Lignes directrices de sécurité IoT pour les opérateurs de réseaux

Lignes directrices de sécurité IoT pour les opérateurs de réseaux

Version 2.0

26 Octobre 2017

Ce document est une référence permanente non contraignante de la GSMA

Classification de sécurité : Non_confidentiel

Copyright

Avertissement

Avis antitrust

Table de Matières

1 Introduction

1.1 Aperçu général

Ce document fournit des directives générales de sécurité aux opérateurs de réseau qui ont l'intention de fournir des services aux fournisseurs de services IoT pour assurer la sécurité du système et la confidentialité des données. Les recommandations sont basées sur des systèmes et des technologies facilement disponibles qui sont déployés aujourd'hui.

1.2 Structure du document

Ce document est destiné aux opérateurs de réseau et aux fournisseurs de services IoT. Les lecteurs de ce document peuvent également être intéressés à lire les autres documents sur les lignes directrices de sécurité IoT de la GSMA [11], comme indiqué ci-dessous.

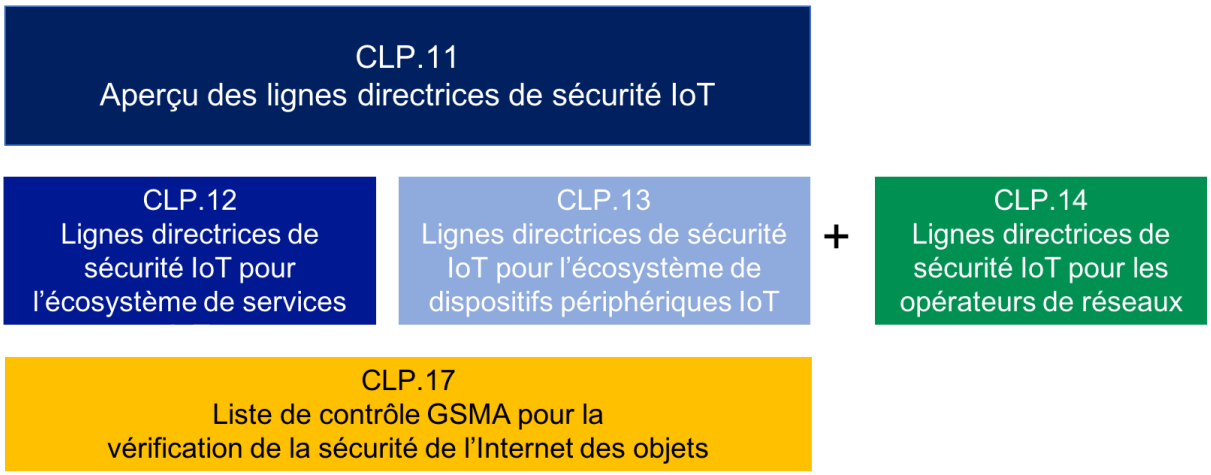

Figure 1- Structure des Documents sur les Directives de Sécurité de la GSMA

1.3 Objet et portée du document

Ce document peut servir comme liste de contrôle dans les accords de fournisseur qui sont négociés entre les fournisseurs de services IoT et les opérateurs réseau agissant comme partenaires.

La portée du document est limitée aux :

- Directives de sécurité relatives aux services IoT.
- Recommandations relatives aux services de sécurité offerts par un opérateur de réseau.
- Technologies de réseau cellulaire.

Ce document n'a pas pour but de créer de nouvelles spécifications ou normes IoT, mais se référera aux solutions, normes et bonnes pratiques actuellement disponibles.

Ce document n'a pas pour but d'accélérer l'obsolescence des services IoT existants. La rétrocompatibilité avec les services IoT existants de l'opérateur de réseau doit être maintenue lorsqu'ils sont considérés comme correctement sécurisés.

Ce document ne traite pas les problèmes de sécurité associés aux interfaces et aux API implémentés sur la plate-forme de services IoT (ou sur la plate-forme de gestion de la connectivité IoT) afin qu'elle puisse partager ses données avec les utilisateurs finaux (par exemple pour partager des données avec une extrémité utilisateur via un smartphone ou une application PC) ou d'autres entités au sein de l'écosystème. De telles interfaces et API doivent être sécurisées à l'aide des technologies et protocoles de sécurité Internet qui suivent les meilleures pratiques de l'industrie.

