



BIENVENUE

Intervenants:

- Antonio Alibrandi**
- Alessandro Paolino**

MAN

Mécanismes d'Authentification des Numéros

OBJECTIF DE CE WEBINAR

DÉFINIR CLAIREMENT CE QUE L'ON ENTEND PAR MAN

DÉFINIR CLAIREMENT LES BESOINS TECHNIQUES

VOUS DONNER DES DÉTAILS SUR NOTRE "OFFRE MAN"

MAN

Mécanismes d'Authentification des Numéros

OBJECTIF DE CE WEBINAR

DÉFINIR CLAIEMENT CE QU'EST LE PROJET MAN

– VOYONS LES DIFFÉRENTES DATES / STEPS

Introduction

En **2020**, a été introduite la loi n° 2020-901 (**Neagelen**):
visant à encadrer le démarchage téléphonique et à lutter contre les appels frauduleux,
imposant l'obligation de l'Authentification des Numéros pour toutes les communications à partir du
25 juillet 2023.

En 2020, l'ARCEP a mis en place un groupe de travail appelé GT-MA pour lutter contre l'usurpation
des numéros. **VNT a été impliqué dès les premières réunions.**

Le GT-MA a permis de définir la «note de cadrage - cas d'usage».

Ensuite, le GT-MA a sollicité l'ARCEP pour demander à l'APNF pour accepter et prendre en charge
l'assistance à maîtrise d'ouvrage du programme MAN pour la mise en place de solutions
centralisées.

En **2022**, la solution «**Le Plan Programme MAN**» a été lancée par l'APNF.

Plan Programme MAN

Le **Plan Programme MAN** présente l'analyse préalable et les différents projets techniques pour apporter des réponses aux obligations fixées par la loi Naegelen aux opérateurs.

Le périmètre du programme est très large, puisqu'il couvre quasiment tous les appels fixes et mobiles, et tous les messages.

Plan Programme - V1.3 - 05/07/2022

Il a donc été nécessaire rédiger le Glossaire MAN pour définir les termes utilisés par les documents du programme MAN.

Ensuite il a été établi le Code de procédures MAN décrit les règles de fonctionnement que chaque opérateur qui souscrit au service MAN s'engage à respecter.

Code de procédures - V1.3 - 04/05/2023

Cela a permis de donner forme à la rédaction de différents documents pour définir, au fur et à mesure, les modes opératoires et réglés techniques de Plateforme MAN.

Plan Programme MAN: En particulier

En particulier:

Le document ci-dessous définit le mode opératoire du mécanisme de confiance MAN, i.e. les processus de validation de l'identité d'un opérateur, d'obtention et d'utilisation des certificats.

[Mode opératoire du mécanisme de confiance MAN - V1.6 - 04/05/2023](#)

Le document ci-dessous définit le mode opératoire et les processus de signalements, incidents et métriques. Il décrit notamment les règles et le format attendu pour les traces d'appels cassables/cassés et les volumétries d'appels que devront déposer les opérateurs sur la plateforme MAN.

[Mode opératoire des incidents, signalements et métriques du MAN - V1.6 - 04/05/2023](#)

L'archive suivante contient le nouveau guide de référence des API de la plateforme MAN ; celui-ci est validé et peut être utilisé pour l'implémentation de vos clients d'API. Les fichiers contenus dans cette archive sont lisibles, par exemple, grâce l'éditeur de texte suivant : <https://editor.swagger.io/>

[Guide de référence des API de la plateforme MAN - V1.2.0 - 04/05/2023](#)

Autres documents

Le document ci-dessous permet à chaque opérateur de bien appréhender ce qu'il va devoir faire pour implémenter le MAN.

[Aide à la décision - V1.1 - 30/03/2023](#)

Au niveau mondial, les mécanismes d'authentification sont mis en place dans quelques pays, avec les États-Unis et le Canada en tête en termes de progression.

Des discussions nationales sont également en cours dans des pays européens tels que le Royaume-Uni et l'Allemagne.

À ce jour, la France est le premier pays européen à définir la mise en œuvre d'un dispositif d'authentification.

Les opérateurs n'ont pas identifié des éléments de solutions techniques pour tous les cas dès juillet 2023.

Des évolutions seront donc mises en place par la suite au fur et à mesure de la normalisation des solutions techniques pour se rapprocher au plus près de la loi.

Autres documents

Le Programme MAN est constitué de solutions pragmatiques, concrètes et réalistes. Ces solutions sont adaptées à la prise à compte à l'international de ces problématiques dans les années à venir.

