des exigences fonctionnelles et techniques du règlement ANSSI et règlementations européennes de portefeuille numérique (eIDAS et eIDAS2).
- **Ingénieur système** : Il est chargé de la mise en route, de la configuration et de la maintenance technique des équipements informatiques de l'entité. Il assure l'administration technique des systèmes et des réseaux de l'entité. Il est également chargé des opérations de restauration.
- **Opérateur** : Un opérateur au sein de la composante du Service concernée réalise, dans le cadre de ses attributions, l'exploitation des applications pour les services délivrés par la composante du Service.
- **Contrôleur** : Personne désignée par le responsable de la composante du Service et dont le rôle est de procéder de manière régulière à des contrôles de conformité de la mise en œuvre des services fournis par la composante du Service par rapport aux politiques du FIE.

- **Opérateur de révocation** : Personne responsable de l'application de la procédure de révocation des MIE.

5.2.2 Nombre de personnes requises par tâches

La documentation interne précise quelles sont les opérations nécessitant l'intervention de plusieurs personnes et quelles sont les contraintes que ces personnes doivent respecter (positions dans l'organisation, liens hiérarchiques, etc.), en particulier, les personnes requises pour la cérémonie des clés.

5.2.3 Identification et authentification pour chaque rôle

Chaque entité opérant une composante du Service fait vérifier l'identité et les autorisations de tout membre de son personnel avant de lui attribuer un rôle et les droits correspondants, notamment :

- Que son nom soit ajouté aux listes de contrôle d'accès aux locaux de l'entité hébergeant les systèmes concernés par le rôle ;
- Que son nom soit ajouté à la liste des personnes autorisées à accéder physiquement à ces systèmes ;
- Qu'un compte soit ouvert à son nom dans ces systèmes ;
- Eventuellement, que des clés cryptographiques et/ou un certificat lui soient délivrés pour accomplir le rôle qui lui est dévolu dans le Service.

Ces contrôles sont décrits dans la documentation interne et sont conformes à la Politique de Sécurité de FIE.

5.2.4 Rôles exigeant une séparation des attributions

Plusieurs rôles peuvent être attribués à une même personne, dans la mesure où le cumul ne compromet pas la sécurité des services offerts.

Les attributions associées à chaque rôle sont décrites dans la documentation interne du FIE et sont conformes à la Politique de Sécurité.

Pour les différents rôles de confiance, il est recommandé qu'une même personne ne détienne pas plusieurs rôles et les cumuls suivants sont interdits :

- Officier de sécurité et ingénieur système / opérateur ;
- Ingénieur système et opérateur.

5.3 Mesures de sécurité vis-à-vis du personnel

Les mesures de sécurité procédurales ci-après complètent celles définies dans le cadre de la Cérémonie des Clés, cérémonie au cours de laquelle est créée la Bi-clé du FIE.

5.3.1 Qualifications, compétences et habilitations requises

Tous les personnels amenés à travailler au sein de composantes du Service sont soumis à une clause de confidentialité.

Le responsable du FIE doit s'assurer que les attributions de ses personnels, amenés à travailler au sein du Service, correspondent à leurs compétences professionnelles.

Le personnel d'encadrement doit posséder l'expertise appropriée à son rôle et être familier des procédures de sécurité en vigueur au sein du Service, ainsi que des mesures de protection des données personnelles.

Le FIE doit informer toute personne intervenant dans des rôles de confiance du Service :

- De ses responsabilités relatives aux services du Service,
- Des procédures liées à la sécurité du système et au contrôle du personnel, auxquelles elle doit se conformer.

Cette nomination est réalisée de façon formelle par le responsable de la sécurité du FIE et est acceptée par écrit par la personne nommée dans un rôle de confiance.

Les qualifications, compétences et habilitations requises pour la cérémonie des clés sont définies dans une procédure spécifique.

Les responsabilités des personnels dans les rôles de confiance sont attribuées de façon à séparer les rôles et responsabilité, éviter les conflits d'intérêt et réduire les opportunités de modification ou de mauvaise utilisation, volontaire ou involontaire, des systèmes du Service.

Les accès et habilitation sont attribués et configurés suivant la politique du moindre privilège.

