Orange programme partenaires

Nomadisme et sécurité avec Orange Business Services

Orange France

Retrouvez l'ensemble de la documentation technique des réseaux Orange France sur Orange Partner

Evolutions du document			
Vers	**Rév.**	**Date**	**Commentaires**
1	0	30 Juin 2004	Création du document
1	1	20 Décembre 2007	Mise à jour réseau UMTS
2	0	25 Février 2011	Mise à jour S1 2011
2	1	8 Mars 2011	MAJ des schémas
2	2	10 juin 2012	Corrections typographiques, précisions sur les protocoles.
2	3	8 Avril 2015	Ajout de l'A5/3 pour la partie CS du GSM Ajout de la sécurisation du réseau d'accès 4G

Sommaire

1 Glossaire

802.11	Voir Wifi
APN	**Access Point Name** : Point d'accès pour le réseau 3G
Autorité de certification	Autorité qui a la confiance d'un ou plusieurs utilisateurs pour générer et assigner des certificats.
Certificat	Document sous forme électronique attestant du lien entre les données de vérification de signature électronique et un signataire. Un certificat contient généralement la clé publique d'un utilisateur, ainsi que d'autres données, rendues infalsifiables à l'aide du chiffrement par la clef privée de l'autorité de certification qui a généré le certificat.
Condensé	Un condensé relatif à un document ou à des données est une somme de contrôle cryptographique, permettant de s'assurer de la non modification accidentelle ou volontaire d'un document ou message lors d'une transmission notamment.
EDGE	**Enhanced Data Rates for GSM Evolution** Norme de téléphonie mobile, évolution logicielle du GSM/GPRS permettant d'atteindre des débits 2 à 3 fois supérieurs à ceux du GPRS.
GSM	**Global System Mobile** : Réseau data mobile en mode circuit
GPRS	**General Packet Radio System** : Réseau data mobile en mode paquet
Hot Spot	Lieu public à forte affluence et clairement délimité (café, hôtel, gare, aéroport, etc.) donnant accès à un réseau sans fil Orange wifi access, qui permet aux utilisateurs de terminaux mobiles (PC portable, assistant personnel par exemple) de se connecter facilement à Internet.
HSDPA	**High Speed Download Packet Access** Protocole pour la téléphonie mobile parfois appelé 3,5G ou encore 3G+ (dénomination commerciale). Ce protocole offre des performances dix fois supérieures à la 3G (UMTS R'99) dont il est une évolution logicielle.
LTE	**Long Term Evolution** Appelée aussi 4G, cette évolution de la 3G est composée d'une partie accès radio (eUTRAN) et d'un cœur de réseau (EPC).
IMSI	**International Mobile Subscriber Identity** L'identité de l'abonnement, spécifique à chaque opérateur et chaque abonnement
IPSec	Suite de protocoles pour IP fournissant les services nécessaires à la sécurisation d'échanges de données au travers d'un réseau partagé.

Non répudiation	Service permettant de prouver à une tierce partie l'occurrence d'un événement. Les applications les plus courantes sont : • la non-répudiation de l'origine : l'émetteur d'un message ne peut nier le fait qu'il est à la fois le créateur et l'émetteur d'un message. • la non-répudiation de remise : le destinataire d'un message ne peut nier le fait qu'il a à la fois reçu le message et pris connaissance de son contenu. Il s'agit en fait de rendre deux services : 1. un service d'authentification de l'émetteur du message (via signature électronique) *2.* un service de garantie de livraison (mécanismes d'accusé de réception ou synchronisation de l'échange par un tiers)
PKI	**Public Key Infrastructure Définition** (ou Infrastructure à clé publique) Correspond à l'industrialisation, à l'intégration et à la gestion des techniques de chiffrement et de signature électronique dans un système d'information et dans une organisation. Ce n'est donc pas un système de sécurisation en soi mais l'infrastructure permettant la mise en place et la gestion des services associés à l'utilisation des certificats numériques.
Radius	**Remote Authentication Dial-In User Service** Service d'authentification (serveur et protocole radius) utilisé pour l'allocation d'adresse IP (vérification d'un couple Identifiant / Mot de passe.
Signature	Le terme signature est utilisé lorsqu'une entité justifie de son identité en tant qu'émetteur d'un document en y ajoutant sa signature numérique.
Signature numérique	Elément ajouté à des données, ou transformation cryptographique de données, qui permet à un destinataire des données de vérifier l'origine et l'intégrité des données et protège contre leur falsification, notamment par le destinataire.
SSL	**Secured Socket Layer** *:* mécanisme de sécurité applicable à HTTP SSL utilise les technologies de chiffrement à clé privée et à clé publique pour assurer les services d'authentification client / serveur (certificats X.509), de confidentialité et d'intégrité. SSL est principalement utilisé sur Internet pour sécuriser HTTP (protocole HTTPS).
TMSI	**Temporary Mobile Subscriber Identity** L'identité de l'abonnement utilisée dans le réseau pour la négociation des clés
UMTS	**Universal Mobile Telecommunication System** Technologies de téléphonie mobile de troisième génération (3G) européenne. Elle est elle-même basée sur la technologie W-CDMA, standardisée par le 3GPP
UTRAN	**UMTS Terrestrial Radio Access Network** Réseau d'accès de l'UMTS composé du RNC et du Node-B
Concentrateur VPN	Matériel actif réseau qui permet d'accepter un nombre considérable de connexions VPN simultanées grâce à des composants cryptographiques spécifiques qui effectuent les calculs cryptographiques, particulièrement gourmands en termes de ressources.
VPN	**Virtual Private Network** Réseau privé virtuel établi au-dessus d'un réseau public qui permet de « protéger » les informations y circulant. Un VPN peut être établi sur un réseau IP par le protocole IPSEC (on parle alors de VPN sur IP ou VPN IPSEC), mais il peut être également établi à un niveau plus bas, avec la technologie

	MPLS par exemple (le tunnel privé est alors garanti par le processus de routage mais les données ne sont pas chiffrées).
Wifi	**Wireless Fidelity** Réseau local de type Ethernet à accès sans fil basé sur la norme 802.11 qui permet d'obtenir des débits pouvant atteindre 11 (802.11b), 54 (802.11g) et 100 (802.11n) Mb/s théorique dans une bande de fréquences de 2,4 Ghz.

2 Introduction

Le présent document a pour objet de présenter un panorama des problématiques de sécurité liées au nomadisme. Seuls les aspects de sécurité « logique » seront abordés, les problématiques de sécurités liées à l'exploitation (disponibilité, administration, etc.) et de sécurité étant spécifiques à chaque organisation utilisant les services mobiles.

Après un rappel sur les différentes techniques de chiffrement, à la base de nombreux services de sécurité nous présenterons les différents services liés au nomadisme et leurs déclinaisons sur les réseaux mobiles Orange avant de détailler l'ensemble des services intégrés ou compatibles avec les solutions data d'accès mobile Orange Business Services.

3 Techniques de chiffrement et mécanismes associés

Les différents services de sécurité qui seront abordés dans ce document reposent aujourd'hui largement sur les techniques de chiffrement. Ce chapitre a donc pour but d'en rappeler succinctement les grands principes ainsi que les mécanismes associés, pour une meilleure compréhension.

Deux méthodes de chiffrement sont couramment utilisées aujourd'hui : le chiffrement symétrique et le chiffrement asymétrique. Nous allons aborder ces deux méthodes après quelques définitions.

3.1 Définitions

Algorithme non inversible
Un algorithme non inversible y=F(x) est un algorithme conçu de telle façon qu'il est facile de calculer y à partir de x, mais connaissant y il est impossible de trouver un x dans un temps raisonnable. Un tel algorithme peut utiliser un paramètre ou clé (y=F(p,x), cas courant en chiffrement) ou non (cas du calcul de condensé).

Algorithme de hashage
Algorithme non inversible permettant de calculer une somme de contrôle cryptographique, généralement de taille fixe. Les algorithmes utilisés pour le calcul de condensés s'apparentent aux algorithmes utilisés pour le chiffrement mais sont en général très peu gourmands en puissance de calcul. Les plus répandus sont MD5 (Message Digest v5) et SHA (Standard Hash Algorithm).
Ce type d'algorithme est utilisé notamment pour le calcul de condensé et en authentification simple afin de ne pas stocker les mots de passe en clair (comparaison de H[mot de passe saisi] avec la valeur H[mot de passe] stocké en base).

Condensé
Un condensé relatif à un document ou des données est une somme de contrôle cryptographique, généralement de taille fixe, obtenue en appliquant un algorithme de hashage non inversible au document ou données. Un condensé permet de s'assurer de la non modification accidentelle ou volontaire d'un document ou message lors d'une transmission notamment : il suffit par exemple de joindre à un message envoyé son condensé MD5, le destinataire pouvant ainsi calculer de même le condensé du message reçu et vérifier que les deux valeurs sont bien identiques.

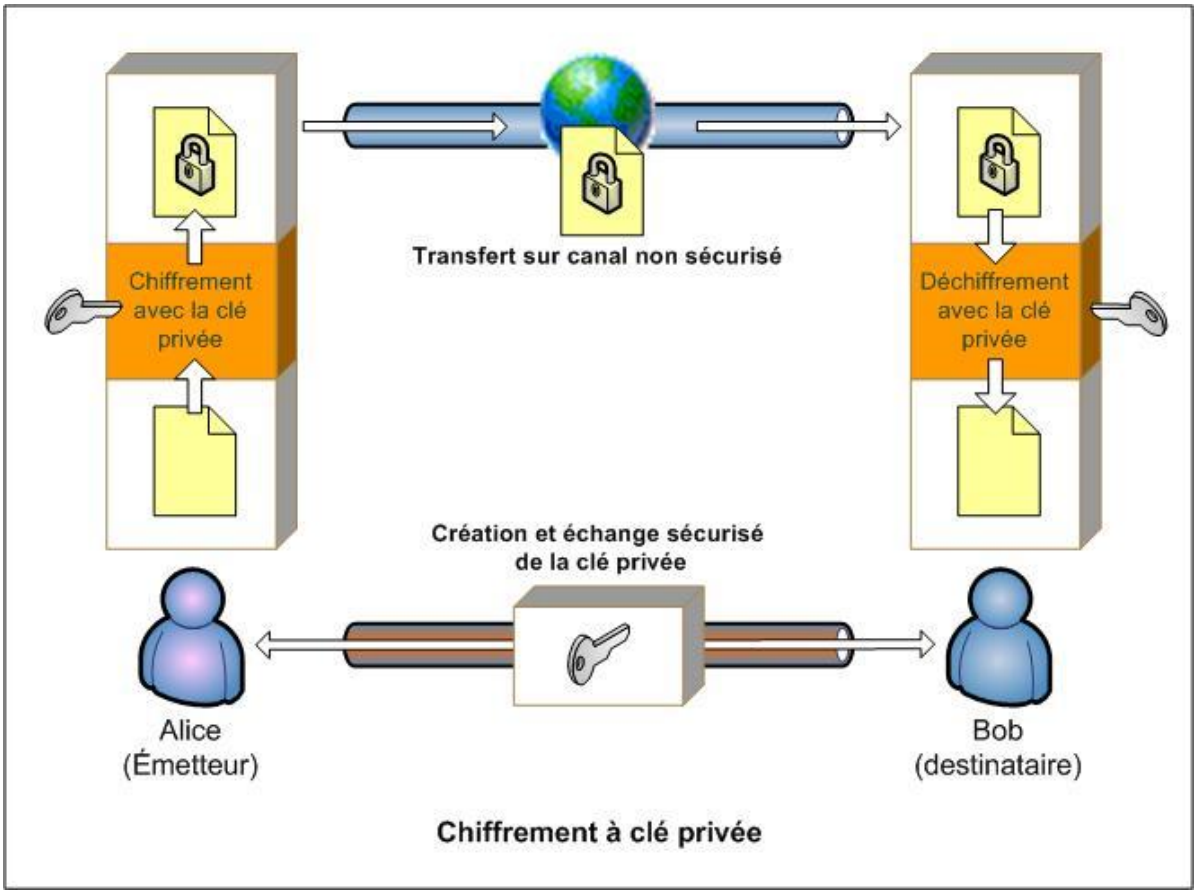
Signature
Relativement proche de la notion d'authentification, le terme de signature est utilisé lorsqu'une entité justifie de son identité sur un document (vérification asynchrone de l'identité), alors que l'authentification est constituée par la déclinaison de son identité à des fins de connexion et transmission (synchrone). Les deux notions se rejoignent lorsque la signature est utilisée dans un processus synchrone.

