Politique de schéma d'identification électronique

ChamberSign France

Objet du document :	Ce document décrit le Service d'Identification Electronique proposé par ChamberSign France et les exigences que respecte Chambersign France dans le cadre de cette activité de Fournisseur d'Identité Electronique.
Version	04
Date de diffusion	18/04/2025
Type de diffusion	Public

Service Juridique
Signature numérique de Service Juridique
Date : 2025.07.02 18:47:03 +02'00'

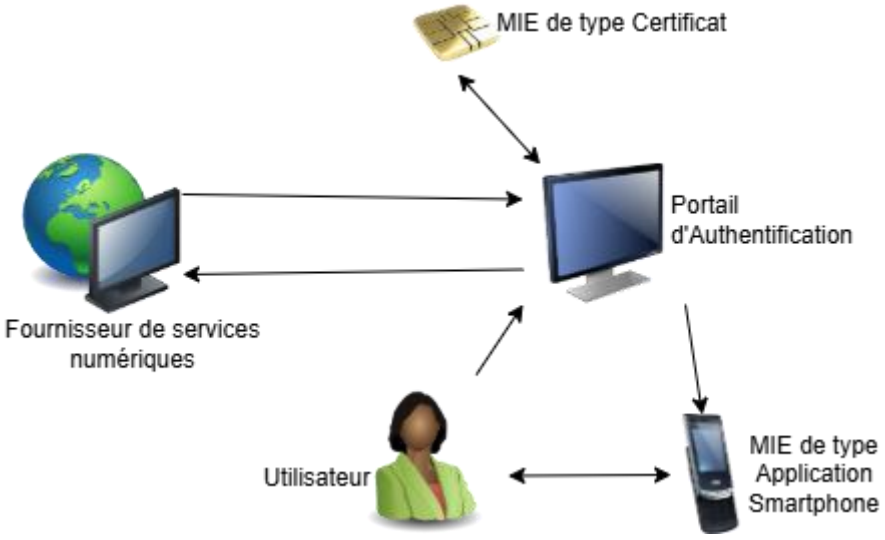
SOMMAIRE

Avertissement

1. Introduction

1.1. *Présentation générale*

Le présent document constitue la politique du schéma d'identification électronique (ci-après « Politique, Politique de Service ou PSIE ») proposé par ChamberSign France CA3 (ci-après dénommée « ChamberSign »). Un Portail Sécurisé d'Authentification Multi-Identités (ci-après « PSAMI ») utilisant différents moyens d'identification électronique (ci-après dénommés « MIE ») constitue ce schéma.
Ci-dessous le mécanisme présentant l'utilisation des MIE sur smartphone ou par certificat :



Les moyens d'identification électronique (MIE) objets de la présente Politique sont mis à la disposition par l'AC ChamberSign France CA3au niveau de garantie faible défini par le règlement eIDAS et proposés à la certification au niveau de garantie substantiel auprès de l'ANSSI au titre du référentiel d'exigences de sécurité des moyens d'identification électronique et dès lors devenir un Fournisseur de MIE. Plus précisément, le schéma d'identification électronique proposé par ChamberSign est conforme au 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 du Parlement européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et de l'article L.102 IV du code des postes et des communications électroniques.

Le Service d'identité électronique ChamberSign implémente cette Politique de schéma d'identification électronique, en y intégrant en particulier la gestion de ces MIE (enregistrement, délivrance, renouvellement, révocation…) ainsi que le PSAMI mis à disposition des Utilisateurs de ces MIE.

L'objectif de la présente Politique est de définir les engagements de ChamberSign relatifs au Service d'identité électronique.

Cette Politique constitue le fondement des relations du Service d'identité électronique avec les tiers : utilisateurs (Utilisateurs des MIE et abonnés), mais également les Fournisseurs de Services Numériques, les partenaires, autorités publiques et organismes privés d'évaluation et de reconnaissance (qualification, référencement, etc.). Elle est complétée par les CGUV des MIE pour les Utilisateurs et par un contrat avec les Fournisseurs de Services Numériques.

Les engagements arrêtés dans la présente Politique correspondent :

- aux exigences imposées à ChamberSign par la réglementation en vigueur ;
- aux objectifs que se fixent ChamberSign en matière de services, de sécurité, de qualité et de performances afin de satisfaire les Utilisateurs de ses MIE et du PSAMI et d'être reconnue, si nécessaire, par les différents schémas d'évaluation / référencement en matière d'identification électronique au niveau français et européen.

La présente Politique est un document public. Les documents qui en découlent sont des documents internes, confidentiels et sous le contrôle de ChamberSign, qui peuvent être accessibles, si besoin, sur demande motivée et moyennant un accord de confidentialité (auditeurs externes, organismes de qualification, autorités publiques, etc.). Cette Politique est complétée par les CGU du Service d'Identité Numérique Professionnelle ainsi que les CGUV de chacun des MIE proposé aux Utilisateurs dans le cadre du Service.

ChamberSign est assujettie aux lois et règlements en vigueur en France.

1.2. *Identification*

La présente Politique est identifiée par son numéro de version.

1.3. *Entités intervenant dans le Service*

Il est distingué les intervenants externes au Service et les intervenants internes au Service. Seuls les intervenants internes sont sous la responsabilité de ChamberSign.

Les intervenants internes réalisent la mise en œuvre des fonctions suivantes :

- **Fonction d'enregistrement des Utilisateurs de MIE** - Cette fonction vérifie les informations d'identification du Demandeur (futur Utilisateur d'un MIE), ainsi qu'éventuellement d'autres attributs professionnels spécifiques, avant de transmettre la demande correspondante à la fonction de délivrance du MIE. Cette fonction a également en charge, lorsque cela est nécessaire, la re-vérification des informations de l'Utilisateur lors du renouvellement du MIE de celui-ci. La fonction d'enregistrement peut intervenir postérieurement à l'enregistrement initial de la personne physique pour gérer des attributs spécifiques ou de nouvelles relations entre l'Utilisateur et une personne morale.
- **Fonction de délivrance du MIE -** Cette fonction intègre la préparation du MIE, la génération d'éléments secrets du Demandeur et la remise au Demandeur du moyen d'identification électronique en face à face. Le Demandeur deviendra alors un Utilisateur du MIE.
- **Fonction de publication** - Cette fonction met à disposition des différentes parties concernées les conditions générales, politiques et pratiques publiées par ChamberSign ainsi que les états de validité d'un MIE sous une forme fonction du type de MIE.
- **Fonction de gestion des révocations** - Cette fonction traite les demandes de révocation des MIE et des attributs professionnels d'un Utilisateur et détermine les actions à mener.
- **Fonction d'identification électronique** - Cette fonction authentifie puis identifie un Utilisateur par l'utilisation de son MIE sur le PSAMI, et renvoie le résultat de cette opération au Fournisseur de Service Numérique qui l'a demandée au Service.