Ce Plan Programme constitue une étape majeure : la définition d'une architecture technique opérante pouvant évoluer dans le futur et faisant consensus parmi les opérateurs ayant participé aux travaux.

- les solutions du programme MAN
- les solutions disponibles pour 2023 sous forme de fiches solution
- les améliorations post-2023,
- les pistes envisageables dans le futur si besoin

Introduction

MAN (Mécanismes d'Authentification des Numéros) est un projet français géré par l'**ARCEP** qui a été mis en place dans le but de lutter contre les appels frauduleux.

Un autre acteur important dans la mise en œuvre de ce projet est l'APNF, qui est chargée de superviser et de gérer les projets liés au programme MAN ainsi que la description de tout projet technique permettant la mise en œuvre de solutions centralisées.

Ce mécanisme ne résout pas à lui seul les problèmes liés au mécanisme de protection des consommateurs, mais constitue une brique fondamentale pour garantir la véracité de l'appelant.

Pourquoi un tel dispositif était-il nécessaire ?

Le Mécanismes d'Authentification des Numéros a été conçu pour protéger les consommateurs et résoudre un certain nombre de problèmes liés aux appels sur le territoire français.

Pourquoi un tel dispositif était-il nécessaire ?

«**Appels SPAM**» (appels téléphoniques abusifs, malveillants ou harcelants)

«**Appels PING**» (Technique frauduleuse consistant à faire sonner un ou plusieurs numéros de téléphone une seule fois afin d'inciter l'utilisateur à rappeler)

«**Spoofing**» (implique généralement la création d'une fausse identité ou d'une fausse source pour induire en erreur les destinataires légitimes)

Ces questions sont également abordées aujourd'hui au niveau mondial. Parmi les pays actuellement actifs dans ce domaine, les États-Unis et le Canada sont les plus avancés.

Parmi les pays européens, le Royaume-Uni et l'Allemagne étudient le problème, mais la France est le premier pays européen à mettre en œuvre le mécanisme d'authentification au niveau national.

Sanctions

Les opérateurs de transit et/ou de terminaison avaient la faculté de casser les appels mal identifiés (pas de PAI, pas de From, etc.).

Avec le projet MAN ils devront «casser» et cela va déclencher des pénalités sur toute la chaîne des opérateurs jusqu'à l'origine de l'appel.

Orange, SFR, Free, Bouygues et beaucoup d'autres opérateurs alternatifs sont en train déjà d'appliquer des sanctions voir 0.02 euro x tentatives d'appel ou **2000 euro x numéro appelant illégitime**. Les pénalités sont cumulables.

Tout en sachant que même autres administrations publiques (DGCCRF et autres) peuvent appliquer des sanctions administratives.

Cela comporte la nécessité de revoir les clauses contractuelles avec des avenants le cas échéant.

Ne pas être en conformité peut produire des conséquences sur le plan juridique, technique et financier.

Sanctions

Conséquences sur:

- La continuité du service : appels cassés par les des opérateurs de collecte et/ou de transit
- Le plan financier : applications pénalités des opérateurs de collecte et/ou de transit
- Le plan réglementaire : Bloc de nouvelle attribution et/ou retrait des tranches déjà attribuées de la part de l'ARCEP
- Le risque de sanction administrative : application jusqu'à 15000.00 euro, par la DGCCRF, par manquement constaté de la non-conformité au dispositif MAN
- Le plan pénal : dans des cas plus graves.

OBJECTIF DE CE WEBINAR

DÉFINIR CLAIREMENT CE QU'EST LE PROJET MAN

– Lois Naegelen et projet MAN

Lois Naegelen

Dans le scénario MAN, une loi fondamentale et sous-jacente est la **loi Naegelen** (LOI n° 2020-901 du 24 juillet 2020). Cette loi vise à garantir une solution à long terme pour réduire et éliminer l'usurpation d'identité.

L'usurpation d'identité est une pratique qui permet à un malveillant de dissimuler la localisation de l'appelant en trompant le consommateur sur l'identité de l'expéditeur en ne figurant pas avec le véritable numéro de téléphone d'où provient l'appel.

Cette pratique est souvent utilisée par les centres d'appel pour apparaître dans une certaine région géographique.

Selon cette Loi, les fournisseurs de services doivent se conformer dans un délai maximum de trois ans à l'utilisation d'un dispositif permettant de vérifier l'authenticité des appels et des messages en utilisant un numéro d'identification de l'appelant, établi par l'autorité et connu sous le nom de Caller ID.