5.3.2 Procédures de vérificaion des antécédents

Les personnels amenés à travailler au sein d'une composante du Service, et en fonction du contexte applicable, sont amenés à remettre une attestation sur l'honneur de non-condamnation, un extrait de casier judiciaire, ou un engagement de confidentialité.

Les personnes disposant d'un rôle de confiance ne doivent pas souffrir de conflit d'intérêts préjudiciables à l'impartialité de leurs tâches.

5.3.3 Exigences en matière de formation initiale

Le personnel est préalablement formé aux logiciels, matériels et procédures internes de fonctionnement et de sécurité qu'il met en œuvre et qu'il doit respecter, au sein de la composante du Service dans laquelle il opère.

Les personnels ont connaissance et comprennent les implications des opérations dont ils ont la responsabilité.

5.3.4 Exigences et fréquence en matière de formation continue

Le personnel concerné reçoit une information et une formation adéquate préalablement à toute évolution dans les systèmes, les procédures, l'organisation, etc. en fonction de la nature de ces évolutions.

De plus, la formation continue inclut une formation annuelle aux nouvelles menaces et aux procédures de sécurité appliquées.

5.3.5 Sanctions en cas d'actions non autorisées

Des sanctions appropriées sont appliquées au personnel qui ne respecterait pas les procédures et politiques de sécurité applicables.

La présente politique ne prévoit pas d'exigences spécifiques à ce sujet. Des précisions peuvent être apportées dans la documentation interne.

5.3.6 Exigences vis-à-vis du personnel des prestataires externes

Le personnel des prestataires externes intervenant dans les locaux du FIE et/ou sur les composantes du Service respecte également les exigences de la présente Politique et de la Politique de Sécurité.

Ceci doit être traduit en clauses adéquates dans les contrats concernés avec les prestataires.

5.3.7 Documentation fournie au personnel

Chaque personnel dispose au minimum de la documentation adéquate concernant les procédures opérationnelles et les outils spécifiques qu'il met en œuvre ainsi que les politiques et pratiques générales de la composante au sein de laquelle il travaille, plus spécifiquement de la Politique de Sécurité l'impactant.

5.4 Procédures de constitution des données d'audit

La journalisation d'événements consiste à enregistrer des événements sous forme électronique par saisie ou par génération automatique.

Les fichiers résultants, sous forme électronique, doivent rendre possible la traçabilité et l'imputabilité des opérations effectuées.

5.4.1 Type d'événements à enregistrer

Chaque entité opérant une composante du Service journalise au minimum les événements suivants, automatiquement dès le démarrage d'un système et sous forme électronique :

- Création / modification / suppression de comptes utilisateur (droits d'accès) et des données d'authentification correspondantes (mots de passe, certificats, etc.) ;
- Démarrage et arrêt des systèmes informatiques et des applications,
- Evénements liés à la journalisation : démarrage et arrêt de la fonction de journalisation, modification des paramètres de journalisation, actions prises suite à une défaillance de la fonction de journalisation,
- Connexion / déconnexion des Utilisateurs ayant des rôles de confiance, et les tentatives non réussies correspondantes.

D'autres événements sont aussi recueillis, par des moyens électroniques ou manuels. Ce sont ceux concernant la sécurité et qui ne sont pas produits automatiquement par les systèmes informatiques, notamment :

- Les accès physiques ;
- Les actions de maintenance et de changements de la configuration des systèmes ;
- Les changements apportés au personnel ;
- Les actions de destruction et de réinitialisation des supports contenant des informations confidentielles (clés, données d'activation, renseignements personnels sur les Utilisateurs...) ;
- La réception d'une demande de MIE (initiale et réémission) ;
- La validation ou le rejet d'une demande de MIE ;
- Les évènements liés à la gestion des matériels cryptographiques sensibles et des clés qu'ils mettent en œuvre (génération (cérémonie des clés), sauvegarde / récupération, révocation, réémission, destruction...) ;
- Le cas échéant, la génération des éléments secrets de l'utilisateur (bi-clé, codes d'activation...) ou publics (certificats...) ;
- La transmission des MIE aux Utilisateurs et, selon les cas, les acceptations ou rejets explicites par les Utilisateurs ;
- Le cas échéant, la remise de son MIE à l'Utilisateur ;
- La publication et mise à jour des CGU ou autres documents publiés par l'entité responsable du schéma d'identification électronique ;
- La réception d'une demande de révocation ;
- La validation ou le rejet d'une demande de révocation ;
- La génération et la publication des LCR (et éventuellement des deltaLCR) ou des requêtes / réponses OCSP.

