# Politique de gestion des certificats

Certificate Policy

## Version 1.0

3 avril 2025

# Table des matières

# 1 POLITIQUE DE GESTION DES CERTIFICATS OPERATEURS

CERTIFICATE POLICY

Ce document présente la politique de délivrance et de gestion des certificats opérateurs appliquée dans le cadre du Mécanisme d'Authentification des Numéros (MAN) ; le MAN est la solution mise en œuvre en France permettant de confirmer l'authenticité des appels et des messages qui utilise un numéro issu du plan de numérotation établi par l'autorité comme identifiant d'appelant, et impliquant la mise en place d'une PKI conforme à l'IETF Public Key Infrastructure X.509 (IETF PKIX).

Ce document a pour vocation de fournir les règles d'utilisation de la PKI à respecter par les différents acteurs, et notamment pour les opérateurs afin de connaître leurs obligations et leurs droits.

## 1.1 Introduction

Introduction

Le **mécanisme de confiance** retenu pour la France embarque les éléments de la solution STIR/SHAKEN, couvrant les besoins suivants :

- Authentification de l'appelant et de son numéro
- Signature des appels par l'opérateur d'origine/signataire
- Vérification de la signature des appels par l'opérateur de terminaison, voire de transit
- Coupure des appels dans le cas d'échec de leur vérification

Cette solution se base sur l'utilisation de certificats – appelés certificats opérateur. C'est le socle du mécanisme d'authentification qui permet de signer et de vérifier les appels SIP, en faisant confiance aux certificats opérateurs délivrés par l'autorité de confiance, ainsi que de faire circuler l'attestation SHAKEN dans les échanges SIP entre opérateurs interconnectés.

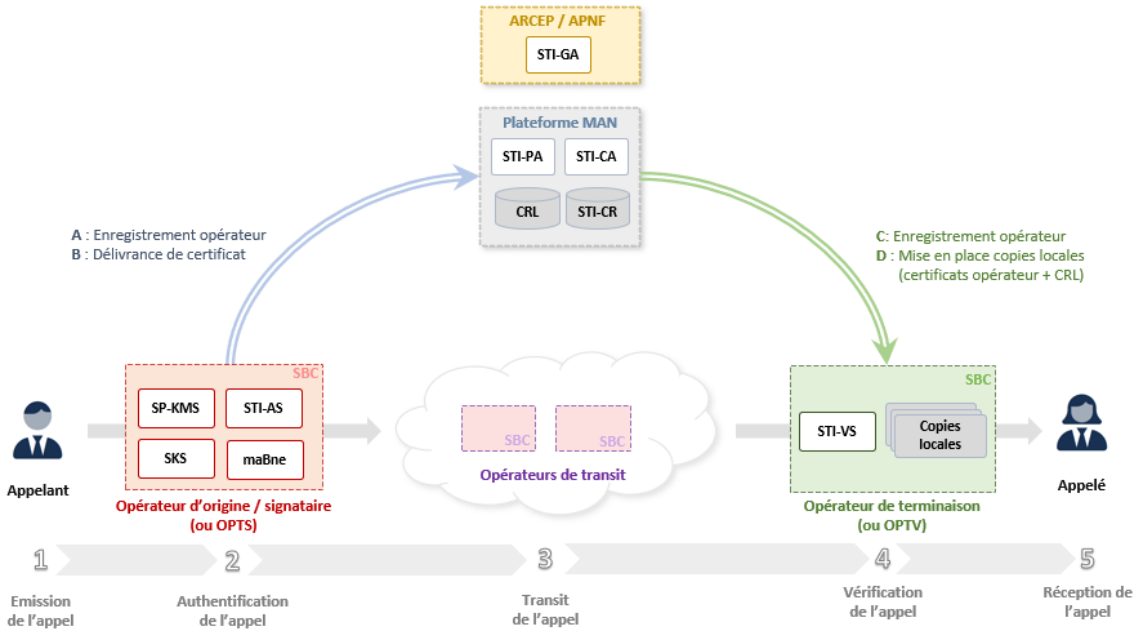
Les échanges utilisant des protocoles non-SIP ne sont pas concernés par ce mécanisme.

Le modèle français reprend l'architecture logique définie par la spécification ATIS-100080, mais en simplifie la gestion en fonctionnant avec une autorité de certification STI-CA unique, permettant ainsi la centralisation des certificats délivrés aux opérateurs français au sein d'un seul STI-CR géré par cette entité.

Le **STI-PA** n'ayant plus à gérer de multiples **STI-CA**, sa mission se réduit à l'application des règles énoncées par le **STI-GA** pour l'admission des opérateurs à la communauté STIR. Pour des soucis de simplification, il est décidé de regrouper les responsabilités de STI-PA et STI-CA au sein d'une seule et même entité, en charge d'une plateforme logicielle regroupant l'ensemble des fonctionnalités et appelée **plateforme MAN**.

D'autres acteurs s'adjoignent enfin à cette plateforme afin de couvrir les autres aspects du mécanisme de confiance :

- Une autorité de gouvernance, prenant la responsabilité du **STI-GA**
- Les opérateurs en charge de l'acheminement des appels



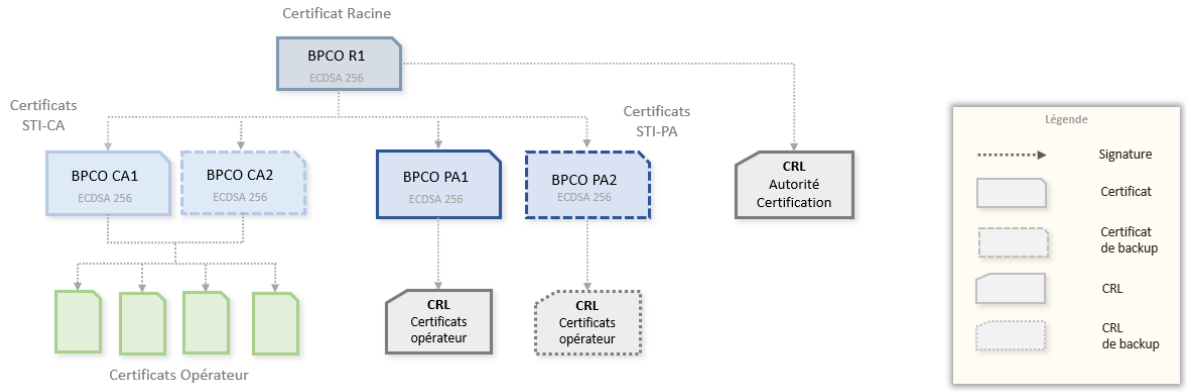

Ce document se focalise sur les règles de gestion de la PKI et les fonctionnalités fournies par l'autorité de certification.

## 1.2 Généralités

Overview

L'infrastructure à clé publique (ICP ou PKI) sécurisée mise en place par l'autorité de certification nécessite la mise en place d'une hiérarchie de certificats :

- Un **certificat racine**, hors-ligne, chargé de signer les certificats intermédiaires, les certificats PA et la liste de révocation des certificats intermédiaires et PA
- Des **certificats intermédiaires**, en ligne, correspondant au STI-CA dans le cadre STIR SHAKEN, chargés de signer les certificats opérateurs
- Des **certificats PA**, correspondant au STI-PA dans le cadre STIR SHAKEN, chargés de signer la liste de révocation des certificats opérateurs et des JSON Web tokens utilisés dans les APIs fournissant les informations de l'autorité de certification.
- Une liste de révocation (CRL) pour les certificats opérateur, signée par un certificat PA
- Une liste de révocation (CRL) pour les certificats intermédiaires et PA, signée par le certificat racine




## 1.3 Nom et date de publication

Document Name and Identification

Ce document décrit la politique de gestion des certificats opérateurs dans le cadre du mécanisme d'authentification des numéros (MAN).

- La version 1.0 a été approuvée pour publication le 3 avril 2025

Ce document est associé à l'OID (Object Identifier) **1.2.250.1.695.1.1.1.0**, inclus au sein de l'extension correspondante des certificats opérateurs.

## 1.4 Acteurs de la PKI

PKI participants

Le modèle français reprend l'architecture logique définie par la spécification ATIS-100080, mais en simplifie la gestion en fonctionnant avec une autorité de certification STI-CA unique, permettant la centralisation des certificats délivrés aux opérateurs français au sein d'un seul STI-CR géré par cette entité.

Cette section présente les différents acteurs concernés par le mécanisme de confiance et la délivrance des certificats opérateur utilisés pour la signature et la vérification des appels.

### 1.4.1 Autorités de certification

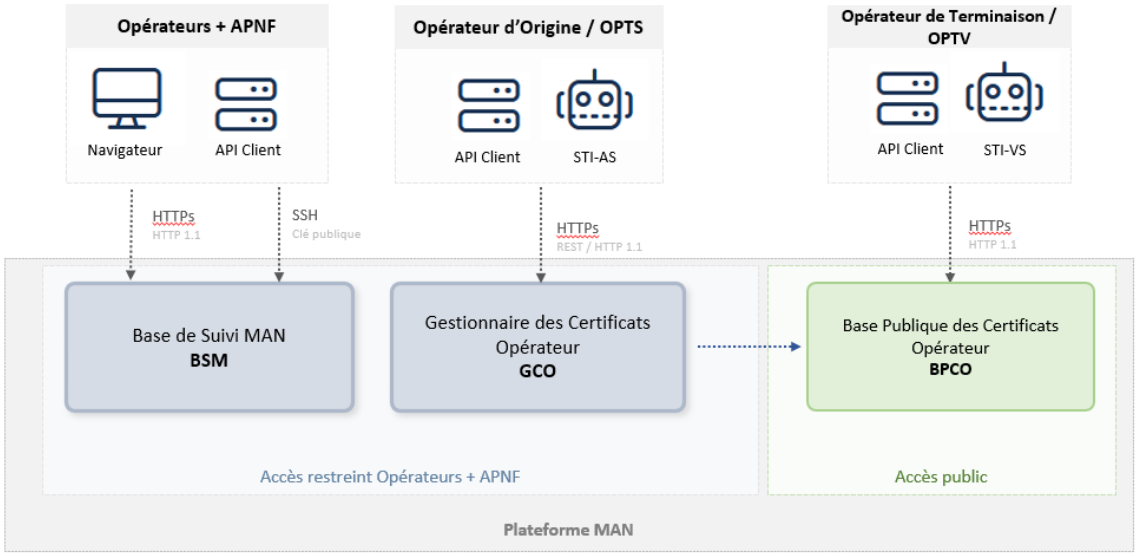
Certification Authorities

L'autorité de certification a la charge de l'infrastructure à clé publique (PKI) permettant la délivrance des certificats aux opérateurs dans le cadre du MAN. La plateforme MAN représente le socle logique et technique permettant à l'autorité de certification d'effectuer ses opérations de délivrance des certificats opérateurs. Cette plateforme a pour vocation d'être utilisée directement ou indirectement

par la totalité des opérateurs télécoms opérant sur le territoire français et procédant à l'acheminement des appels voix et des messages.

Les composants de la plateforme en charge de la mise en œuvre du mécanisme de confiance sont :

- Le Gestionnaire des Certificats Opérateur (**GCO**), en charge de l'ensemble des processus métier liés à la délivrance, publication et gestion des certificats opérateurs
- La Base Publique des Certificats Opérateur (**BPCO**), regroupant les certificats et données
- L'autorité de certification en charge de l'infrastructure à clé publique utilisée par le GCO pour la délivrance des certificats opérateur




### 1.4.2 Autorités de régulation

Registration Authorities

L'autorité de gouvernance (**STI-GA)** du mécanisme de confiance est représentée par le Comité d'orientation MAN. Le rôle de cette entité est de définir les politiques et règles de gestion du mécanisme de confiance en France, incluant :

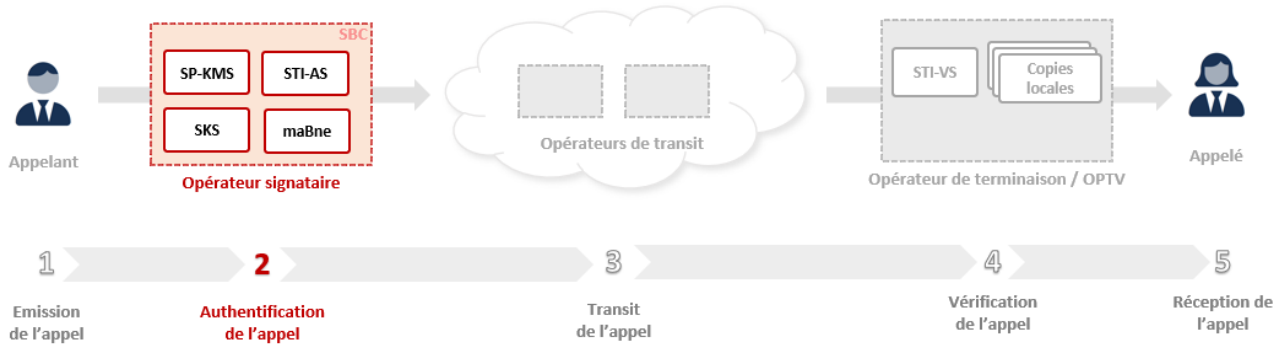
- la rédaction des règles de fonctionnement de l'entité STI-CA / STI-PA
- les règles de gestion des certificats (durée de validité, cycle de vie)
- la définition des critères d'appartenance d'un opérateur à la communauté STIR
- la fourniture à la plateforme MAN de la liste des opérateurs approuvés
- la fourniture à la plateforme MAN de la liste d'opérateurs à révoquer

### 1.4.3 Souscripteurs

Subscribers

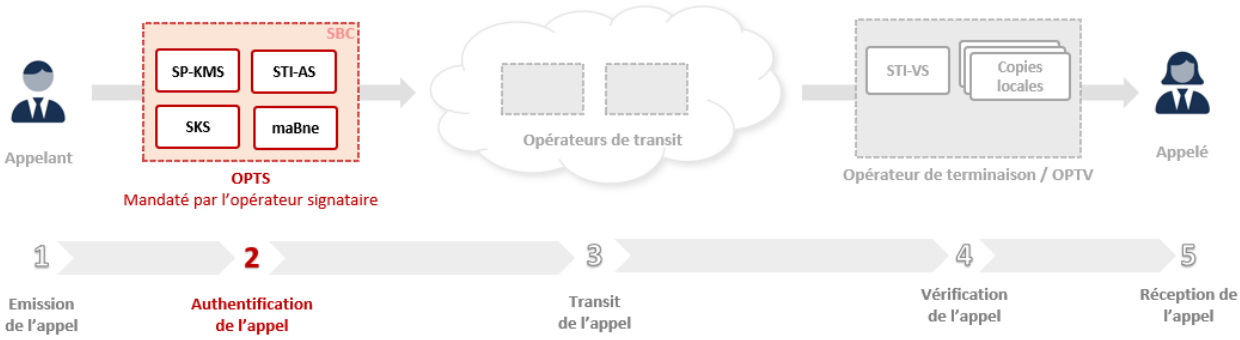
L'**opérateur d'origine** est l'opérateur qui détient le contrat de service avec le client final émetteur de l'appel. Il collecte physiquement les appels émis par le client final. Lorsqu'un appel est émis en SIP sur le réseau public, l'opérateur signataire correspond à l'opérateur d'origine, sauf pour les cas de mises à disposition et certains cas d'appels pour les MVNO.