Les intervenants externes sont :

- **Autorités publiques** – Il s'agit d'entités administratives ou gouvernementales qui peuvent être amenées, en conformité avec les lois et règlementations applicables, à accéder à tout ou partie des systèmes et informations du Service ;

- **Client –** désigne l'Entité qui contracte avec ChamberSign France pour faire bénéficier d'un MIE ses collaborateurs, clients ou partenaires. Toute obligation applicable au Client s'applique également à son Représentant Légal et à l'Utilisateur du MIE ;
- **Entités d'audit / de qualification/certification / de référencement** – Ces entités sont amenées à auditer tout ou partie du Service, soit à la demande d'un client de ChamberSign, soit à la demande de ChamberSign (en vue de l'obtention d'une qualification/certification ou d'un label), soit à la demande d'autorités publiques ;
- **Représentant légal** – Il s'agit d'une personne physique chargée de représenter légalement le Client personne morale auquel l'Utilisateur du MIE est rattaché. Une même personne physique peut être liée à plusieurs personnes morales (entreprise, association, collectivité, …) et chacune à un représentant légal ;
- **Fournisseurs de Services Numériques ou FSN**– désigne un opérateur proposant des services en ligne et ayant recours pour authentifier et/ou identifier ses Utilisateurs à l'identité numérique professionnelle de ChamberSign. Le FSN signe une convention avec ChamberSign ;
- **Utilisateur du MIE** – désigne une personne physique, majeure (plus de 18 ans) et non sous tutelle ou toute autre mesure de protection, identifiée par un MIE objet de la présente Politique. Cette personne utilise son MIE pour s'authentifier ou s'identifier auprès d'un Fournisseur de Service Numérique dans le cadre de ses activités professionnelles (en relation dans ce cas avec une entité déclarée sur le Service avec laquelle elle a un lien contractuel, hiérarchique ou réglementaire). Conformément aux CGUV que l'Utilisateur accepte et signe, et si l'entité ne l'interdit pas, celui-ci peut utiliser son MIE pour des usages non professionnels en n'autorisant que la transmission de ses attributs personnels. L'Utilisateur peut également être désigné sous le nom de « demandeur de MIE » avant la délivrance du MIE. En tout état de cause, le Client et l'Utilisateur sont pleinement responsables à l'égard de ChamberSign de l'utilisation du MIE faite par l'Utilisateur.

Dans le cadre de ses fonctions opérationnelles, les exigences qui incombent à ChamberSign en tant que responsable de l'ensemble du Service sont les suivantes :

- Être une entité légale au sens de la loi française ;
- Rendre accessible l'ensemble des prestations déclarées dans la présente Politique, aux Clients, aux Utilisateurs de MIE abonnés au Service, aux Fournisseurs de Services Numériques ;
- Dans la mesure du possible et selon l'état d'avancement des technologies, ChamberSign France travaille à adapter ses MIE aux personnes en situation de handicap ;
- S'assurer que les exigences de la présente Politique et les procédures associées sont appliquées par chacune des composantes du Service et sont adéquates et conformes aux normes en vigueur ;
- Mettre en œuvre les différentes fonctions identifiées dans la présente Politique, correspondant au minimum aux fonctions obligatoires de la présente Politique, notamment en matière de génération des MIE, de remise aux Utilisateurs et de gestion des révocations et des renouvellements ;
- Mener une analyse de risques permettant de déterminer les objectifs de sécurité propres à couvrir les risques métiers de l'ensemble du Service et les mesures de sécurité techniques et non techniques correspondantes à mettre en œuvre ;
- Mettre en œuvre tout ce qui est nécessaire pour respecter les engagements définis dans la présente Politique, notamment en termes de fiabilité, de qualité et de sécurité ;
- Générer, et renouveler lorsque nécessaire, les secrets des composantes du Service et diffuser les moyens nécessaires à la vérification par les Fournisseurs de Services Numériques de l'intégrité des attributs d'un Utilisateur.

1.4. *Usage des MIE*

1.4.1. **Domaines d'utilisation applicables**

OID applicables	Usage	Description
1.2.250.1.96.1.8.1.1 1.2.250.1.96.1.8.2.6 1.2.250.1.96.1.8.2.8	Authentification & signature	Les usages sont : - la signature électronique de données par l'Utilisateur du certificat (signataire). Une telle signature électronique apporte, outre l'authenticité et l'intégrité des données ainsi signées, la manifestation du consentement du signataire quant au contenu de ces données. - l'authentification des Utilisateurs auprès de serveurs distants ou auprès d'autres personnes. Il peut s'agir d'authentification dans le cadre d'un contrôle d'accès à un serveur ou une application, ou de l'authentification de l'origine de données dans le cadre de la messagerie électronique. Nota : L'authentification ne constitue pas une signature au sens juridique du terme, car elle ne signifie pas que l'Utilisateur manifeste son consentement sur les données échangées (la garantie de non répudiation n'est donc pas offerte).
1.2.250.1.96.1.100.1.1	Authentification	L'usage est l'authentification des Utilisateurs auprès de serveurs distants ou auprès d'autres personnes. Il peut s'agir d'authentification dans le cadre d'un contrôle d'accès à un serveur ou une application, ou de l'authentification de l'origine de données dans le cadre de la messagerie électronique.

Un MIE a pour fonction l'authentification de son Utilisateur avec le PSAMI permettant l'identification électronique de son Utilisateur auprès d'un Fournisseur de Service Numérique, que ce soit en lien ou non avec une personne morale :

- Identification électronique personnelle : le Service transmet au Fournisseur de Service Numérique uniquement les attributs d'identité relatifs à la personne physique ;
- Identification électronique professionnelle : le Service transmet au Fournisseur de Service Numérique les attributs d'identité relatifs à la personne physique ainsi que d'autres attributs identifiant une personne morale et décrivant potentiellement le lien entre l'Utilisateur et celle-ci.

L'Utilisateur reste libre, après son authentification, de diffuser ou non les attributs ci-dessus (détails des attributs en annexe). Selon les besoins du Fournisseur de Service Numérique en matière d'identification, la non-divulgation des attributs demandés et considérés nécessaire par le FSN peut empêcher la délivrance du Service.

Dans le cadre de la présente Politique, le Service de délivrance des MIE est fourni par ChamberSign et son réseau consulaire/public/privé sur l'ensemble du territoire français et ses DROM-COM. Le PSAMI est disponible sans limitation d'origine des connexions.

Dans la présente Politique, le Service de délivrance d'un MIE suppose le contrôle de l'identité personnelle et permet donc son utilisation es-qualité.

1.4.2. Domaines d'utilisation interdits

Toute utilisation d'un MIE autre que celles prévues dans le cadre de la présente Politique et des CGUV applicables est interdite. En cas de non-respect de cette interdiction, la responsabilité de ChamberSign ne saurait être engagée.

1.5. *Gestion de la Politique*

1.5.1. Entité gérant la Politique

ChamberSign est responsable de la gestion de la présente Politique.

Le processus d'évolution et d'amendements à la présente Politique est précisé au chapitre 8.12 ci-dessous.

1.5.2. Point de contact

Toute question ou remarque concernant la présente Politique peut être adressée par courriel à l'adresse suivante : qualite_mie@chambersign.fr en précisant dans l'objet du mail : ***[Demande d'informations Politique de Schéma d'Identification Electronique].***

1.6. *Définitions et acronymes*

1.6.1. Acronymes

A
AC Autorité de Certification
AED Autorité d'Enregistrement Déléguée
ANSSI Agence Nationale de la Sécurité des Systèmes d'Information (Française)

B
BE Bureau d'Enregistrement

C
CGUV Conditions Générales d'Utilisation & de Vente

D
DPS Déclaration des Pratiques du Service

E
eIDAS Règlement n°910/2014 du Parlement européen et du Conseil

F
FIE Fournisseur d'identité électronique
FSN Fournisseur de Services Numériques

I
IGC Infrastructure de Gestion de Clés.

L
LCR Liste des Certificats Révoqués

M
MC Mandataire de certification
MIE Moyen d'identification électronique

O
OCSP Online Certificate Status Protocol
OID Object Identifier
OIDC OpenID Connect

P
PC Politique de Certification
PIN Personal Identification Number
PP Profil de Protection
PSIE Politique de Schéma d'identification électronique
PSCE Prestataire de Services de Certification Electronique

R
RGPD Règlement Général sur la Protection des Données
RL Représentant Légal
RSA Rivest Shamir Adelman

S
SIE Service d'identité électronique

U
URL Uniform Resource Locator

1.6.2. **Définitions**

A

Abonné
Personne qui signe un Contrat d'abonnement aux services de ChamberSign.

AED
Désigne l'une des composantes de l'IGC, approuvée par l'AC, qui intervient pour délivrer des MIE en face à face.

ANSSI
Ou « **Agence nationale de la sécurité des systèmes d'information** » désigne l'autorité nationale en matière de sécurité et de défense des systèmes d'information.