L'objectif est de résoudre le problème de la véritable origine de l'appel, afin de prévenir les pratiques de spoofing

Le programme MAN

Le programme MAN comprend:

- Un mécanisme d'authentification des numéros.
- Des solutions pour lutter contre les appels et les messages frauduleux ou les numéros d'appelant/d'expéditeur incorrects.

Le mécanisme d'authentification des numéros comprend:

- Une procédure permettant de vérifier l'authenticité de l'opérateur d'origine et du numéro de l'appelant afin de garantir l'intégrité des informations transmises.
- La gestion des scénarios d'utilisation des appels, y compris le traitement de l'appel et la vérification de l'authenticité.
- Le traitement des cas de non-respect des règles établies entre les opérateurs.

Solutions pour lutter contre les appels et les messages frauduleux ou les numéros d'appelant/d'expéditeur incorrects:

- Le système de signalement des réclamations des clients s'accompagne de moyens d'enquête et de sanctions efficaces pour mettre fin à de telles pratiques. Il recueille également des mesures et des statistiques pour analyser l'efficacité du système et, le cas échéant, l'améliorer.

OBJECTIF DE CE WEBINAR

DÉFINIR CLAIREMENT LES BESOINS TECHNIQUES

- Mécanisme d'authentification STIR/Shaken
- Niveau d'attestation STIR/Shaken

Mécanisme d'authentification STIR/Shaken

Le mécanisme d'authentification est basé sur le protocole STIR/Shaken, un protocole utilisé à l'échelle industrielle et internationale.

Ce protocole permet également une meilleure traçabilité des appels en garantissant la traçabilité de l'appelant grâce à un mécanisme d'authentification fort. Les appels auront alors un **certificat SHAKEN** de niveau **A**, **B** ou **C**.

Niveau d'attestation STIR/Shaken

Le STIR/Shaken définit trois niveaux de certificats.

Attestation complète (A): le fournisseur de services a authentifié l'appelant qui est alors autorisé à utiliser le numéro avec lequel il a démarré l'appel.

Attestation partielle (B): Le fournisseur de services a authentifié l'auteur de l'appel, mais ne peut pas vérifier que l'appel a été autorisé à l'origine à utiliser un numéro donné.

Attestation de passerelle (C): le fournisseur de services a authentifié l'endroit d'où il a reçu l'appel, mais ne peut pas authentifier l'origine de l'appel. Un exemple de ce cas est un appel provenant d'une passerelle internationale.

Mécanisme d'authentification STIR/Shaken

Le mécanisme d'authentification propose une série de points qui définissent son fonctionnement :

- L'opérateur d'origine est identifié et est responsable de la signature et des informations qu'il transmet
- Un appel non signé ou dont la signature n'est pas valide est interrompu par l'opérateur de terminaison
- Un appel dont le champ d'identité est manquant ou mal formé est interrompu par l'opérateur de Transit. L'opérateur d'origine est responsable du placement d'un niveau de certificat conformément aux définitions de la norme Shaken et aux critères spécifiques définis entre opérateurs
- Dans un premier temps, les appels avec des certificats de niveaux B et C ne seront pas interrompus jusqu'à ce que des solutions techniques soient trouvées pour traiter tous les cas d'utilisation existants.

Mécanisme d'authentification STIR/Shaken

Un mécanisme de lutte contre le « spoofing » comprend une fonction d'authentification:

- Les signalements permettent d'alerter les opérateurs sur d'éventuels abus et de remonter ainsi jusqu'aux fraudeurs. En cas de signalement, l'opérateur d'origine doit fournir toute justification nécessaire pour permettre de retrouver l'opérateur ou l'entreprise incriminée.
- Le fonctionnement du système et du mécanisme d'authentification fera l'objet d'un suivi permanent afin de le maintenir à jour.
- Ce mécanisme peut être défini comme complet et efficace lorsqu'il est accompagné de sanctions.

Mécanisme d'authentification STIR/Shaken

Le schéma de fonctionnement du MAN est divisé en plusieurs étapes.

Phase préliminaire:

- Un opérateur (s'il répond à certains critères) peut demander à être inscrit sur la liste des opérateurs STIR auprès de l'APNF
- L'APNF vérifie l'identité du requérant. S'il est agréé, il est considéré comme un opérateur STIR
- Un opérateur STIR peut demander un certificat sur le GCO, qui sera ensuite accessible aux autres opérateurs via le BGCO.