L'**opérateur signataire** est l'opérateur détenteur du certificat utilisé pour la signature de l'appel et qui est responsable des informations véhiculées dans le cadre du MAN (dont le niveau d'attestation shaken).




Le mécanisme de confiance permet de plus à un opérateur signataire de mandater l'opérateur qui émet vers le réseau public ses appels pour les signer pour son compte. Ce dernier est dit « **OPérateur Technique de Signature (OPTS)** ».

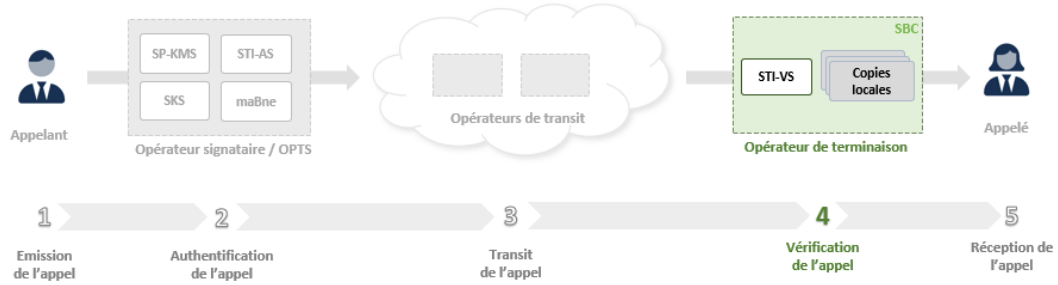
L'OPTS se substitue par conséquent à l'opérateur signataire dans la phase d'émission de l'appel et devient responsable de la procédure à suivre. Le certificat généré pour un opérateur signataire mandatant un OPTS par la plateforme MAN est appelé certificat indirect et la procédure liée à sa délivrance est sensiblement différente que pour un certificat direct, car nécessitant l'intervention de l'opérateur signataire et de l'OPTS.



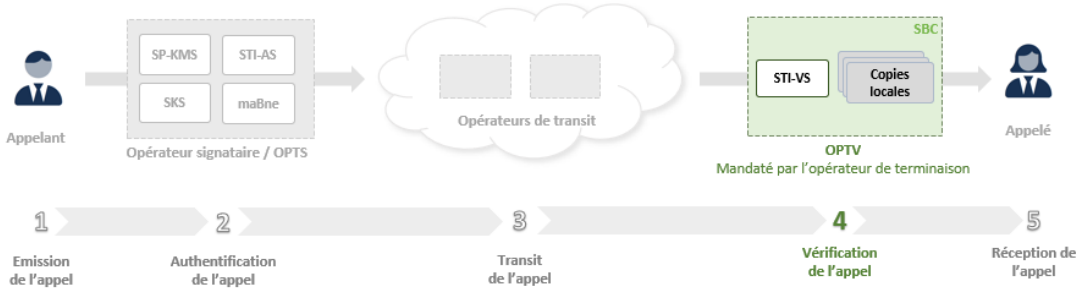
### 1.4.4 Consommateurs

Relying Parties

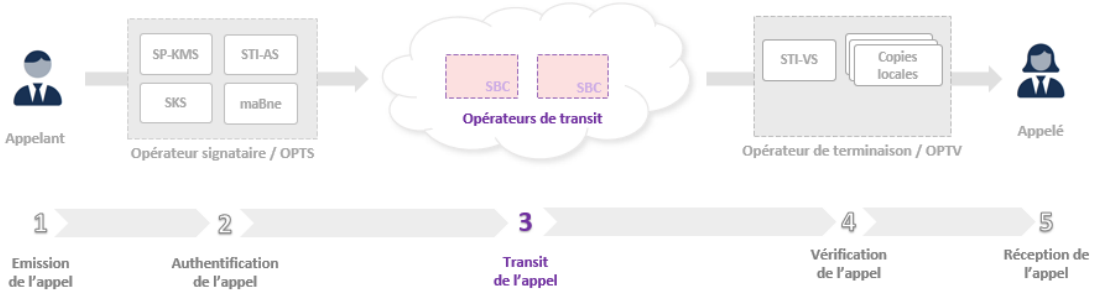
L'**opérateur de terminaison** est à la réception de l'appel SIP ; il est en charge de vérifier la signature de l'appel tel que défini par les documents RFC 8224, ATIS-100074 et ATIS-1000082 et de casser l'appel en cas d'échec.




Le mécanisme de confiance introduit aussi un **OPérateur Technique de Vérification (OPTV)**, mandaté par un opérateur de terminaison pour appliquer les règles MAN pour son compte. L'OPTV doit par conséquent effectuer les mêmes contrôles attendus de l'opérateur de terminaison.




**L'opérateur de transit** voit l'appel SIP transiter par son réseau. Sa responsabilité est limitée à la vérification de la présence de la signature de l'appel et au format de la signature de l'appel.



## 1.5 Modalités d'utilisation des certificats

Certificate Usage

### 1.5.1 Cas d'utilisation attendus

Appropriate Certificate Usage

Les certificats délivrés dans le cadre du MAN sont utilisés exclusivement pour permettre aux opérateurs, qu'ils soient signataire ou OPTS, de signer leurs appels en émission et aux opérateurs de terminaison, voire de transit, de vérifier la signature de ces appels, opérations détaillées par le protocole STIR/SHAKEN et notamment dans l'ATIS-1000074.

Deux types de certificats opérateurs sont supportés, directs et indirects, pour lesquels la procédure de délivrance des certificats diffère. Une fois le certificat délivré, les procédures de signature d'un appel et de vérification restent inchangées.

**Certificats Directs**

Un certificat direct permet à un opérateur signataire de signer en son nom les appels.

**Certificats Indirects**

Un certificat indirect permet à un opérateur signataire de mandater un autre opérateur pour signer ses appels, dénommé OPTS. Comme pour le certificat direct, le certificat indirect permet toujours d'identifier l'opérateur signataire dans la signature de l'appel, mais cette signature utilise une paire de clés détenue par l'OPTS. La procédure de création du certificat indirect nécessite par conséquent l'intervention des deux opérateurs :

- L'opérateur signataire, qui initie la demande de création du certificat indirect en choisissant l'OPTS à mandater
- L'OPTS pour finaliser la création en fournissant le CSR lié à ses clés de chiffrement

Les contextes d'utilisation de ces certificats sont détaillés au sein du document « Mode Opératoire du Mécanisme de Confiance ».

### 1.5.2 Cas d'utilisation interdits

Prohibited Certificate Uses

Toute utilisation des certificats opérateur en dehors du cadre défini par la section §0, et plus généralement en dehors du cadre du MAN, est prohibée.

De plus, le MAN ne supporte pas la gestion des certificats délégués décrits dans le document ATIS-1000092.

## 1.6 Organisation en charge de ce document

Policy Administration

### 1.6.1 Organisme

Organization Administering the Document

La rédaction et la publication de ce document sont prises en charge par l'APNF (Association des Plateformes de Normalisation des Flux inter opérateurs) :

*APNF*
*17, Rue de l'Amiral Hamelin*
*Paris, 75016*
*France*

### 1.6.2 Contact

Contact Person

Toute question concernant ce document ou le programme MAN dans son ensemble doit contacter l'APNF par email à l'adresse contact@apnf.fr

### 1.6.3 Procédures d'approbation

CPS Approval Procedures

Le contenu de ce document est soumis au Comité d'Orientation MAN, qui l'approuve pour publication. Une fois approuvée, la plateforme MAN doit mettre à jour la procédure de génération et gestion des certificats opérateurs afin de se conformer à la nouvelle politique mise en place sous un délai de 60 jours.

## 1.7 Documents de références

References

### 1.7.1 Standards internationaux

International References

Le mécanisme d'authentification des numéros (MAN) s'appuie sur le protocole STIR/SHAKEN, solution industrielle, normalisée, interopérable et utilisée à l'international. Les documents de référence suivants ont été utilisés lors de son élaboration :

- ATIS-1000074 Signature-based Handling of Asserted Information using Tokens (SHAKEN).
- ATIS-1000080 Signature-based Handling of Asserted Information using Tokens (SHAKEN): Governance Model and Certificate Management
- ATIS-1000082 Technical Report on SHAKEN APIs for a Centralized Signing and Signature Validation Server
- ATIS-1000084 Operational and Management Considerations for SHAKEN STI Certification Authorities and Policy Administrator
- RFC 3261 SIP: Session Initiation Protocol
- RFC 3326 Reason Header Field for the Session Initiation Protocol
- RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
- RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
- RFC 7515 JSON Web Signatures (JWS)
- RFC 7516 JSON Web Algorithms (JWA)
- RFC 7517 JSON Web Key (JWK)
- RFC 7518 JSON Web Algorithm (JWA)
- RFC 7519 JSON Web Token (JWT)
- RFC 8224 Authenticated Identity Management in the Session Initiation Protocol
- RFC 8225 PASSporT: Personal Assertion Token
- RFC 8226 Secure Telephone Identity Credentials: Certificates
- RFC 8588 Personal Assertion Token (PaSSporT) Extension for Signature-based Handling of Asserted information using toKENs (SHAKEN)

### 1.7.2 Références locales

Country Specific References

Les règles du MAN et leur implémentation sont définies par les documents énumérés ci-dessous :

- Plan Programme MAN, version 1.3
- Glossaire MAN, version 1.3
- Code de procédures MAN, version 1.9
- Mode opératoire du mécanisme de confiance, version 1.16
- Mode opératoire des incidents, signalements et métriques du MAN, version 1.15
- Règles techniques MAN, version 1.7
- MAN_Cas_Usages_Voix, version 1.3
- MAN_Cas_Usages_Messages, version 1.0
- Guides de référence des APIs de la plateforme MAN, version 1.7.0

Le présent document « Certificate policy » s'appuie sur les documents ci-dessus. Les numéros de versions mentionnées ci-dessus sont ceux à la date de la publication du présent document. Ces documents sont librement accessibles sur le site de la Fédération Française des Télécoms :
https://www.fftelecoms.org/man/man-mecanisme-dauthentification-des-numeros/

L'ensemble de ces documents sont sujets à révision. Toute nouvelle version de ces documents reste applicable à cette version du document tant qu'elle n'introduit pas de nouvelles notions ou modifications pouvant amener à une quelconque incompatibilité avec le mécanisme décrit par les versions de documents présentées ci-dessus.

Dans le cas où des incompatibilités sont introduites, une nouvelle version de ce document sera publiée et tout nouveau certificat délivré dans le cadre du MAN devra se référer à cette nouvelle version comme stipulé en section §4.3.

## 1.8 Glossaire

Definitions and Acronyms

Pour une liste complète des termes et acronymes utilisés dans le cadre du MAN, il convient de se référer au document « Glossaire MAN » disponible sur l'extranet de l'APNF et accessible à tous les opérateurs adhérents de l'APNF.

### 1.8.1 Définitions

Definitions

Les termes énumérés ci-dessous permettent de faciliter la lecture du présent document. Il est extrait du document « Glossaire MAN » qui fait référence.

**MAN - Mécanisme d'Authentification du Numéro** : Désigne la solution mise en œuvre en France permettant de confirmer l'authenticité des appels et messages utilisant un numéro issu du plan de numérotation établi par l'autorité comme identifiant d'appelant

**Client final** : Le client final désigne l'utilisateur du service de téléphonie, il peut générer ou recevoir un appel téléphonique., le client final a un contrat actif avec l'opérateur exploitant de son numéro.

**Code APNF :** Code à 6 caractères défini par l'APNF et permettant d'identifier de façon unique chaque opérateur

**Opérateur attributaire :** L'opérateur attributaire est l'opérateur qui s'est vu attribué des tranches de numéros par l'ARCEP conformément aux dispositions du plan national de numérotation.

**Opérateur exploitant :** L'opérateur exploitant est l'opérateur qui fournit un service de téléphonie au client final et ayant un contrat actif avec le client final. L'opérateur exploitant peut fournir le service de téléphonie avec des numéros dont il est l'opérateur attributaire, des numéros portés ou des numéros mis à sa disposition par des opérateurs attributaires tiers.

**Opérateur de terminaison :** L'opérateur de terminaison est l'opérateur de boucle locale qui livre l'appel au client final destinataire de l'appel.

**Opérateur de transit :** Un opérateur de transit est un opérateur intermédiaire connecté à des opérateurs de boucle locale ou de transit. Il collecte des appels depuis un opérateur de boucle locale ou depuis un autre opérateur de transit et livre les appels collectés à un opérateur de boucle locale ou à un autre opérateur de transit.

**Opérateur d'origine :** Un opérateur d'origine est l'opérateur qui collecte physiquement les appels émis par le client final. Lorsque l'appel est émis en SIP sur le réseau public, l'opérateur d'origine est l'opérateur signataire (sauf pour les cas de mises à disposition et certains cas d'appels pour les MVNO)

**Opérateur signataire :** C'est l'opérateur détenteur du certificat utilisé pour la signature de l'appel. Il est responsable des informations véhiculées dans le cadre du MAN (dont le niveau d'attestation Shaken).

**Opérateur émetteur d'un message :** Opérateur émettant un message depuis un SMS-C

**OPTS - Opérateur Technique de Signature** : Opérateur connecté au réseau public et mandaté par un opérateur signataire « au plus proche » du client pour signer les appels pour son compte. L'OPTS remplit la fonction STI-AS pour les appels collectés à signer

**OPTV Opérateur Technique de Vérification** : Opérateur mandaté par un opérateur de terminaison pour appliquer les règles MAN pour le compte de l'opérateur de terminaison, notamment vérifier (fonction STI-VS), voire casser les appels

**STI-AS - Secure Telephone Identification – Authentication Service :** Il s'agit du serveur d'application SIP qui exécute la fonction du service d'authentification défini dans la FC 8224. Il doit être lui-même hautement sécurisé et contenir le magasin de clés sécurisé (SKS) de la ou des clés privées secrètes ou avoir une interface authentifiée et cryptéesous le protocole TLS (Transport Layer Security) avec le SKS qui stocke la ou les clés privées secrètes utilisées pour créer des signatures PASSporT.

**STI-VS Secure Telephone Identity Verification Service :** Dans l'architecture STIR/SHAKEN, le STI-VS - Service de vérification - est le serveur d'application SIP qui exécute la fonction du service de vérification défini dans la RFC 8224. Il dispose d'une interface HTTPS (Hypertext Transfer Protocol Secure) avec le référentiel de certificats d'identité téléphonique sécurisé référencée dans le champ d'en-tête Identity pour récupérer le certificat de clé publique de l'opérateur.