Chaque enregistrement d'un événement dans un journal contient, lorsque cela est applicable, les champs suivants :

- Type de l'événement,
- Nom de l'exécutant ou référence du système déclenchant l'événement,

- Date et heure de l'événement,
- Résultat de l'événement (échec ou réussite).

L'imputabilité d'une action revient à la personne, à l'organisme ou au système l'ayant exécutée. Le nom ou l'identifiant de l'exécutant figure explicitement dans l'un des champs du journal d'événements. De plus, en fonction du type de l'événement, chaque enregistrement contient également les champs suivants :

- Demandeur et destinataire de l'opération (dans la mesure du possible),
- L'opération ou référence du système effectuant la demande,
- Nom des personnes présentes (s'il s'agit d'une opération nécessitant plusieurs personnes),
- Cause de l'événement,
- Toute information caractérisant l'événement (par exemple, pour la génération d'un Certificat, le numéro de série de ce Certificat).

Les opérations de journalisation sont effectuées au cours du processus. En cas de saisie manuelle, l'écriture se fait, sauf exception, le même jour ouvré que l'événement.

5.4.2 Fréquence de traitement des journaux d'événements

Les journaux d'événements du Service sont analysés en moyenne 2 à 3 fois chaque semaine.

De plus, les journaux d'événements font l'objet d'analyses automatiques permettant d'identifier des activités anormales et alerter les personnels de l'occurrence potentielle d'événements critiques de sécurité.

5.4.3 Période de conservation des journaux d'événements

Les journaux d'événements sont conservés sur site pendant au moins un mois. Les journaux sont conservés et archivées pour la durée nécessaire dans le cadre de la Législation en vigueur, même en cas de cessation d'activité du Service.

5.4.4 Protection de sauvegarde des journaux d'événements

Le FIE met en œuvre une protection des journaux d'événements adaptée au niveau de sensibilité des informations contenues dans ces journaux. Ce niveau de sensibilité est issu d'une analyse de risque.

5.4.5 Procédure de sauvegarde des journaux d'événements

Le FIE met en œuvre un processus de sauvegarde des journaux d'événements adapté au niveau de sensibilité des informations contenues dans ces journaux. Ce niveau de sensibilité est issu d'une analyse de risque.

5.4.6 Système de collecte des journaux d'événements

Le FIE met en œuvre un système de journalisation des événements qui intègre une datation.

5.4.7 Notification de l'enregistrement d'un événement au responsable de l'événement

La présente politique ne prévoit pas d'exigences spécifiques à ce sujet. Des précisions peuvent être apportées dans la documentation interne du FIE.

5.4.8 Evaluation des vulnérabilités

Le FIE met en œuvre une gestion des vulnérabilités de systèmes du FIE en conformité avec la Politique de Sécurité du FIE.

Les journaux d'événements sont contrôlés régulièrement selon des modalités définies dans le paragraphe 3.4.2.

Les journaux sont analysés dès la détection d'une anomalie. Cette analyse donne lieu à un résumé dans lequel les éléments importants sont identifiés, analysés et expliqués. Le résumé fait apparaître les anomalies et les falsifications constatées. Toute vulnérabilité critique est adressée par le FIE dans une période de 48 heures après sa découverte. Selon le résultat de son analyse, le FIEs :

- Mettra en place un plan de correction de la vulnérabilité ;
- Documentera les raisons pour lesquelles aucune correction ne sera appliquée.

5.5 Archivage des données

5.5.1 Types de données à archiver

Cet archivage permet d'assurer la pérennité des journaux constitués par les différentes composantes du Service. Il permet également la conservation des pièces papier liées aux opérations de certification, ainsi que leur disponibilité en cas de nécessité.