Mécanisme d'authentification STIR/Shaken

Le schéma de fonctionnement du MAN est divisé en plusieurs étapes

Phase de communication (opérateur d'origine):

- Le client (appelant) tente d'établir une communication avec l'opérateur d'origine
- L'opérateur de départ peut décider de bloquer l'appel sortant si les contrôles de numérotation effectués par la maBNE échouent ou, si la validation est réussie, décider de prendre en charge l'appel.
- L'opérateur de départ, s'il décide de reprendre l'appel, utilise le champ Identité du STIR et certifie son identité avec son certificat APNF
- L'opérateur de départ ajoute ensuite une attestation SHAKEN au jeton PASSporT de la STIR avec la valeur A, B ou C.

Phase de communication (opérateur de transit):

- L'opérateur de transit vérifie ensuite le champ "Identity".
- A ce stade, il peut décider soit d'interrompre l'appel si le champ Identity de l'opérateur d'origine est incorrect ou inexistant, soit d'accepter l'appel. Une exception à cette procédure est faite pour les appels aux services d'urgence (avec rapport ultérieur au MAN).

Mécanisme d'authentification STIR/Shaken

Le schéma de fonctionnement du MAN est divisé en plusieurs étapes

Phase de communication (opérateur de terminaison):

- A ce stade, l'opérateur de terminaison vérifie le certificat de l'opérateur de départ (en se synchronisant en permanence avec le BPCO pour obtenir les certificats à vérifier).
- L'opérateur peut alors décider de mettre fin à l'appel si la signature de l'opérateur d'origine est manquante ou invalide (sauf pour les appels d'urgence), ou de transmettre l'appel au client final.

Mécanisme d'authentification STIR/Shaken

Le schéma de fonctionnement du MAN est divisé en plusieurs étapes

Contrôle a posteriori:

- L'opérateur de terminaison ou de transit analyse les communications en temps réel et effectue un certain nombre de contrôles.
- Si une anomalie est détectée, l'opérateur ouvre un incident de manière centralisée afin que l'opérateur fautif puisse éventuellement justifier son comportement ou corriger sa non-conformité aux règles du MAN si nécessaire.

Mécanisme d'authentification STIR/Shaken

Plainte du client:

- Un opérateur reçoit une plainte d'un client final en relation avec MAN.
- L'opérateur examine la plainte et, après avoir vérifié qu'il s'agit bien d'une plainte concernant le MAN, procède à une vérification de tout comportement anormal.
- L'opérateur initie alors un rapport centralisé fournissant toutes les informations nécessaires à une éventuelle enquête de l'opérateur.
- Une demande d'enquête est alors transmise à l'opérateur concerné, qui doit alors fournir toute justification utile, y compris au moyen des informations contenues dans le maBNE.

OBJECTIF DE CE WEBINAR

DÉFINIR CLAIREMENT LES BESOINS TECHNIQUES

- Diverses composantes du MAN

Diverses composantes du MAN

Base des Certificats Opérateurs (BCO)

Parmi les différentes composantes du MAN, on trouve la BCO qui se compose de deux modules principaux, GCO et BPCO.

- Le GCO (Gestionnaire des Certificats Opérateurs) est un système centralisé permettant la création, le renouvellement et la révocation des certificats opérateurs ainsi que la publication du BPCO.
- La BPCO (Base Publique des Certificats Opérateurs) est un système centralisé de type STI-CR (Secure Telephony Identity - Certificate Repository) qui regroupe tous les certificats opérateurs STIR (clés publiques) pour le MAN.

Ma Base des Numéros Exploités (maBNE)

Base de données interne à chaque opérateur qui est responsable de l'archivage de tous les clients qui effectuent des appels depuis les réseaux fixes ou mobiles à partir de numéros français.

maBNE est un bloc fonctionnel qui peut être composé de plusieurs solutions techniques ou de plusieurs bases au choix de l'opérateur.

Diverses composantes du MAN

STIR (Secure Telephony Identity Revisited) PASSporT (Personal ASSertion Token)

Le PASSporT, qui signifie Personal ASSertion Token, également appelé Identity, est un jeton contenant les informations dont le STIR/SHAKEN a besoin pour l'authentification et la vérification de l'appel. Les informations contenues dans ce jeton sont formatées en JWT (JSON Web Tokens).