3.2 Le chiffrement à clé secrète (chiffrement symétrique)

Ce type de chiffrement utilise deux fonctions symétriques, une fonction de chiffrement et une fonction de déchiffrement, toutes deux non inversibles et utilisant une unique clé privée.

Deux entités souhaitant chiffrer leurs échanges doivent donc générer et se mettre d'accord sur **une clé secrète partagée** (ou PSK, Pre-Shared Key) qui leur est propre et doit rester confidentielle puisqu'elle permet le déchiffrement.

3.2.1 Utilisation en chiffrement



Les algorithmes de chiffrement symétrique sont en général assez rapides. C'est la gestion de clés secrètes qui peut poser problème avec ce type de chiffrement : l'échange des clés doit être sécurisé et le nombre de clés devient vite conséquent.
Dans le cadre d'une PKI, le chiffrement à clé publique est donc largement utilisé en complément de ce type de chiffrement.

3.2.2 Utilisation en authentification

En supposant que deux entités Alice et Bob ont échangé par un moyen sécurisé une clé privée K, l'authentification de Bob par Alice sur un canal non sécurisé peut se faire de la façon suivante :

1. Alice génère un nombre aléatoire **rand** appelé challenge et le transmet à Bob
2. Bob chiffre **rand** via un algorithme A à clé privée et retourne le résultat **r = A(rand, K)** à Alice
3. Alice chiffre **rand** via le même algorithme A à clé privée pour obtenir **r' = A(rand, K)**
4. Alice compare r et r' : si r = r' alors Bob est bien Bob puisqu'il dispose de la clé secrète K

3.2.3 Exemples d'algorithmes de chiffrement symétrique

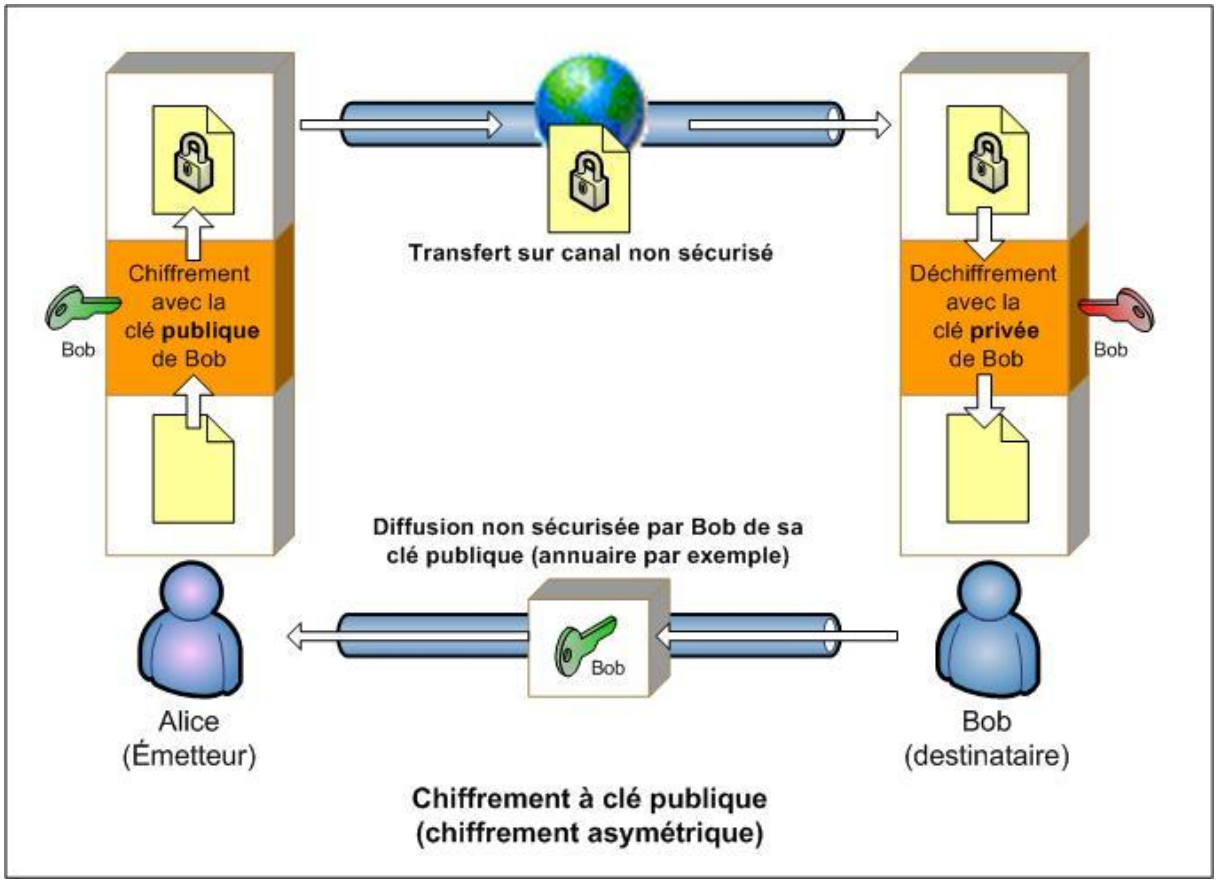
- **DES :** Data Encryption Standard
- **3DES** : extension de DES (DES à trois étages), utilisé par SSH
- **RC2/4/5 :** de RSA Data Security
- **IDEA :** International Data Encryption Standard utilisé par PGP
- **AES :** Advanced Encryption Standard
- **AKA :** Authentication and Key Agreement

3.3 Le chiffrement à clé publique (chiffrement asymétrique)

Le chiffrement asymétrique repose quant à lui sur **une paire de clés**, l'une publique et l'autre privée, et sur l'utilisation de deux fonctions non symétriques (le chiffrement et le déchiffrement se font donc à l'aide de deux clés différentes).

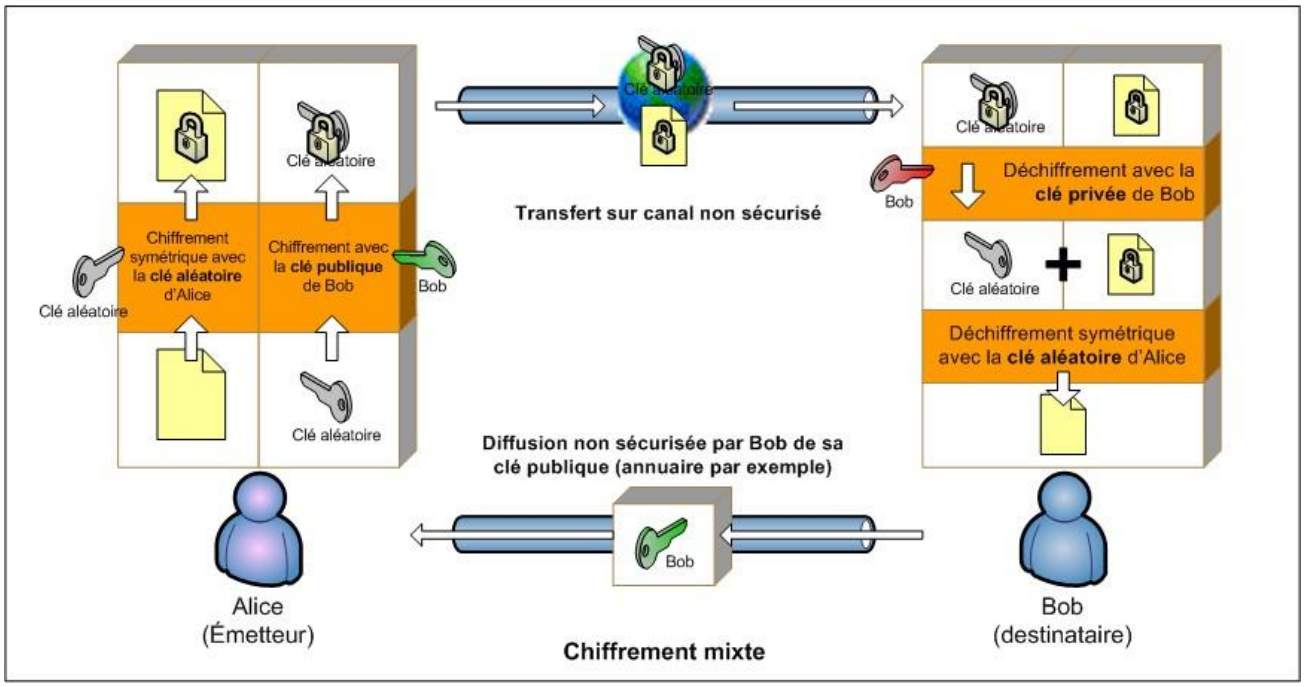
Le terme asymétrique provient du fait qu'un message chiffré à l'aide de la clé publique –non secrète donc diffusable- n'est déchiffrable qu'en utilisant la clé privée associée (utilisation en chiffrement ou authentification), alors qu'inversement un message chiffré grâce à la clé privée n'est déchiffrable que par la clé publique (utilisation en signature). L'intérêt par rapport au chiffrement symétrique est l'absence d'échange de secret, seule la clé publique, ne permettant pas de lire les données chiffrées, étant diffusée.