Les données à archiver sont au moins les suivantes :

- Les logiciels (exécutables) et les fichiers de configuration des équipements informatiques ;
- Les politiques ;

- Les documentations internes ;
- Les récépissés ou notifications (à titre informatif).

Le FIE a mis en place les mesures nécessaires pour que ces archives soient conservées sur les durées mentionnées même en cas d'arrêt d'activité.

5.5.2 Période de conservation des archives

Les informations de type :

- Personnel ;
- Trafic ;
- Connexion ;
- Facturation ;

et issue d'un processus automatique de traitement de données, n'est pas archivée pendant plus d'un an.

Les durées d'archivage sont les suivantes :

- La politique : durée de vie du FIE ;
- Les documents organisationnels de cérémonies des clés : durée de vie du FIE ;
- La documentation interne : durée de vie du FIE ;

Les autres informations tels que :

- Les dossiers de demande de MIE ;
- Les journaux d'événements après leur génération ;

sont conservées par le FIE pour cinq ans après expiration des MIE.

5.5.3 Protection des archives

Pendant tout le temps de leur conservation, les archives, et leurs sauvegardes, doivent :

- Être protégées en intégrité ;
- Être accessibles aux personnes autorisées ;
- Pouvoir être relues et exploitées.

La documentation interne précise les moyens mis en œuvre pour archiver les pièces en toute sécurité.

5.5.4 Procédure de sauvegarde des archives

La procédure est précisée dans la documentation interne.

Le niveau de protection des sauvegardes doit être au moins équivalent au niveau de protection des archives.

5.5.5 Système de collecte des archives

La documentation interne précise les moyens mis en œuvre pour collecter les archives en toute sécurité.

5.5.6 Procédures de récupération et de vérification des archives

Les archives (papier et électroniques) sont récupérables dans un délai inférieur à 2 jours ouvrés, étant précisé que seul le FIE peut accéder à toutes les archives (par opposition à une entité opérant une composante du Service qui ne peut récupérer et consulter que les archives de la composante considérée).

Les conditions de récupération des archives sont précisées dans la documentation interne.

5.6 Reprise suite à une compromission et/ou un sinistre

5.6.1 Procédures de remontée et de traitement des incidents et des compromissions

Chaque composante du Service met en œuvre des procédures et des moyens de remontée et de traitement des incidents conformément aux exigences de la Politique de Sécurité du FIE.

En cas d'incident majeur de sécurité ou de perte d'intégrité ayant un impact important sur ses opérations de service de confiance ou sur les données personnelles, le FIE notifiera les parties concernées, en particulier l'organe de contrôle et la CNIL, dans les 24 heures après l'identification de l'incident, conformément aux exigences du Règlement eIDAS et, le cas échéant, les clients impactés.

5.6.2 Procédures de reprise en cas de corruption des ressources informatiques (matériels, logiciels et/ou données)

Conformément à la Politique de Sécurité, le FIE dispose d'un plan de continuité d'activité permettant de répondre aux exigences de disponibilité de ses différentes fonctions, et découlant :

- De la présente politique ;
- Des engagements en termes de qualité de service des différentes composantes du Service, notamment pour ce qui concerne les fonctions liées à la publication et / ou liées à la révocation des Certificats.

Ce plan est testé au minimum une fois tous les trois (3) ans.

5.6.3 Procédures de reprise en cas de compromission de la clé privée d'une composante

En cas de compromission d'un algorithme, le FIE appliquera les mesures ci-dessus à l'exception de la révocation immédiate de tous les MIE compromis. Le FIE programmera une révocation programmée en adéquation avec l'état de l'art sur les faiblesses de l'algorithme compromis.

5.6.4 Capacités de continuité d'activités à la suite d'un sinistre

Les différentes composantes du Service disposent des moyens raisonnablement nécessaires permettant d'assurer la continuité de leurs activités en conformité avec les exigences de la présente Politique.

Le FIE dispose d'un plan de continuité d'activité à jour afin de réagir efficacement en cas de désastre et de restaurer le système dans les délais précisé dans ce plan.