Il est noté que le respect des lois et règlements nationaux pour un territoire particulier peut, si nécessaire, annuler les directives énoncées dans le présent document.

1.4 Public visé

Le principal public visé par ce document est :

- Premièrement, les opérateurs de réseaux qui souhaitent fournir des services aux fournisseurs de services IoT.
- Deuxièmement, les entreprises et les organisations qui cherchent à développer de nouveaux produits et services connectés IoT utilisant des réseaux cellulaire ou fixe. Dans ce document, nous désignons ces entreprises par « Fournisseurs de Services IoT ».

1.5 Définitions

Terme	Description
Rapport d'identité de l'hôte du dispositif	Possibilité pour un dispositif périphérique de signaler des informations d'hôte à un opérateur de réseau. Voir le document « GSMA Connection Efficiency Guidelines » [17]
Diameter	Diameter est un protocole d'authentification, d'autorisation et de comptabilité pour les réseaux informatiques. Voir IETF RFC 6733 [18]
Dispositif Périphérique	Un dispositif périphérique IoT est un périphérique informatique physique qui exécute une fonction ou une tâche dans le cadre d'un produit ou d'un service connecté à Internet. Voir la section 3 du document CLP.13 [29] pour une description des trois classes communes de périphériques IoT et des exemples de chaque classe de dispositif périphérique.
Passerelle	Un dispositif périphérique complexe qui relie généralement les dispositifs périphériques légers (connectés via un réseau local) et un réseau étendu. Voir CLP.13 [29] pour plus d'informations.
Internet des Objets	L'Internet des objets (IoT) décrit la coordination de plusieurs machines, appareils et appareils connectés à Internet via plusieurs réseaux. Ces dispositifs comprennent des objets du quotidien tels que les tablettes et l'électronique grand public, ainsi que d'autres machines telles que des véhicules, des moniteurs et des capteurs dotés de capacités de communication leur permettant d'envoyer et de recevoir des données.

Terme	Description
Plate-forme de gestion de connectivité IoT	Un système, généralement hébergé par l'opérateur de réseau, pour permettre l'autogestion des abonnements IoT et des plans de prix par le fournisseur de services IoT.
Service IoT	Tout programme informatique qui tire parti des données des périphériques IoT pour rendre un service.
Plate-forme de services IoT	La plate-forme de services, hébergée par le fournisseur de services IoT qui communique avec un dispositif périphérique pour fournir un service IoT.
Fournisseur de Service IoT	Entreprises ou organisations qui cherchent à développer de nouveaux produits et services liés à l'Internet des objets connectés.
Dispositif Périphérique Léger	Typiquement, un dispositif contraint en ressources (par exemple un capteur ou un actionneur) qui se connecte à un service IoT via une passerelle.
Opérateur de Réseau	L'opérateur et le propriétaire du réseau de communication qui connecte le dispositif périphérique IoT à l'écosystème de service IoT.
UICC	Plateforme d'élément sécurisé spécifiée dans la norme ETSI TS 102 221 et pouvant prendre en charge plusieurs applications d'authentification de réseau ou de service normalisées dans des domaines de sécurité crypto graphiquement séparés. Il peut être incorporé dans des facteurs de forme incorporés spécifiés dans la norme ETSI TS 102 671.
Réseau Étendu	Un réseau de télécommunications qui s'étend sur une grande distance géographique.

1.6 Abréviations

Terme	Description
3GPP	Projet de Partenariat sur la Troisième Génération (« 3rd Generation Project Partnership »)
AKA	Authentification et accord de clé (« Authentication and Key Agreement »)
APDU	Unité de données du protocole d'application (« Application Protocol Data Unit »)
API	Interface de Programmation d'Applications (« Application Program Interface »)
APN	Nom du Point d'Accès (« Access Point Name »)
BGP	Protocole d'échange de route externe (« Border Gateway Protocol »)
CEIR	Registre d'identité d'équipement central (« Central Equipment Identity Register »)
CERT	Équipe d'Intervention d'Urgence Informatique (« Computer Emergency Response Team »)
DNS	Système de noms de domaines (« Domain Name System »)
DoS	Déni de Service (« Denial of Service »)
DPA	Accord de traitement de données (« Data Processing Agreement »)
EAB	Interdiction d'accès étendu (« Extended Access Barring »)
EAP	Protocole d'authentification extensible (« Extensible Authentication Protocol »)
EID	Identité de l´eUICC (« eUICC Identity »)