3.3.1 Utilisation en chiffrement



3.3.2 Utilisation en chiffrement mixte

Les algorithmes de chiffrement asymétrique étant par nature plus demandeurs en terme de puissance de calcul que les algorithmes symétriques (à niveau de sécurité équivalent), **ils ne sont en général pas utilisés pour chiffrer directement un message mais pour chiffrer une clé secrète destinée à chiffrer le message à l'aide d'un algorithme plus rapide de type symétrique (cas de TLS, SSL, PGP, etc.).**



A noter qu'à niveau de sécurité équivalent, les clés utilisées par les algorithmes asymétriques sont de taille plus importante que les clés utilisées par les algorithmes symétriques (4096 bits contre 128 bits par exemple). La longueur des clés nécessaires pour assurer un niveau de sécurité donné évolue bien sûr en même temps que les puissances de calcul disponibles deviennent plus importantes.

3.3.3 Utilisation en signature

Signer un document (ou message) consiste à y joindre le résultat du chiffrement d'un condensé de ce document à l'aide de la clé privée de l'émetteur (la signature).
Le destinataire peut ainsi valider que le document provient bien de l'émetteur déclaré en

- déchiffrant la signature à l'aide de la clé publique de l'émetteur (le condensé du message est obtenu)
- calculant le condensé du message par le même algorithme que l'émetteur
- comparant les deux résultats obtenus qui doivent être identiques

Pour les mêmes raisons que pour l'utilisation en chiffrement, on n'utilise pas en général le chiffrement asymétrique pour signer directement un message mais pour signer un condensé caractéristique du message, le calcul du condensé étant fait par un algorithme rapide non inversible.

3.3.4 Utilisation en authentification

Très proche de l'utilisation précédente, l'authentification peut être réalisée via challenge :

1. Alice connaît la clé **publique** Kb de Bob
2. Alice choisit un nombre n et le transmet à Bob
3. Bob encode ce nombre via un algorithme asymétrique A avec sa clé **privée** K'b et retourne le résultat à Alice : r = A(n, K'b)
4. Alice déchiffre r à l'aide de la clé publique de Bob et obtient un nombre n'=A'(r, Kb)
5. Alice compare n et n' : si n=n' alors Bob est bien Bob car il connaît la clé **privée** de Bob

3.3.5 Exemples d'algorithmes à chiffrement asymétrique

- **RSA** : du nom de ses inventeurs Rivest, Shamir et Adleman
- **ElGamal**
- **DSA / DSS**

4 Services de sécurité liés au nomadisme

4.1 Contrôle d'accès logique

Définition
Le contrôle d'accès logique aux ressources du système d'information consiste à contrôler :

- l'accès aux données du SI via des connexions distantes : garantir que seuls les flux autorisés transitent effectivement au niveau réseau. Cela revient à mettre en œuvre des filtres autorisant une identité numérique donnée à accéder ou non à une ressource via tel ou tel protocole.

- l'accès non autorisé aux données stockées dans les terminaux mobiles : garantir que seules les entités autorisées ont accès aux données confidentielles.

Le contrôle d'accès est le pré-requis aux autres services de sécurité : il est en effet inutile de mettre en œuvre des mécanismes à base de certificats et de clés si par exemple le simple accès aux serveurs n'est pas contrôlé.

Solutions techniques
- accès via connexion distantes
  - filtrage protocolaire :
    - architecture à base de firewall
    - règles au niveau de la couches 3 voire 4 (filtrage applicatif)
  - surveillance et détection des attaques

- accès aux données stockées sur les terminaux mobiles
  - protection par mot de passe spécifique aux OS
  - chiffrement des données stockées par clé secrète (type AES)
  - stockage (et chiffrement) sur mémoire amovible
  - verrouillage des terminaux

4.2 Authentification

4.2.1 Principes et définitions

L'authentification consiste à associer de manière unique une identité à un utilisateur. On regroupe en fait par abus de langage deux fonctions dans le terme unique « authentification » :

- **L'identification** : consiste à associer une identité numérique présumée à une entité se connectant (utilisateur ou ressource).

- **L'authentification** : consiste à vérifier et à confirmer que l'entité qui s'est identifiée est bien celle qu'elle prétend être.

En pratique, l'authentification repose toujours sur l'utilisation d'un secret, dont la nature peut être de différents types :
- « ce que je sais » : mot de passe par exemple
- « ce que je possède » : possession physique d'un objet (clé, carte ou autre support) et d'un secret associé
- « ce que je suis » : biométrie (empreintes digitales, rétine ou voix)

Chacun de ces types d'authentification pris individuellement peut poser problème : « ce que je sais » peut être deviné ou partagé, « ce que je possède » peut être volé et « ce que je suis », bien qu'étant le plus sûr, est coûteux à mettre en place et reste vulnérable.

Authentification forte : une technique d'authentification est dite forte lorsqu'elle combine **au moins deux types différents de secrets**, par exemple quelque chose que je sais et quelque chose que je possède. Un mécanisme d'authentification forte peut être utilisé en combinaison avec des solutions d'authentification courantes telles que Radius, VPN, etc.

Techniques d'authentification
Les techniques d'authentification les plus courantes aujourd'hui, qui peuvent s'appuyer sur un support physique, sont les mots de passe et les certificats, les techniques de biométrie restant peu normalisées. Ces techniques sont explicitées dans les paragraphes suivants. A noter que les solutions type VPN, décrites plus loin dans ce document prennent généralement en charge l'authentification bilatérale.

4.2.2 Les mots de passe

Les mots de passe constituent la technique d'authentification la plus commune. Il y a deux types de mots de passe :

- **Le mot de passe réutilisable** (ou statique) : une même suite de caractères alphanumérique est utilisée à chaque authentification.

  Les mots de passe réutilisables peuvent être facilement divulgués (écrit sur un papier voire donné à des tiers) et sont vulnérables à un certain nombre d'attaques simples (attaque « brute force » par dictionnaire, écoute du réseau pour être rejoué, interception de frappe de touches, etc.)

- **Le mot de passe à usage unique** (ou dynamique) : la suite de caractères alphanumériques utilisée à chaque authentification est différente. La validité d'une suite donnée peut en outre être limitée dans le temps.

  L'unicité de l'usage permet d'éviter que le secret soit divulgué et empêche que la séquence d'authentification soit rejouée, limitant les risques liés à une éventuelle écoute.

  Les mots de passe à usage unique sont générés via un algorithme non inversible (chiffrement, hash) qui prend un paramètre en entrée et calcule le mot de passe à saisir. Cet algorithme, est utilisé à la fois côté serveur et côté utilisateur (souvent intégré dans une calculette ou dans un logiciel) pour comparer les deux résultats. On distingue plusieurs modes de génération en fonction de la nature du paramètre utilisé par l'algorithme :

  - asynchrone (challenge) : le serveur transmet à l'utilisateur un nombre aléatoire lorsque celui ci souhaite s'identifier. C'est ce nombre qui est utilisé comme paramètre par l'algorithme pour calculer le mot de passe.

  - synchrone dépendant du temps : le mot de passe généré est fonction du temps. L'heure et la date sont souvent utilisées comme paramètre de calcul, ce qui exige que la calculette et le serveur soient correctement synchronisés. Cela qui peut se faire par synchronisations régulières et/ou en donnant au mot de passe une durée de vie de quelques secondes à quelques minutes.

  - synchrone indépendant du temps : la date et l'heure sont remplacées ici par un compteur incrémenté côté client et chiffré par un algorithme qui produit le mot de passe. Le mot de passe

est ici réellement à usage unique car il n'est plus valide dès son utilisation (et non pas pendant une certaine durée, même très courte).

4.2.3 Les certificats

Un certificat est en quelque sorte une carte d'identité électronique utilisée pour l'identification et l'authentification, ainsi que le chiffrement que nous aborderons plus loin dans ce document. Il permet de justifier de l'identité d'un individu, sa validité qui peut être vérifiée reposant sur la certification par un tiers de confiance.

Techniquement parlant, il s'agit d'un fichier qui peut être stocké de différentes façons, sur un support fixe (poste) ou -ce qui est mieux- sur un support amovible (clé USB, carte à puce par exemple), contenant les informations sur l'entité à identifier et notamment sa clé publique. Dans la cadre d'un usage professionnel, la confiance dans les informations qu'il contient repose sur la signature d'une autorité de certification reconnue (technique de chiffrement asymétrique).

La norme X.509 de l'IETF est actuellement la norme la plus utilisée. Un tel certificat permet :

- de s'assurer de l'identité d'une entité : la signature du certificat par une autorité de certification reconnue permet de garantir que le certificat identifie bien l'entité qui y est décrite.

  En effet, la signature étant un condensé du certificat chiffré par la clé privée de l'autorité de certification, il suffit de déchiffrer cette signature à l'aide de la clé publique de l'autorité et de vérifier que le résultat de correspond bien à la valeur obtenue par calcul local du condensé.

- de l'authentifier : la présence de la clé publique de l'entité identifiée permet de vérifier et de confirmer que l'entité qui s'est identifiée est bien celle qu'elle prétend être (via challenge par exemple).

4.2.4 Les algorithmes de chiffrement

Les techniques de chiffrement explicitées en première partie de ce document peuvent être avantageusement utilisées pour assurer un niveau d'authentification maximum, couplés à un support physique ou un certificat.

4.2.5 Les supports physiques de l'authentification

L'utilisation d'un support physique consiste à baser l'authentification au moins en partie sur un objet (« quelque chose que je possède ») afin d'assurer une authentification forte.

Certains de ces supports permettent également le stockage des clés et certificats nécessaires à la mise en œuvre des services de confidentialité et d'intégrité abordés plus loin dans ce document.