5.7 Fin de vie du schéma

Une ou plusieurs composantes du Service peut être amenée à cesser son activité, en tout ou partie, ou à la transférer à une autre entité. Dans ces cas, le FIE a provisionné les moyens nécessaires. Ces derniers sont décrits dans un plan de cessation de l'activité tenu à jour.

Dans l'hypothèse d'une cessation d'activité, le FIE ou, en cas d'impossibilité, toute entité qui lui serait substituée par l'effet d'une loi, d'un règlement, d'une décision de justice ou bien d'une convention antérieurement conclue avec cette entité, assure la révocation des MIE conformément aux engagements pris dans sa politique.

Avant de mettre fin à ses services, le FIE doit :

- informer les personnes suivantes : tous les Utilisateurs et autres entités avec lesquels le FIE a conclu des contrats ou une autre forme de relations établies, entre lesquelles les Parties utilisatrices, les autorités compétentes et les autres parties prenantes ;
- mettre fin à l'autorisation de tous les sous-traitants pour agir au nom du FIE dans l'exécution de toute fonction liée au processus de délivrance des jetons ;
- transférer les obligations à une partie fiable pour maintenir toutes les informations nécessaires pour fournir une preuve du fonctionnement du FIE pendant une période raisonnable, à moins qu'il ne puisse être démontré que le FIE ne détient pas de telles informations ;
- détruire ou retirées de l'utilisation les clés privées, y compris les copies de sauvegarde, de manière à ce que les clés privées ne puissent pas être récupérées ;
- dans la mesure du possible, prendre des dispositions pour transférer la prestation de services de confiance pour ses Utilisateurs et Clients existants à un autre prestataire de services de confiance

Le FIE a pris des dispositions pour couvrir les coûts liés au respect de ces exigences minimales si le FIE fait faillite ou, pour d'autres raisons, n'est pas en mesure de couvrir les coûts par lui-même, dans la mesure du possible et dans les limites de la législation applicable en matière de faillite.

Le FIE doit maintenir ou transférer à une partie fiable ses obligations de mettre à la disposition sa clé ou ses jetons de service de confiance aux Parties utilisatrices pendant une période raisonnable.

6 MESURES DE SECURITE TECHNIQUES

6.1 Sécurité de la fonction d'authentification

Le mécanisme d'authentification du moyen d'identification électronique utilise deux facteurs de catégories distinctes :

- La possession du téléphone sur lequel est installée l'instance de l'application mobile KIPMI, initialisée avec des secrets propres à l'utilisateur ;
- La connaissance du code PIN de l'Utilisateur.

Le protocole d'authentification utilise un défi généré par le service d'authentification, lequel est ensuite envoyé au téléphone de l'utilisateur pour signature. La validation s'effectue en signant et en validant le défi signé à l'aide de la paire de clés FIDO2 générée lors de l'inscription : l'utilisateur déverrouille d'abord la clé privée FIDO2 avec son code PIN, puis le défi est signé avec cette clé privée et renvoyé au service d'authentification. Le service d'authentification possède la clé publique FIDO2 (obtenue lors de l'inscription) et l'utilise pour valider le défi signé. Les contrôles de sécurité nécessaires sont mis en œuvre afin de rendre extrêmement improbable toute tentative de décryptage, d'écoute clandestine, d'attaque par rejeu ou de manipulation des communications par un attaquant aux capacités techniques modérées, susceptible de compromettre les mécanismes d'authentification

L'application mobile intègre plusieurs fonctions de sécurité notamment contre les menaces de vol du téléphone, de compromission des secrets ou d'attaque par force brute :

- Gestion sécurisée du code PIN, intégrant par exemple un clavier virtuel sécurisé et une fonction sécurisée de changement de code PIN par l'utilisateur ;
- Confidentialité des secrets utilisés par l'application sur l'ensemble de leur cycle de vie (génération, stockage, utilisation, destruction) ;

6.2 Sécurité de la diffusion des attributs d'identité

Authentification des services numériques clients

Signature des jetons

Durée de vie des jetons

Niveau de sécurité des composantes

6.3 Mesures de sécurité des systèmes informatiques

Un niveau minimal d'assurance de la sécurité offerte sur les systèmes informatiques du Service est défini dans la documentation interne du FIE. Il répond en particulier aux objectifs de sécurité suivants :