Extention SHAKEN

L'extension SHAKEN est placée à l'intérieur d'un jeton PASSporT pour classer le type d'appel. Comme nous l'avons vu plus haut, cette extension peut être:

- A** - Attestation complète
- B** - Attestation partielle
- C** - Attestation de passerelle

Diverses composantes du MAN

Gestion des incidents MAN

- Un incident peut être ouvert en cas de suspicion de défaut ou de non-respect des règles MAN. Un incident doit être ouvert avec une cause.
- L'objectif d'un incident est d'alerter un opérateur ou l'APNF et d'obtenir ainsi une intervention/correction en cas de défaut avéré.
- Un incident peut être détecté par un opérateur ou par l'APNF par l'analyse en temps réel ou à posteriori des données du réseau, ou suite à la réception et à la qualification d'une ou plusieurs plaintes de clients.
- Les KPI (indicateurs de performance) des incidents sont établis et partagés (voir mesures).

Métriques

L'objectif des métriques est de disposer d'un mécanisme utile pour assurer l'évolution et le bon fonctionnement de la plate-forme MAN.

Diverses composantes du MAN

Processus et outils de signalement

- Un signalement est une demande faisant suite à une suspicion, par exemple un niveau de certification douteux.
- L'objectif d'un signalement est d'obtenir des justifications de la part d'un opérateur tiers sur son application des règles du MAN.
- L'APNF met en place un outil centralisé de collecte et de traitement des déclarations des opérateurs.
- Un signalement est communiqué par un opérateur à la suite d'analyses effectuées par l'opérateur ou à la suite de la réception et de la qualification d'une ou plusieurs plaintes de clients.
- Un signalement peut concerner un ou plusieurs appels ou messages.
- Le ou les opérateurs concernés sont affectés et répondent aux demandes en enquêtant et en fournissant les justifications demandées.

Diverses composantes du MAN

Opérateur Technique de Signature (OPTS)

Un opérateur technique de signature (**OPTS**) est un opérateur connecté au réseau public et chargé par un autre opérateur "signataire" de signer les appels en son nom. L'opérateur signataire reste responsable de l'utilisation de sa signature vis-à-vis de la communauté MAN.

Un opérateur peut donc être amené à signer des appels s'il est autorisé par un ou plusieurs opérateurs:

- En son nom propre pour les appels dont il est l'opérateur d'origine et avec son propre certificat.
- Pour le compte d'un ou plusieurs opérateurs signataires avec le certificat de l'opérateur spécifique

Un opérateur ne peut être OPTS (signataire pour le compte d'autres opérateurs) que s'il est lui-même opérateur d'origine (signant les appels en son nom propre).

Un opérateur signataire peut avoir plusieurs OPTS*

NOTA: L'opérateur signataire est l'opérateur détenteur du certificat.

Diverses composantes du MAN

Opérateur Technique de Vérification (OPTV)

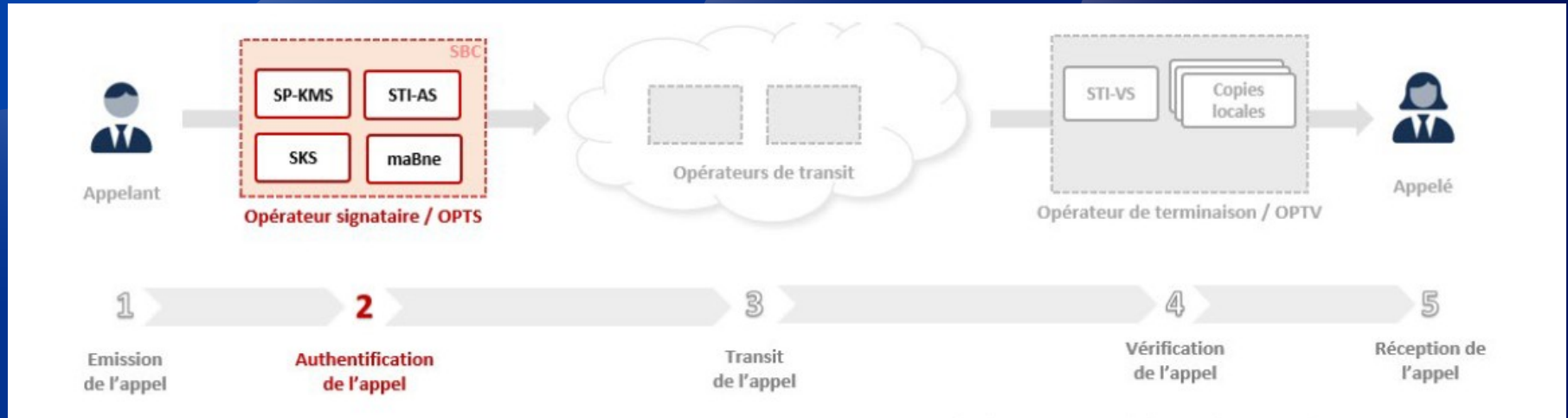
Un opérateur technique de vérification (**OPTV**) est un opérateur chargé par un opérateur de terminaison d'appliquer les règles du MAN en son nom, notamment de surveiller, voire d'interrompre les appels pour le compte de l'opérateur de terminaison.