Les types de supports physiques les plus courants aujourd'hui sont :

- **Les calculettes** : de format carte de crédit ou porte-clés, elles permettent une authentification forte via saisie d'un code PIN (« ce que je sais ») et d'un code à usage unique généré à fréquence donnée par la calculette (« ce que je possède »). Pour s'authentifier au service cible, l'utilisateur doit :
  - soit saisir son code PIN ainsi que le code généré par sa calculette
  - soit saisir le code généré après première saisie de son code PIN sur sa calculette

services rendus : authentification forte (deux facteurs)

exemples :

RSA SecureID^{tm}

Safeword

- **Les cartes à puce** : elles permettent de stocker des certificats numériques et mots de passe et les plus élaborées constituent de vrais mini-ordinateurs (ROM, RAM, EEPROM) assurant elles mêmes des fonctions de chiffrement et pouvant faire tourner des applications Java. Elles permettent ainsi de combiner plusieurs fonctions de sécurité permettant un accès sécurisé à des applications multiples.
  Ne disposant d'aucune forme d'affichage, de saisie ou d'alimentation propre, elles nécessitent par contre un lecteur de carte connecté au terminal hôte pour interagir avec un tiers logiciel. La création / gestion des supports nécessite en outre la mise en place d'une infrastructure à clé publique dédiée (PKI).

  services rendus :
  - authentification forte (deux facteurs : code PIN (« ce que je sais » associé à la carte à puce elle-même (« ce que je possède »))
  - stockage sécurisé des clés privées, certificats et mots de passe relatifs à plusieurs applications ou services permettant in fine l'authentification distante, le chiffrement, la signature et autres services associés.

  exemples :

  - cartes SIM Orange

    Chaque carte SIM, protégée par un code PIN, contient entre autres
    - un numéro dit IMSI (cf. glossaire) représentant l'identité de l'abonnement,
    - une clé individuelle de 128 bits qui lui est propre,
    - un algorithme d'authentification.

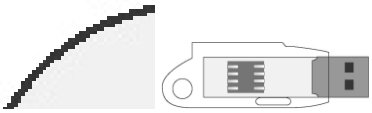
    Le mécanisme d'authentification, basé sur le chiffrement à clé secrète, est décrit en détail dans le paragraphe consacré à la sécurité des accès GSM / GPRS.

  - Cartes USIM Orange

    La carte USIM est l'équivalent de la carte SIM mais pour le réseau UMTS (3G). Outre des capacités de stockage plus importantes, elle se distingue de la carte SIM par ses mécanismes d'authentification plus évolués EAP-AKA (=Authentification and Key agreement) basé sur un chiffrement à clefs symétriques.

- Smart Card (RSA, GemPlus, etc.)

- **Les dongles USB** : ce sont de simples cartes à puce présentées sous un format différent. Plutôt que de déployer la puce sur une carte plastique, elle est insérée dans un support directement enfichable dans tout port USB, ne nécessitant donc pas de lecteur spécifique. Ce type de support combine donc les fonctionnalités des cartes à puce tout en permettant un usage plus universel.



4.3 Confidentialité et intégrité

4.3.1 Principes et définitions

La confidentialité des données consiste à s'assurer que les données stockées sur une entité ne peuvent être lues que par leur propriétaire et que les messages transmis ne peuvent être lus par qui que ce soit d'autre que l'émetteur et le destinataire lors d'une transmission.

L'intégrité consiste à s'assurer que des données n'ont pas été modifiées ou supprimées sur leur entité de stockage ou pendant leur transmission sur un réseau, et que les messages qui arrivent à un destinataire sont bien ceux qui ont été envoyés par l'émetteur.

La confidentialité n'assure pas l'intégrité (un message peut être rejoué). De même, l'intégrité n'assure pas la confidentialité (messages en clair). Ces deux services peuvent être mis en œuvre séparément mais les techniques utilisées permettant généralement de garantir les deux, ils sont ici regroupés.

A noter que l'ensemble des solutions permettant d'assurer la confidentialité et l'intégrité reposent sur les techniques de chiffrement symétrique et asymétrique abordées plus haut dans ce document, les clés privées / publiques voire certains algorithmes pouvant avantageusement être stockés dans les supports physiques décrits au chapitre 4.2.4.

4.3.2 Approches

Il existe deux approches permettant d'assurer confidentialité et intégrité :

- **l'utilisation d'un canal non sécurisé :** les messages eux-mêmes sont sécurisés et circulent sur un réseau non sécurisé

- **l'utilisation d'un canal sécurisé :** on fait confiance à une infrastructure de transport et à la sécurisation de celle-ci pour acheminer des messages (VPN par exemple). C'est cette approche, associée à une gestion de clés publiques, qui est privilégiée dans un contexte professionnel.

4.3.3 Solutions techniques

4.3.3.1 Canal non sécurisé

- **S/MIME : Secure MIME**

Version sécurisée du protocole MIME permettant la mise en œuvre de l'authentification et du chiffrement dans le cadre des applications de messageries électroniques classiques de type Outlook (utilisation de certificats personnels). Utilise RC2 et 3DES pour le chiffrement, RSA pour la signature et SHA1 / MD5 pour le calcul de condensés.

- **PGP : Pretty Good Privacy**

Crée dans un but de promotion de l'usage de la cryptographie à des fins personnelles, PGP repose sur la création de certificats (paires de clés publique / privée pour algorithmes à clé publique) qui ne reposent pas sur une autorité de certification pour assurer le chiffrement et la signature. Chacun génère donc son propre certificat et le distribue à ses interlocuteurs, la confiance se faisant de proche en proche un peu sur le modèle du peer to peer (chacun est sa propre autorité de certification). Ce type de solution n'est toutefois pas envisageable pour un usage professionnel.

4.3.3.2 Canal sécurisé

Un réseau privé virtuel (VPN) est un réseau de données privé pouvant utiliser des infrastructures réseau mutualisées grâce à un protocole d'acheminement ou de tunneling et des dispositifs de protection des données. Les VPN IP utilisent le protocole IP sur le réseau Internet public (VPNs basés sur des équipements d'extrémité) ou le réseau du fournisseur de services (VPN basés sur le réseau).

VPNs basés sur un réseau privé

VPN Implémentés sur les couches 2 (Liaison) ou 3 (Réseau) dans lesquels les services de sécurité sont pris en charge par le réseau de l'opérateur : majoritairement IP VPN sur MPLS (IP VPN), dans le cas du réseau Orange. C'est la solution retenue dans le cadre de l'offre Secure Mobile Access Intranet. Plus d'infos sur www.orange-programmepartenaires.com.

VPNs IP basés sur des équipements d'extrémité

Le réseau peut dans ce cas être un réseau IP public (tunneling de niveau 3), les services de sécurité étant assurés par des équipements d'extrémité (firewall, concentrateur VPN, client/serveur logiciel VPN ou routeur). Ce type de VPN est décrit de façon plus détaillée sur le site Orange programme partenaires www.orange-programmepartenaires.com. C'est la solution retenue dans le cadre de l'offre Secure Mobile Access Internet.

Couche OSI	Protocole de tunneling	
niveau 2	**PPTP**	**Point to Point Tunneling Protocol :** PPTP est un protocole de niveau 2 (Liaison) proposé par Microsoft et utilisant l'encapsulation GRE (Generic Routing Encapsulation). Il permet des accès VPN à des applications distantes sur réseaux mutualisés IP via encapsulation de trames PPP dans des datagrammes IP. Techniquement dépassé au profit de L2TP.
	L2TP	**Layer 2 Tunneling Protocol :** Combinaison de PPTP et L2F (Layer 2 Forwarding), L2TP est un protocole réseau, proposé conjointement par Cisco, Microsoft et 3COM, qui permet l'encapsulation des trames PPP sur réseaux IP.
niveau 3	**IPSec**	Situé au niveau de la couche réseau (niveau 3), IPSec est une suite de protocoles pour IP développée par l'IETF, conçue pour fournir les services nécessaires à la sécurisation d'échanges de données au travers d'un réseau partagé. Véritable extension de IP, IPSec repose sur les protocoles AH (Authentification Header) et ESP (Encapsulation Security Payload), assurant l'authentification bilatérale, la confidentialité et l'intégrité, sans imposer d'algorithme de chiffrement ou de hashage particulier. IPSec assure l'authentification bilatérale ainsi que la confidentialité et l'intégrité au niveau IP, permettant ainsi de sécuriser sans distinction tout flux sur IP.
niveaux 4/5	**SSL/TLS**	**Secure Socket Layer :** Intégré à TLS (Transport Layer Secure), SSL utilise les technologies de chiffrement à clé privée et à clé publique pour assurer les services d'authentification client / serveur (échange de certificats X.509 contenant les clés publiques respectives), de confidentialité et d'intégrité (chiffrement par algorithme à clé secrète après échange de la clé secrète sécurisé via chiffrement à clé publique). Il est principalement utilisé sur Internet pour sécuriser HTTP (protocole HTTPS) et a été également été transposé au monde WAP (protocole WTLS). TLS 1.0 est le nouveau nom du protocole SSL v3.1, il n'est pas compatible avec les anciennes versions de SSL (3.0 et inférieures).

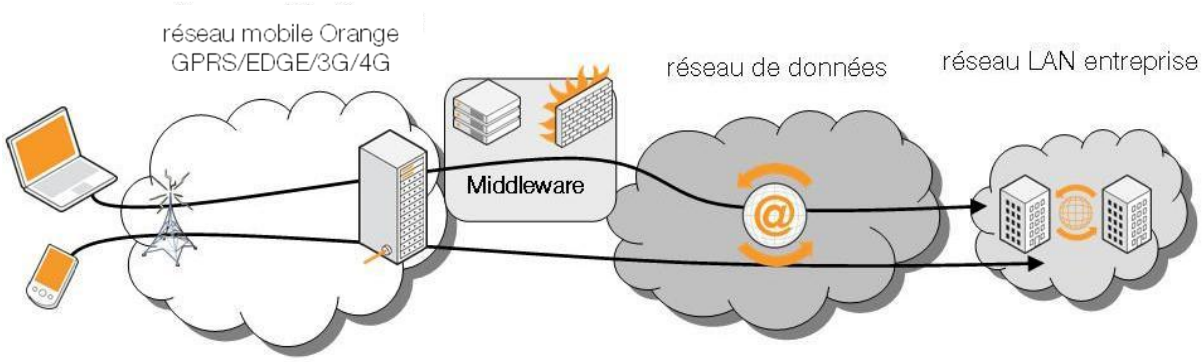
4.4 Gestion des habilitations

Définition :
La gestion des habilitations consiste à offrir un accès personnalisé aux services ou ressources auxquels un utilisateur a droit sur le système d'information, interdire ceux auxquels il n'a pas droit. Elle repose donc sur l'authentification préalable et fait en général appel à la notion de groupes d'utilisateurs. Les habilitations peuvent intervenir à plusieurs niveaux :

- au niveau applicatif : accès ou non à une application ou site web
- au niveau fonctionnel : accès ou non à certaines fonctionnalités d'une application ou service donné
- au niveau des données

L'approche la plus courante est celle des habilitations déclaratives, c'est à dire la définition des droits d'accès à un service ou ressource à travers un outil qui lui est externe. C'est l'approche proposée sur la *Plateforme entreprise* Orange.

5 La Chaîne d'accès mobile



5.1 Le terminal

Le terminal (tout terminal disposant de connectivité mobile) se connecte au réseau mobile Orange en fonction des capacités du terminal et des droits de l'utilisateur.