- Identification et authentification forte des Utilisateurs pour l'accès au système (authentification à deux facteurs, de nature physique et/ou logique) ;
- Gestion des droits des Utilisateurs (permettant de mettre en œuvre la politique de contrôle d'accès définie par le FIE, notamment pour implémenter les principes de moindres privilèges, de contrôles multiples et de séparation des rôles) ;
- Gestion de sessions d'utilisation (déconnexion après un temps d'inactivité, accès aux fichiers contrôlé par rôle et nom d'utilisateur) ;
- Protection contre les virus informatiques et toutes formes de logiciels compromettants ou non-autorisés et mises à jour des logiciels ;
- Gestion des comptes des Utilisateurs, notamment la modification et la suppression rapide des droits d'accès ;
- Protection du réseau contre toute intrusion d'une personne non autorisée ;
- Protection du réseau afin d'assurer la confidentialité et l'intégrité des données qui y transitent ;
- Fonctions d'audits (non-répudiation et nature des actions effectuées) ;
- Eventuellement, gestion des reprises sur erreur.

La protection en confidentialité et en intégrité des clés privées ou secrètes d'infrastructure et de contrôle doit être cohérente avec la Politique de Sécurité.

Pour atteindre ces objectifs de sécurité, le FIE utilise des systèmes et des produits fiables permettant de mettre en œuvre de façon sécurisé les différents processus du Service. Les systèmes et produits sont choisis et/ou développé en prenant en compte les exigences de sécurité.

Des dispositifs de surveillance (avec alarme automatique) et des procédures d'audit des paramétrages du système sont mis en place. Ces dispositifs permettent :

- De détecter, enregistrer et réagir dans les meilleurs délais à un accès ou une tentative d'accès non autorisée aux ressources du Service ;
- De surveiller l'usage du service et les requêtes ;
- De déclencher des alarmes en cas de détection de potentielles violations des mesures de sécurité ;
- De surveiller l'activation ou la désactivation des fonctions de génération de traces ;
- De surveiller la disponibilité et le trafic réseau.

Les dispositifs de surveillance prennent en compte la sensitivité de l'information collectée et analysée. Le suivi des alertes sur les événements critiques de sécurité est assuré par des personnels en rôle de confiance. Ces derniers s'assurent que les incidents sont analysés et sont traités suivant les procédures en places.

6.4 Mesures de sécurité des systèmes durant leur cycle de vie

6.4.1 Mesures de sécurité liées au développement des systèmes

L'implémentation d'un système permettant de mettre en œuvre une fonction du Service est documentée.

La configuration du système des composantes du Service ainsi que toute modification et mise à niveau sont documentées. Des procédures de contrôle des changements sont mises en œuvre et appliquées à chaque modification (planifiée ou urgente) du système d'information ou de sa configuration.

Tout développement doit être cohérent avec la Politique de Sécurité et avec les exigences contenues dans la présente politique.

6.4.2 Mesures liées à la gestion de la sécurité

6.6.2.1. Mise à jour des composantes

Toute évolution significative d'un système d'une composante du Service doit être signalée au FIE pour validation. Elle doit être documentée.

En particulier, le FIE a spécifié et mis-en place des procédures de gestion des mises-à-jour de sécurité, afin que celles-ci soient appliquées dans les meilleurs délais. En cas d'introduction potentielle de nouvelles vulnérabilités ou de mise en danger de la stabilité du système, le FIE documentera les raisons de non-application d'une mise à jour de sécurité.

6.6.2.2. Analyse de risque

Le FIE a réalisé une analyse de risque pour identifier, analyser et évaluer les risques pesant sur l'IGC en prenant en compte les risques techniques et métier. À la suite de cette analyse de risque, le FIE a sélectionné et mis en œuvre des mesures de traitement du risque et les procédures opérationnelles associées, de telle façon que le niveau de sécurité soit approprié vis-à-vis du degré de risque.

L'analyse de risque est approuvée par le Responsable du Service qui accepte, par cette approbation, le risque résiduel identifié.

Les mesures de traitement du risque sont décrites dans la documentation interne du FIE ainsi que dans sa PSSI.