L'opérateur de terminaison reste responsable vis-à-vis de la communauté MAN des appels interrompus.

Un opérateur OPTV ne peut donc être défini sur la plate-forme MAN qu'en tant qu'opérateur de terminaison, sans nécessairement être défini également en tant qu'opérateur d'origine/signataire.

VNT en tant que:

- signataire direct
- OPTS



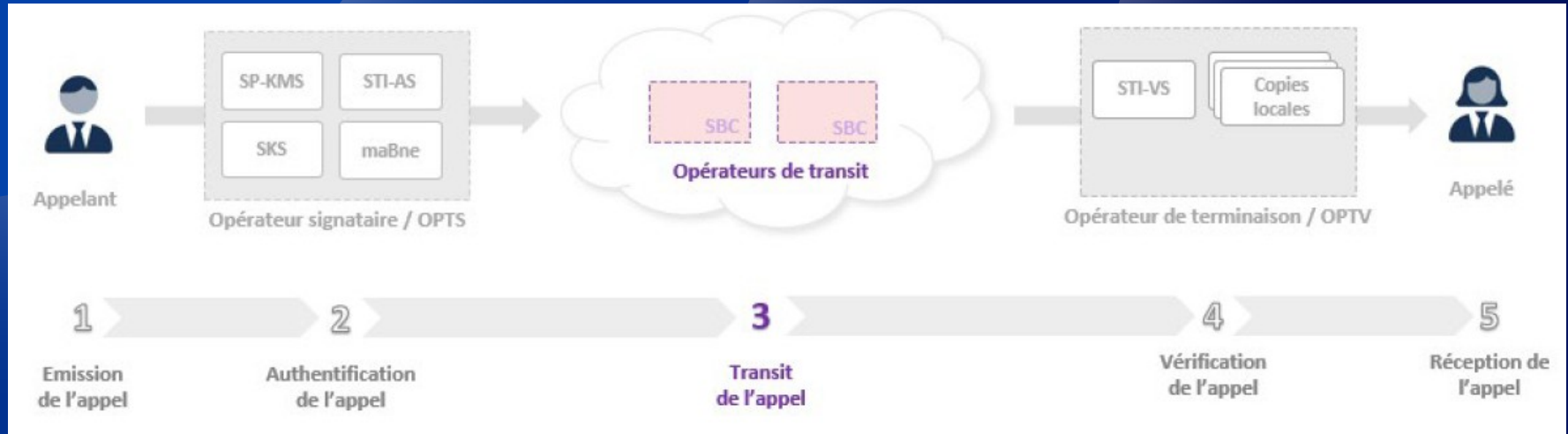
MAN

Mécanismes d'Authentification des Numéros

VNT en tant que OPTV



VNT en tant qu'Opérateur de Transit



MAN

Mécanismes d'Authentification des Numéros

OBJECTIF DE CE WEBINAR

VOUS DONNER DES DÉTAILS SUR NOTRE "OFFRE MAN"

MAN

Mécanismes d'Authentification des Numéros

NOTRE OFFRE POUR LE MAN

Trafic Numérotations VNT	OPTS/OPTV	MPM
BASIC	STANDARD	MAN pour moi
Frais d'activation: Aucun	Frais d'activation: OUI (One Shot)	Frais d'activation: OUI (One Shot)
Redevance mensuelle: Aucun	Redevance mensuelle: OUI (récurrente)	Redevance mensuelle: OUI (récurrente)
Cout par appel: Aucun	Cout par appel: OUI (par palier de volumes)	Cout par appel: OUI (par palier de volumes)
VNT géré et facture le trafic	VNT géré et facture le trafic	VNT NE GERE PAS LES APPELS mais s'occupe seulement de les signer
VNT «signe» avec son propre certificat (direct)	VNT «signe» avec le certificat intermédiaire du Client (VNO, etc.)	VNT «signe» avec le certificat du Client (direct) VNT, pour ce service, met à disposition, du Client, une machine dédiée VNT fourni la «location clé en main», de la prestation du service technique, pour la gestion du MAN