5.2 Le réseau mobile

Orange opère cinq types de réseaux mobiles (bearers) utilisés pour l'accès data mobile au système d'information :

- le réseau GSM Data (dit « CSD ») (*)
- le réseau GPRS – EDGE (*)
- le réseau Wi-Fi,
- le réseau UMTS.
- le réseau LTE (la « 4G »)

(*) ne pourront probablement être maintenus au-delà de fin 2017 : les équipementiers ne souhaitent pas s'engager au-delà.

Quel que soit le réseau utilisé, le paramétrage dans le terminal d'un point d'accès associé au réseau mobile est nécessaire. Ce point d'accès détermine le réseau mais aussi le ou les service(s) associés.

- cas du CSD : le point d'accès est un numéro de téléphone correspondant à un NAS (Network Access Server) du client (Orange a démonté les siens en 2013). C'est une communication « analogique », vouée à disparaître.

- cas du GPRS- EDGE / UMTS / LTE : un point d'accès réseau GPRS, UMTS ou LTE est appelé APN (Access Point Name). Il est transmis par le terminal lors de sa demande d'activation d'un contexte (une « session IP ») et correspond au point par lequel un utilisateur sort du réseau mobile pour se connecter à une plate-forme de service, à Internet, à un Intranet, etc. A noter qu'en 4G, la session une fois activée est conservée et le contexte est appelé Default Bearer.

- cas du Wi-Fi : les points d'accès Wi-Fi, ou bornes Wi-Fi permettent aux terminaux d'accéder au réseau filaire auquel ils sont reliés (mode infrastructure).

Les caractéristiques des différents points d'accès et des services auxquels ils donnent accès sont disponibles sur le site Orange programme partenaires, et son accessibles à cette adresse : http://www.orange-programmepartenaires.com/fr/documentation-technique, rubrique « *les réseaux d'accès/les apns : points d'accès pour la data mobile* ».

5.3 Le réseau de données

Le raccordement du système d'information de l'entreprise se fait par l'intermédiaire d'un réseau fixe de données, public (Internet) ou privé (solution IP VPN d'Orange Business Services par exemple). Le type de réseau de données utilisé est un point essentiel dans la mise en œuvre de la solution et la gestion de la sécurité. Il dépend de la solution d'accès choisie.

5.4 Les composants intermédiaires

Sur certains points d'accès, Orange met en œuvre un ensemble de composants intermédiaires (middlewares) dont la présence et le rôle dépendent de la solution d'accès choisie. Ils permettent d'assurer les accès data mobile, de les sécuriser ou encore de fournir des services à valeur ajoutée pour l'entreprise.

6 Services de sécurité sur la partie radio GSM et GPRS/EDGE/UMTS/HSDPA /LTE Orange

6.1 Sécurité mis en œuvre sur le réseau d'accès Orange

6.1.1 Sécurité de l'équipement

Tous les terminaux mobiles ont un identifiant international unique (IMEI) qui est stocké dans le registre d'identité de l'équipement (EIR). Cet identifiant unique est totalement indépendant de la carte SIM.
L'EIR a des classifications pour chaque type d'IMEI : Blanc : Téléphone valide. Gris : Téléphone à pister. Noir : Téléphone suspendu (perdu ou volé).

6.1.2 Authentification

Chaque carte SIM ou USIM contient entre autres l'IMSI (cf. glossaire) représentant l'identité de l'abonné. C'est cette identité qui est transmise au réseau GSM pour identification.

L'authentification sur le réseau **GSM** permet de vérifier que l'identité transmise par le mobile (IMSI) est exacte et d'empêcher une tierce personne de se faire passer pour un abonné.

Elle repose sur :
- la saisie éventuelle par l'utilisateur de son code PIN sur le terminal (le fait de demander le code PIN ou non est un choix de l'utilisateur)
- une clé individuelle **Ki**, propre à chaque abonnement, stockée dans la carte SIM ainsi que dans le cœur de réseau (clé secrète).
- un algorithme de chiffrement symétrique non-inversible spécifique à chaque opérateur (algorithme **A3** implémenté dans la SIM, norme GSM)

Cette clé **Ki** n'est jamais transmise sur le réseau. En effet, lors de la procédure d'authentification sur le réseau GSM, le réseau transmet un nombre aléatoire **rand** au mobile. Le mobile utilise alors l'algorithme **A3** avec la clé secrète **Ki** contenue dans la carte SIM pour chiffrer **rand**. Le résultat, **SRES=A3(Ki, rand)** est envoyé au réseau qui le compare au résultat calculé de son côté. L'abonné est authentifié si les deux résultats sont identiques.

6.1.3 Confidentialité sur le GSM, et le GPRS

Outre les mécanismes d'authentification vus précédemment, les mécanismes de confidentialité mis en œuvre dans le système GSM permettent d'atteindre des niveaux de protection élevés, bien que nécessitant de nos jours des protections complémentaires (cf. plus loin).

Principes :
La confidentialité sur les réseaux GSM et GPRS intervient à deux niveaux :

- **La confidentialité de l'identité de l'abonné** : elle est assurée par l'utilisation d'identités temporaires (TMSI) en lieu et place de l'identité de l'abonné (IMSI, cf. glossaire) une fois l'authentification initiale réalisée.

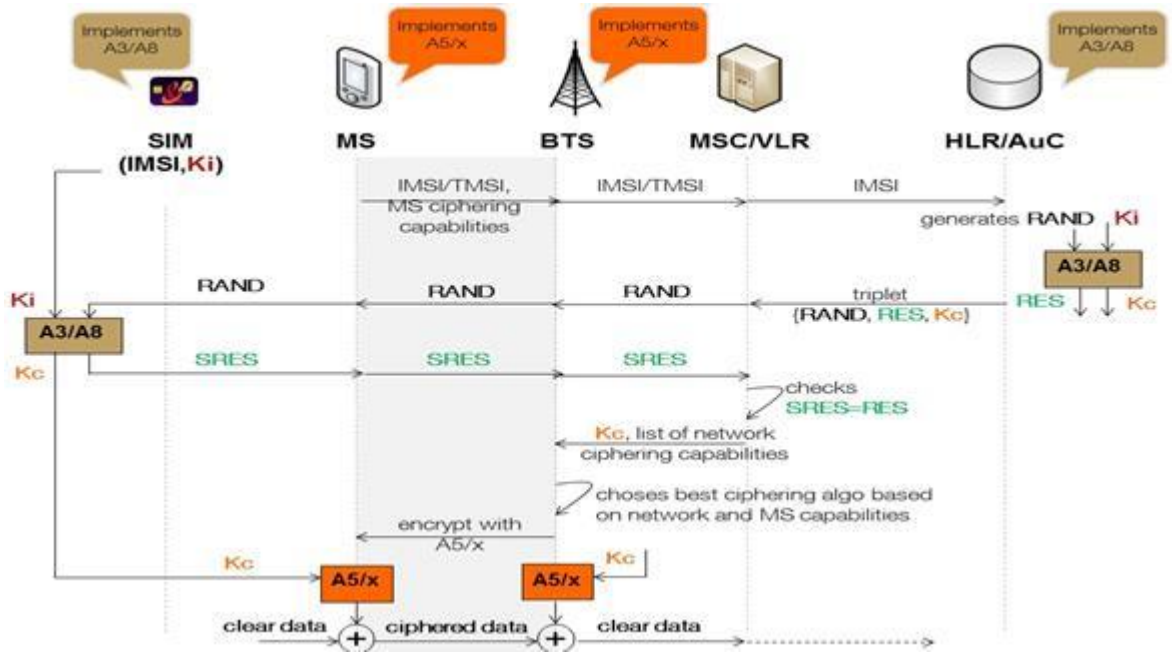
- **La confidentialité des données** : un mécanisme de chiffrement interdit l'interception et le décodage et assure donc la confidentialité des données transmises sur la voie radio, qu'il s'agisse des données usager ou des informations de signalisation.

Mécanismes :
Comme expliqué au paragraphe précédent, la carte SIM de l'utilisateur contient une clé individuelle Ki, son propre IMSI. La clé Ki est utilisée pour l'authentification mais elle intervient également dans le processus de chiffrement.

Le chiffrement des données transmises s'effectue en deux étapes :

1. calcul de la clé de chiffrement **Kc** :
   Cette clé secrète est calculée à partir de la clé **Ki** et d'un nombre aléatoire **rand** envoyé par le réseau. C'est l'algorithme **A8, spécifique à chaque opérateur**, qui sert au calcul, à la fois côté terminal (carte SIM) et côté réseau : **Kc=A8(rand, Ki)**.

2. le chiffrement proprement dit :
   Le chiffrement est réalisé par l'algorithme de chiffrement symétrique **A5** (norme GSM, public et implémenté dans le terminal) en utilisant la clé Kc calculée précédemment. Il existe plusieurs versions de cet algorithme A5, dont la version A5/1 est maintenant considérée comme faible. Une version renforcée d'A5 est en cours de déploiement sur le réseau Orange, l'A5/3. Initialement utilisé pour l'UMTS, cet algorithme sert au chiffrement/déchiffrement sur la voix radio de la signalisation et du trafic utilisateur. Ce dernier ne concerne que la partie circuit du réseau 2G, et opère entre les équipements BTS et les terminaux :



A noter que du fait de ce mécanisme, aucune information confidentielle (clés Ki ou Kc) n'est transmise sur le réseau.

L'algorithme A5/1 étant maintenant considéré comme faible par les experts, il est prudent de ne pas permettre la réutilisation de la clé Kc au-delà d'un échange (appel, SMS, …). Le réseau Orange impose donc systématiquement un recalcul de la clé Kc, ile ne peut y avoir d'appel ou SMS émis à l'insu de l'abonné.

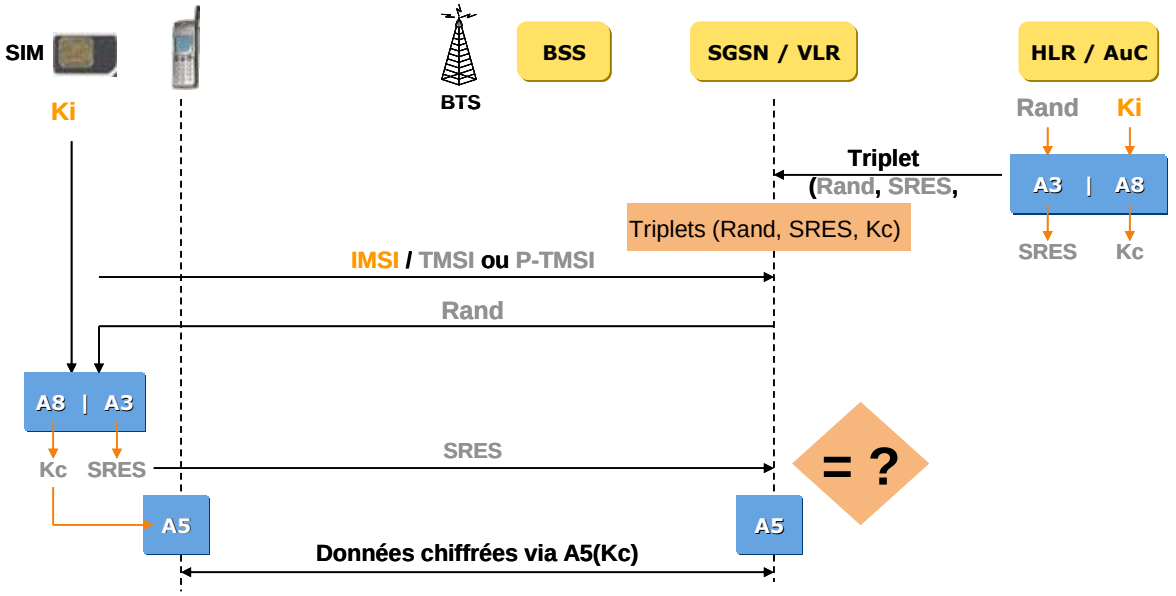
Similarités et différences entre GSM et GPRS :
Pour le GPRS, ce sont les mêmes algorithmes A3 et A8 qu'en GSM qui sont utilisés, qui aboutissent au calcul d'une clé Kc spécifique au GPRS (puisque basée sur un rand différent).