**Protocole SIP STIR** protocole SIP FFT en version 3.1 ou supérieure ou SIP respectant les spécifications MAN telles que définies dans la section 11 du profil SIP FFT>=3.1

**Protocole SIP non STIR :** Protocole SIP ne respectant pas les spécifications MAN telles que définies dans la section 11 du profil SIP FFT>=3.1

**Protocole non SIP** : Tout protocole autre que SIP (ISUP, SIP-I par exemple)

### 1.8.2 Acronymes

Acronyms

**3GPP** 3rd Generation Partnership Project

**AC / CA** Autorité de Certification / Certificate Authority

**ACME** Automated Certificate Management Environment (Protocol)

**API** Application Programming Interface

**APNF** Association des Plateformes de Normalisation des Flux interopérateurs

**ATIS** Alliance for Telecommunications Industry Solutions

**CN** Common Name

**CRL** Certificate Revocation List

**CP** Certificate Policy
**CPS** Certification Practice Statement
**CR** Certificate Repository
**CSR** Certificate Signing Request
**DN** Distinguished Name
**DTPG** Documentation Technique des Pratiques Générales
**ECDSA** Elliptic Curve Digital Signature Algorithm
**HTTPS** Hypertext Transfer Protocol, Secure
**HSM** Hardware Security Module
**IETF** Internet Engineering Task Force
**IGC** Infrastructure de Gestion de Clés
**IHM** Interface Homme Machine
**JSON** JavaScript Object Notation
**JWT** JSON Web Token
**MAN** Mécanisme d'Authentification du Numéro
**MNO** Mobile Network Operator
**MVNO** Mobile Virtual Network Operator
**OCSP** Online Certificate Status Protocol
**OID** Object Identifier
**OPTS** OPérateur Technique de Signature
**OPTV** OPérateur Technique de Vérification
**PKI** Public Key Infrastructure
**PKIX** Public Key Infrastructure for X.509 Certificates
**PMA** Policy Management Authority
**REST** Representational state transfer
**SHAKEN** Signature-based Handling of Asserted information using toKENs
**SIP** Session Initiation Protocol
**SKS** Secure Key Store
**SP** Service Provider
**SPC** Service Provider Code
**SP-KMS** SP Key Management Server
**STI** Secure Telephone Identity
**STI-AS** Secure Telephone Identity Authentication Service
**STI-CA** Secure Telephone Identity Certification Authority
**STI-CR** Secure Telephone Identity Certificate Repository
**STI-GA** Secure Telephone Identity Governance Authority
**STI-PA** Secure Telephone Identity Policy Administrator
**STI-VS** Secure Telephone Identity Verification Service
**STIR** Secure Telephone Identity Revisited
**TN** Telephone Number
**UH** Unité d'Horodatage
**URI** Uniform Resource Identifier
**VoIP** Voice over Internet Protocol

# 2 PUBLICATION DES CERTIFICATS ET RESPONSABILITES

PUBLICATION AND REPOSITORY RESPONSIBILITIES

Pilotée par l'entité unique STI-CA/STI-PA, la plateforme MAN représente le socle logique et technique du plan programme MAN, fournissant l'ensemble des fonctionnalités prévues par celui-ci, dont la publication des certificats opérateurs et des certificats de l'autorité de certification.

Cette plateforme a pour vocation d'être utilisée directement ou indirectement, par la totalité des opérateurs télécoms opérant sur le territoire français et procédant à l'acheminement des appels voix et des messages.

La publication étant gérée de façon centrale par la plateforme MAN, les opérateurs n'ont aucune obligation de maintenir de leur côté une base de leurs certificats accessible publiquement.

## 2.1 Dépôt des certificats

Repositories

La plateforme MAN publie l'ensemble des certificats opérateurs au sein d'une base unique et publique appelée **BPCO** (Base Publique des Certificats Opérateur), dont une explication détaillée est disponible au sein du document "Mode Opératoire du Mécanisme de Confiance".

## 2.2 Modalités de publication

Publication of Certification Information

La BPCO consiste en un service Web accessible publiquement sur Internet et de façon sécurisée via le protocole HTTPs.

Cette base fournit un accès à l'ensemble des certificats opérateurs générés dans le cadre du MAN, mais aussi à tous les composants publics de la PKI utilisée dans la cadre de la signature des certificats opérateur, à savoir:

- Les certificats racines valides de l'autorité de certification
- Les certificats intermédiaires valides de l'autorité de certification
- Les certificats PA valides de l'autorité de certification
- La CRL valide des certificats opérateur
- La CRL valide des certificats de l'autorité de certification.

Une fois révoqué, un certificat reste disponible au sein de la BPCO pendant une durée définie dans le cycle de vie des certificats et précisée dans le "Mode Opératoire du Mécanisme de Confiance" avant d'être retiré.

## 2.3 Date et fréquence des publications

Time or Frequency of Publication

Tout nouveau certificat opérateur généré par la plateforme MAN est immédiatement publié au niveau de la BPCO. De même, les CRLs sont publiées immédiatement après leur mise à jour.

Les certificats racines, intermédiaires et PA de l'autorité de certification sont renouvelés suivant leur cycle de vie et publiés immédiatement après leur génération. Une période de recouvrement avec les certificats actuels est mise en place, permettant aux opérateurs de pouvoir récupérer ces certificats avant toute utilisation effective de ces derniers.

Le cycle de vie ainsi que les procédures de mise à jour de ces composants sont détaillées au sein du document "Mode Opératoire du Mécanisme de Confiance".

## 2.4 Contrôles d'accès aux dépôts

Access Controls on Repositories

Les données publiées par la BPCO sont des données publiques accessibles de tous. Des procédures sont mises en place afin d'assurer la disponibilité du service et de prévenir toute possibilité de modification des données publiées à partir de celui-ci.

# 3 IDENTIFICATION ET VALIDATION

IDENTIFICATION AND AUTHENTICATION

Seuls les opérateurs de la communauté MAN peuvent se voir délivrer des certificats dans le cadre du MAN, les conditions d'appartenance à cette communauté étant spécifiées au sein du document "Code de Procédures MAN".

Cette section précise les procédures d'admission de ces opérateurs à la communauté, les méthodes d'identification de chaque opérateur et d'authentication aux services leur permettant d'accéder aux fonctionnalités de la PKI de la plateforme MAN.

## 3.1 Nomenclature

Naming

Chaque opérateur de la communauté MAN est identifié de façon unique par un code régi par l'APNF, appelé "code APNF".

Le code APNF de l'opérateur est inclus au sein du Common Name (CN) de chaque certificat et qui, associé aux autres propriétés C, O, OU et autres, permet de créer un Distinguish Name (DN) unique à chaque opérateur pour tous les certificats qui lui sont délivrés.

Chaque certificat d'un opérateur peut être identifié de manière unique grâce au Serial Number qui lui est associé, la plateforme MAN garantissant une valeur unique pour chaque certificat qu'elle délivre.

La notion d'anonymat des certificats et des opérateurs n'est pas retenue dans le cadre du MAN, l'association d'un opérateur à un certificat étant nécessaire au bon fonctionnement de la solution.

## 3.2 Vérification initiale de l'entité

Initial Identity Validation

### 3.2.1 Vérification de l'identité de l'organisation

Authentication of Organization Identity

Avant de pouvoir accéder aux fonctionnalités de la plateforme MAN, les opérateurs doivent être admis au sein de la communauté MAN via une procédure initiale d'admission où l'opérateur doit faire valider son identité. La procédure détaillée de vérification est décrite dans le document "Code de Procédures MAN".

### 3.2.2 Vérification de l'identité des individus de l'organisation

Authentication of Individual Identity

Lors de sa souscription au service MAN, une personne physique est désignée par l'opérateur comme point de contact légal ; Lors de la phase de vérification initiale de l'identité de l'opérateur, l'identité de cette personne est vérifiée avant de pouvoir créer effectivement l'opérateur au niveau de la plateforme MAN.

### 3.2.3 Validation des autorisations

Validation of Authority

Une fois l'opérateur et le point de contact vérifiés, un compte est créé pour le point de contact légal ; celui-ci a alors la possibilité de créer des comptes individuels pour chaque collaborateur devant participer au MAN au sein de son entité.

Un profil est appliqué à chaque compte qui permet de définir les permissions octroyées.

Une authentification forte obligatoire est appliquée pour chaque compte créé au niveau de la plateforme afin de renforcer la sécurité des accès à la plateforme.

### 3.2.4 Modalités d'interopérabilité

Criteria for Interoperation

Aucune interaction avec des PKIs externes n'est prévue ou autorisée dans le cadre du MAN.

## 3.3 Vérification périodique de l'identité

Regular Identity Validation

En plus de la vérification initiale effectuée lors de l'admission à la communauté MAN, chaque opérateur fait l'objet d'une vérification annuelle afin de vérifier que les données de l'opérateur dont les coordonnées de son administrateur légal sont toujours valides.

En cas de succès, les droits de l'opérateur (accès à la plateforme MAN, gestion de ses certificats) sont prorogés d'une année.

Dans le cas contraire, des actions seront menées à l'encontre de l'opérateur.

## 3.4 Identification et authentification des demandes

Identification and Authentication for Requests

La plateforme MAN met à disposition des opérateurs les fonctionnalités de délivrance, de renouvellement et de révocation des certificats par l'intermédiaire de deux interfaces distinctes:

- Une IHM accessible aux personnes physiques, dont l'accès est protégé par une authentification forte et les fonctionnalités accessibles en fonction du rôle associé au compte utilisateur.

- Des services web dont l'accès est restreint par l'utilisation d'access tokens dont la délivrance est régie par le protocole OpenAPI et des API credentials créés à partir de l'IHM de la plateforme.

### 3.4.1 Identification et authentification des demandes de changement de clé

Identification and Authentication for Re-key Requests

La fonctionnalité de "rekey" de certificats n'est pas possible dans le cadre du MAN. L'opérateur doit révoquer le certificat existant et créer un nouveau certificat avec une nouvelle clé privée.

Les fonctionnalités de révocation et création de certificats sont restreintes aux utilisateurs de l'opérateur disposant des droits nécessaires et pouvant s'authentifier auprès de la plateforme.

### 3.4.2 Identification et authentification des demandes de révocation

Identification and Authentication for Revocation Requests

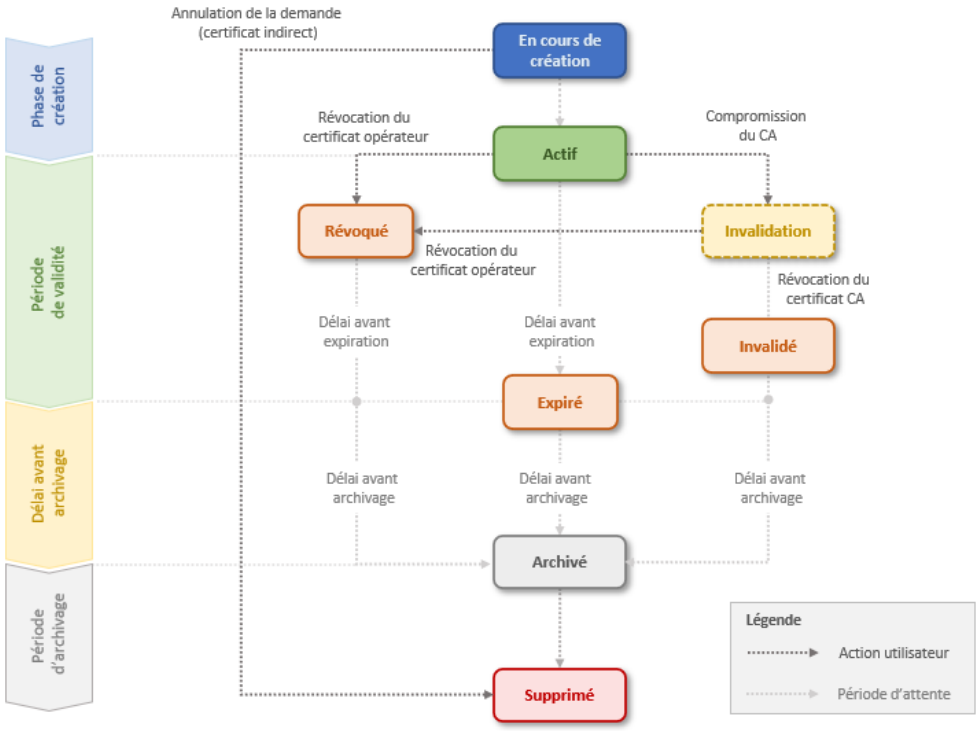
La révocation de certificats opérateur directs ne peut être effectuée que par l'opérateur signataire. Dans le cas des certificats opérateurs indirects, la révocation peut être effectuée par l'opérateur signataire ou l'OPTS ayant finalisé le certificat. L'opérateur a la charge de sélectionner quel certificat il souhaite révoquer et la raison de cette révocation.

Les fonctionnalités de révocation de certificats sont restreintes aux utilisateurs ou clients API de l'opérateur disposant des droits nécessaires et pouvant s'authentifier auprès de la plateforme.

# 4 GESTION DU CYCLE DE VIE DES CERTIFICATS

CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

Le document « Mode opératoire du mécanisme de confiance » fournit une explication détaillée du cycle de vie des certificats opérateurs et des procédures mises en place pour la gestion de ces certificats tout au long de leur cycle de vie. Un grand nombre de références est par conséquent utilisé au sein de cette section pour permettre aux lecteurs d'obtenir de plus amples détails sur les procédures et les prérequis demandés.




*Cycle de vie d'un certificat opérateur tiré du document « Mode opératoire du mécanisme de confiance »*

## 4.1 Demande de certificat

Certificate Application

### 4.1.1 Entités eligibles

Who Can Submit a Certificate Application

La délivrance de certificats est réservée aux opérateurs de la communauté MAN disposant d'un compte en activité sur la plateforme MAN, et pour lesquels l'identité a été confirmée lors de la vérification initiale ou de la dernière vérification annuelle d'identité gérée par le STI-PA.

Seuls les utilisateurs de l'opérateur disposant des droits adéquats, ainsi que les clients d'API utilisant des credentials d'API valides peuvent initier la procédure de délivrance de certificats.

### 4.1.2 Modalités d'enregistrement et responsabilités

Enrollment Process and Responsibilities

Les procédures d'enrollement d'un opérateur au sein de la communauté MAN et de la vérification de son identité sont explicitées en section §3.2 de ce document.

Les demandes de certificats se font exclusivement de manière numérique via la plateforme MAN, où l'opérateur fournit le CSR nécessaire à la création du certificat opérateur, et contenant les informations propres à son identification.

L'opérateur a la charge de générer sa paire de clés et de conserver la clé privée de manière sécurisée. Cette clé n'est en aucun cas générée par la plateforme MAN ou fournie à celle-ci dans un quelconque contexte.

## 4.2 Traitement des demandes de certificats

Certificate application processing

### 4.2.1 Authentifications requises

Performing Identification and Authentication Functions

Les demandes de délivrance de certificats opérateur ne peuvent s'effectuer que par l'intermédiaire de la plateforme MAN, soit par des utilisateurs créés par l'opérateur et authentifiés à travers une procédure nécessitant l'utilisation d'une authentication forte, soit par des clients API implémentés par l'opérateur et devant s'authentifier chacun de ses appels par le biais du protocole OAuth 2.0, où des access tokens sont délivrés pour une durée de vie limitée.

### 4.2.2 Validation des demandes

Approval or Rejection of Certificate Applications

Toute demande de certificats effectuée par un opérateur dont l'identité n'a pu être vérifiée, ou par un utilisateur d'un opérateur ne disposant pas des droits nécessaires ou dont le compte a été désactivé sera rejetée.

Un opérateur ne peut demander de certificats que pour son propre compte. Toute demande effectuée avec le nom d'un autre opérateur dans le CSR est rejetée.