Terme	Description
ETSI	Institut européen des normes de télécommunications (« European Telecommunications Standards Institute »)
EU	Union Européenne (« European Union »)
eUICC	UICC Embarquée (« Embedded UICC »)
FASG	Groupe de fraude et de sécurité (« Fraud and Security Group »)
GCF	Forum mondial de certification (« Global Certification Forum »)
GGSN	Dispositif de support de la passerelle GPRS (« Gateway GPRS Support Node »)
GPRS	Service général de radiocommunication par paquets (« General Packet Radio Service »)
GRX	Commutateur pour l'itinérance GPRS (« GPRS Roaming eXchange »)
GSM	Système global de communication mobile (« Global System for Mobile communication »)
GSMA	Association GSM (« GSM Association »)
GTP	Protocole de tunneling GPRS (« GPRS Tunnelling Protocol »)
HLR	Registre de localisation d'origine (« Home Location Register »)
HSS	Serveur d'abonnés d'origine (« Home Subscriber Server »)
ICCID	Identité de la carte de circuit intégré (« Integrated Circuit Card Identity »)
IMEI	Identité internationale de l'équipement de la station mobile (« International Mobile station Equipment Identity »)
IMSI	Identité internationale d'abonné mobile (« International Mobile Subscriber Identity »)
IoT	Internet des objets ("Internet of Things")
IP	Protocole d'Internet ("Internet Protocol")
IPSec	Sécurité du protocole Internet (« Internet Protocol Security »)
L2TP	Protocole de tunnellisation de la deuxième couche (« Layer Two Tunnelling Protocol »)
LBO	Dégroupage vers un fournisseur alternatif de roaming (« Local Break Out »)
LPWAN	Réseau étendu de faible puissance (« Low Power Wide Area Network »)
LTE	Évolution à long terme (« Long-Term Evolution »)
M2M	Machine à Machine (« Machine to Machine »)
MAP	Partie d'application mobile (« Mobile Application Part »)
MME	Entité de gestion de la mobilité (« Mobility Management Entity »)
OMA	Alliance Mobile Ouverte (« Open Mobile Alliance »)
OSS	Système de soutien aux opérations (« Operations Support System »)
OTA	Accès aux Paramètres SIM à Distance (« Over The Air »)
PTCRB	Conseil d'examen de certification de type PCS (« PCS Type Certification Review Board »)
RAN	Réseau d'accès radio (« Radio Access Network »)
SAS	Système d'accréditation de sécurité (« Security Accreditation Scheme »)
SGSN	Dispositif serveur de support GPRS (« Serving GPRS Support Node »)

Terme	Description
SIM	Module d'Identité d'Abonné (« Subscriber Identity Module »)
SMS	Service de messages courts (« Short Message Service »)
SoR	Pilotage d'itinerance (« Steering of Roaming »)
SS7	Système de signalisation n ° 7 (« Signalling System No. 7 »)
UMTS	Service universel de télécommunications mobiles (« Universal Mobile Telecommunications Service »)
USSD	Données de service supplémentaires non structurées (« Unstructured Supplementary Service Data »)
VLR	Registre de la localisation des visiteurs (« Visitor Location Register »)
VPN	Réseau privé virtuel (« Virtual Private Network »)
VoLTE	Voix sur LTE (« Voice over LTE »)
WAN	Réseau étendu (« Wide Area Network »)

1.7 Références

Réf.	Numéro du Document	Titre
[1]	ETSI TS 102 225	Secured packet structure for UICC based applications www.etsi.org
[2]	ETSI TS 102 226	Remote APDU structure for UICC based applications www.etsi.org
[3]	3GPP TS 31.102	Characteristics of the Universal Subscriber Identity Module (USIM) application www.3gpp.org
[4]	N/A	Open Mobile API specification www.simalliance.org
[5]	OMA DM	OMA Device Management www.openmobilealliance.org
[6]	OMA FUMO	OMA Firmware Update Management Object www.openmobilealliance.org
[7]	GSMA SGP.02	Remote Provisioning Architecture for Embedded UICC Technical Specification www.gsma.com
[8]	ETSI TS 102 310	Extensible Authentication Protocol support in the UICC www.etsi.org
[9]	3GPP TS 23.122	Non-Access-Stratum (NAS) functions related to Mobile Station (MS) in idle mode www.3gpp.org
[10]	NISTIR 7298	Glossary of Key Information Security Terms www.nist.gov
[11]	GSMA CLP.11	IoT Security Guidelines Overview Document https://www.gsma.com/iot/future-iot-networks/iot-security-guidelines/