MAN

Mécanismes d'Authentification des Numéros

OBJECTIF DE CE WEBINAR

VOUS DONNER DES DÉTAILS SUR NOTRE OFFRE MAN - MPM”

MAN

Mécanismes d'Authentification des Numéros

VOUS DONNER DES DÉTAILS SUR NOTRE "OFFRE MAN"

Passons en revue les offres:

- **Offre BASIC** (sera certainement similaire aux offres concurrentes).
- **Offre STANDARD** (sera certainement similaire aux offres concurrentes).
- **MPM** pas tous nos concurrents seront en mesure d'offrir une solution similaire.

MAN

Mécanismes d'Authentification des Numéros

VOUS DONNER DES DÉTAILS SUR NOTRE "OFFRE MAN"

Détails de l'offre MPM:

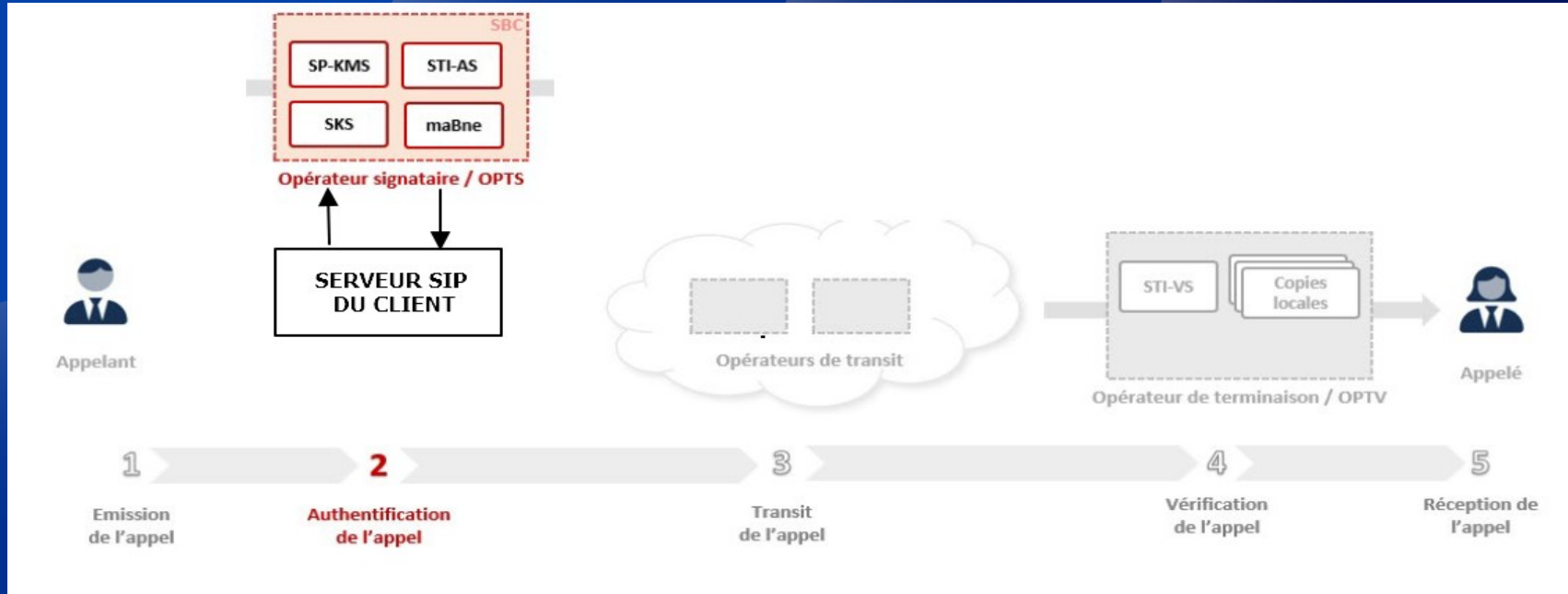
- **SBC-MAN dédié au client** (signataire direct)
- **Gestion des certificats:** à la fois du client lui-même (signataire direct) et de ses clients (directement ou en tant qu'OPTS/OPTV) avec vérification quotidienne des dates d'expiration et notification éventuelle (alerte).
- **Signature des appels téléphoniques:** tant pour le client lui-même (signataire direct) que pour ses clients (directement ou en tant qu'OPTS/OPTV)
- **Assistance:** pour la prise et le traitement des appels, le débogage et/ou le dépannage.