Les algorithmes GPRS de chiffrement confidentiels GEA1 et GEA2 différent des algorithmes utilisés pour le GSM A5/1 et A5/2, GEA3 est similaire à A5/3.

Les algorithmes A5 du GSM sont utilisés entre le terminal et la BTS (donc uniquement sur la partie radio), alors que les algorithmes GEA du GPRS sont utilisés entre le terminal et le SGSN du réseau auquel le terminal est attaché.

6.2 Sécurité mise en œuvre sur le réseau d'accès GPRS/EDGE d'Orange

Les services de sécurité propres au réseau GPRS Orange sont identiques à ceux du réseau GSM.



Authentification / chiffrement GSM-GPRS-EDGE

6.3 Services de sécurité mis en œuvre sur le réseau UTRAN (réseau d'accès UMTS/HSDPA) d'Orange

6.3.1 Sécurité de l'équipement

Tous les terminaux mobiles ont un identifiant international unique (IMEI) qui est stocké dans le registre d'identité de l'équipement (EIR). Cet identifiant unique est totalement indépendant de la carte SIM.
L'EIR a des classifications pour chaque type d'IMEI : Blanc : Téléphone valide. Gris : Téléphone à pister. Noir : Téléphone suspendu (perdu ou volé).

6.3.2 Authentification

Dans le réseau UMTS, une carte USIM est nécessaire. Tout comme la carte SIM elle contient l'IMSI (International Mobile Subscriber Identity) représentant l'identité de l'abonné qui est transmise au réseau pour identification.

L'authentification sur le réseau UMTS conserve les principes et avantages de la solution GSM et est **enrichie de nouveaux algorithmes plus robustes aux attaques** pour renforcer la sécurité du mécanisme d'authentification.

De plus, contrairement au GSM/GPRS qui utilise seulement une authentification de l'utilisateur envers réseau, la norme UMTS se dote d'une **authentification mutuelle** entre l'utilisateur mobile et le réseau visité (home ou roaming), fournissant une protection supplémentaire contre les attaques de type « Man in the middle » (ou « fausses stations de base »).

Cette authentification mutuelle emploie un **quintet d'authentification** (et non plus un triplet comme en GSM)…

Elle repose sur :
- la saisie par l'utilisateur de son code PIN sur le terminal
- 2 algorithmes d'authentification f1 et f2
- 3 algorithmes de génération de clé f3, f4 et f5
- le mécanisme de clé individuelle **Ki** du GSM, propre à chaque abonné, est conservé. Cette clé est stockée dans la carte USIM ainsi que dans le cœur de réseau (clé secrète). L'UMTS utilise une clef de 128 bits (64 bits dans le cas du GSM).

Le quintet d'authentification comprend le nombre aléatoire **Rand** transmis par le réseau, la réponse prévue d'utilisateur **(X(RES))**, une clef de chiffrage **(CK)**, une clef d'intégrité **(IK)** et la marque d'authentification **(AUTN)** pour l'authentification du réseau. De plus un numéro de séquence est ajouté ce qui empêche tout rejeu du quintet.

6.3.3 Confidentialité et intégrité renforcés

L'UTMS met en œuvre des algorithmes supplémentaires de chiffrement et de vérification de l'intégrité des données : ces mécanismes **protègent les messages de signalisation et les données de l'utilisateur** entre la station mobile et le contrôleur par radio de réseau (RNC) pour prévenir de toute attaque radio.

Principes : ils restent les mêmes qu'en GSM/GPRS mais les mécanismes mis en jeu sont rendus plus robustes par l'utilisation de ces nouveaux algorithmes.

- **La confidentialité de l'identité de l'abonnement** : elle est assurée par l'utilisation d'identités temporaires (TMSI) en lieu et place de l'identité de l'abonné (IMSI, cf. glossaire) une fois l'authentification initiale réalisée.

- **La confidentialité des données** : un mécanisme de chiffrement interdit l'interception et le décodage et assure donc la confidentialité des données transmises sur la voie radio, qu'il s'agisse des données usager ou des informations de signalisation.

Nouveaux mécanismes mis en place entre le terminal mobile et le RNC :

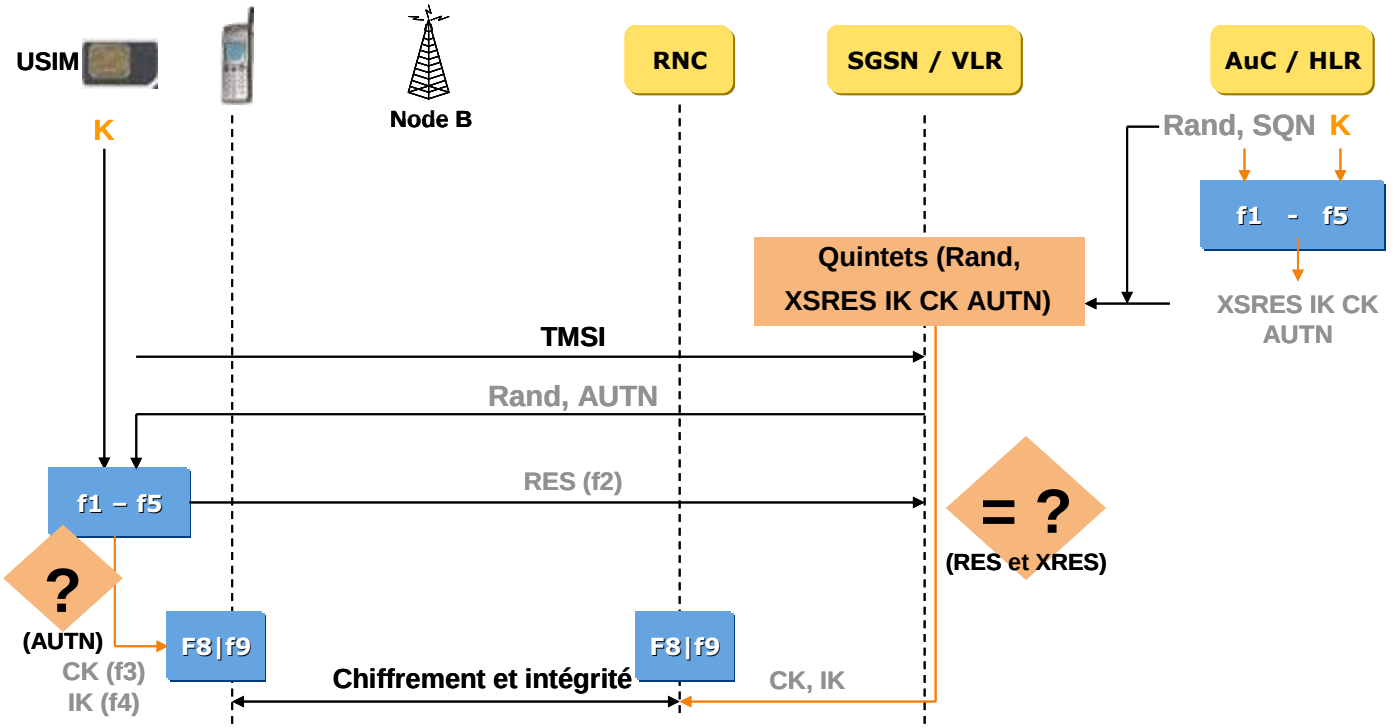
- algorithme de chiffrement symétrique **f8** :

La signalisation et les données utilisateurs sont protégées par l'utilisation d'un algorithme de chiffrement par bloc de 64 bits basé sur une clef secrète de 128 bit **CK=f3(Rand, Ki)**.

- algorithme de contrôle d'intégrité **f9** :

Assure la vérification de l'intégrité des données ainsi que de leur provenance : algorithme utilisant une clef d'intégrité de 128 bits **IK=f4(Rand,Ki)** et gérant des codes d'authentification de 64 bits.

Encore une fois, du fait de ce mécanisme, aucune information confidentielle (clés Ki, CK, IK) n'est transmise sur le réseau, seules des informations chiffrées circulent.



Authentification / chiffrement UMTS

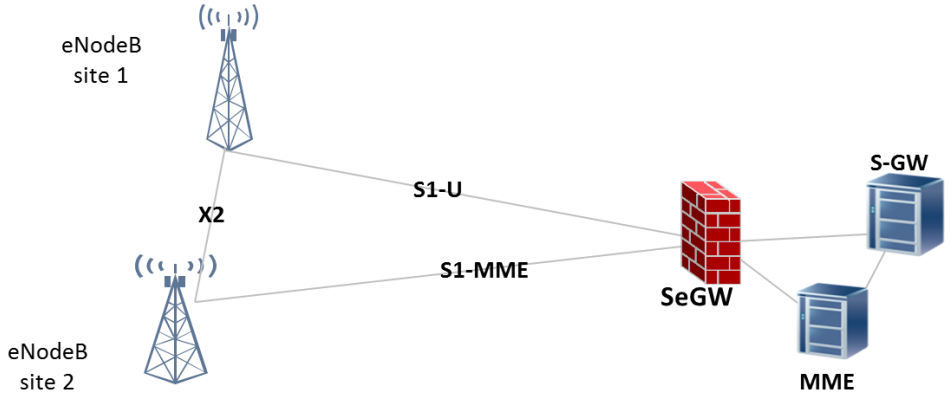
6.4 Services de sécurité mis en œuvre sur le réseau eUTRAN (réseau d'accès LTE) d'Orange

6.4.1 Sécurité de l'équipement

Tous les terminaux mobiles ont un identifiant international unique (IMEI) qui est stocké dans le registre d'identité de l'équipement (EIR). Cet identifiant unique est totalement indépendant de la carte SIM.
L'EIR a des classifications pour chaque type d'IMEI : Blanc : Téléphone valide. Gris : Téléphone à pister. Noir : Téléphone suspendu (perdu ou volé).