Autorité de certification
Désigne « ChamberSign France », la personne morale qui, au sein d'un prestataire de service de certification électronique (PSCE) a en charge, au nom et sous la responsabilité de celui-ci, l'application d'une politique de Certification et a qualité pour émettre des Certificats électroniques au titre de cette politique de Certification. ChamberSign France est une Autorité de Certification qualifiée selon le décret N° 2017-1416 du 28 septembre 2017 relatif à la signature électronique, pris pour l'application de l'article 1367 du Code civil. Elle a fait l'objet d'un contrôle de conformité par l'Agence Nationale de la Sécurité des Systèmes d'Information et est inscrite sur la liste de confiance européenne. Dans le cadre de son service de délivrance de MIE, ChamberSign utilise la composante « Autorité d'Enregistrement » de son AC.

B

Bi-clé
Couple composé d'une clé privée (devant être conservée secrète) et d'une clé publique correspondante, nécessaire à la mise en œuvre d'une prestation de cryptologie basée sur des algorithmes asymétriques.

BE
Désigne l'une des composantes du service de l'identité électronique professionnelle de ChamberSign, qui intervient pour vérifier les informations d'identification du futur Utilisateur de MIE, ainsi qu'éventuellement d'autres attributs spécifiques, avant de transmettre la demande correspondante à la fonction adéquate de l'Identité électronique professionnelle.

C

Certificat
Ensemble d'informations d'un utilisateur, y compris la clé publique, rendu infalsifiable par le chiffrement, avec la clé secrète de l'AC qui l'a délivré, d'un condensat calculé sur l'ensemble de ces informations. Un certificat contient des informations telles que :

- l'identité du porteur de certificat et Utilisateur de celui-ci comme MIE ;
- la clé publique du titulaire de certificat et Utilisateur de celui-ci comme MIE ;
- usage(s) autorisé(s) de la clé ;
- la durée de vie du certificat ;
- l'identité de l'AC qui l'a émis ;
- la signature de l'AC qui l'a émis.

Un format standard de certificat est défini dans la recommandation X.509 v3.

Contrat d'abonnement
Désigne un engagement contractuel signé par une personne physique pour elle-même ou en représentation d'une personne morale aux fins d'accéder aux services de ChamberSign et dont les modalités sont précisées dans les Conditions générales d'utilisation du ou des produit(s) sélectionné(s) par l'Utilisateur, accessibles sur le Site à l'adresse suivante : https://pc.chambersign.fr/ca3/index.html

Contrôle de conformité
Action qui consiste à réaliser un examen le plus exhaustif possible afin de vérifier l'application stricte des procédures et de la réglementation au sein d'un organisme.

D

Déclaration des Pratiques de Service (DPS)
Une DPS identifie et décrit en détail les pratiques (organisation, procédures opérationnelles, moyens techniques et humains) que ChamberSign applique dans le cadre de la fourniture de ses services d'identités numériques aux Utilisateurs afin de respecter la ou les politiques de schéma d'identification électronique qu'elle a promulguée(s).

Données d'activation
Données privées associées à un MIE d'un Utilisateur et permettant de mettre en œuvre son MIE, c'est-à-dire répondre à une demande d'authentification sur ce MIE (Code PIN d'un certificat activant la clef privée, Code secret d'une application permettant de valider la détention de celui-ci).

E

Enregistrement
Action qui consiste pour une autorité à valider une demande de MIE, conformément à une politique de certification ou de délivrance de MIE.

F

Fournisseur de moyens d'identification électronique (FIE)
Un FIE fait référence à une personne morale, publique ou privée, délivrant au demandeur le moyen d'identification électronique (selon le Référentiel d'exigences de sécurité pour les moyens d'identification électronique – Version 1.2 du 11 août 2022).

G

Génération (émission) d'un certificat
Action qui consiste pour l'AC à intégrer les éléments constitutifs d'un certificat, à les contrôler et à signer le certificat.

I

Infrastructure de gestion de clés (IGC)
Ensemble de composantes, fonctions et procédures dédiées à la gestion de clés cryptographiques et de leurs certificats utilisés par des services de confiance. Une IGC peut être composée d'une autorité de certification, d'un opérateur de certification, d'une autorité d'enregistrement centralisée et/ou locale, de mandataires de certification, d'une entité d'archivage, d'une entité de publication, etc.

J

Journalisation
Fait d'enregistrer dans un fichier dédié à cet effet certains types d'événements provenant d'une application ou d'un système d'exploitation d'un système informatique. Le fichier résultant facilite la traçabilité et l'imputabilité des opérations effectuées.

Jeton OIDC (OpenID Connect)
Désigne un objet informatique sécurisé au format JSON qui permet d'échanger des données d'identification d'un utilisateur.

M

Moyen d'identification électronique (MIE)
Un moyen d'identification électronique est un élément matériel ou immatériel contenant des données d'identification personnelle et utilisé pour s'authentifier pour un service en ligne (article L.102 du Code des postes et des communications électroniques). A minima, ChamberSign propose la délivrance de MIE de niveau substantiel, conformément au référentiel d'exigences de sécurité pour les moyens d'identification électronique – Version 1.2 du 11 août 2022.

N

Nakeyo
Désigne le nom et la marque déposée auprès de l'INPI du Service de l'Identité Numérique Professionnelle conçue et développée par la société ChamberSign via le site https://nakeyo.fr/.

O

Online Certificate Status Protocol (OCSP)
OCSP est un protocole Internet utilisé pour valider un certificat numérique X.509. OCSP est standardisé par l'IETF dans la RFC 6960.Ce protocole est une alternative réglant certains des problèmes posés par les listes de révocation de certificats (CRL) dans une infrastructure à clés

publiques (PKI). Les communications OCSP étant de la forme « requête/réponse », les serveurs OCSP sont appelés répondeurs OCSP.

Opérateur d'enregistrement
Rôle de confiance accordé à une personne spécialement formée au domaine de la certification électronique, et plus particulièrement à la délivrance de certificats électroniques et MIE. Le rôle est attribué *intuitu personae* et fait l'objet d'évaluation et de supervision régulières.

P

Politique de certification (PC)
Ensemble de règles, identifié par un nom (OID), définissant les exigences auxquelles une AC déclare se conformer dans la mise en place et la fourniture de ses prestations et indiquant l'applicabilité d'un certificat à une communauté particulière et/ou à une classe d'applications avec des exigences de sécurité communes. Une PC peut également, si nécessaire, identifier les obligations et exigences portant sur les autres intervenants, notamment les porteurs et les utilisateurs de certificats.

Politique de schéma d'identification électronique
Ensemble de règles, identifié par un nom (OID), définissant les exigences auxquelles un Fournisseur de moyens d'identification électronique déclare se conformer dans la mise en place et la fourniture de ses prestations et indiquant l'applicabilité d'un MIE à une communauté particulière et/ou à une classe d'applications avec des exigences de sécurité communes. Une Politique peut également, si nécessaire, identifier les obligations et exigences portant sur les autres intervenants, notamment les porteurs et les utilisateurs de MIE.

Porteur(s) de certificats
Désigne une personne physique identifiée dans un certificat de personne physique objet de la PC et fourni par l'IGC. Cette personne utilise sa clé privée et le certificat correspondant dans le cadre de ses activités professionnelles en relation avec l'entité identifiée dans le certificat et avec laquelle elle a un lien contractuel, hiérarchique ou réglementaire. Conformément aux CGU que le porteur signe, si l'entité ne l'interdit pas, le porteur peut utiliser son certificat pour des usages non professionnels et en ne revendiquant que la certification de ses nom et prénom(s) présents dans le certificat.

Prestataire de Services de Certification Electronique (PSCE)
Toute personne ou entité qui est responsable de la gestion de certificats électroniques tout au long de leur cycle de vie, vis-à-vis des porteurs et utilisateurs de ces certificats. Un PSCE peut fournir différentes familles de certificats correspondant à des finalités différentes et/ou des niveaux de sécurité différents. Un PSCE comporte au moins une AC mais peut en comporter plusieurs en fonction de son organisation. Les différentes AC d'un PSCE peuvent être indépendantes les unes des autres et/ou liées par des liens hiérarchiques ou autres (AC Racines / AC Filles). Un PSCE est identifié dans un certificat dont il a la responsabilité au travers de son AC ayant émis ce certificat et qui est elle-même directement identifiée dans le champ « issuer » du certificat.