SOLUTION CLÉS EN MAIN

MAN

Mécanismes d'Authentification des Numéros

VOUS DONNER DES DÉTAILS SUR NOTRE "OFFRE MAN - MPM"

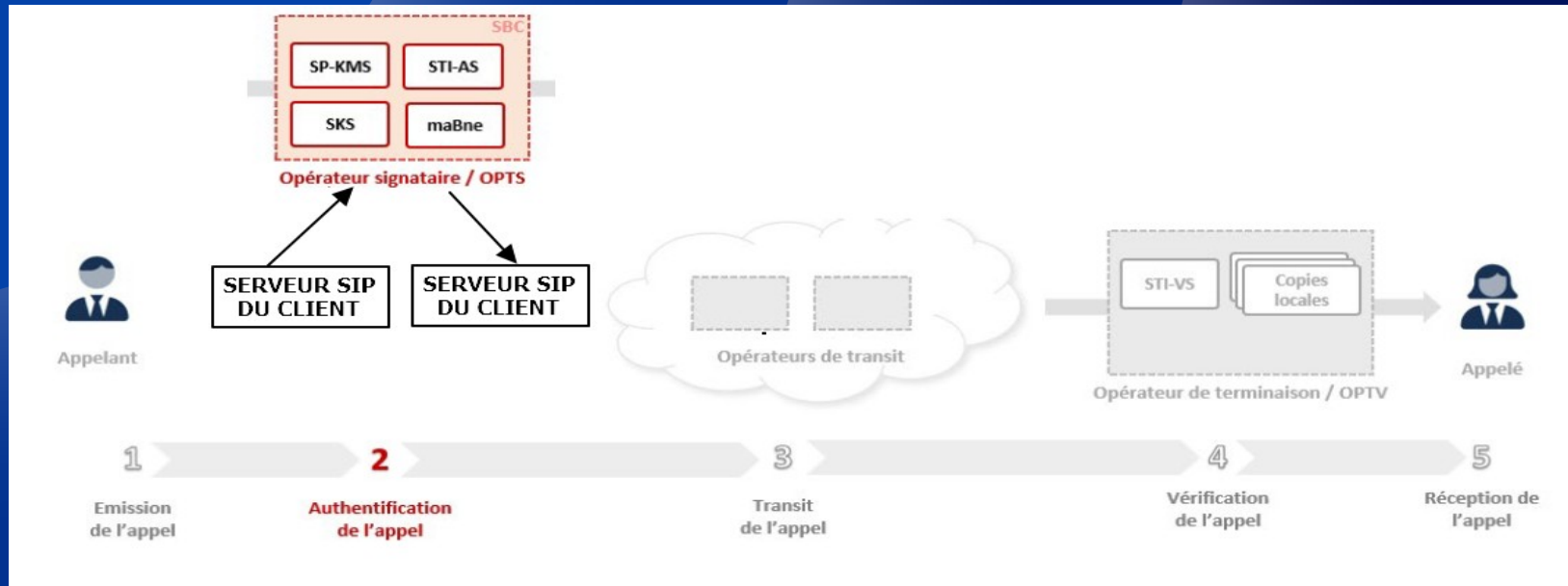


L'APPEL DU CLIENT SIGNATAIRE EST TRANSMIS AU MPM QUI SIGNE ET RENVOIE L'APPEL AU MÊME IP

MAN

Mécanismes d'Authentification des Numéros

VOUS DONNER DES DÉTAILS SUR NOTRE "OFFRE MAN - MPM"



L'APPEL DU CLIENT SIGNATAIRE EST TRANSMIS AU MPM QUI SIGNE ET RENVOIE L'APPEL À UN AUTRE IP (ÉGALEMENT DU CLIENT SIGNATAIRE)

MAN

Mécanismes d'Authentification des Numéros

VOUS DONNER DES DÉTAILS SUR NOTRE "OFFRE MAN"

FIABILITÉ, ÉVOLUTION ET PERFORMANCE

Toute notre infrastructure dédiée à MAN se trouve dans le Cloud d'**Azure Paris**.

Ce choix a été fait afin d'offrir aux clients un maximum de performance et de (haute) fiabilité.



Merci!

Questions ?

Pour les questions techniques,
nous organisons des séances
privés.