6.4.2 Sécurisation du réseau

Comme le veut la norme, les interfaces du réseau d'accès doivent être protégées par des tunnels IPsec. La solution retenu par Orange est de positionner une SeGW (Security Gateway) entre le réseau d'accès et le réseau cœur.



Elle a en charge les fonctions suivantes :

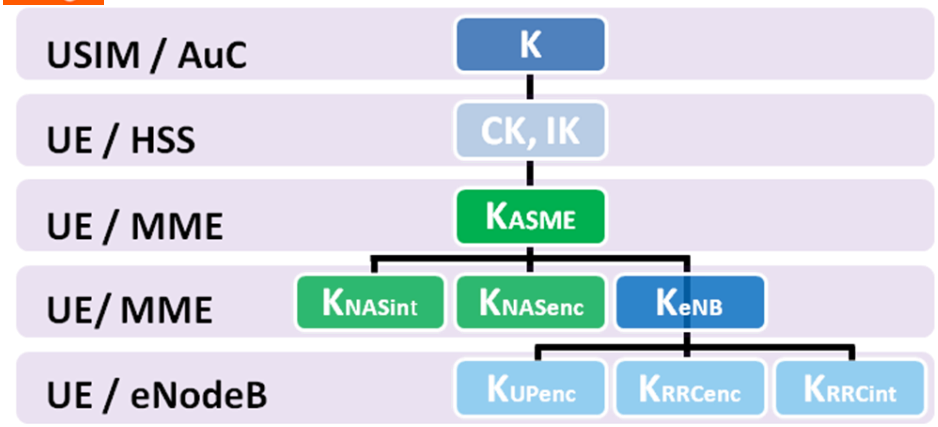
Chiffrement
Protection de la **confidentialité** et garantie de **l'intégrité** des échanges :
↳ **Tunnel IPSec**

Authentification
Protection contre les **intrusions** :
↳ **Authentification** des eNBs par **certificats**

Filtrage
Protection du **réseau cœur** :
↳ **Filtrage stateful** sur la SeGW

Disponibilité
Redondance géographique (nationale / régionale) :
↳ **Mécanismes de détection de défaillance** et de **bascule automatisée**

Les clés sont hiérarchisées comme suit :



Avec :

- **K_{ASME}**: clé primaire, gérée par le MME
- **$K_{NASenc/int}$** et **K_{eNB}** derivées de K_{ASME}
- **K_{eNB}**: envoyée à l'eNodeB
- **$K_{RRCenc/int}$** et **K_{UPenc}** derivées de K_{eNB}
- **NH**: paramètre de Next Hop dans le MME, et envoyé aux eNodeBs
- **K_{UPenc}** : Données utilisateur ou User plane (PDCP) entre le terminal client (User Entity) et l'eNodeB sont chiffrées
- Données de signalisation ou Control plane (commande RRC/PDCP) entre l'UE et l'eNodeB sont chiffrées (**K_{RRCenc}**) et protégées en intégrité (**K_{RRCint}**).
- Données de signalisation (NAS/RRC) entre l'eNodeB et le MME sont chiffrées (clé **K_{NASenc}**) et protégées en intégrité (**K_{NASint}**)

7 Sécurité de bout en bout des accès GSM DATA /GPRS/ EDGE UMTS/HSDPA/LTE Orange

7.1 Introduction

En plus des mécanismes de sécurité dans le réseau d'accès d'Orange décrit précédemment, d'autres services de sécurité supplémentaires peuvent être mis en place :

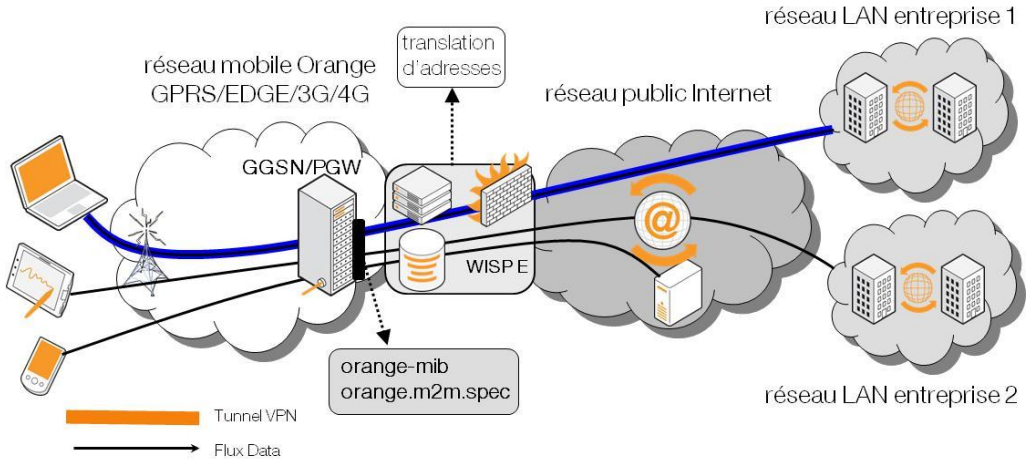
Ces services sont de 2 natures différentes qu'il convient de bien distinguer :

- les services de sécurité intégrés aux solutions d'accès Orange.
- les solutions de sécurité tierces, mises en œuvre en complément de ces services par une entreprise et/ou son partenaire intégrateur. Dans ce dernier cas, il faut s'assurer de la compatibilité de la solution et de l'offre d'accès choisies.

Les services de sécurité intégrés aux solutions d'accès d'Orange peuvent intervenir sur les différents maillons de la chaîne d'accès décrite au paragraphe précédent, selon l'offre choisie :

- au niveau du terminal,
- au niveau du réseau mobile GSM, GPRS, 3G ou 4G,
- au niveau du réseau fixe de données.

7.2 APNs orange-mib et orange.m2m.spec



L'APN orange-mib et l'APN orange.m2m.spec sont des APN mutualisés recommandés pour des usages téléphone / smartphone et MachineToMachine, qui allouent **des adresses IP privées** et permettent de bénéficier du bouquet de services et fonctionnalités à valeur ajoutée de la *Plateforme entreprise*.

Le réseau de données utilisé dans ce cas est l'Internet public.

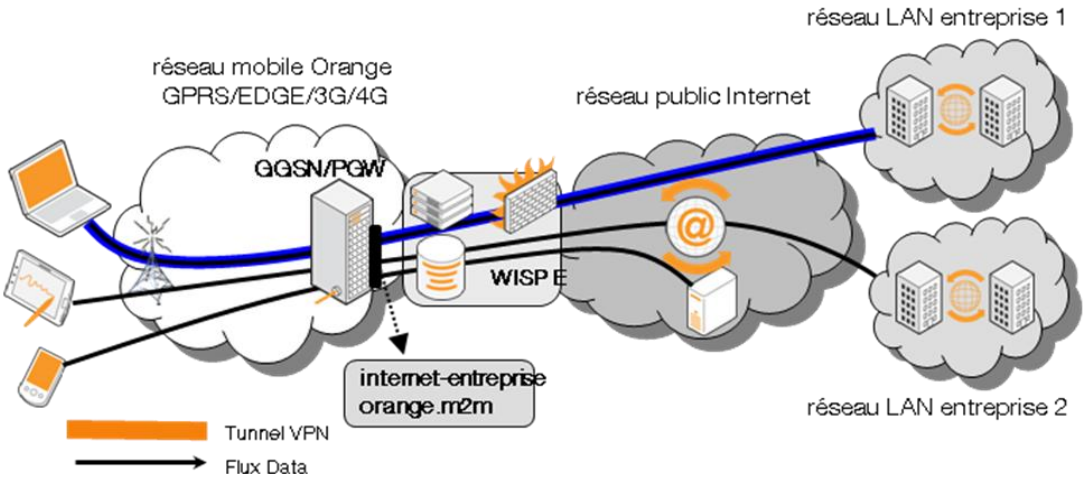
A noter que de plus amples informations sur la ***Plateforme entreprise*** et ses services sont disponibles sur le site Orange Programme Partenaires à cette adresse : http://www.orange-programmepartenaires.com/spip.php?article118 .

Services de sécurité Orange	En Standard	En Option sur la plateforme Entreprise

• authentification forte et confidentialité du réseau mobile • contrôle d'accès logique : blocage de tous les flux entrants non sollicités	X	
• gestion d'habilitations déclaratives basée sur l'authentification transparente du numéro appelant (option navigation contrôlée) • enrichissement des requêtes http avec le msisdn (numéro de téléphone) pour contrôle d'accès et gestion des habilitations côté SI (niveau applicatif)		X

Solutions et processus tiers compatibles	**En Standard**	**En Option sur la plateforme Entreprise**
• SSL • tout VPN IP supportant le NAT • contrôle de l'adresse IP source (IP publiques des firewalls de la *Plateforme entreprise*)	X	
• récupération et contrôle du numéro appelant côté SI (rendu possible via enrichissement http)		X

7.3 APNs internet-entreprise et orange.m2m



Les APN internet-entreprise et orange.m2m sont des APN mutualisés recommandés pour des usages PC et MachineToMachine, **qui allouent des adresses IP publiques** et donnent un accès à Internet full IP dans le sens mobile vers Internet et très largement ouvert dans le sens Internet vers mobile (tous les détails sur le site Orange programme partenaires / Les réseaux d'accès / Les APN). Le réseau de données utilisé ici est l'Internet public. Ils permettent de bénéficier également du bouquet de services et fonctionnalités à valeur ajoutée de la *Plateforme entreprise*.

Les caractéristiques protocolaires de ces APNs permettent d'utiliser avantageusement un tunnel VPN IP entre le terminal et le système d'information de l'entreprise (IPSec et solutions VPN classiques basées sur PPTP ou L2TP notamment, ou plus simplement SSL), associé ou non à une solution d'authentification forte au concentrateur VPN. L'utilisation d'un VPN de type IPSec permettra ainsi de garantir l'authentification bilatérale ainsi que la confidentialité et l'intégrité de tout protocole IP entre le terminal et le Système d'Information.

L'intérêt principal de l'usage de ces APNs à adresses IP publiques est qu'ils permettent la prise en main à distance du terminal, par exemple depuis le site central du client.