R

Réactivation du MIE
Désigne l'une des étapes du cycle de vie d'un MIE. La réactivation consiste à activer de nouveau son MIE après l'avoir suspendu pendant un délai indéterminé. Dans le cadre de la délivrance de MIE par ChamberSign, la fonction « réactivation » n'est pas applicable car la fonction suspension n'est pas proposée.

Remplacement du MIE

Désigne l'une des étapes du cycle de vie d'un MIE. Le remplacement consiste à réaliser une nouvelle commande de MIE suivant la procédure d'enregistrement initial avec un face à face.

Renouvellement de MIE
Action effectuée à la demande d'un Utilisateur ou en fin de période de validité d'un MIE et qui consiste à générer un nouvel MIE pour un Utilisateur selon les règles propres à chaque type de MIE et disponible dans les CGUV correspondantes.

Révocation de MIE
Action demandée par une entité autorisée (FIE, Utilisateur de MIE, etc.) et dont le résultat est la suppression de la caution de ChamberSign sur un MIE donné, avant la fin de sa période de validité. Cette action peut être la conséquence de différents types d'événements tels que la perte du support, la compromission d'un secret, le changement d'informations contenues dans un MIE, etc. Sa révocation rend le MIE inutilisable pour s'authentifier sur PSAMI.

Révocation d'une Relation ou d'un Attribut
Action demandée par une entité autorisée (FIE, Utilisateur de MIE, entité, etc.) et dont le résultat est la suppression d'une relation entre l'Utilisateur (personne physique) et une Personne Morale dans le système d'information de ChamberSign. Cette relation ne sera plus disponible sur le PSAMI mais le MIE est toujours actif pour s'authentifier sur les autres Identités et Attributs.

S

Service
Service d'Identité Electronique Professionnelle de ChamberSign permettant de garantir l'identité d'une personne et éventuellement ses attributs professionnels associés et vérifiés.

Fournisseur de Services Numériques
Désigne un opérateur proposant des services en ligne et ayant recours pour identifier et/ou authentifier ses utilisateurs à l'identité numérique de ChamberSign. Le Fournisseur de Services Numériques signe une convention avec ChamberSign.

Service de Publication
Le Service de Publication rend disponible les moyens nécessaires pour la vérification des jetons d'identité numérique et les documents publics associés au Service à l'ensemble des utilisateurs potentiels de ces MIE. Le service répond aussi au statut de révocation ou non d'un MIE.

Suspension du MIE
Désigne l'une des étapes du cycle de vie du MIE. La suspension d'un MIE consiste en la non-possibilité pour l'Utilisateur d'interrompre l'utilisation de son MIE pendant un délai indéterminé. Seule la révocation d'un MIE est réalisable.

U

Utilisateur
Utilisateur de MIE ou porteur de certificat utilisant celui-ci comme MIE dans le cadre du Service.

V

Vérification de signature
La vérification d'une signature consiste à déchiffrer la signature d'un message, en mettant en œuvre la clé publique du signataire supposé. Si le hash clair obtenu est identique à l'empreinte calculée à partir du message reçu, alors il est garanti que le message est intègre et qu'il a été

signé par le porteur de la clé privée correspondante à la clé publique utilisée pour la vérification.

2. Responsabilités concernant la mise à disposition des informations devant être publiées

2.1. *Entités chargées de la mise à disposition des informations*

Pour la mise à disposition des informations devant être publiées à destination des Utilisateurs et du Fournisseur de Service Numérique, ChamberSign met en œuvre au sein de son Service un service de publication.

Le service de publication s'appuie sur un serveur Web, accessible en HTTPs à l'adresse www.chambersign.fr.

Les engagements de disponibilité et de continuité d'activité de ces services (serveur Web) sont précisés au chapitre 4.9 ci-dessous.

2.2. *Informations devant être publiées*

Les informations suivantes sont diffusées via le site Web de ChamberSign :

- la présente Politique et les CGU du Service ;
- les CGU/CGUV de chacun des MIE proposés dans le cadre du Service ;
- les certificats de signature des jetons OIDC ;
- les éléments de publication liés à chaque famille de MIE.

La Politique et les CGUV sont validées par le Responsable du Fournisseur des moyens d'identification électronique avant leur publication.

2.3. *Délais et fréquences de publication*

Les informations liées au Service (Politique, CGUV, etc.) sont publiées dès leur validation par la direction de ChamberSign.
La disponibilité des systèmes publiant les certificats, et leurs révocations de ChamberSign est assurée 24h/24 et 7j/7 ainsi que le service de vérification de la révocation d'un M.I.E. Smartphone, automatiquement géré par le PSAMI.

2.4. *Contrôle d'accès aux informations publiées*

L'accès en modification aux systèmes de publication (ajout, suppression, modification des informations publiées) est strictement limité aux fonctions internes habilitées du Service, au travers d'un contrôle d'accès fort (basé sur une authentification à au moins deux facteurs).

2.5. *Intégrité des éléments publiés*

Tous les éléments publiés dans le cadre du présent Service sont scellés numériquement par un cachet d'entreprise RGS** ou qualifié eIDAS ou signés par les rédacteurs.

3. Identification et authentification

La présente Politique prévoit l'identification d'une personne physique, ou d'une personne physique dans le cadre d'une relation avec une personne morale (donc associé à des attributs professionnels). La délivrance d'une Identité Numérique professionnelle ne peut être réalisée que dans le cadre d'un lien professionnel, ensuite ce lien peut être révoqué et seule l'identité personnelle perdure et reste parfaitement opérationnelle.

Les éléments techniques de la mise en œuvre de l'authentification et de l'identification pour le Fournisseur de Service Numérique sont disponibles dans le cadre d'une convention entre ChamberSign et le Fournisseur de Service Numérique.

3.1. *Nommage*

3.1.1. Attributs disponibles pour la personne physique

- Prénoms
- Nom de naissance
- Nom d'usage le cas échéant
- Genre
- Date de naissance
- Pays de naissance
- Ville de naissance si le pays est la France
- Téléphone mobile

3.1.2. Attributs disponibles pour la personne morale (une personne morale ou un établissement lié au moins à une personne physique)

- Dénomination (Raison sociale pour les sociétés commerciales)
- Numéro d'immatriculation : SIREN
- Adresse physique
- Pays
- Ville
- Téléphone (déclaratif)

Pour chaque établissement

- Nom de l'établissement
- SIRET
- Adresse physique
- Pays
- Ville
- Téléphone du site

3.1.3. Attributs de lien entre une personne physique et une personne morale

Ces attributs sont validés pendant la phase d'inscription par l'opérateur d'enregistrement et doivent avoir été validés par le représentant légal de l'entité.

- Titre réglementé : si un titre réglementé est revendiqué dans une liaison personne morale – personne physique, l'opérateur contrôlera la présence dans le dossier de demande ou auprès des sources de confiance la licéité de la demande ;
- Fonction : Fonction de la personne physique au sein de la personne morale. Le libellé de la fonction est libre mais celui-ci est vérifié pendant la validation et les libellés de fonctions ambiguës sont refusées aussi bien vis-à-vis d'une profession réglementée que d'un rôle de Représentant Légal.
- La fonction est associée automatiquement à son statut : Représentant Légal Oui/Non selon les éléments du dossier vérifiés au moment de l'enregistrement ;
- Service : Service de rattachement sous forme d'un texte libre ;
- Email professionnel ;
- …

3.1.4. Anonymisation ou pseudonymisation des Utilisateurs de MIE

L'anonymisation ou la pseudonymisation ne sont pas autorisées dans le cadre de la présente Politique.

3.1.5. Règles d'interprétation des différentes attributs

Les significations et codifications des différents attributs publiés par le Service sont disponibles dans le document « Profils des attributs publiés par le Service d'Identité Electronique de ChamberSign ».