### 4.2.3 Délai de traitement des demandes

Time to Process Certificate Applications

Si elle est approuvée par la plateforme MAN, la délivrance de certificats opérateurs est traitée de manière synchrone par rapport à la demande effectuée, et l'opérateur se voit immédiatement octroyé le certificat demandé.

## 4.3 Génération de certificats

Certificate Issuance

Les procédures de délivrance de certificats opérateur directs et indirects, leurs étapes et les responsabilités de chacune des parties sont propres à la solution MAN implémentée pour la France et sont détaillées dans le document « Mode Opératoire du Mécanisme de Confiance ».

La date de début de validité de tout certificat délivré par la plateforme MAN ne peut être inférieure à la date de délivrance ajoutée d'une semaine, afin de permettre aux opérateurs tiers de pouvoir récupérer ce certificat au sein de leurs copies locales avant son utilisation effective.

Tout certificat délivré au plus tard 90 jours après la publication de ce document doivent faire référence à cette version du document, et ce tant qu'une nouvelle version ne soit publiée.

Il est attendu que tous les certificats générés par la plateforme MAN avant la date de publication de ce document n'incluent pas d'extension *Certificate Policy*. Il n'est pas nécessaire de révoquer ces certificats et ils peuvent être exploités par les opérateurs jusqu'à leur expiration ou révocation.

Dans le cas où une nouvelle version de ce document est publiée, il est attendu que tout certificat délivré 90 jours après la publication de cette nouvelle version devront faire référence à cette nouvelle version et se conformer aux spécifications détaillées dans celle-ci. Les certificats délivrés avec la version de ce document resteront valides et exploitables jusqu'à leur expiration ou révocation.

### 4.3.1 Actions de l'autorité de certification

STI-CA Actions During Certificate Issuance

La plateforme MAN se charge de publier pour l'opérateur le certificat nouvellement délivré au sein de la base publique des certificats opérateurs (BPCO) décrite en section §2.1 de ce document, afin de le rendre accessible de l'ensemble des opérateurs.

De plus, la plateforme MAN inclut ce nouveau certificat dans une archive privée, récupérable des opérateurs de la communauté MAN via les APIs sécurisées de la plateforme afin de leur permettre de mettre à jour leur copie locale des certificats opérateurs.

### 4.3.2 Notification de la délivrance des certificats au souscripteur

Notification to Subscriber by the STI-CA of Issuance of Certificate

La délivrance du certificat s'accompagne d'une notification par mail envoyée aux opérateurs concernés, à savoir l'opérateur signataire pour un certificat direct, l'opérateur signataire et l'OPTS pour un certificat indirect.

## 4.4 Acceptation des certificats délivrés

Certificate Acceptance

### 4.4.1 Fonctionnalités d'accès aux informations en vue de l'approbation

Conduct Constituting Certificate Acceptance

La plateforme MAN garde à disposition de l'opérateur la liste des certificats dont ce dernier a fait la demande, avec les informations nécessaires permettant à l'opérateur de confirmer l'accès à ses certificats et les données incluses. Dans le cas où l'opérateur décèle un problème, il peut immédiatement révoquer le certificat comme décrit en section §4.9.

### 4.4.2 Publication du certificat par l'autorité de certification

Publication of the Certificate by the STI-CA

La plateforme MAN se charge de publier pour l'opérateur le certificat nouvellement délivré au sein de la base publique des certificats opérateurs (BPCO) décrite en section §2.1 de ce document, afin de le rendre accessible de l'ensemble des opérateurs.

### 4.4.3 Notification de la délivrance du certificat aux autres acteurs

Notification of Certificate Issuance by the STI-CA to Other Entities

Aucune notification explicite n'est effectuée par la plateforme MAN aux autres opérateurs de la communauté MAN.

La plateforme indique néanmoins qu'un nouveau certificat opérateur a été publié par la mise à jour de la date de dernière modification de la BPCO retournée par les API de la plateforme MAN dédiées à cet objectif. Les opérateurs effectuant des vérifications régulières peuvent ainsi être notifiés et récupérer ce nouveau certificat afin de mettre à jour leur copie telle que préconisée par le document « Mode Opératoire du Mécanisme de Confiance ».

## 4.5 Modalités d'utilisation des paires de clé et des certificats

Key Pair and Certificate Usage

### 4.5.1 Gestion de la clé privée et du certificat par le souscripteur

Subscriber Private Key and Certificate Usage

Chaque opérateur est responsable de la génération de sa paire de clés et ne doit en aucun cas divulger ou communiquer la clé privée. Il ne doit utiliser sa clé privée que dans le cadre du protocole STIR/SHAKEN, dans un premier temps pour la génération du CSR qui est fourni à la plateforme MAN pour la génération du certificat conformément au document ATIS-1000080, et dans un second temps pour la signature des appels qu'il émet via le protocole SIP. Le certificat délivré est utilisé par l'opérateur émetteur dans la génération du token PASSPorT et de l'entête Identity tel que précisé dans les RFC 8224 et 8225.

Le document « Mode Opératoire du Mécanisme de Confiance » détaille les procédures à suivre par l'opérateur pour la génération de sa paire de clé et la création de l'entête Identity à inclure dans ses appels SIP émis.

### 4.5.2 Gestion de la clé publique et du certificat par le consommateur

Relying Party Public Key and Certificate Usage

Les certificats opérateurs délivrés par la plateforme MAN ne peuvent être utilisés que dans la mise en place du protocole STIR/SHAKEN tel que décrit par les RFCs 8224, 8225 et les documents ATIS 1000074 et 100082. Tout opérateur de terminaison recevant un message SIP INVITE contenant un entête Identity se doit ainsi de vérifier la signature du token PASSPorT via le certificat opérateur dont l'URL est indiqué par ce dernier.

Le mode de récupération du certificat et de son utilisation lors de la vérification du token PASSPorT et de sa signature sont détaillés au sein du document « Mode Opératoire du Mécanisme de Confiance ».

## 4.6 Renouvellement des certificats

Certificate Renewal

La plateforme MAN met à disposition des opérateurs différentes solutions de renouvellement de ses certificats, toutes optionnelles :

- Un renouvellement manuel peut être déclenché par l'opérateur.
- L'opérateur peut aussi configurer la plateforme pour renouveler automatiquement un certificat après une période spécifiée par l'opérateur.

### 4.6.1 Cas de renouvellement

Circumstance for Certificate Renewal

Les certificats opérateurs ayant une durée de validité limitée, il est nécessaire que l'opérateur remplace régulièrement les certificats arrivant à expiration avec de nouveaux certificats. Le renouvellement de certificat permet à l'opérateur de garder la même paire de clé et de réduire ainsi la complexité lors du changement de certificat.

Il est demandé aux opérateurs d'effectuer le renouvellement au moins une semaine avant l'expiration du certificat actuel, afin de s'assurer que le nouveau certificat puisse être récupéré par les opérateurs tierces avant son utilisation effective.

### 4.6.2 Entités éligibles

Who May Request Renewal

Seul l'opérateur pour lequel le certificat a été délivré peut décider du renouvellement de ce certificat.

Ainsi, que ce soit pour un certificat direct ou indirect, seul l'opérateur signataire peut être à l'initiative du renouvellement.

### 4.6.3 Traitement des demandes de renouvellement

Processing Certificate Renewal Requests

Le renouvellement de certificats ne peut être effectué que pour des certificats n'ayant pas été préalablement révoqués ou invalidés par la plateforme MAN.

Les procédures de renouvellement de certificats opérateur directs et indirects, leurs étapes et les responsabilités de chacune des partie sont propres à la solution MAN implémentée pour la France et sont détaillées dans le document « Mode Opératoire du Mécanisme de Confiance ».

La plateforme MAN se charge de publier pour l'opérateur le certificat renouvelé au sein de la base publique des certificats opérateurs (BPCO) décrite en section §2.1 de ce document, afin de le rendre accessible de l'ensemble des opérateurs.

De plus, la plateforme MAN inclut ce nouveau certificat dans une archive privée, récupérable des opérateurs de la communauté MAN via les APIs sécurisées de la plateforme afin de leur permettre de mettre à jour leur copie locale des certificats opérateurs.

### 4.6.4 Notification de la délivrance du certificat au souscripteur

Notification of New Certificate Issuance to Subscriber

Les mêmes procédures présentées en section §4.3.2 s'appliquent dans le cadre du renouvellement de certificats.

### 4.6.5 Modalités d'approbation du certificat renouvelé

Conduct Constituting Acceptance of a Renewal Certificate

Les mêmes procédures présentées en section §4.4.1 s'appliquent dans le cadre du renouvellement de certificats.

### 4.6.6 Publication du certificats renouvelé par l'autorité de certification

Publication of the Renewal Certificate by the STI-CA

Les mêmes procédures présentées en section §4.4.2 s'appliquent dans le cadre du renouvellement de certificats.

### 4.6.7 Notification de la délivrance du certificat renouvelé aux autres acteurs

Notification of Certificate Issuance by the STI-CA to Other Entities

Les mêmes procédures présentées en section §4.4.3 s'appliquent dans le cadre du renouvellement de certificats.

### 4.6.8 Impact du renouvellement sur le certificat actuel

Certificate Issuance Impact on Current Certificate

Le certificat renouvelé est laissé tel quel par la plateforme MAN, et n'est en aucun cas révoqué une fois la procédure de renouvellement terminée. Il reste ainsi valide et utilisable jusqu'à son expiration effective.

L'opérateur a la possibilité, comme indiqué en section 4.9, de révoquer ce certificat une fois que celui-ci n'est plus utilisé.

## 4.7 Changement de clé publique du certificat

Certificate Re-key

Dans le cadre du MAN, il n'est en aucun cas possible de conserver le même certificat tout en changeant sa clé publique.

Si l'opérateur a besoin de changer sa clé publique (par exemple pour des raisons de compromission de clé privée, de perte de clé privée, etc), il doit générer de nouveaux certificats en suivant les procédures décrites en section §4.3 et, si besoin, révoquer ses anciens certificats.

## 4.8 Modification de certificat

Certificate Modification

Dans le cadre du MAN, il n'est pas possible d'effectuer de modifications aux données incluses dans un certificat, telles que les informations incluses dans le Distinguished Name ou toute extension spécifique à l'opérateur.

Si l'opérateur a besoin de changer une partie des informations incluses dans un certificat, il doit générer un nouveau certificat en suivant les procédures décrites en section §4.3 et, si besoin, révoquer l'ancien certificat.

## 4.9 Révocation et suspension de certificat

Certificate Revocation and Suspension

La révocation des certificats opérateurs est traitée par l'intermédiaire d'une liste de révocation des certificats (CRL), créée et maintenue par la plateforme MAN, et accessible publiquement de tous les opérateurs.

### 4.9.1 Cas de révocation

Circumstances for Revocation

La révocation de certificats doit être envisagée dans les cas où une possibilité de compromission de la clé privée associée au certificat, voire des clés privées utilisées dans la chaîne de certification est envisagée.

La révocation peut aussi avoir lieu dans les cas suivants :

- Cessation d'activité de l'opérateur
- Perte d'habilitation de l'opérateur
- Remplacement du certificat par un nouveau certificat
- Changement des informations de l'opérateur incluses dans le certificat

### 4.9.2 Entités éligibles

Who Can Request Revocation

Seuls les opérateurs partie prenante dans un certificat peuvent faire la demande de révocation de ce certificat. Ainsi, pour un certificat indirect, l'opérateur signataire et l'OPTS peuvent être à l'origine de la demande de révocation du certificat.

L'autorité de certification du MAN peut aussi être à l'initiative de la révocation des certificats opérateurs dans des cas très précis comme la résiliation d'un opérateur, cf. section §4.11.

### 4.9.3 Traitement des demandes de révocation

Procedure for Revocation Request

Toute demande de révocation à l'initiative d'un opérateur s'effectue par l'intermédiaire de la plateforme MAN, via son IHM ou ses APIs dédiées.

### 4.9.4 Période de grâce

Revocation Request Grace Period

Toute demande de révocation validée par la plateforme MAN est traitée immédiatement sans application d'un quelconque délai.

### 4.9.5 Délai de traitement de la demande de révocation

Time within which the Revocation Request must be Processed

Le traitement de la révocation est immédiat lors de la réception de la demande effectuée par l'opérateur. La plateforme ajoute ainsi le certificat à la CRL et publie cette dernière dans la foulée avant de confirmer le succès de la demande à l'opérateur.

### 4.9.6 Modalités de prise en compte de la révocation par les consommateurs

Revocation Checking Requirement for Relying Parties

Le MAN préconise que chaque opérateur garde une copie locale de la CRL publique, ainsi que la CRL de l'autorité de certification, afin d'optimiser les délais de vérification des appels. L'accès à la CRL publique ne doit être effectuée qu'en dernier recours, si jamais la copie locale est temporairement indisponible.

Le document « Mode Opératoire du Mécanisme de Confiance » précise la procédure à appliquer pour la mise en place et la synchronisation des copies locales.

### 4.9.7 Fréquence de délivrance de la CRL des certificats opérateurs

CRL Issuance Frequency (If Applicable)

La plateforme MAN publie une nouvelle version de la CRL des certificats opérateurs dès le traitement de la révocation d'un certificat. La plateforme s'assure aussi que la CRL n'expire pas en renouvelant automatiquement la CRL une fois par jour.

### 4.9.8 Latence maximale autorisée pour la CRL des certificats opérateurs

Maximum Latency for CRLs (If Applicable)

La publication de la CRL sur la BPCO est immédiate, la latence lors de la consultation de cette ressource est donc nulle. Dans le cas où l'opérateur utilise sa copie locale, une latence égale à la fréquence de mise à jour de sa copie locale est à prévoir.

### 4.9.9 Procédure de vérification en ligne du statut des certificats opérateurs

Online Revocation/Status Checking Availability

La plateforme MAN met à disposition de tous les opérateurs la CRL en accès public au sein de la BPCO (Base Publique des Certificats Opérateurs) via une URL HTTPs dédiée.

### 4.9.10 Modalités pour la vérification du statut des certificats

Online Revocation Checking Requirements

Bien que la CRL soit disponible en accès public, il est demandé à chaque opérateur de garder une copie locale de cette CRL, ainsi que la CRL de l'autorité de certification, afin d'optimiser les délais de vérification des appels. Voir la section §4.9.6.

### 4.9.11 Autres solution de notification de la révocation des certificats

Other Forms of Revocation Advertisements Available

Toute opération de révocation est accompagnée d'un mail envoyé par la plateforme MAN aux opérateurs associés au certificat révoqué, si tant est que les opérateurs ont bien configuré dans leur profil leur liste de diffusion.

### 4.9.12 Cas de révocation / suspension dû à la compromission de clé privée

Special Requirements Re-key Compromise

Non applicable.

### 4.9.13 Cas possibles de suspension de certificats

Circumstances for Suspension

La plateforme MAN ne propose pas la possibilité de suspendre les certificats opérateurs.

### 4.9.14 Entités pouvant effectuer une demande de suspension

Who Can Request Suspension

Non applicable comme indiqué en section §4.9.13.

### 4.9.15 Traitement des demandes de suspension

Procedure for Suspension Request

Non applicable comme indiqué en section §4.9.13.