Réf.	Numéro du Document	Titre
[12]	n/a	Introducing Mobile Connect – the new standard in digital authentication https://www.gsma.com/identity/mobile-connect
[13]	3GPP TS 34.xxx	3GPP 34 series specifications www.3gpp.org/DynaReport/34-series.htm
[14]	3GPP TS 37.xxx	3GPP 37 series specifications www.3gpp.org/DynaReport/37-series.htm
[15]	3GPP TS 31.xxx	3GPP 31 series specifications www.3gpp.org/DynaReport/31-series.htm
[16]	GSMA FS.04	Security Accreditation Scheme for UICC Production http://www.gsma.com/aboutus/leadership/committees-and-groups/working-groups/fraud-security-group/security-accreditation-scheme
[17]	GSMA CLP.03	IoT Device Connection Efficiency Guidelines https://www.gsma.com/iot/iot-device-connection-efficiency-guidelines/
[18]	IETF RFC 6733	Diameter Base Protocol www.ietf.org
[19]	ETSI TS 102 690	Machine-to-Machine communications (M2M); Functional architecture www.etsi.org
[20]	TR-069	CPE WAN Management Protocol www.broadband-forum.org
[21]	n/a	OpenID Connect openid.net/connect/
[22]	n/a	FIDO (Fast IDentity Online) Alliance fidoalliance.org/
[23]	ETSI TS 102 204	Mobile Commerce (M-COMM); Mobile Signature Service; Web Service Interface www.etsi.ord
[24]	n/a	National Institute of Standards and Technology (NIST) www.nist.gov
[25]	n/a	European Network of Excellence in Cryptology (ECRYPT) www.ecrypt.eu.org
[26]	GSMA CLP.12	IoT Security Guidelines for IoT Service Ecosystem https://www.gsma.com/iot/future-iot-networks/iot-security-guidelines/
[27]	IETF RFC 5448	Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA) tools.ietf.org/html/rfc5448
[28]	IETF RFC 4186	Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM) tools.ietf.org/html/rfc4186

Réf.	Numéro du Document	Titre
[29]	GSMA CLP.13	IoT Security Guidelines for IoT Endpoint Ecosystem https://www.gsma.com/iot/future-iot-networks/iot-security-guidelines/
[30]	n/a	Wireless Security in LTE Networks www.gsma.com/membership/wp-content/uploads/2012/11/SenzaFili_WirelessSecurity_121029_FINAL.pdf
[31]	n/a	oneM2M Specifications www.oneM2M.org
[32]	GSMA CLP.17	IoT Security Assessment Checklist https://www.gsma.com/iot/iot-security-assessment/
[33]	n/a	LPWA Technology Security Comparison. A White Paper from Franklin Heath Ltd https://goo.gl/JIOlr6
[34]	CLP.28	NB-IoT Deployment Guide www.gsma.com/iot
[35]	CLP.29	LTE-M Deployment Guide www.gsma.com/iot
[36]	3GPP TS33.163	Battery efficient Security for very low Throughput Machine Type Communication (MTC) devices (BEST) www.3GPP.org

2 Les actifs des services IoT que les opérateurs de réseaux peuvent protéger

Les fonctions de sécurité qui doivent être implémentées pour protéger correctement les actifs d'un service IoT sont spécifiques à chaque service. Par conséquent, c'est important pour un fournisseur de services IoT d'utiliser des processus d'évaluation des risques et de l'impact sur la vie privée appropriés pour déterminer leurs besoins de sécurité spécifiques. Les opérateurs de réseau et les fournisseurs de services IoT partagent souvent des exigences de sécurité similaires pour protéger leurs actifs. Il est donc logique qu'ils utilisent des solutions de sécurité communes plutôt que d'implémenter des infrastructures de sécurité dupliquées (et potentiellement redondantes). De plus, dans de nombreux cas, les opérateurs de réseau seront également le fournisseur de services IoT.