3.1.6. Unicité des Utilisateurs, multiplicité des identités

Chaque Utilisateur Personne Physique est présent une seule fois dans le répertoire d'identité Electronique de ChamberSign France. Son/ses MIE permet(tent) à son Utilisateur d'accéder à ses différentes identités professionnelles et personnelle.

3.1.7. Identification, authentification et rôle des marques déposées

Il n'y a pas d'utilisation dans l'Identité Electronique Professionnelle de nom de marque autres que la dénomination de l'organisme correspondant, tel que mentionné sur les documents officiels faisant l'objet d'une vérification lors des procédures d'enregistrement (Kbis, etc.).

3.2. *Validation initiale de l'identité*

3.2.1. Validation de l'identité d'un organisme

Les informations concernant la structure à laquelle l'Utilisateur est rattaché font l'objet de vérification lors de l'enregistrement par le contrôle de la validité et de l'authenticité des documents listés ci-après :

- Document attestant de l'existence juridique de l'organisme et de l'habilitation de son représentant légal ;
- Document d'identité du représentant légal de l'entité valide. Les documents d'identité recevables dans ce cadre sont les suivants :
    - Carte Nationale d'identité ;
    - Passeports ;
    - Titres de séjour délivrés par la France et contenant une date de validité, y compris les titres avec une validité permanente, sans date de fin.

3.2.2. Validation de l'identité d'un individu

L'identité de l'Utilisateur est vérifiée via le contrôle de la validité et de l'authenticité des documents officiels d'identité listés ci-après lors de l'enregistrement de la demande, ainsi que lors d'un face-à-face physique avec le futur Utilisateur.

La liste des documents recevables dans le cadre de la fourniture de MIE est la suivante :

- Carte Nationale d'identité ;
- Passeports ;
- Titres de séjour délivrés par la France et contenant une date de validité, y compris les titres avec une validité permanente, sans date de fin.

Les pièces d'identité sans photographie ne sont pas acceptées par ChamberSign. Le détail de la liste des pièces acceptées est disponible dans les conditions générales d'utilisation du Service d'Identité Numérique Professionnelle.

Tout autre type de document ou Etat de délivrance que ceux listés précédemment sont exclus et ne peuvent être acceptés dans le cadre du processus de validation de l'identité pour la délivrance d'un MIE.

3.2.3. Informations non vérifiées de l'Utilisateur

Toutes les informations concernant les informations de la personne physique font l'objet de vérifications à l'exception :

- Du pays de naissance qui est déclaratif.

3.2.4. Validation de l'autorité du Demandeur

Cette étape est effectuée en même temps que la validation de l'identité de l'organisme.

3.2.5. Critères d'interopérabilité pour accepter des identités numériques tierces

La décision que la Politique de ChamberSign reconnaisse et/ou soit reconnue par un autre FIE est du ressort de la Direction de ChamberSign mais c'est une volonté de ChamberSign d'assurer cette interopérabilité entre opérateurs de même niveau de certification. Cette interopérabilité doit être réciproque.

3.3. Identification et validation d'une demande de renouvellement d'un MIE

Si le renouvellement est autorisé par la réglementation au moment de l'expiration d'un MIE, il est possible de réaliser une commande et la délivrance d'un nouveau MIE en ligne sans face à face. Il devra alors être réalisé avant la date d'expiration du précédent MIE ou sous la période de validité d'un autre MIE de même niveau substantiel. Pour les MIE concernés et sous réserve de conformité à la réglementation applicable, la nouvelle délivrance est réalisée sans procéder de nouveau à un face à face. L'Utilisateur valide en ligne que les informations liées au MIE à « *renouveler* » sont toujours exactes. Pour tout autre renouvellement ultérieur ou remplacement à la suite d'une révocation, il faut procéder à une commande d'un nouveau MIE suivant la procédure d'enregistrement initial avec face à face.
En l'état actuel de notre interprétation, un face à face est nécessaire selon l'offre initiale souscrite. ChamberSign ne propose pas de renouvellement en ligne.

3.4. *Identification et validation d'une demande de révocation*

Toute demande de révocation, de MIE, de relation personne physique – personne morale ou d'attributs, fait l'objet d'une authentification de la personne demandant la révocation, demande signée par le Demandeur et qui fait l'objet d'une vérification de son autorité à agir.

4. Exigences opérationnelles sur le cycle de vie des MIE

Ce paragraphe rappelle les principes communs aux différents types de MIE. Les conditions opérationnelles de chaque type sont disponibles dans les CGUV propres aux différents MIE.

4.1. *Demande de MIE*

4.1.1. Origine d'une demande de MIE

Les dossiers de demande de MIE proviennent soit :

- du futur Utilisateur (dénommé Demandeur) ;
- du représentant légal de l'entité concernée, le client ;

Quelle que soit l'origine de la demande, le futur Utilisateur valide la demande et participe personnellement au face à face de délivrance.

4.1.2. Processus et responsabilités pour l'établissement d'une demande de MIE

L'établissement d'une demande de MIE associé à des attributs professionnels, des mandats et des droits afférents est de la responsabilité de l'entité liée aux attributs associés.

4.2. *Traitement d'une demande de MIE*

4.2.1. Exécution des processus d'identification et de validation de la demande

Le service d'enregistrement des Utilisateurs de MIE s'assure de l'origine, de l'intégrité et de la cohérence de la demande transmise (cf. chapitre 3.2).

4.2.2. Acceptation ou rejet de la demande

Ensuite, si aucun problème n'est détecté, il valide les informations contenues dans la demande et transmet cette dernière au service de délivrance du MIE.

4.2.3. Durée d'établissement du MIE

Dès la demande de MIE reçue par le service de délivrance des MIE, l'Utilisateur est sollicité pour la remise de son MIE.

4.3. *Délivrance du MIE*

4.3.1. Actions de ChamberSign concernant la délivrance du MIE

MIE	Description
Certificat qualifié	Suite à la validation du dossier de demande de certificat par la fonction d'enregistrement, le processus consiste à remettre au titulaire en mains propres, un support cryptographique vierge, identifié de façon unique et lié au titulaire, qui fera l'objet d'une personnalisation sous le contrôle du titulaire : personnalisation du code d'activation (code PIN), génération de la bi-clé dans le support, envoi de la clé publique à la fonction de génération des certificats, téléchargement sur le support du certificat généré. Les supports cryptographiques sur lesquels le MIE peut être intégré sont mis en œuvre par l'Autorité de Certification racine ChamberSign France CA3 Root, et sont limités aux certificats suivants : **Pour l'AC Fille ChamberSign France CA3 NG Qualified eID :** - 1.2.250.1.96.1.8.2.6 : Certificats d'authentification et de signature qualifiés eIDAS personne physique - 1.2.250.1.96.1.8.2.8 : Certificats d'authentification et de signature qualifies eIDAS personne physique avec Qualified Signature Creation Device (QSCD) **Pour l'AC Fille ChamberSign France CA3 NG RGS :** - 1.2.250.1.96.1.8.1.1 : Certificats d'authentification ** RGS personne physique
Mobile	Suite à la validation du dossier de demande de MIE sur smartphone par la fonction d'enregistrement de l'IGC, le processus consiste à activer sur le smartphone de l'Utilisateur le logiciel MIE en lien avec l'identité de l'Utilisateur sous son contrôle exclusif. Cette activation se fait lors d'un face à face, en présence d'un opérateur de confiance.

4.3.2. Notification par ChamberSign de la délivrance du MIE à l'Utilisateur

Le MIE est remis à l'Utilisateur au moment de son face à face, en main propre.

4.4. *Acceptation du MIE*

4.4.1. Démarche d'acceptation du MIE

Le MIE fait l'objet d'une acceptation explicite par son Utilisateur au moment de sa remise.

Pour chaque MIE, la procédure d'acceptation, fonction de sa nature, est décrite dans les CGUV du MIE.

4.4.2. Publication du MIE

Les MIE certificats et MIE sur smartphone objets de la présente Politique ne font pas l'objet de publication par ChamberSign.