### 4.9.16 Limites de la période de suspension

Limits on Suspension Period

Non applicable comme indiqué en section §4.9.13.

## 4.10 Services de vérification de statut des certificats

Certificate Status Services

L'objectif de la solution MAN est de pouvoir maintenir le mécanisme d'authentification des numéros même dans le cas d'indisponibilité temporaire de la plateforme MAN et de la Base Publique des Certificats Opérateurs (BPCO).

La plateforme MAN fournit pour cela des solutions afin de permettre non seulement aux opérateurs de vérifier le statut des certificats qui leur ont été délivrés, mais aussi aux opérateurs tiers d'être tenus à jour des créations et révocations effectuées par la plateforme afin de conserver une copie en locale des certificats valides.

### 4.10.1 Modalités d'utilisation

Operational Characteristics

La plateforme MAN permet à chaque opérateur de consulter via l'IHM ou les APIs dédiées la liste des certificats lui ayant été délivrés, avec le statut actuel de chaque certificat.

Il est de plus demandé à chaque opérateur de conserver une copie locale des certificats en cours d'activité afin de pallier à tout dysfonctionnement temporaire de la plateforme. Cette dernière met ainsi à disposition des opérateurs une API leur permettant de récupérer la liste de l'ensemble des certificats opérateurs valides, mais aussi la liste des certificats de l'autorité de certification. Les opérateur de la communauté MAN s'assurent ainsi de connaître l'ensemble des certificats valides et d'effectuer leurs opérations de vérification sans besoin d'effectuer de requêtes externes.

Les procédures de mise en place et de mise à jour de ces copies locales sont décrites au sein du document « Mode Opératoire du Mécanisme de Confiance ».

### 4.10.2 Disponibilité du service

Service Availability

L'IHM de la plateforme MAN reste accessible 24h/24, sauf périodes de maintenance préalablement déclarées aux opérateurs. Il en est de même des APIs publiées par la plateforme, avec des limites d'accès concurrents pour prévenir tout utilisation abusive des ressources de la plateforme.

### 4.10.3 Fonctionnalités additionnelles

Optional Features

Si l'opérateur a configuré la liste de diffusion adéquate au sein de la plateforme MAN, celle-ci peut le notifier dès qu'un de ses certificats est révoqué ou expiré.

## 4.11 Cessation d'activité

End of Subscription

La cessation d'activité d'un opérateur mène à sa résiliation de la communauté MAN :

- Les certificats actifs de l'opérateur sont révoqués ;
- L'opérateur est désactivé de la plateforme MAN.

## 4.12 Mise sous séquestre et récupération des clés

Key Escrow and Recovery

La plateforme MAN ne prévoit pas de solution de mise sous séquestre des clés des opérateurs, ces derniers ayant la charge de les conserver et préserver leur intégrité et disponibilité.

# 5 CONTROLES PHYSIQUES ET OPERATIONNELS

MANAGEMENT, OPERATIONAL AND PHYSICAL CONTROLS

Cette section décrit les procédures et contrôles opérationnels mis en place par le gestionnaire de la plateforme MAN pour garantir que les opérations offertes par la plateforme MAN, et notamment celles liées à la gestion de la PKI pour la délivrance et la gestion des certificats opérateurs, soient effectués dans un cadre sécurisé.

## 5.1 Sécurité des installations physiques

Physical Security Controls

Le prestataire en charge de la plateforme MAN et de sa PKI met à disposition de l'autorité de gouvernance et des parties prenantes un document officiel décrivant l'ensemble des mesures de protection appliquées. Le partage de ce document nécessite l'existence et la signature au préalable d'un "accord de non divulgation" (DNA).

### 5.1.1 Situation géographique et construction des sites

Site Location and Construction

Les environnements de la plateforme MAN sont installés sur les sites sécurisés de production conçus pour héberger des systèmes informatiques et télécom.

Les équipes administratives et opérationnelles de la PKI de la plateforme MAN opèrent sur les sites Worldline européens.

En particulier, l'ensemble des locaux hébergeant des systèmes impliqués dans le cadre de la génération et de la révocation des certificats sont opérés dans un environnement qui protège physiquement les services contre les menaces de compromission dues à un accès non-autorisé aux systèmes ou aux données. Le périmètre de la zone sécurisé est clairement identifié et ne peut être accédé par des personnels ou des organisations tierces non-autorisées.

### 5.1.2 Accès physique

Physical Access

Les sites et locaux qui accueillent la PKI de la plateforme MAN garantissent la sécurité physique des moyens mis en œuvre pour fournir les Service de Confiance.

Des mesures de contrôle d'accès physiques sont mis en place afin que les systèmes critiques des services de confiances ne puissent être accédés par des personnes non autorisées. Ces mesures de contrôle permettent de minimiser les risques associés à la sécurité physique des biens.

En particulier :

- les composants critiques sont isolés dans des périmètres de sécurité clairement définis ne sont accessibles qu'aux personnes autorisées ;
- les périmètres de sécurité font l'objet de mesures de protection physique contre les intrusions, de mesures de contrôle d'accès et d'alarmes en cas d'intrusion ;
- des mesures sont en place pour éviter le vol, la destruction ou la compromission des composants, ainsi que l'interruption de service ;
- des mesures sont en place contre la compromission ou le vol d'informations sensibles ;
- des mesures sont mises en place pour empêcher que des équipements, des informations, des supports et des logiciels ayant trait aux services de la PKI de la plateforme MAN soient sortis du site sans autorisation.

### 5.1.3 Alimentation électrique et climatisation

Power and Air Conditioning

Des mesures (générateurs de secours, …) sont mis en place afin de prévenir les pannes électriques et de simplifier les interventions de maintenance.

De même, des mesures (redondance du système, …) sont mises en place pour parer à des défaillances au niveau du système de climatisation. Ces mesures de prévention sont régulièrement maintenues et testées.

### 5.1.4 Vulnérabilité aux dégâts des eaux

Water Exposures

Des moyens de surveillances (capteurs, monitoring, …) sont en place pour prévenir les dégâts des eaux. Ces moyens de surveillances sont régulièrement maintenus et testés.

### 5.1.5 Prévention et protection incendie

Fire Prevention and Protection

Des mesures de prévention et de lutte contre les incendies (détecteurs, portes coupe-feu, …) sont en place pour prévenir tout risque d'incendie et protéger les composants de la plateforme MAN le cas échéant. Ces mesures de prévention et de protection sont régulièrement maintenues et testées.

### 5.1.6 Conservation des supports

Media Storage

Dans le cadre des activités de la PKI de la plateforme MAN, des sauvegardes de nature différente sont effectués. Des mesures sont mises en place pour assurer la disponibilité, la confidentialité et l'intégrité

des supports de sauvegarde utilisés. Ces mesures adressent les problématiques d'obsolescence et de détérioration des supports, en particulier lorsqu'il est nécessaire de conserver des données sur des périodes longues.

### 5.1.7 Mise hors service des supports

Waste Disposal

Tous les documents papier contenant des données confidentielles (PIN code, mot de passe, …) devenus inutiles ou obsolètes sont physiquement détruits.

Pour les supports physiques (disque, HSM, …) une procédure spéciale de stockage tampon en vue d'un broyage est mise en place. Cette destruction donne lieu à la production d'un Procès-Verbal. Notamment, en cas de mise hors service d'un HSM, les clés sont effacées au préalable en s'appuyant sur les fonctions de héroïsation du HSM.

### 5.1.8 Sauvegardes hors site

Off-site Backup

La PKI de la plateforme MAN met en place des sauvegardes hors site conformément aux procédures définies par le prestataire en charge de la plateforme. Les règles de sécurité relatives à la sortie des supports en dehors des locaux Worldline sont décrites dans la PSSI du prestataire.

## 5.2 Contrôles des procédures métier

Procedural Controls

### 5.2.1 Rôle de confiance

Trsuted Roles

La PKI de la plateforme MAN définit explicitement les rôles de confiance requis pour assurer le fonctionnement et la sécurité de celle-ci. Les définitions des rôles de confiance sont rendus disponibles à l'ensemble des personnels concernés.

Les fonctions opérées sur toutes les composantes des services de la PKI de la plateforme MAN sont réparties sur plusieurs types d'intervenants afin de veiller à la séparation des connaissances pour les tâches ou rôles sensibles. Les rôles de confiance intervenants dans l'organisation de la PKI de la plateforme MAN sont les suivants :

- **Administrateur HSM** : il est en charge des installations et configurations des boîtiers cryptographiques (HSM) de la PKI de la plateforme MAN ;

- **Administrateur système** : il est en charge des installations, configurations et maintenances des systèmes de confiance de la PKI de la plateforme MAN pour la gestion des services. Il est autorisé à effectuer la restauration de ces systèmes ; Il joue également le rôle d'opérateur système en étant notamment responsable de l'exploitation quotidienne des systèmes de confiance de la PKI de la plateforme MAN.
- **Auditeur système** : il est autorisé à consulter les archives et l'ensemble des journaux d'évènements des systèmes de confiance de la PKI de la plateforme MAN ;
- **Maître de cérémonie** : il est en charge de gérer la préparation et le déroulement des cérémonies de clés ;
- **Officier de sécurité** : il est en charge d'administrer l'implémentation des pratiques de sécurité et d'appliquer les contraintes techniques définies dans l'analyse de risque ;
- **Opérateur d'enregistrement** : il est chargé d'intervenir dans le processus de création de Certificats ;
- **Porteur de secrets** : il assure la confidentialité, l'intégrité et la disponibilité des secrets. Il est dépositaire des secrets et des clés physiques d'accès à leurs coffres. Il est membre d'une équipe dont l'ensemble des membres dispose des mêmes droits sur les accès aux coffres ;
- **Responsable d'application** : il est en charge d'assurer le suivi du service et de ses performances. Il coordonne et/ou réalise la maintenance corrective et évolutive de l'application ;
- **Responsable de la PKI de la plateforme MAN** : il est en charge de la mise en œuvre de la présente Certificate Policy, des PC-DPC et des PH-DPH ainsi que de la vérification de leur application. Il est notamment en charge de la révocation d'un certificat émis par les AC de la PKI de la plateforme MAN. Membre du Comité de gestion la PKI, il est aussi en charge de l'approbation des politiques (PC-DPC, PH-DPH et PA) et des analyses de risques de la PKI de la plateforme MAN ;
- **Responsable adjoint de la PKI de la plateforme MAN** : il est en charge des mêmes fonctions supportées par le Responsable de la PKI de la plateforme MAN ;
- **Responsable sécurité** : il est en charge de la définition des règles de sécurité autour de la PKI de la plateforme MAN ;
- **Responsable de Centre (datacenter)** : Il est en charge de la gestion du datacenter et des contrôles d'accès opérés.

Lors de l'enrôlement d'un nouveau membre dans un rôle de confiance au sein de la PKI de la plateforme MAN, un document actant de sa désignation doit être signé par la personne concernée, pour acceptation du rôle, par la responsable des ressources humaines et par le responsable de la PKI de la plateforme MAN ou l'un de ses adjoints. Ce document fait référence à la Documentation Technique des Pratiques Générales (DTPG) afin que le futur membre du personnel de confiance ait connaissance de la description de son rôle et des responsabilités qui lui sont affectées.

Il spécifie notamment :

- les engagements du signataire et leur bonne compréhension ;
- en cas de modification du document DTPG, le signataire en sera informé.
- Lors des prises de fonction du rôle de confiance, il est rappelé à la personne désignée qu'elle s'engage sur la non-utilisation frauduleuse des services et qu'elle s'engage à ne pas utiliser les

informations dont elle a connaissance pour d'autres finalités que celles définies par le service de confiance.

- De même, lors de la cessation d'un rôle de confiance au sein de la PKI de la plateforme MAN, un document actant de la cessation doit être signé par la personne concernée.

### 5.2.2 Nombre de personnes requises par tâche

Number of Persons Required Per Task

Selon le type d'opération effectuée, le nombre et les rôles des personnes devant être présentes, en tant qu'acteurs ou témoins, peut être différent.

Certaines tâches sensibles, telle que la génération du Certificat d'une autorité de certification, nécessitent plus d'une personne occupant un rôle de confiance au sein de la PKI de la plateforme MAN pour des raisons de sécurité.

### 5.2.3 Identification et authentification de chacun des rôles

Identification and Authentication for Each Role

Certains rôles de confiance sont occupés par plusieurs personnes pour que la PKI de la plateforme MAN puisse assurer la continuité de ses services sans dégrader la sécurité des services offerts.

Il est régulièrement vérifié que l'ensemble des rôles de confiance définis ci-dessus sont pourvus.

### 5.2.4 Rôles nécessitant une séparation des fonctions

Roles Requiring Separation of Duties

Il est autorisé que plusieurs rôles soient opérés par une même personne. Cependant, dans le cadre des activités de la PKI de la plateforme MAN et pour des raisons de sécurité, certains rôles ne peuvent pas être opérés par la même personne.

De façon générale, les rôles et responsabilités sont attribués sur le principe du moindre privilège afin de limiter le risque de conflit d'intérêt et limiter les opportunités de réalisation d'actions non autorisées ou de mauvaise utilisation des biens mis en œuvre par le Service de Confiance.

## 5.3 Procédures de qualification et vérification du personnel

Personnel Security Controls

### 5.3.1 Qualifications, compétences et habilitations requises

Qualifications, Experience, and Clearance Requirements

La plateforme MAN est opérée par du personnel, ou le cas échéant des fournisseurs, possédant l'expérience, les compétences, les qualifications et l'expertise nécessaires aux opérations d'un Service de Confiance.

Le personnel opérant des rôles de confiance au sein de la plateforme MAN est informé de ses responsabilités ainsi que des procédures liées à la sécurité des systèmes et au contrôle du personnel auxquelles il doit se conformer.

Le personnel d'encadrement est formé et sensibilisé à la sécurité et à la gestion des risques, sont familiers des procédures de sécurité en place et ont une expérience de la sécurité informatique suffisante pour assumer pleinement ses responsabilités vis-à-vis des services fournis par la plateforme MAN.

Les procédures administratives et d'encadrement des personnels sont conçues et maintenues en ligne avec les procédures de gestion de la sécurité de l'information.

Le prestataire en charge de la plateforme MAN s'assure de la qualification et de la compétence de son personnel opérant un rôle de confiance.

### 5.3.2 Procédures de vérification des antécédents

Background Check Procedures

Des procédures de vérification des antécédents judiciaires sont mises en place par le prestataire en charge de la plateforme MAN pour les personnes qui sont appelées à endosser un rôle de confiance au sein de la PKI de la plateforme MAN. Ces personnes ne doivent notamment pas avoir fait l'objet de condamnation judiciaire susceptible de compromettre leur participation aux activités de la PKI de la plateforme MAN, ni être en situation de conflit d'intérêt avec leurs attributions. En France, les personnes concernées doivent remettre les informations permettant la vérification de l'authenticité de l'extrait de casier judiciaire (bulletin n°3) au responsable de la PKI de la plateforme MAN lors de la signature du document par lequel ils acceptent leur rôle, leurs obligations et leurs responsabilités dans le cadre de leur participation à ces activités.

Les personnes opérant un rôle de confiance pour le compte de la PKI de la plateforme MAN sont notamment chargées de communiquer tout changement dans ce domaine. Toutefois, la PKI de la plateforme MAN met en place une vérification régulière de l'adéquation des antécédents judiciaires de ses membres avec le rôle qu'ils opèrent pour son compte.