Les services de sécurité fournis par les opérateurs de réseau peuvent jouer un rôle essentiel dans la sécurisation des ressources utilisées pour fournir un service IoT. Ceux-ci peuvent inclure :

- Les données de service IoT envoyées entre un dispositif périphérique IoT et la plate-forme IoT de services comprennent à la fois des données primaires confidentielles (par exemple, des données relatives à l'utilisateur final) et des données exploitables commercialement (telles que des données de contrôle pour un actionneur par exemple) qui peuvent aussi avoir un impact sur la vie privée.

- Les actifs de sécurité (IMSI, jeux de clés, etc.) et les paramètres de configuration réseau (APN, valeurs de minuterie, etc.) utilisés dans les dispositifs périphériques (y compris les passerelles).
- Les informations sensibles du fournisseur de services IoT, y compris la réputation de la marque, les données client / utilisateur sous la responsabilité de l'entreprise, les informations stratégiques, les données financières et les dossiers de santé, etc.
- Les infrastructures commerciales, les plates-formes de service, les réseaux d'entreprise et les autres éléments de réseau privé d'un fournisseur de services IoT.
- Infrastructures des centres de données publiques (c'est-à-dire partagées) fournies par l'opérateur de réseau et utilisées par les services IoT. Cela peut inclure des services publics, des capacités hébergées, des infrastructures de virtualisation, des installations de cloud, etc.
- Infrastructure de réseau de communication, y compris les réseaux d'accès radio, le réseau central, les réseaux dorsaux, les fonctions de service de base (DNS, BGP, etc.), l'accès et l'agrégation des réseaux fixes et cellulaires, etc.

3 Principes de sécurité des réseaux

Des mécanismes de sécurité appropriés et fiables doivent être mis en place par les opérateurs de réseau dans leurs réseaux.

Dans cette section, il est décrit comment les réseaux peuvent apporter de la valeur au sein de l'écosystème IoT.

Les mécanismes de sécurité les plus fondamentaux fournis par un réseau de communication sont :

- Identification et authentification des entités impliquées dans le service IoT (c'est-à-dire les passerelles, les terminaux, le réseau domestique, les réseaux d'itinérance, les plates-formes de services).
- Contrôle d'accès aux différentes entités devant être connectées pour créer le service IoT.
- Protection des données afin de garantir la sécurité (confidentialité, intégrité, disponibilité, authenticité) et la confidentialité des informations transmises par le réseau pour le service IoT.
- Processus et mécanismes pour garantir la disponibilité des ressources réseau et les protéger contre les attaques (par exemple en déployant des technologies appropriées de pare-feu, de prévention des intrusions et de filtrage des données)

3.1 Identification sécurisée des utilisateurs, des applications, des terminaux, des réseaux et des plates-formes de service

L'identification consiste à fournir des identifiants uniques aux entités du service IoT, et à corréler ces identités électroniques avec des identités réelles et juridiquement contraignantes.

Au sein d'un service IoT connecté à un réseau cellulaire, les dispositifs périphériques sont identifiés à l'aide d'IMSI et / ou d'IMEI (les EID peuvent également être utilisés pour les dispositifs qui intègrent une puce eUICC). Les réseaux sont identifiés à l'aide de codes de

réseau et de codes de pays. Chaque méthode pour fournir les identités, a des niveaux différents d'assurance sécurisée qui lui sont associés.

L'identité joue un rôle crucial dans le processus d'authentification, car une authentification sécurisée ne peut être réalisée que sur la base d'une identité sécurisée. Il est donc essentiel que les identités (par exemple un IMSI, un IMEI ou un ICCID) émises et utilisées dans un service IoT soient protégées de façon sécurisée contre toute modification, usurpation d'identité ou vol non autorisé.

Un problème pratique auquel un fournisseur de services IoT peut être confronté est que son service IoT peut nécessiter des communications avec de nombreuses plates-formes de service IoT, chacune pouvant nécessiter une identification unique distincte. Chaque identité utilisée pour établir un lien de communication vers chaque plate-forme de service IoT devra ensuite être sécurisée, stockée et gérée de manière sécurisée par le service IoT.

Lorsque cela est approprié pour le service IoT, les opérateurs de réseau recommandent l'utilisation de mécanismes basés sur UICC pour identifier de manière sécurisée les dispositifs périphériques. Les opérateurs de réseau peuvent également faciliter la fonctionnalité de stockage sécurisé fournie par l'UICC au fournisseur de services IoT pour leur permettre de stocker des identités supplémentaires liées au service IoT sur l'UICC. Cette technique peut être appliquée à la fois aux dispositifs périphériques cellulaires et non cellulaires (par exemple EAP-AKA [27]).