4.4.3. Notification par ChamberSign aux autres entités de la délivrance du MIE

Les différentes composantes concernées de l'IGC sont informées de la délivrance du MIE via le système d'information de l'IGC.
Les MIE sur smartphone délivrés font l'objet d'une communication aux autres composantes de l'IGC en fonction de leurs droits spécifiques d'en connaitre.

4.5. *Usages du MIE*

4.5.1. Utilisation du MIE et du PSAMI par l'Utilisateur

Dans le cadre de cette Politique, l'Utilisateur utilise son MIE sur sollicitation du PSAMI pour s'authentifier et choisir l'Identité et les attributs qu'il va exposer au Fournisseur de Services Numériques.

Le PSAMI s'assure de la validité du MIE utilisé par l'Utilisateur : dates de validité, non révocation.

4.5.2. Utilisation de l'Identité Numérique par le Fournisseur de Services Numériques

Le Fournisseur de Services Numériques intègre dans le parcours de son client un appel au PSAMI en indiquant les paramètres de l'identification attendue (l'ensemble des paramètres d'appels est détaillé dans le document : « Profils des attributs publiés par le Service d'Identité numérique de ChamberSign »).

4.6. *Renouvellement d'un MIE*

Se référer au chapitre 3.3 « *Identification et validation d'une demande de renouvellement d'un MIE* ».

4.7. *Délivrance d'un nouveau MIE*

Un Utilisateur peut demander un nouveau MIE avant ou après révocation de son MIE actuel. La procédure est identique à la commande d'un premier MIE.
Les procédures opérationnelles de délivrance d'un nouveau MIE sont disponibles dans les CGUV de chaque MIE.
Selon chaque type de MIE, il est possible de disposer ou non de deux MIE de même type pour une même personne physique.

4.8. *Usage du MIE*

La diffusion de données d'identification personnelle et/ou professionnelle est précédée par la vérification de la légitimité et de l'authentification du Fournisseur de Services Numériques et de la vérification fiable du moyen d'identification électronique de l'Utilisateur et de sa validité.

4.9. *Révocation et suspension d'un MIE*

Il n'y a pas de suspension possible de MIE. Seule la révocation définitive des MIE peut être réalisée.
ChamberSign assure la disponibilité des fonctions de révocation et de la mise à disposition du statut de révocation à tout moment selon le type de MIE et au-delà de la période de validité du MIE en mettant en œuvre les mesures suivantes :

- Certificats :
    - Publication sans limite de temps des certificats révoqués dans les LCR publiées ;

- Conformité de la réponse OCSP, révoqué, en cas de sollicitation après la date de fin de vie du certificat ;

- MIE Smartphone :
  - Désactivation du MIE concerné ;
  - Historisation et traçabilité de la révocation des MIE dans le compte de l'Utilisateur.

4.9.1. Causes possibles d'une révocation d'un MIE

Les circonstances suivantes peuvent être à l'origine de la révocation d'un MIE utilisé dans le cadre de la présente Politique, les modalités opérationnelles sont disponibles dans les CGUV de chaque MIE ainsi que d'éventuelles causes complémentaires liées à la nature du MIE :

- demande de révocation du MIE par l'Utilisateur du MIE ;
- dysfonctionnement du MIE ;
- résiliation de l'abonnement ;
- non-paiement de l'abonnement ou du MIE par le Client ;
- compromission des secrets d'activation du MIE ;
- les algorithmes cryptographiques mis en œuvre sont obsolètes et ne sont plus considérés sûrs ;
- il a été démontré que l'Utilisateur n'a pas respecté les modalités applicables d'utilisation du MIE ;
- l'Utilisateur n'a pas respecté ou ne respecte plus les conditions générales d'utilisation du moyen d'identification électronique ;
- une erreur (intentionnelle ou non) a été détectée dans le dossier d'enregistrement ;
- le moyen d'identification électronique ou les données d'activation associées sont suspectés de compromission, sont compromis, sont perdus ou volés ;
- l'utilisateur est décédé ;
- l'Utilisateur a porté plainte pour usurpation d'identité. En cas de suspicion d'une usurpation d'identité détectée par ChamberSign, ChamberSign s'oblige à contacter sans délai l'Utilisateur pour faire un point sur la situation et s'autorise, éventuellement, à révoquer le MIE.

Les causes de révocation ne sont jamais publiées mais sont mémorisées dans le système d'information.

4.9.2. Causes possibles d'une révocation d'une relation personne physique – personne morale ou d'un attribut

Le Service permet de révoquer des relations personne physique – personne morale sans révoquer son ou ses MIE. Après authentification sur le système d'information avec son MIE, l'Utilisateur ou toute personne habilitée, sélectionnera la ou les relations à révoquer.
Cette révocation est à effet immédiat et irrévocable, et le PSAMI sera mis à jour dans un délai maximum de 2 heures.
Les circonstances suivantes peuvent être à l'origine de la révocation de la relation personne physique – personne morale ou d'un attribut :

- Demande de révocation de la relation ou d'un attribut par l'Utilisateur ou le représentant légal ;
- Cessation d'activité du Client.

4.9.3. Origine d'une demande de révocation

Les entités qui peuvent demander la révocation d'un MIE objet de la présente Politique sont les suivantes :

- l'Utilisateur au nom duquel le MIE a été émis ou pour toute relation dans laquelle il est responsable ;
- le représentant légal pour la relation ou les attributs concernés ;
- les participants à une délégation ;
- ChamberSign ;
- les Bureaux d'Enregistrement.

4.9.4. Procédure de traitement d'une demande de révocation

La validation de la demande inclut la vérification de l'origine de la demande et de l'applicabilité de la cause invoquée. Après cette validation, le service de gestion des révocations applique la révocation et les informations sont mises à jour en fonction de leur nature et selon les modalités opérationnelles de chaque MIE.

4.9.5. Délai accordé aux parties concernées pour formuler la demande de révocation

La demande de révocation doit être formulée dès connaissance de l'évènement correspondant.

4.9.6. Délai de traitement par l'AC d'une demande de révocation

Les demandes de révocation sont traitées dans un délai inférieur à 24h suivant la réception de la demande par les dispositifs en ligne, 7 jours / 7 (week-ends et jours fériés compris), hors révocations consécutives à des demandes de modification des données du titulaire. Ce délai s'entend entre la réception de la demande et la mise à disposition de l'information de révocation auprès des tiers.

La fonction de gestion des révocations est disponible 24 heures sur 24, 7 jours sur 7. La durée maximale d'indisponibilité par interruption (panne ou maintenance) de la fonction de gestion des révocations est de 2h. La durée maximale totale d'indisponibilité par mois de la fonction de gestion des révocations est de 8h.

La révocation demandée en ligne par l'Utilisateur au moyen de ses identifiants personnels est exécutée sans délai.

4.9.7. Exigences de vérification de la révocation par les accepteurs de MIE

Le PSAMI vérifie la révocation des MIE, des relations personne physique – personne morale et des attributs à chaque utilisation.

4.10. *Expiration de l'abonnement des Utilisateurs*

A l'expiration de l'abonnement des Utilisateurs, ou en cas d'interruption ou de non-renouvellement, le MIE est révoqué.

5. Mesures de sécurité non techniques

5.1. *Mesures de sécurité physiques*

ChamberSign met en œuvre les mesures de sécurité physique, au sein des différentes composantes du Service, nécessaire pour assurer le fonctionnement sécurisé de ses services conformément aux engagements pris dans le présent document, notamment en termes de disponibilité (contrôle d'accès physique, services supports (alimentation électrique, climatisation, etc.), protection contre les dégâts des eaux, protection contre les incendies et protection des supports).

5.2. *Mesures de sécurité procédurales*

Au sein de chaque composante de l'IGC et du SIE, des rôles fonctionnels de confiance sont identifiés et formellement attribués, en respectant des règles strictes de séparation des attributions.
Toute attribution d'un rôle et des droits correspondants fait l'objet d'une vérification préalable de l'identité et des autorisations correspondantes.