Le dossier de candidature du postulant est soumis à la validation du service Ressources Humaines et à celle du responsable de la PKI de la plateforme MAN.  Aucun droit d'accès n'est attribué tant que le dossier n'est pas validé.

Les personnels chargés d'opérer les services de confiance de la PKI de la plateforme MAN ne sont pas chargés des aspects commerciaux liés à ces services et sont dégagés de tout conflit d'intérêts qui pourraient influencer la manière de mener les opérations dont ils sont chargés et obérer la confiance.

À cet égard, ils s'engagent à confirmer par écrit, lors de leur acceptation du rôle de confiance au sein de la PKI de la plateforme MAN, l'absence de tout conflit d'intérêt lié à l'exercice de cette nouvelle activité.

Tout personnel ayant une situation connue de la PKI de la plateforme MAN pouvant engendrer un conflit d'intérêt jugé incompatible ou pouvant porter préjudice à l'impartialité des opérations de service de confiance :

- Ne pourra se voir attribuer un rôle de confiance ;
- Pourra se voir retirer un rôle de confiance précédemment attribué

### 5.3.3 Exigences en matière de formation initiale

Training Requirements

Le personnel est formé aux logiciels, matériels et procédures de fonctionnement de la PKI de la plateforme MAN. Il est également sensibilisé à la sécurité de l'information et en particulier :

- Aux enjeux de sécurité ;
- Aux règles à respecter ;
- Aux bons comportements à adopter en matière de sécurité des systèmes d'information.

Ce personnel a pris la mesure et la connaissance de ce qu'impliquent les opérations dont il a la responsabilité.

L'ensemble des personnels de confiance du prestataire en charge de la plateforme MAN reçoit une formation concernant typiquement :

- La sécurité et la protection des données personnelles ;
- La législation en vigueur ;
- Les principaux risques et menaces ;
- Le maintien en condition de sécurité ;
- L'authentification et le contrôle d'accès ;
- Le paramétrage fin et le durcissement des systèmes ;
- Le cloisonnement réseau ;
- La journalisation.

Cette formation est éventuellement adaptée suivant le service et le poste occupé. Elle peut prendre la forme d'une formation théorique, d'une formation pratique à travers un accompagnement de personnels déjà formés ou d'une combinaison des deux.

Quand un rôle de confiance est attribué à un sous-traitant du prestataire, de dernier s'assure que celui-ci a bien reçu une formation suffisante ou qu'il a une compétence pour assurer le rôle.

### 5.3.4 Exigences et fréquence en matière de formation continue

Retraining Frequency and Requirements

Une équipe dédiée a la charge des plans de formation des collaborateurs du prestataire en charge de la plateforme MAN. Cette équipe en lien avec les managers des équipes veille au maintien à niveau des collaborateurs en fonction des exigences opérationnelles.

Le personnel reçoit la formation nécessaire préalablement à toute évolution dans les systèmes, dans les procédures, dans l'organisation ou autres en fonction de la nature de ces évolutions. Il est notamment formé sur les enjeux en matière de sécurité des systèmes d'information et sensibilisé au traitement des incidents.

En particulier, les personnes reçoivent des formations régulières afin de maintenir leur niveau d'expertise, de connaissance et de qualifications.

De plus, des actions de sensibilisation destinées à l'ensemble des personnels sont régulièrement mises en œuvre. Celles-ci abordent des sujets tel que :

- Les objectifs et enjeux que rencontre la PKI de la plateforme MAN en matière de sécurité des systèmes d'information (nouvelles menaces et pratiques courantes de sécurité) ;
- Les informations considérées comme sensibles ;
- Les réglementations et obligations légales ;
- Les règles et consignes de sécurité régissant l'activité quotidienne : respect de la politique de sécurité, non-connexion d'équipements personnels au réseau de l'entité, non-divulgation de mots de passe à un tiers, non réutilisation de mots de passe professionnels dans la sphère privée et inversement, signalement d'événements suspects, etc. ;
- Les moyens disponibles et participant à la sécurité du système : verrouillage systématique de la session lorsque l'utilisateur quitte son poste, outil de protection des mots de passe, etc.

### 5.3.5 Fréquence et séquence de rotation entre différentes attributions

Job Rotation Frequency and Sequence

Un système de backup interpersonnel est mis en place de sorte à prévoir l'absence temporaire de certaines ressources essentielles au fonctionnement des services essentiels à la PKI. Aucune garantie de présence à tout moment de chacun des rôles clés n'est cependant apportée.

Il n'y a pas de rotation définie entre les différentes attributions.

### 5.3.6 Sanctions en cas d'actions non autorisées

Sanctions for Unauthorized Actions

Le règlement intérieur du prestataire en charge de la plateforme MAN indique que des sanctions disciplinaires administratives appropriées sont applicables en cas de faute (non-respect de la présente Certificate Policy, …). Ceci est notamment rappelé au personnel dans l'engagement de responsabilités qu'il accepte lors de l'acceptation de son rôle au sein de la PKI de la plateforme MAN.

Les entités externes au prestataire et participantes aux activités de la PKI de la plateforme MAN s'exposent à des sanctions définies lors de la contractualisation en cas de faute (non-respect de la présente Certificate Policy, …).

### 5.3.7 Exigences vis-à-vis du personnel des prestataires externes

Independent Contractor Requirements

Le personnel des éventuels prestataires externes intervenant dans les locaux et/ou sur les composantes de la PKI de la plateforme MAN doit respecter les exigences énoncées dans les chapitres 5.3.1 à 5.3.4 du présent document.

### 5.3.8 Documentation fournie au personnel

Documentation Supplied to Personnel

Chaque personne dispose au minimum de la documentation relative aux procédures opérationnelles et aux outils spécifiques qu'il met en œuvre, ainsi que des politiques et pratiques générales de la composante du service au sein duquel il travaille.

## 5.4 Procédures d'enregistrement des événements

Audit Logging Procedures

### 5.4.1 Types d'événements journalisés

Types of Events Recorded

La PKI de la plateforme MAN journalise les évènements liés :

- à la sécurité (incluant les accès ou tentatives d'accès) ;
- aux activités et au cycle de vie des systèmes des services de confiances qu'il fournit.

Ces journaux d'évènements peuvent être sous forme électronique ou manuscrite. L'ensemble de ces évènements est listé dans la documentation technique DTPG relative au présent document.

### 5.4.2 Fréquence de traitement des journaux d'événements

Frequency of Processing Log

Les systèmes de surveillance mis en œuvre traitent les journaux dès lors qu'ils sont collectés.

### 5.4.3 Fréquence de conservation des journaux d'événements

Retention Period for Audit Log

Les journaux d'évènements sont exportés au fil de l'eau sur un serveur distant.

### 5.4.4 Protection du journal d'événements

Protection of Audit Log

Les journaux d'évènements électroniques sont collectés puis externalisés vers deux types d'environnements (supervision et notarisation) dont les administrations sont différentes. L'accès à ces éléments sont rendus possibles uniquement au personnel autorisé par la plateforme MAN comme défini dans le document DTPG du prestataire et ne sont pas modifiables ou effaçables sans autorisation.

Les journaux d'évènements manuscrits sont protégés grâce à des systèmes physiques sécurisés de type coffre-fort ou armoire forte dont les accès sont contrôlés par la plateforme MAN. Ces systèmes garantissent l'intégrité et la confidentialité des journaux d'événements.

### 5.4.5 Procédures de sauvegarde des journaux d'événement

Audit Log Backup Procedures

La procédure de sauvegarde des journaux d'évènements de la PKI de la plateforme MAN est interne et est spécifiée dans le document DTPG.

### 5.4.6 Système de collecte des audits (interne ou externe)

Audit Collection System (Internal vs. External)

Le système de collecte des journaux d'évènements de la PKI de la plateforme MAN est interne et est spécifié dans le document DTPG. Celui-ci tient compte de la sensibilité de l'information collectée et analysée.

### 5.4.7 Notification au sujet à l'origine de l'événement

Notification to Event-Causing Subject

Il n'y a pas systématiquement de notification de l'enregistrement d'un évènement au responsable de l'évènement.

### 5.4.8 Évaluation de la vulnérabilité

Vulnerability Assessments

Les vulnérabilités sont évaluées au cours d'une analyse de risque. Le contrôle des journaux des événements fonctionnels est réalisé à la demande en cas de litige, ou pour analyse de comportement des IGC.

## 5.5 Archivage des données

Records Archival

### 5.5.1 Types d'enregistrements archivés

Types of Records Archived

Les données à archiver sont les suivantes :

- les logiciels (exécutables) et les fichiers de configuration des équipements informatiques ;
- les documents « Politique de Certification – Déclaration des Pratiques de Certification » ;
- les documents techniques des pratiques de certification;
- les dossiers d'enregistrement ;
- les Certificats émis ;
- les listes des autorités et certificats révoqués émises ou publiées ;
- les différents engagements signés par le Comité de gestion de la PKI;
- les journaux d'événements des différentes entités de l'IGC (cf. chapitre 5.4.1)

### 5.5.2 Durée de rétention des archives

Retention Period for Archive

Les périodes de conservations minimales sont les suivantes :

7 ans après la fin de vie de l'AC

- les logiciels (exécutables) et les fichiers de configuration des équipements informatiques ;
- les documents « Politique de Certification – Déclaration des Pratiques de Certification »;
- les documents techniques des pratiques de certification ;
- les Certificats émis ;

- les listes des autorités et certificats révoqués émises ou publiées ;
- les différents engagements signés par le Comité de gestion de la PKI.

7 ans après l'expiration du Certificat associé

- les dossiers d'enregistrement;

  Remarque : spécificité pour les dossiers d'enregistrement liés aux Certificats à usage unique, la durée de conservation de l'archive est de huit (8) ans, ceci en raison du caractère spécial de la durée de vie de cette gamme de Certificats.

- les éléments du cycle de vie du Certificat (génération, révocation, ...).

10 ans après leur génération

- Autres données d'audits (par exemple, démarrages et arrêts des systèmes)

### 5.5.3 Protection des archives

Protection of Archive

La confidentialité des archives est assurée par une gestion d'accès physique, système et réseau appropriée. Elle permet d'assurer la complétude et la confidentialité des archives.

Durant leur période de rétention au sein des locaux sécurisés de la PKI de la plateforme MAN, les archives sont protégées en intégrité et ne sont accessibles qu'aux personnes habilitées. La demande d'accès à une archive ne peut être uniquement faite que par le responsable de la PKI de la plateforme MAN, un responsable adjoint de la PKI de la plateforme MAN ou l'officier sécurité de la PKI de la plateforme MAN afin d'assurer la confidentialité des informations.

Des procédures sont en place afin de parer à l'obsolescence et à la détérioration des archives. Celles-ci sont notamment stockées dans des locaux sujets à des mesures de protection contre les menaces naturelles.

Les moyens de protection des archives mis en œuvre par la PKI de la plateforme MAN dans le cadre des autorités de certification (AC) en ligne diffèrent selon le type de donnée. Typiquement :

- les archives documentaires numériques sont protégées grâce à un coffre-fort numérique dont les accès sont contrôlés par la PKI de la plateforme MAN.
- les archives manuscrites sont protégées grâce à des systèmes physiques sécurisés de type coffre-fort ou armoire forte dont les accès sont contrôlés par la PKI de la plateforme MAN.

### 5.5.4 Procédure de backup automatique des archives

Archive Backup Procedure

Le niveau de protection des archives est équivalent au niveau de protection des sauvegardes. Les procédures de sauvegarde des archives sont internes et sont spécifiées dans le document DTPG.

### 5.5.5 Horodatage des archives

Requirements for Time-Stamping of Records

Les évènements sont datés précisément avec l'heure système des serveurs de la PKI de la plateforme MAN. Les serveurs de la PKI de la plateforme MAN synchronisent leur horloge interne régulièrement (au moins toutes les 24h) sur des serveurs de référence afin de garantir la cohérence de l'heure (UTC) indiquée dans les différents journaux électroniques.

### 5.5.6 Système de collecte des archives

Archive Collection System (Internal vs. External)

Le système de collecte des archives d'évènements de la PKI de la plateforme MAN est interne et est spécifié dans le document DTPG

### 5.5.7 Procédure de récupération et de vérification des archives

Procedures to Obtain and Verify Archive Information

Les archives peuvent être récupérées dans un délai inférieur à deux (2) jours ouvrés à compter de l'enregistrement de la demande. L'accès aux archives est sujet à des restrictions.

Les archives seront rendues disponibles en cas de réquisition judiciaire.

## 5.6 Procédures en cas de changement de clés

Key Changeover

Les AC ne peuvent pas générer de Certificat dont la date de fin serait postérieure à la date d'expiration du Certificat correspondant de l'AC. Pour cela la période de validité du Certificat de l'AC doit être supérieure à celle des Certificats qu'elle signe.

Au regard de la date de fin de validité de ce Certificat, son renouvellement sera demandé dans un délai au moins égal à la durée de vie des Certificats signés par la clé privée correspondante.

Dès qu'une nouvelle paire de clés d'une AC est générée, seule la nouvelle clé privée sera utilisée pour signer des certificats.

Le certificat précédent reste utilisable pour valider les certificats opérateurs émis sous cette clé et ce jusqu'à ce que tous les certificats signés avec la clé privée correspondante aient expirés.

## 5.7 Plan de Continuité d'Activité

Compromise and Disaster Recovery

### 5.7.1 Procédures de remontée et de traitement des incidents et des compromissions

Incident and Compromise Handling Procedures

Des procédures ont été définies avec le prestataire en charge de la plateforme MAN pour traiter les différents types d'incidents pouvant subvenir sur la plateforme MAN, et notamment les cas de compromission de clés de l'autorité racine, des autorités de certification ou des opérateurs.

Ces différentes procédures sont décrites au sein d'un document dédié et mis à disposition de l'ensemble des parties prenantes.

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

Computing Resourcs, Software, and/or Date are Corrupted

La PKI de la plateforme MAN dispose d'un plan de continuité d'activité (cf. chapitre 5.7.4) permettant de répondre aux exigences de disponibilité des différentes fonctions des IGC découlant de la présente PC-DPC, des engagements des AC en ligne dans la présente PC-DPC notamment en ce qui concerne les fonctions liées à la publication et/ou la révocation des certificats. Ce plan est régulièrement testé.

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

Entity Private Key Compromise Procedures

La compromission d'une clé d'infrastructure ou de contrôle d'une composante est traitée dans le plan de continuité et de reprise d'activité de la composante (cf. chapitre 5.7.4) en tant que sinistre.

Dans le cas d'une compromission de la clé privée d'AC, la PKI de la plateforme MAN suivra la procédure définie dans le document mentioné au chapitre 5.7.2 ain de prévenir les parties prenantes et appliquer les actions correctives telles que spécifiées dans la procédure.

### 5.7.4 Capacités de continuité suite à un sinistre

Business Continuity Capabilities After a Disaster

En cas d'interruption ou de corruption des ressources informatiques (matériels, logiciels et/ou données), notamment en cas de compromission de la clé privée d'une composante, la PKI de la plateforme MAN appliquera alors le Plan de Continuité et de Reprise d'Activité du service concerné afin d'assurer la continuité et/ou le rétablissement du service dans les plus brefs délais. Des mesures de remédiation sont mises en place afin de limiter les risques d'occurrence d'un nouvel incident.