Cette analyse de risque est revue régulièrement, a minima annuellement et lors de toute évolution significative d'un système ou d'une composante du Service.

6.6.2.1. Scan de vulnérabilité

Le FIE réalise régulièrement des scans de vulnérabilité sur ses adresses IP publiques et privées. Chaque scan est réalisé par une personne ou une entité qualifiée et indépendante.

6.6.2.1. Test d'intrusion

Le FIE réalise des tests d'intrusion lors de la mise en place de nouvelles infrastructures ou lors de modification significatives d'une composante. Le FIE garde des éléments de preuves de la qualification et de l'indépendance du testeur.

6.5 Mesures de sécurité réseau

6.5.1 Segmentation en zone

Fondé sur les résultats de l'analyse de risque, le FIE a segmenté son réseau en zone séparées (fonctionnellement, logiquement ou physiquement). Des mesures de contrôle similaire sont mis-e-place pour l'ensemble des éléments d'une même zone. Chaque système du Service est exploité dans une zone réseau sécurisée et est installé suivant des procédures et une configuration assurant une exploitation sécurisée.

Les systèmes les plus critiques, tels que les AC Racines, sont opérés dans les zones les plus sécurisées.

Le FIE a également mis en place une séparation stricte entre les systèmes de production et les autres systèmes (test, qualification, …).

6.5.2 Interconnexions

L'interconnexion vers des réseaux publics ainsi que l'interconnexion entre chaque zone réseau est protégée par des passerelles de sécurité configurées pour n'accepter que les protocoles nécessaires au fonctionnement de la composante au sein du Service.

Le FIE garantit que les composants du réseau local (routeurs, par exemple) sont maintenus dans un environnement physiquement et logiquement sécurisé.

De plus, les échanges entre composantes au sein du Service font l'objet de la mise en place de canaux sécurisés logiquement distincts et permettant d'assurer l'authentification de la destination des données et d'assurer l'intégrité et la confidentialité des données échangées.

6.5.3 Connexions

Seuls les personnels en rôle de confiance ont accès aux zones réseaux sécurisées.

Toute connexion d'un compte permettant de créer directement un certificat n'est possible qu'après une authentification multi-facteur. Les réseaux permettant d'opérer et d'administré l'IGC sont séparés. Le réseau d'administration est dédié à cet usage.

Tous les systèmes du FIE sont configurés de façon à supprimer ou désactivé les comptes, applications, services et ports qui ne sont pas utilisés pour les opérations du Service.

6.5.4 Disponibilité

Afin de répondre aux besoins de disponibilité de ses composantes, le FIE a mis en place des mesures de redondances permettant d'offrir une haute disponibilité des services critiques.

6.6 Horodatage / Système de datation

Les systèmes de datation sont synchronisés par rapport à une source fiable du temps universel (UTC) et un système de synchronisation temporelle (NTP) avec une précision au moins égale à une minute.

6.7 Protection des données personnelles

La fourniture de MIE suppose un traitement de données à caractère personnel au sens de l'article 4-2 du RGPD. A ce titre, le FIE respecte, dès la conception du schéma d'identification électronique et par défaut, les principes essentiels en matière de protection des données à caractère personnel rappelés dans les exigences du RGPD et de la Loi no 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Les données d'identité minimales qui seront transmises à chaque identification électronique de la personne (telles que définies dans le règlement d'exécution [2015/1501], notamment nom de famille tel qu'il résulte de l'acte de naissance, nom d'usage le cas échéant, prénoms, sexe, date et lieu de naissance) sont recueillies.

Le traitement des données à caractère personnel, et plus particulièrement pour des données dites « sensibles », est effectué en application du règlement RGPD. Le demandeur est informé des traitements réalisés sur les données recueillies conformément aux articles 13 et 14 du RGPD.

La collecte de données autres que celles mentionnées dans le présent document est limitée au strict nécessaire au regard de la finalité du traitement permettant la délivrance du MIE.

Le FIE a mis en place une Politique de confidentialité qui peut être consultée sur le site du Service et sur l'application mobile

7 EXIGENCES OPERATIONNELLES

Pour obtenir et utiliser MIE, l'Utilisateur doit disposer d'un smartphone avec une connexion Internet, d'une adresse e-mail valide, d'un numéro de téléphone et un titre d'identité.