Pour la réalisation de certaines opérations, l'intervention de plusieurs personnes peut être requise.
ChamberSign met en œuvre des rôles de porteurs de secrets qui ont pour responsabilité de recevoir et conserver de manière sécurisée une part du secret nécessaire à la mise en œuvre de la chaîne d'AC et d'éventuellement d'autres secrets.

L'ensemble des opérations d'enregistrement, de contrôle et de délivrance fait l'objet d'une surveillance active et contextuelle par le contrôle qualité de ChamberSign France.

5.3. *Mesures de sécurité vis-à-vis du personnel*

Tous les personnels, internes et externes à ChamberSign, amenés à travailler au sein des composantes de l'IGC et du SIE sont soumis à des obligations de qualifications, de compétences, de formations initiales et continues et d'habilitations en fonction de leurs rôles.

L'honnêteté de ces personnels est vérifiée conformément à ce qui est autorisé par la loi.

5.4. *Procédures de constitution des données d'audit*

Les différents évènements liés au fonctionnement de l'IGC et du SIE font l'objet d'une journalisation d'évènements enregistrée de façon manuelle ou automatique. Les fichiers résultants, sous forme papier ou électronique, rendent possible la traçabilité et l'imputabilité des opérations effectuées.
Ces journaux d'évènements sont datés, protégés et font l'objet d'un archivage. Ils sont régulièrement contrôlés afin d'évaluer les éventuelles vulnérabilités pesant sur l'IGC ou le SIE.

5.5. *Archivage des données*

Des dispositions en matière d'archivage, papier et électronique, sont prises afin d'assurer la pérennité des journaux constitués par les différentes composantes de l'IGC et du SIE et d'autres données. Les durées de conservation des archives liées aux MIE sont précisées dans l'ensemble des CGUV de ChamberSign.

5.6. *Reprise suite à compromission et sinistre*

Chaque entité opérant une composante de l'IGC et du SIE met en œuvre des procédures et des moyens de remontée et de traitement des incidents, notamment au travers de la sensibilisation et de la formation de ses personnels et au travers de l'analyse des différents journaux d'évènements, y compris dans le cas d'incidents majeurs (compromission de clés privées, faiblesse des algorithmes utilisés, indisponibilité des serveurs, …). Ces procédures et moyens doivent permettre de minimiser les dommages dus à des incidents de sécurité et des dysfonctionnements.

Chaque composante de l'IGC et du SIE dispose d'un plan de continuité d'activité permettant de répondre aux exigences de disponibilité des différentes fonctions de l'IGC et du SIE découlant des engagements de ChamberSign dans la présente PSIE et à l'égard de la réglementation notamment en ce qui concerne les fonctions liées à la publication et à la révocation.

Les différentes composantes de l'IGC et du SIE disposent des moyens nécessaires permettant d'assurer la continuité de leurs activités en conformité avec les engagements de la présente Politique.

En cas de détection d'un incident de sécurité sur l'infrastructure de confiance, ChamberSign s'engage à fournir les informations liées à cet incident en envoyant un message à l'adresse cert-fr.cossi@ssi.gouv.fr

5.7. *Fin de vie du Service*

Une ou plusieurs composantes du Service, ou la totalité du Service, peuvent être amenées à cesser leur activité ou à la transférer à une autre entité pour des raisons diverses.
ChamberSign mettra en œuvre les mesures requises pour assurer au minimum la continuité de l'archivage des informations et la continuité des services de révocation.

ChamberSign a pris les dispositions nécessaires pour couvrir les coûts permettant de respecter ces exigences minimales dans le cas où ChamberSign serait en faillite ou pour d'autres raisons serait incapable de couvrir ces coûts par elle-même, ceci, autant que possible, en fonction des contraintes de la législation applicable en matière de faillite.

Dans la mesure où les changements envisagés peuvent avoir des répercussions sur les engagements vis-à-vis des Utilisateurs, ChamberSign les en avisera aussitôt que nécessaire et, au moins, sous le délai d'un mois. De même, ChamberSign informera les autorités publiques concernées.

6. Mesures de sécurité techniques

6.1. Conception des MIE

Deux familles de MIE sont acceptées dans le cadre de cette Politique : Certificats Qualifiés et Application smartphone. Les principes généraux de conception de ces MIE sont exposés ci-après, les modalités opérationnelles sont disponibles dans les CGUV de chacun des MIE. Les moyens d'identifications électroniques utilisés proposent au moins deux facteurs d'authentification de différentes catégories.

Le moyen d'identification électronique est conçu et mis en œuvre de sorte qu'on puisse présumer qu'il est utilisé uniquement sous le contrôle exclusif de la personne physique à laquelle il appartient ou en sa possession.

6.2. Mécanisme d'authentification

Le mécanisme d'authentification met en œuvre des contrôles de sécurité pour la vérification du moyen d'identification électronique, de sorte qu'il est hautement improbable que des activités telles que les tentatives de décryptage, l'écoute, l'attaque par rejeu ou la manipulation d'une communication par un attaquant ayant un potentiel d'attaque modéré puissent nuire aux mécanismes d'authentification.
Le statut de révocation du MIE est systématiquement vérifié à chaque authentification par l'Utilisateur sur le PSAMI.

6.3. Autres aspects de la gestion des secrets

Les secrets des porteurs ont une durée de vie de trois (3) ans pour les supports cryptographiques et trois ans ou plus selon l'offre souscrite pour les MIE smartphones.

6.4. Données d'activation

Les données d'activation correspondent aux codes PIN ou aux codes secrets des MIE, qui sont personnalisés par les Utilisateurs lors de la délivrance de leur MIE et qu'ils ne doivent communiquer à personne. Les différentes composantes de l'IGC et du SIE n'ont à aucun moment connaissance de ces codes.

6.5. Mesures de sécurité des systèmes informatiques

Au sein des différentes composantes du Service, les mesures de sécurité relatives aux systèmes informatiques satisfont aux objectifs de sécurité qui découlent d'analyses de risques menées au niveau de chaque composante.

6.6. Mesures de sécurité des systèmes durant leur cycle de vie

L'implémentation d'un système permettant de mettre en œuvre les composantes du Service est documentée. La configuration du système des composantes de l'IGC ou du SIE ainsi que toute modification et mise à niveau sont documentées et contrôlées.
Les objectifs de sécurité sont définis lors des phases de spécification et de conception. Les systèmes et les produits utilisés sont fiables et sont protégés contre toute modification.

6.7. Mesures de sécurité réseau

L'interconnexion vers des réseaux publics est protégée par des passerelles de sécurité configurées pour n'accepter que les protocoles nécessaires au fonctionnement de la composante au sein de l'IGC et du SIE. Les composants du réseau local (routeurs, par exemple) sont maintenus dans un environnement physiquement sécurisé et les configurations sont périodiquement auditées en vue de vérifier leur conformité avec les exigences spécifiées par ChamberSign.

6.8. Horodatage

La datation des évènements au sein du Service utilise l'heure système des composantes en assurant une synchronisation des horloges des systèmes du service entre elles, au minimum à la minute près, et par rapport à une source fiable de temps UTC, au minimum à la seconde près.
Pour les opérations faites hors ligne, cette précision de synchronisation par rapport au temps UTC n'est pas requise. Le système peut toutefois ordonner les évènements avec une précision suffisante.

7. Profils des jetons d'identité et attributs

Les profils de jetons d'identité et les attributs sont décrits dans le document : « Profils des attributs publiés par le Service d'Identité électronique de ChamberSign ».

8. Autres problématiques métiers et légales

8.1. *Tarifs*

8.1.1. Tarifs pour la fourniture ou le renouvellement de MIE

Cf. l'ensemble des CGUV de ChamberSign.

8.1.2. Tarifs pour utiliser l'abonnement au SIE

L'Utilisateur s'abonne au Service d'Identification Electronique selon le tarif disponible sur le site de ChamberSign. Cet abonnement peut être distinct du prix d'acquisition de son MIE.