## 5.8 Cas de terminaison de l'autorité racine ou de l'autorité de certification

CA or RA termination

Le mécanisme d'authentification des numéros en France se basant sur une solution sectorielle unique, avec un seul STI-CA et une seule autorité de certification, une procédure prévoyant la résiliation d'un STI-CA ou d'une autorité de certification n'est pas prévue.

Un plan de réversibilité a par contré été défini avec le fournisseur de service opérant la plateforme technique du service MAN pour l'APNF afin d'assurer la transition vers un autre fournisseur en garantissant la disponibilité du service durant cette phase. Une procédure de renouvellement des certificats opérateurs vers la nouvelle autorité de certification sera mise en place, ainsi que la révocation des certificats encore valides et signés par l'ancienne autorité de certification. Ces informations sont détaillées au sein du document "Code de Procédures MAN".

# 6 CONTROLES DE SECURITE TECHNIQUES

TECHNICAL SECURITY CONTROLS

Cette section décrit les contrôles techniques mis en place par le gestionnaire de la plateforme MAN pour garantir que la sécurité des opérations offertes par la plateforme MAN, et notamment celles liées à la gestion de la PKI pour la délivrance et la gestion des certificats opérateurs.

## 6.1 Modalités de génération et d'installation des paires de clé

Key Pair Generation and Installation

### 6.1.1 Génération des paires de clé

Key Pair Generation

#### 6.1.1.1 Clés des autorités de certification

CA Key Pair Generation

La génération des paires de clés des autorités de certification (AC) ou des unités d'horodatage est réalisée au cours d'une cérémonie de clés. Ces cérémonies de clés se déroulent :

- à l'aide d'un HSM physiquement isolé
- dans les locaux sécurisés de la PKI de la plateforme MAN
- sous le contrôle permanent d'au moins deux (2) personnes occupant un rôle de confiance au sein de la PKI de la plateforme MAN parmi le porteur de secrets, le maître de cérémonie, l'administrateur HSM, le responsable de la PKI de la plateforme MAN et le responsable
- suivant le procès-verbal de cérémonie des clés, rédigé par le maître de cérémonie en amont, complété par celui-ci au cours de la cérémonie et contresigné par tous les participants en fin de cérémonie. Ce document trace les informations telles que les participants, le matériel, la date et les actions menées.

La clé privée de chaque autorité de certification et unité d'horodatage est mise en œuvre et reste dans les locaux sécurisés de la PKI de la plateforme MAN

Les clés de signature des autorités de certification en ligne sont générées et mises en œuvre dans un module cryptographique ayant fait l'objet d'une évaluation sécuritaire comme défini dans ce document.

Ces clés de signatures possèdent un identifiant unique qui est nécessairement spécifié lors de la configuration des applicatifs afin de ne pas compromettre leur utilisation.

#### 6.1.1.2 Paire de clés des certificats opérateurs générées par l'AC

Service Provider Key Pair Generation

Les autorités de certification en ligne ne génèrent pas les clés des certificats opérateurs.

### 6.1.2 Transmission de la clé privée au bénéficiaire

Private Key Delivery to Subscriber

Sans objet. La clé privée est générée par le souscripteur (cf. 4.5.1)

### 6.1.3 Transmission de la clé publique à l'AC

Public Key Delivery to Certificate Issuer

La clé publique est transmise par le Dispositif Porteur de Certificat à l'Autorité d'Enregistrement qui la transmet à l'AC cible au sein d'un gabarit au format PKCS#10 (CSR) pour la génération du Certificat à usage unique / d'Organisation. La fonction de hachage à respecter est décrite au chapitre 6.1.5.

### 6.1.4 Transmission de la clé publique de l'AC aux opérateurs

CA Public Key Delivery to Relying Parties

Les certificats contenant les clés publiques des AC sont publiés sur son site web dont l'adresse est définie au chapitre 2.2 du présent document.

### 6.1.5 Taille des clés

Key Sizes

La taille des clés et les algorithmes utilisés par la PKI de la plateforme MAN sont conformes aux exigences [ETSI 119 312], aux exigences [RGS B1] ainsi qu'aux recommandations de l'ANSSI [SOGIS_CRYPTO] et de la RFC 8226.

Les clés utilisées par les souscripteurs doivent quant à elles être de type ECDSA associés aux algorithmes P-256 et SHA-256.

Les exigences et pratiques complémentaires spécifiques définies ci-dessous s'appliquent également.

### 6.1.6 Vérification de la génération des paramètres des clés et de leur qualité

Public Key Parameters Generation and Quality Checking

Les équipements de génération de clés utilisés pour la génération des paramètres des clés des AC sont des modules cryptographiques configurés pour répondre aux exigences mentionnées au chapitre 6.1.1.1. Les clés ne peuvent être générées que sur un module conforme à cette exigence, ou d'un niveau cryptographique et sécuritaire supérieur.

### 6.1.7 Objectifs d'usage de la clé

Key Usage Purposes (as per X.509 v3 Key Usage Field)

Les clés des AC servent exclusivement à signer les certificats opérateurs et les CRL utilisés pour les certificats opérateurs. Leur certificat est signé par l'Autorité de Certification de niveau supérieur.

## 6.2 Contrôles de protection de la clé privée et des modules cryptographiques

Private Key Protection and Cryptographic Module Engineering Controls

### 6.2.1 Standards et mesures de sécurité pour les modules cryptographiques

Cryptographic Module Standards and Controls

Les HSM utilisés par la PKI de la plateforme MAN, pour la génération des Bi-clés d'AC, d'UH et celles correspondants aux différents certificats délivrés par les AC, sont des HSM répondant aux exigences définies dans les politiques associées à chaque service de confiance concernées.

Ces HSM sont dédiés aux services fournis par la PKI de la plateforme MAN.

Le prestataire en charge de la plateforme MAN s'assure de la sécurité des HSM qu'elle utilise tout au long de leur cycle de vie. Des procédures sont notamment mises en place pour :

- s'assurer de l'intégrité de ces HSM durant leur transport ;
- s'assurer de l'intégrité de ces HSM durant leur stockage ;
- s'assurer de l'intégrité de ces HSM durant leur fonctionnement ;
- s'assurer de la maintenance de ces HSM durant leur durée de vie ;
- s'assurer du bon fonctionnement de ces HSM.

Pour les services qualifiés au sens du Règlement eIDAS, la PKI de la plateforme MAN utilise exclusivement des HSM ayant fait l'objet d'une qualification au niveau renforcé par l'ANSSI.

### 6.2.2 Contrôle de la clé privée

Private Key (n out of m) Multi-person Control

Le contrôle des clés privées d'AC, des copies de sauvegarde correspondantes et des clés privées d'UH est assuré par du personnel de confiance : porteur de secrets et administrateur HSM ; dans un environnement protégé. Ce contrôle est assuré à l'aide de données d'activations, appelées « secrets », réparties entre plusieurs personnes identifiés dans le rôle de porteur de secrets.

De plus, le contrôle des clés privées de signature des AC est assuré par du personnel de confiance (porteurs de secrets) et via un outil mettant en œuvre le partage des secrets.

### 6.2.3 Séquestre de la clé privée

Private Key Escrow

La PKI de la plateforme MAN ne propose pas de service de séquestre des clés privées à des fins de recouvrement.

### 6.2.4 Copie de secours de la clé privée

Private Key Backup

Les clés privées des AC n'étant pas en permanence activées au sein du module cryptographique, ces clés privées font l'objet de copies de secours hors d'un module cryptographique. Cette copie de secours est réalisée sous forme chiffrée et avec un mécanisme de contrôle d'intégrité. Le chiffrement utilisé offre un niveau de sécurité équivalent ou supérieur au stockage au sein du module cryptographique et, notamment, s'appuie sur un algorithme, une longueur de clé et un mode opératoire capables de résister aux attaques par cryptanalyse pendant au moins la durée de vie de la clé ainsi protégée. Les opérations de chiffrement et de déchiffrement sont effectuées à l'intérieur du module cryptographique de telle manière que les clés privées d'AC ne soient à aucun moment en clair en dehors du module cryptographique. Les supports de stockages des copies de secours sont stockés dans un coffre-fort. Le contrôle des opérations de chiffrement / déchiffrement est conforme aux exigences du chapitre 6.2.2.

Pour les clé privées d'AC hors ligne, les procédures de sauvegardes sont opérées selon les spécifications du fournisseur des HSM de la PKI de la plateforme MAN
Le nombre de copies est limité au minimum requis pour assurer la continuité des services de la PKI de la plateforme MAN.

### 6.2.5 Archivage de la clé privée

Private Key Archival

La PKI de la plateforme MAN ne propose pas de service d'archivage des clés privées.

### 6.2.6 Transfert de la clé privée vers/depuis le module cryptographique

Private Key Transfer Into or From a Cryptographic Module

Les clés privées d'AC hors ligne sont générées au sein d'un HSM et ne sont transférées vers une clé de stockage uniquement dans le cas des copies de sauvegarde. Cette clé de stockage est stockée dans un coffre sous le contrôle exclusif des porteurs de secret.

Lors d'un transfert, la clé privée est chiffrée avec un algorithme préconisé par le constructeur de HSM permettant d'assurer la sécurité de l'information. La clé privée chiffrée ne peut alors pas être déchiffrée sans l'utilisation de composants cryptographiques matériels et sans l'action des personnes identifiées dans les rôles de confiances nécessaires.

### 6.2.7 Stockage de la clé privée dans un module cryptographique

Private Key Storage on Cryptographic Module

Les clés privées d'AC et d'UH sont stockées au sein d'un HSM physiquement sécurisé répondant aux exigences définies au sein de ce document. Il en est de même pour le stockage des copies de sauvegarde des clés privées d'AC.

Des procédures autour de ces HSM sont en place afin de s'assurer de la confidentialité de leur contenu.

### 6.2.8 Méthode d'activation de la clé privée

Method of Activating Private Key

Les clés privées d'AC ne peuvent être activées qu'avec des données d'activation détenues par deux (2) personnes occupant un rôle de confiance au sein de la PKI de la plateforme MAN.

L'activation d'une clé privée d'AC ne peut se faire qu'au cours d'une Cérémonie de clés, documentée et tracée.

### 6.2.9 Méthode de désactivation de la clé privée

Method of Deactivating Private Key

La désactivation des clés privées d'AC dans le HSM est automatique dès qu'il y a arrêt de celui-ci.

### 6.2.10 Méthode de destruction de la clé privée

Method of Destroying Private Key

Les clés privées d'AC, les copies de sauvegarde correspondantes et les clés privées d'UH sont détruites par effacement sur la ressource cryptographique conformément aux procédures du constructeur. Les

opérations de destruction sont effectuées au cours d'une procédure auditée de type Cérémonie de clés.

En fin de vie normale ou anticipée (pour cause de révocation) d'une clé privée d'AC ou d'UH, celle-ci est systématiquement détruite, ainsi que toute copie et tout élément permettant de la reconstituer. Par ailleurs, dans le cas où la ressource cryptographique matérielle hébergeant les clés privées susvisées doit être mise hors service, alors celles-ci le sont aussi.

Par ailleurs, la destruction définitive d'une clé privée d'AC est réalisée par la destruction des moyens de restauration de la clé privée :

- la destruction de de la clé privée et de toutes les copies de secours, et
- la destruction des moyens d'activation de la clé privée si applicable.

### 6.2.11 Niveau de qualification du module cryptographique

Cryptographic Module Rating

Le module cryptographique matériel utilisé pour héberger les clés privées des AC est évalué aux niveaux de Certifications autorisés par la norme ETSI EN 319411-1.

## 6.3 Points additionnels de gestion des paires de clés

Other Aspects of Key Pair Management

### 6.3.1 Archivage des clés publiques

Public Key Archival

Les clés publiques des AC sont archivées conformément au chapitre 5.5 du présent document.

### 6.3.2 Durée de vie des clés et des certificats

Certificate Operational Periods and Key Pair Usage Periods

La durée de vie des clés et des certificats diffère selon le type de certificat.

- Les certificats et clés de l'autorité racine ont une durée de vie maximale de 10 ans.
- Les certificats et clés des autorités de certification ont une durée de vie maximale de 5 ans.
- Les certificats opérateurs ont une durée de vie maximale de 1 an.

La durée de vie des clés pour l'autorité racine et les autorités de certification utilise le même principe que pour les certificats : 10 ans pour les clés utilisées pour les certificats de l'autorité racine, 5 ans pour les certificats des autorités de certification.

La durée de vie des clés des certificats opérateur est à la discrétion de chaque opérateur.

## 6.4 Données d'activation

Activation data

### 6.4.1 Génération est installation

Activation Data Generation and Installation

Les données d'activation des clés privées d'AC sont générées dans un HSM durant les cérémonies de clés sous le contrôle de deux (2) personnes dans des rôles de confiance, stockées sur des cartes à puces puis sont remises aux porteurs de secrets qui détiennent alors les données d'activation. Ces données d'activations ne sont connues que par les responsables nommément identifiées dans le cadre du rôle de confiance qui leur est attribué.

### 6.4.2 Protection

Activationd Data Protection

Les données d'activation sont protégées par des mécanismes cryptographiques et de contrôle d'accès physique. Les porteurs de secret sont responsables de la protection des secrets dont ils ont la responsabilité. Un porteur de secret ne détient pas plus d'une donnée d'activation par AC.

## 6.5 Contrôles de la sécurité des systèmes d'information

Computer Security Controls

### 6.5.1 Exigences de sécurité technique spécifiques aux systèmes informatiques

Specific Computer Security Technical Requirements

Les exigences minimales de sécurité technique mises en œuvre par la PKI de la plateforme MAN répondent aux objectifs suivants :

- **identification et authentification forte** des utilisateurs pour l'accès au système. Les accès logiques aux serveurs, aux outils de développement collaboratifs et aux applications de la PKI de la plateforme MAN sont contrôlés et régulièrement vérifiés ;
- **protection du réseau** contre tout accès non-autorisé. Les connexions d'équipements personnels sont notamment interdites sur le réseau de la PKI de la plateforme MAN ;

  - Cloisonnement réseau

  Les plateformes de la PKI de la plateforme MAN sont hébergées dans des zones réseau distinctes en fonction de leur rôle et sensibilité. Les composants critiques du réseau sont maintenus dans un environnement sécurisé. La sensibilité des différents éléments est établie en ligne avec les résultats de l'analyse de risque. la PKI de la plateforme MAN applique les mêmes contrôles de sécurité à l'ensemble des composants d'une zone réseau.

Les flux réseaux en direction de la PKI de la plateforme MAN, ainsi qu'entre chaque zone réseau distincte, sont notamment contrôlés afin d'interdire tout flux non autorisés (y compris des flux émanant d'utilisateurs ou d'abonnés aux services). En particulier, les dispositifs de contrôle réseau sont configurés pour interdire l'ensemble des protocoles et accès qui ne sont pas nécessaires pour les opérations des services de confiance.

Les configurations font l'objet d'une revue régulière.

Les environnements de production et de test/développement font également l'objet d'un cloisonnement.