8 GESTION DES RISQUES

8.1 Analyse des risques

Avant le lancement du service qualifié, le FIE a effectué une évaluation des risques afin d'identifier, d'analyser et d'évaluer les risques, en tenant compte des aspects techniques, métiers et commerciaux. L'analyse de risques identifie, en particulier, les systèmes « critiques » du service.

Les mesures de sécurité sont prises en tenant compte du résultat de cette analyse.

Le FIE fixe, dans sa PSSI, les exigences de sécurité et les procédures opérationnelles nécessaires pour mettre en œuvre les mesures identifiées.

L'analyse de risques est examinée, et révisée si besoin, annuellement. Elle est aussi mise à jour à chaque modification ayant un impact important sur le service, notamment en cas de modification des politiques ou pratiques relatives à sa fourniture.

Les risques résiduels identifiés sont acceptés explicitement par le responsable du service MIE et soumis à approbation du C2SC et de la Direction.

8.2 Politique générale de la sécurité de l'information

Le FIE dispose d'une politique de sécurité du système d'information (PSSI) du service, qui définit l'organisation de la sécurité de l'information. La PSSI couvre les mesures de sécurité et les procédures appliquées concernant les infrastructures physiques et techniques et les biens sensibles du Service. La PSSI et toutes ses évolutions sont approuvées par la direction de BeYs.

La PSSI est communiquée aux employés et aux éventuels sous-traitants, aux prestataires, aux clients du Service, aux organismes d'évaluation.

Le FIE conserve la responsabilité globale de la conformité avec les procédures prévues dans sa PSSI, même lorsque certaines fonctions sont mises en œuvre par des sous-traitants. En particulier, le FIE s'assure de la mise en œuvre effective des mesures prévues dans la PSSI et prévoie des clauses d'audit dans ses relations contractuelles avec des tiers.

La PSSI établit un inventaire des actifs du système d'information. Cet inventaire est revu régulièrement et à l'occasion de toute modification sensible du système d'information.

Tout changement susceptible d'avoir un impact sur le niveau de sécurité fourni doit être approuvé par le C2SC.

La configuration du SI est auditée à minima chaque année afin de détecter tout changement pouvant être à l'origine d'une violation des politiques de sécurité.

8.3 Homologation de sécurité du service

Avant sa mise en production le FIE procède à l'homologation de sécurité de son service. Cette homologation permet à la direction du FIE d'avoir connaissance du niveau de sécurité de son service et des systèmes en support et d'accepter explicitement les risques résiduels.

La décision d'homologation est établie formellement par le FIE et cette décision est revue avant chaque renouvellement de qualification de son service.

9 GESTION ET EXPLOITATION

9.1 Organisation interne

9.1.1 Fiabilité

Le FIE met en place une organisation fiable pour la délivrance du Service.

Des responsabilités sont définies en son sein pour piloter les processus définis pour la fourniture et la gestion du Service, que ceux-ci soient pris en charge en interne ou par des sous-traitants. Les sous-traitants du Prestataire prenant part à la fourniture du service sont soumis à des obligations contractuelles permettant au FIE d'assumer la responsabilité globale de conformité du Service à cette politique, en particulier concernant les exigences de sécurité et de qualité de service. Le service repose en particulier sur des partenaires soumis à des obligations au titre du règlement eIDAS, dont le Prestataire s'assure de l'adéquation avec les exigences de son propre Service.

Les pratiques mises en œuvre par le FIE sont non-discriminatoires. Le service MIE est accessible à toute personne morale ou physique ciblée par le service, à la condition que celles-ci respectent les obligations qui leur sont données par la présente politique et déclaration de pratiques. Des procédures de support et de gestion des différends sont définies afin de répondre aux sollicitations ou difficultés des Utilisateurs ou parties prenantes du service.

Le FIE dispose des moyens matériels, humains et financiers suffisants pour assurer l'exploitation du Service conformément à cette Politique, y compris pour couvrir les conséquences financières de sa responsabilité résultant de dommages qui pourraient être causés aux Utilisateurs.