8.1.3. Tarifs pour d'autres services

Cf. l'ensemble des CGUV de ChamberSign et services proposés sur ses sites Internet https://www.chambersign.fr/ et https://nakeyo.fr/.

8.2. *Responsabilité financière*

8.2.1. Couverture par les assurances

ChamberSign est titulaire d'une Assurance Responsabilité Civile Professionnelle couvrant son activité de Fournisseur d'Identité Electronique.

8.3. *Confidentialité des données professionnelles*

8.3.1. Périmètre des informations confidentielles

Les informations suivantes sont considérées comme confidentielles et font l'objet de procédures de protection adéquates :

- la partie non-publique de la déclaration de pratiques du Service ;
- les secrets des composantes du service et des Utilisateurs de MIE ;
- les données d'activation associées aux secrets des composantes du service et des Utilisateurs de MIE ;
- les journaux d'évènements des composantes du service ;
- les dossiers d'enregistrement des Utilisateurs ;
- les causes de révocations.

8.3.2. Responsabilités en termes de protection des informations confidentielles

Les informations confidentielles soit ne sont pas accessibles (par exemple, secrets des porteurs qui ne sont sous forme déchiffrée qu'à l'intérieur de supports sécurisés), soit sont accessibles uniquement aux personnes justifiant du besoin d'en connaître et dûment autorisées (par exemple, parties de « secrets du Service »).

8.4. *Protection des données personnelles*

8.4.1. Politique de protection des données personnelles

Les informations à caractère personnel sont explicitement identifiées et font l'objet de procédures de protection adéquates, en conformité avec les exigences légales et règlementaires applicables.

Cf. l'ensemble des CGUV de ChamberSign.

Dans le cadre de son Service, Chambersign demande systématiquement à l'Utilisateur son autorisation pour communiquer des données personnelles.

8.4.2. Informations à caractère personnel

Toutes les données d'enregistrement des Utilisateurs sont considérées comme personnelles. Les données personnelles inhérentes à l'Utilisateur sont les suivantes : nom(s), prénom(s), date de naissance, genre, lieu de naissance, qualité (Représentant Légal ou non), service, fonction, email professionnel, téléphone professionnel, preuve de l'identité et tout autre attribut professionnel enregistré sur demande de l'Utilisateur.

8.4.3. Informations à caractère non personnel

N/A.

8.4.4. Responsabilité en termes de protection des données personnelles

Conformément au Règlement UE 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des données physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (« RGPD ») et à la règlementation française en vigueur, les traitements de ChamberSign sont inscrits au registre des traitements et font l'objet de

mesures de sécurité techniques et organisationnelles appropriées afin de garantir la conformité à la législation.

8.4.5. Notification et consentement d'utilisation des données personnelles

Conformément aux législations et réglementations en vigueur, en particulier sur le territoire français, les informations personnelles remises par les Utilisateurs à ChamberSign ne sont ni divulguées ni transférées à un tiers sauf dans les cas suivants : consentement préalable de l'Utilisateur dans le cadre du SIE, décision judiciaire ou autre autorisation légale.

8.4.6. Conditions de divulgation d'informations personnelles aux autorités judiciaires ou administratives

Cf. législations et réglementations en vigueur.

8.5. *Droits sur la propriété intellectuelle et industrielle*

Cf. l'ensemble des CGUV de ChamberSign.

8.6. *Interprétations contractuelles et garanties*

8.6.1. Autorités de Certification

Au titre de la présente Politique, et pour le domaine qu'elle couvre (cf. chapitres 1.3 et 1.4 ci-dessus), ChamberSign garantit le respect des engagements décrits dans le présent document et dans l'ensemble des CGUV de ChamberSign.

8.6.2. Service d'enregistrement

Cf. chapitre 9.6.1.

8.6.3. Utilisateurs de MIE

Cf. l'ensemble des CGUV de ChamberSign.

8.6.4. Autres participants

Cf. l'ensemble des CGUV de ChamberSign.

8.7. *Limite de garantie*

Cf. l'ensemble des CGUV de ChamberSign.

8.8. *Limite de responsabilité*

Cf. l'ensemble des CGUV de ChamberSign.

8.9. *Indemnités*

Cf. l'ensemble des CGUV de ChamberSign.

8.10. *Durée et fin anticipée de validité de la Politique*

8.10.1. Durée de validité

La Politique entrée en vigueur reste en application jusqu'à la fin de vie du dernier MIE émis au titre cette Politique.

8.10.2. Fin anticipée de validité

La cessation d'activité du Service, programmée ou suite à sinistre, entraîne la fin de validité de la présente Politique.

8.10.3. Effets de la fin de validité et clauses restant applicables

La fin de validité de la présente Politique rend caduques les engagements de ChamberSign qui y sont portés, à l'exception des clauses traitant de la fin de vie du Service, de l'archivage et du transfert d'activité.

8.11. *Notifications individuelles et communications entre les participants*

En cas de changement de toute nature intervenant dans la composition du Service, ChamberSign s'engage à :

- au plus tard un mois avant le début de l'opération, faire valider ce changement au moyen d'une expertise technique, afin d'évaluer les impacts sur le niveau de qualité et de sécurité des fonctions du Service et de ses différentes composante ;
- au plus tard un mois après la fin de l'opération, en informer, le cas échéant, les organes de supervision.

8.12. *Amendements à la Politique*

8.12.1. Procédures d'amendements

Les Politique sont revues régulièrement afin d'assurer leur conformité avec les évolutions à la fois techniques (normes, référentiels, …) et juridiques (lois, règlements, …).

8.12.2. Mécanisme et période d'information sur les amendements

Toute nouvelle version est disponible en format électronique sur les sites Internet de ChamberSign et Nakeyo dès son approbation par la Direction de ChamberSign.
Elle prend effet dès sa publication.

8.12.3. Circonstances selon lesquelles l'OID doit être changé

L'OID de chacune des Politiques comporte le numéro de version principale. Toute évolution significative de la Politique, notamment les évolutions ayant un impact sur les MIE déjà émis ou les échanges avec les Fournisseurs de Services Numériques, entraîne une évolution du numéro de version principale et donc, une évolution de l'OID.

8.13. *Dispositions concernant la résolution de conflits*

Cf. l'ensemble des CGUV de ChamberSign.

8.14. *Juridictions compétentes*

Cf. l'ensemble des CGUV de ChamberSign.

8.15. *Conformité aux législations et réglementations*

Cf. l'ensemble des CGUV de ChamberSign.

8.16. *Dispositions diverses*

8.16.1. Conséquences d'une clause non valide

Au cas où une clause de la présente Politique s'avèrerait être non valide au regard de la loi applicable, ceci ne remettrait pas en cause la validité et l'applicabilité des autres clauses.

8.16.2. Application et renonciation

Cf. l'ensemble des CGUV de ChamberSign.

8.16.3. **Force majeure**

Sont considérés comme cas de force majeure tous ceux habituellement retenus par les tribunaux français ainsi que toutes autres conventions pouvant lier les parties.

8.17. ***Autres dispositions***

Les politiques et procédures du Service sont non-discriminatoires.
Cf. l'ensemble des CGUV de ChamberSign.

ANNEXE 1 - DOCUMENTS DE REFERENCE

9. Documents externes de nature juridique

[eIDAS]	Règlement n°910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique des services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, modifié par l'adoption du Règlement eIDAS 2 (N° 2024/1183)
[RGS]	Référentiel Général de Sécurité – ANSSI – Version 2.0 du 13 juin 2014
[CPCE]	Article L.102 IV du code des postes et des communications électroniques
[MIE]	Référentiel d'exigences de sécurité pour les moyens d'identification électronique – ANSSI – Version 1.2 du 11 août 2022
[RGPD]	Règlement (UE) n°2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)
[LIL]	Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004.

10. Documents externes de nature technique

[RFC3647]	IETF - Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practice Framework - novembre 2003
[RFC6749]	OpenID Connect Core 1.0

11. Documents internes ChamberSign France

ChamberSign France – « Profils des attributs publiés par le Service d'Identité Electronique de ChamberSign »