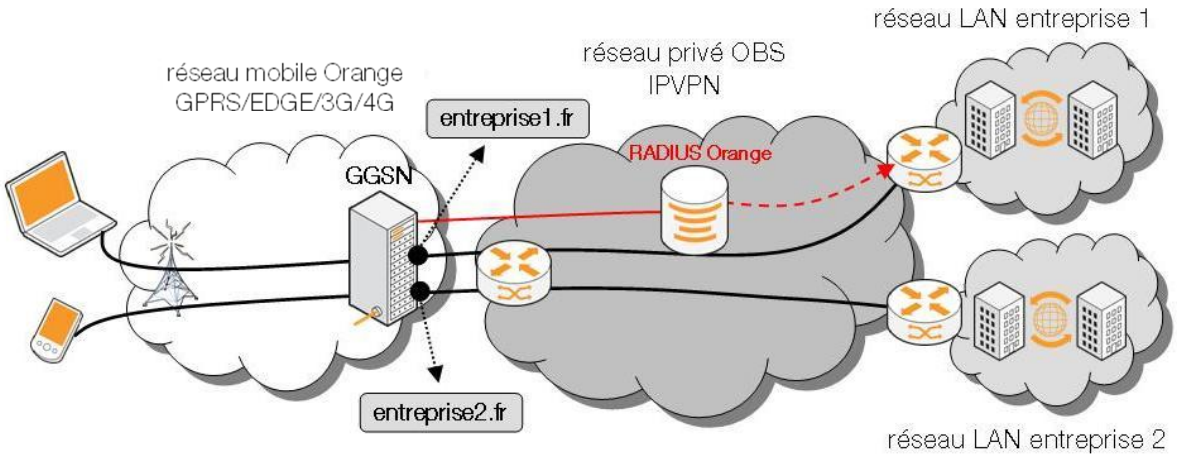
Le plus gros inconvénient des APNs à adressage IP public est que le terminal est justement accessible depuis internet, ce qui peut poser des problèmes de :

- sécurité (le terminal est-il bien résistant aux éventuelles tentatives de piratage provenant de tout internet ?)
- Montant de la facture (les volumes comptabilisés sont ceux provenant ou à destination du terminal, qu'ils soient volontaires ou non).

Services de sécurité Orange	En Standard	En Option sur la plateforme Entreprise
• authentification forte et confidentialité du réseau mobile • contrôle d'accès logique : blocage des flux TCP entrants sur les ports reconnus ou réservés (ports < 1024)	X	
• gestion d'habilitations déclaratives basée sur l'authentification transparente du numéro appelant (option navigation contrôlée) • enrichissement des requêtes http avec le msisdn (numéro de téléphone) pour contrôle d'accès et gestion des habilitations côté SI (niveau applicatif)		X

Solutions et processus tiers compatibles	En Standard	En Option sur la plateforme Entreprise
• SSL • tout VPN IP • contrôle de l'adresse IP source (IP publique des terminaux mobiles)	X	
• récupération et contrôle du numéro appelant côté SI (rendu possible via enrichissement http)		X

7.4 APN dédié : Secure Mobile Access Intranet



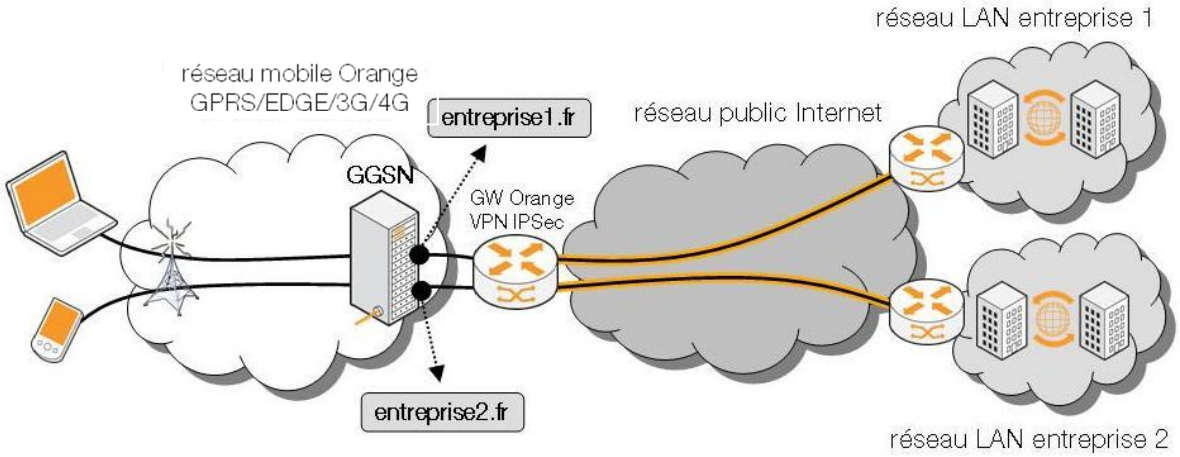
Un APN dédié est un point d'accès full IP dédié à un client sur le réseau GPRS/UMTS/LTE Orange, le raccordement au réseau de l'entreprise se faisant via le réseau de données privé IP MPLS d'Orange Business Services dans le cas de l'offre Secure Mobile Access Intranet.

Les flux d'authentification RADIUS sont gérés par Orange Business Services avec relais possible vers le serveur RADIUS de l'Intranet client et allocation d'adresses IP dans le plan d'adressage de l'entreprise.

Services de sécurité Orange
• authentification forte et confidentialité du réseau mobile • contrôle d'accès : seules les lignes du client peuvent accéder à cet APN dès l'attachement au réseau • authentification Radius à la connexion GPRS/3G/4G • confidentialité et intégrité sur le réseau de données (réseau privé)

Solutions et processus complémentaires compatibles
• solutions d'authentification forte [calculette type SecureID^{tm}, dongle USB , carte à puce] • TLS/SSL • Tout VPN IP entre le terminal et une passerelle client

7.5 APN dédié : Secure Mobile Access Internet



Un APN dédié est un point d'accès full IP dédié à un client sur le réseau Orange, le raccordement au réseau de l'entreprise se faisant via le réseau de données public Internet à travers un tunnel VPN sécurisé, dans le cas de l'offre Secure Mobile Access Internet.

Dans cette configuration, l'utilisation d'un serveur RADIUS client n'est pas possible.

Services de sécurité Orange
• authentification forte et confidentialité du réseau mobile • contrôle d'accès : seuls les SIMs du client peuvent accéder à cet APN dès l'attachement au réseau • confidentialité et intégrité sur le réseau de données (utilisation d'un tunnel VPN sur la partie publique)

Solutions et processus complémentaires compatibles
• TLS/SSL • Tout VPN IP entre le terminal et une passerelle client

8 Sécurité des réseaux WLAN (Wi-Fi) d'Orange

8.1 Introduction

La sécurité sur les réseaux 802.11 a souvent été l'objet de controverses du fait des faiblesses avérées de certains mécanismes de sécurité prévus par la norme initiale et en particulier au niveau du protocole de chiffrement WEP (Wired Equivalent Privacy) qui sous-estimait les mesures nécessaires pour assurer à un réseau basé sur des ondes radio, le même niveau de sécurité que celui d'un réseau filaire.

La norme 802.11i est venue depuis corriger le tir en proposant les sous ensemble WPA puis WPA2 (Wi-Fi Protected Access). WPA permet :

- une authentification bilatérale soit via mécanisme de clé partagée (PSK pour Pre-Shared Key) soit via EAP (Extensible Authentication Protocol)
- chiffrement / intégrité via TKIP / MIC

Le méchanisme WPA était plus robuste. Seuls bémols à noter : l'utilisation d'une authentification en mode PSK doit se faire à l'aide d'une Passphrase suffisamment robuste pour éviter toute attaque au dictionnaire.Néanmoins, depuis fin 2010, l'utilisation de WPA TKIP est déconseillée du fait de sa vulnérabilité aux attaques les plus sophistiquées.

WPA2 utilise les mêmes mécanismes d'authentification mais repose sur AES / CCMP pour le chiffrement et l'intégrité. **WPA2 EAP et WPA2 PSK (avec utilisation d'une Passphrase robuste) sont considérés comme aujourd'hui résistantes et sont donc conseillés lorsque les matériels sont compatibles.**

Selon l'usage souhaité, une bonne utilisation de ces mécanismes permet de profiter en toute sécurité des nombreux bénéfices de cette technologie.

8.2 Sécurité sur les hotspots public Orange wifi access

Les hotspots Orange répondent aux besoins d'accès haut débit, et en particulier à ceux des collaborateurs nomades des entreprises. Avec l'installation de bornes wifi dans ces lieux de passage, ils peuvent en effet accéder depuis leur PC portable, en toute sécurité et avec la même ergonomie, à leur messagerie et à l'ensemble des applications partagées de leur intranet.
Orange wifi access alloue des adresses IP privées et effectue une translation d'adresse vers Internet. Aucun flux entrant non sollicité n'est donc possible, ce qui ajoute une protection supplémentaire contre d'éventuelles attaques extérieures.
Les services de sécurité suivants sont assurés sur les hotspots Orange :

Services de sécurité Orange

• confidentialité de l'authentification (identifiant / mot de passe) via chiffrement TLS (certificat serveur)
• contrôle d'accès réseau :
  ○ les échanges entre stations sont bloqués de façon à empêcher toute attaque locale
  ○ les flux entrants non sollicités sont bloqués

Les services de sécurité WEP ou WPA de la norme 802.11 ne sont pas activés sur les hotspots car ils mettent en jeux des mécanismes incompatibles avec la notion même de hotspot public.

Du fait de la nature diffuse du réseau et des éléments évoqués en introduction, les recommandations suivantes s'appliquent et permettent d'adapter le niveau de sécurité à l'usage :

Recommandations en usage nomade sur hotspot Orange wifi access
• utiliser un firewall personnel • utiliser un web mail sécurisé SSL pour l'accès aux comptes de messageries POP/SMTP plutôt qu'un client de messagerie embarqué, qui n'assure pas la confidentialité des données transmises. • utiliser une solution de type VPN pour l'accès à un Intranet (authentification bilatérale, confidentialité et intégrité des échanges) • de manière générale, s'assurer de la confidentialité (TLS, VPN, etc.) avant toute saisie de données confidentielles sur le web ou utilisation d'un service connecté pouvant envoyer de telles données (messagerie par exemple).

Solutions et processus complémentaires compatibles
• TLS/SSL • IPSec et tout VPN IP supportant le NAT 1 pour 1

8.3 Sécurité sur les hotspots privés en entreprise

Le réseau wifi en entreprise, même s'il est parfois décrit comme étant une extension du LAN de l'entreprise, doit être vu comme un réseau d'accès externe à ce dernier. Les politiques de sécurité adaptées à un accès externe doivent donc s'appliquer en termes de :

- contrôle d'accès : filtrage protocolaire via Firewall
- authentification forte : certificat stocké sur le poste ou sur dongle USB ou carte à puce, mot de passe à usage unique de type SecureID^{tm} couplée avec WPA
- confidentialité et intégrité : utilisation de WPA/TKIP ou WPA2/AES
- gestion des habilitations