Afin de documenter le cloisonnement, la PKI de la plateforme MAN crée et maintient à jour un schéma simplifié du réseau (ou cartographie) représentant les différentes zones IP et le plan d'adressage associé, les équipements de routage et de sécurité (pare-feu, relais applicatifs, etc.) et les interconnexions avec l'extérieur (Internet, réseaux privés, etc.) et les partenaires. Ce schéma permet de localiser les serveurs détenteurs d'informations sensibles de l'entité.

- Accès aux plateformes

Les plateformes de la PKI de la plateforme MAN sont soumises à des restrictions d'accès logiques et ne sont pas en accès direct. Le processus d'accès logique aux plateformes de la PKI de la plateforme MAN est interne et décrit dans la DTPG du prestataire. La gestion de contrôle d'accès est sous le contrôle du prestataire en charge de la plateforme MAN. Cette gestion inclut la gestion des comptes et permet de modifier ou de supprimer des accès sans délai. Les droits et privilèges d'accès aux plateformes sont attribués suivant la politique d'accès logique définie par la PKI de la plateforme MAN. Le système de contrôle d'accès en place permet une gestion efficace et adéquate des accès, en particulier :

  - il permet une séparation des rôles, en particulier entre les opérations d'administration et les autres opérations de niveau métier par l'utilisation de réseaux dédiés à chacun des usages ;
  - il permet de contrôler et de restreindre l'utilisation des différentes applications et utilitaires.

Les systèmes utilisés pour l'administration sont dédiés à cet usage.

Des tests de pénétration sont effectués lors de la mise en place de l'infrastructure des services puis à chaque évolution ou modification majeure. Du fait de leur criticité, et de l'importance de fourniture un rapport fiable, les tests de pénétrations ne peuvent être effectués que par des personnels sélectionnés sur des critères tels que leurs compétences, connaissances, efficacité, éthique et indépendance.

- Accès aux services

Les services de la PKI de la plateforme MAN ne sont pas en contact direct avec des réseaux ouverts sur internet. Les passerelles permettant les accès sont protégées contre des tentatives d'intrusion ou d'attaque.

Ces passerelles limitent les services ouverts et protocoles aux seuls services indispensables au fonctionnement des services délivrés par la PKI de la plateforme MAN. Elles sont régulièrement

mises à jour pour prendre en compte les évolutions des systèmes anti-intrusions et combler les failles de sécurité potentielles.

- **gestion des droits** des utilisateurs et des comptes ;

  - Gestion des droits

  La PKI de la plateforme MAN met en place une gestion des droits d'accès sur la base du principe de moindre privilège et procède régulièrement à une revue de l'attribution de ces droits d'accès.

  - Gestion des comptes

  Des règles de gestion des comptes, des mots de passe et sessions d'accès aux systèmes de la PKI de la plateforme MAN sont en place afin de garantir une robustesse minimum des informations d'identification et une protection minimale des accès aux systèmes.

- **gestion de sessions d'utilisation** : déconnexion après un temps d'inactivité, accès aux fichiers contrôlé par rôle et nom d'utilisateur. Des règles de gestion des comptes, des mots de passe et sessions d'accès aux systèmes de la PKI de la plateforme MAN sont en place afin de garantir une robustesse minimum des informations d'identification et une protection minimale des accès aux systèmes ;

- **fonctions d'audits** : non-répudiation, imputabilité et nature des actions effectuées (application de procédures de changement pour les actions de livraison, modification et résolution urgente de problèmes logiciels) ;

  - Les procédures d'exploitation de la PKI de la plateforme MAN sont documentées et sont mises à disposition des équipes concernées, en particulier tous les personnels administratifs ou en rôle de confiance pouvant avoir un impact sur la fourniture du Service de Confiance.
  - Des procédures de suivi des changements sont notamment en place afin de contrôler les déploiements, les mises à jour et les corrections d'urgence des logiciels, ainsi que les modifications des configurations des systèmes impliqués dans la fourniture des Services de Confiance. La PKI de la plateforme MAN s'appuie notamment sur un outil interne à Worldline pour assurer le suivi des changements et des incidents liés à l'exploitation de ses services. L'outil permet de documenter tous les changements opérés.
  - La PKI de la plateforme MAN s'assure de distinguer les différents environnements de l'environnement de production pour l'ensemble des systèmes des Services de Confiances opérés.

- **protection contre les virus**, les logiciels malveillants ou non-autorisés et mises à jour des logiciels;

- **application de procédures de changement** pour toute modification des configurations logicielles

  - L'implémentation, la configuration et toute modification ou mise à jour d'un système permettant de mettre en œuvre les composantes d'un service de la PKI de la plateforme MAN est documentée et contrôlée. Tout changement ayant un impact sur le niveau de sécurité doit être approuvé par le Comité de gestion de la PKI.
  - Les développements se font selon la politique de développement sécurisée du prestataire en charge de la plateforme MAN. Celle-ci couvre les aspects de conception, développements,

tests et déploiement en production. Elle s'appuie sur les bonnes pratiques de sécurité reconnues. Une analyse des exigences de sécurité est réalisée au moment de la conception ou de la sélection de chacun des composants de l'architecture afin d'être assuré que la sécurité est bien prise en compte dans les systèmes informatiques.
- La plateforme MAN ne fait pas appel à des développements externalisés pour les services de confiance.
- Les développements sont systématiquement passés dans un outil d'analyse automatique visant à contrôler la qualité du code.
- Les développements font l'objet de tests fonctionnels et de recette avant livraison en production.
- Les données de production ne sont pas recopiées sur les environnements de préproduction, test ou développement. Des jeux de données de tests ou de données anonymisées sont utilisés pour les tests et développements.

- **protection du réseau** afin d'assurer la confidentialité et l'intégrité des données qui y transitent ;

- **redondance des connexions réseau** pour assurer l'accessibilité en cas de panne simple.

Des dispositifs de surveillance, avec enregistrement et alarme automatique, ainsi que des procédures d'audit des paramétrages du système, en particulier des éléments de routage, et des procédures de réaction en cas d'incident sont mis en place.

### 6.5.2 Niveau de qualification des systèmes informatiques

Computer Security Rating

Sans objet.

## 6.6 Contrôles de la sécurité du développement

Life Cycle Security Controls

### 6.6.1 Mesures de sécurité liées au développement des systèmes

System Development Controls

Tous les développements réalisés par le prestataire de la plateforme MAN et impactant l'Infrastructure de Gestion de Clés (IGC) sont documentés et réalisés via un processus de manière à en assurer la qualité. La configuration du système des composantes de l'IGC ainsi que toute modification et mise à niveau est documentée et contrôlée.

De plus, un cloisonnement est opéré entre les environnements de développement et test, de pré-production et de production. Ceci permet d'assurer une mise en production de qualité.

### 6.6.2 Mesures liées à la gestion de la sécurité

Security Management Controls

Toute évolution d'un système d'une composante de l'Infrastructure de Gestion de Clés (IGC) est documentée et tracée. Elle apparaît dans les procédures de fonctionnement interne de la composante.

### 6.6.3 Niveau d'évaluation sécurité du cycle de vie des systèmes

Life Cycle Security Controls

Toute évolution significative d'un système d'une composante des IGC est testée et validée avant déploiement. Ces opérations sont réalisées par du personnel de confiance.

## 6.7 Contrôles sur la sécurité du réseau

Network Security Controls

La plateforme MAN, et notamment sa PKI, met en place des mesures pour protéger son réseau contre d'éventuelles attaques.

### 6.7.1 Cloisonnement réseau

Network Segmentation

Les services de la plateforme MAN sont hébergés dans des zones réseau distinctes en fonction de leur rôle et sensibilité. Les composants critiques du réseau sont maintenus dans un environnement sécurisé. La sensibilité des différents éléments est établie en ligne avec les résultats de l'analyse de risque. La PKI de la plateforme MAN applique les mêmes contrôles de sécurité à l'ensemble des composants d'une zone réseau.

Les flux réseaux en direction de la PKI de la plateforme MAN, ainsi qu'entre chaque zone réseau distincte, sont notamment contrôlés afin d'interdire tout flux non autorisés (y compris des flux émanant d'utilisateurs ou d'abonnés aux services). En particulier, les dispositifs de contrôle réseau sont configurés pour interdire l'ensemble des protocoles et accès qui ne sont pas nécessaires pour les opérations des services de confiance.

Les configurations font l'objet d'une revue régulière.

Les environnements de production et de test/développement font également l'objet d'un cloisonnement.

Afin de documenter le cloisonnement, la PKI de la plateforme MAN crée et maintient à jour un schéma simplifié du réseau (ou cartographie) représentant les différentes zones IP et le plan d'adressage associé, les équipements de routage et de sécurité (pare-feu, relais applicatifs, etc.) et les

interconnexions avec l'extérieur (Internet, réseaux privés, etc.) et les partenaires. Ce schéma permet de localiser les serveurs détenteurs d'informations sensibles de l'entité.

### 6.7.2 Accès aux plateformes

Platform Access Restrictions

Les composants de la plateforme MAN sont soumiss à des restrictions d'accès logiques et ne sont pas en accès direct. Le processus d'accès logique est interne et décrit dans la DTPG du prestataire de la plateforme.

La gestion de contrôle d'accès est sous le contrôle du prestataire en charge de la plateforme. Cette gestion inclut la gestion des comptes et permet de modifier ou de supprimer des accès sans délai. Les droits et privilèges d'accès aux services sont attribués suivant la politique d'accès logique définie par la plateforme MAN.

Le système de contrôle d'accès en place garantit une séparation des rôles, en particulier entre les opérations d'administration et les autres opérations de niveau métier par l'utilisation de réseaux dédiés à chacun des usages ; il permet de plus de contrôler et de restreindre l'utilisation des différentes applications et utilitaires.

Des tests de pénétration sont effectués lors de la mise en place de l'infrastructure des services puis à chaque évolution ou modification majeure. Du fait de leur criticité, et de l'importance de fourniture un rapport fiable, les tests de pénétrations ne peuvent être effectués que par des personnels sélectionnés sur des critères tels que leurs compétences, connaissances, efficacité, éthique et indépendance.

### 6.7.3 Accès aux services

Service Access Restrictions

Les services de la PKI de la plateforme MAN ne sont pas en contact direct avec des réseaux ouverts sur internet. Les passerelles permettant les accès sont protégées contre des tentatives d'intrusion ou d'attaque.

Ces passerelles limitent les services ouverts et protocoles aux seuls services indispensables au fonctionnement des services délivrés par la plateforme MAN. Elles sont régulièrement mises à jour pour prendre en compte les évolutions des systèmes anti-intrusions et combler les failles de sécurité potentielles.

## 6.8 Horodatage

Time-Stamping

Les serveurs de la plateforme MAN sont synchronisés en utilisant le protocole NTP. Les serveurs de la PKI synchronisent leur horloge interne à minima toutes les 24h au plus sur des  erveurs de référence afin de garantir la cohérence de l'heure (UTC) indiquée dans les différents journaux électroniques.

# 7 CERTIFICATS, CRLS ET OCSP

CERTIFICATE, CRL, AND OCSP PROFILES

## 7.1 Certificats

Certificate Profile

Les certificats délivrés aux opérateurs par la plateforme MAN correspondent à des certificats X509 v3 tels que décrits dans la RFC 5280, et dont le contenu est conforme à la RFC 8226 et la spécification ATIS-1000080.

Le document « Mode Opératoire du Mécanisme de Confiance » précise tous les détails de ces certificats, appelés « Certificats Opérateur », et en particulier leur format, les extensions utilisées, les contraintes algorithmiques, leur durée de validité et leur cycle de vie.

## 7.2 CRLs

CRL Profile

Une liste publique de révocation (CRL) des certificats opérateurs est maintenue par la plateforme MAN et est accessible via une URL publique à tous les opérateurs. Conforme à la RFC 5280, cette CRL est mise à jour régulièrement, soit lors de la révocation de certificats opérateurs, soit automatiquement pour prévenir son expiration.

L'accès à cette CRL, son format, les extensions utilisées, ainsi que les données stockées pour chaque certificat révoqué sont détaillés au sein du document « Mode Opératoire du Mécanisme de Confiance ».

## 7.3 OCSP

OCSP Profile

Le protocole OCSP n'est pas utilisé dans le cadre du MAN.

# 8 AUDIT DE CONFORMITE ET AUTRES EVALUATIONS

COMPLIANCE AUDIT AND OTHER ASSESSMENTS

La PKI de la plateforme MAN fait l'objet d'audits réguliers conforme aux exigences de la norme ETSI EN 319 401, norme de référence sur la gestion de la sécurité pour les services conformes au règlement européen eIDAS.

## 8.1 Déclenchement et fréquence des audits

Frequency or Circumstances of Assessment

Le prestataire en charge de la plateforme MAN peut être amené à effectuer un audit de surveillance (interne ou externe) entre deux audits externes de Certification aux normes en vigueur sur le service de confiance de la PKI de la plateforme MAN.

## 8.2 Identification et qualification de l'assesseur

Identity/Qualifications of Assessor

### 8.2.1 Audit de certification

Le contrôle de la composante du service de confiance est effectué par une équipe d'auditeurs faisant partie d'un organisme d'audit habilité et accrédité à procéder à des évaluations selon les spécifications des normes applicables à la plateforme MAN et plus spécialement au service de confiance de la PKI de la plateforme.

## 8.3 Relation entre évaluateurs et l'entité evaluée

Assessor's Relationship to Assessed Entity

### 8.3.1 Audit de certification

Le ou les évaluateurs effectuant le contrôle de la ou des composantes du service de confiance évalué sont indépendants et exempts de tout conflit d'intérêts.

### 8.3.2 Audit de surveillance

Le ou les évaluateurs effectuant le contrôle de la ou des composantes du service de confiance évalué n'ont en aucun cas un quelconque rôle de confiance au sein de la plateforme MAN.

## 8.4 Sujets couverts par les évaluations

Topics Covered by Assessment

Les contrôles effectués par les auditeurs portent sur une partie ou sur l'ensemble des composantes de la plateforme MAN afin de contrôler le respect de la mise en œuvre de la présente DTPG ainsi que la conformité des procédures et pratiques du service de confiance vis-à-vis des exigences auxquelles il est sujet.

A cet égard, avant chaque audit, l'évaluateur responsable de l'audit envoie au prestataire en charge de la plateforme MAN un plan d'audit, spécifiant les composantes et procédures qu'il souhaitera contrôler lors de l'audit avec son ou ses confrères ainsi que le programme détaillé de l'audit.

## 8.5 Actions prises en cas de défaut

Actions Taken as a Result of Deficiency

A l'issue d'une évaluation, le prestataire en charge de la plateforme MAN définit un plan d'actions correctives avec un délai de réalisation, qui doit être validé par la gouvernance avant son application. Un nouveau contrôle pourra être effectué pour vérifier la mise en place des corrections.

## 8.6 Communication des résultats

Communication of Results

Les résultats détaillés des audits sont tenus à la disposition de la gouvernance.

# 9 AUTRES QUESTIONS COMMERCIALES ET JURIDIQUES

OTHER BUSINESS AND LEGAL MATTER

## 9.1 Coûts

Fees

Les coûts d'enregistrement et d'utilisation de la plateforme sont disponibles auprès de l'APNF, Association Pour la Normalisation des Flux inter-opérateurs.