Des services de «connexion unique» peuvent également être fournis par les opérateurs de réseau pour permettre aux dispositifs périphériques d'établir et de prouver leur identité une seule fois, puis de se connecter à plusieurs plates-formes de service IoT sans autre inconvénient. Les compromis en matière de sécurité et les risques liés à l'utilisation d'un tel service doivent être pris en compte à travers les multiples plates-formes utilisées.

3.2 Authentification sécurisée des utilisateurs, des applications, des dispositifs périphériques, des réseaux et des plates-formes de service

Selon le NIST [10], l'authentification consiste à vérifier l'identité d'un utilisateur, d'un processus ou d'un dispositif périphérique, souvent comme condition préalable à l'accès aux ressources dans un système d'information.

Les opérateurs de réseau peuvent fournir des services pour garantir que les utilisateurs, les applications, les terminaux, les réseaux et les plates-formes de services associés à un service IoT sont authentifiés de manière sécurisée.

L'authentification a une propriété connexe - celle de la non-répudiation. Selon le NIST [10], une définition de la non-répudiation est la suivante : « c’est l’assurance que l'expéditeur de l'information reçoit une preuve de livraison et que le destinataire a la preuve de l'identité de l'expéditeur ». La non-répudiation dépend de l'affirmation que l'authenticité n'a pas été violée lors de l'identification de la source de cette transaction ou de ce message.

3.3 Fournir des canaux de communication sécurisés

Les opérateurs de réseau fournissent des mécanismes de sécurité des communications pour les réseaux cellulaires et fixes étendus, garantissant l'intégrité, la confidentialité et l'authenticité des communications utilisant les meilleures solutions existantes sur le marché.

Le cas échéant, les opérateurs de réseau peuvent fournir et gérer des connexions sécurisées aux réseaux d'entreprise à l'aide de réseaux privés virtuels (VPN) et de connexions Internet cryptées.

Le but d'un canal de communication sécurisé est de garantir que les données envoyées sur le canal ne sont pas traitées, utilisées ou transmises sans que la personne concernée en soit informée et ait donné son consentement. Les technologies de cryptage jouent un rôle crucial dans la sécurisation de la transmission des données en garantissant les propriétés de confidentialité, d'intégrité et d'authenticité. Le cryptage doit être adapté au système en cours de conception et de déploiement en tenant compte des dispositifs périphériques légers, des aspects réseau (tels que les contraintes d'une connexion par satellite) et du service fourni.

Les opérateurs de réseau peuvent faciliter aux fournisseurs de services IoT des services de cryptage de données pour assurer l'intégrité de la communication et la résilience du réseau.

Les opérateurs de réseau fournissent traditionnellement une infrastructure de télécommunications publique ou une combinaison d'infrastructures de réseau publiques ou privées. De nombreux opérateurs de réseau peuvent garantir que les données client / utilisateur qui transitent sur leur infrastructure de réseau public sont cryptées entre le point où les données entrent dans l'infrastructure de réseau publique et le moment où elles quittent le réseau. Si nécessaire, les opérateurs de réseau peuvent également aider les fournisseurs de services IoT à déployer ou à dériver leurs propres identifiants de cryptage afin d'assurer la confidentialité des données IoT pendant le transit à travers l'infrastructure de l'opérateur de réseau.

Les opérateurs de réseau peuvent fournir à leurs clients des réseaux privés où des canaux de communication dédiés à l'usage d'un seul client pour s'assurer qu'aucune donnée ne traverse un réseau public tel qu'Internet. De tels réseaux privés pourraient être créés :

1. En utilisant un protocole de tunnellisation tel que L2TP (« Layer Two Tunneling Protocol ») et sécurisé à l'aide de protocoles tels que IPsec (« Internet Protocol Security »), ou
2. En fournissant aux clients une sécurité de bout en bout entre le dispositif périphérique et le serveur d'application en utilisant par exemple BEST [36] ou
3. En créant un réseau dédié pour le service IoT en déployant une instance différente du réseau central avec le réseau radio partagé - comme dans l'exemple ci-dessous.

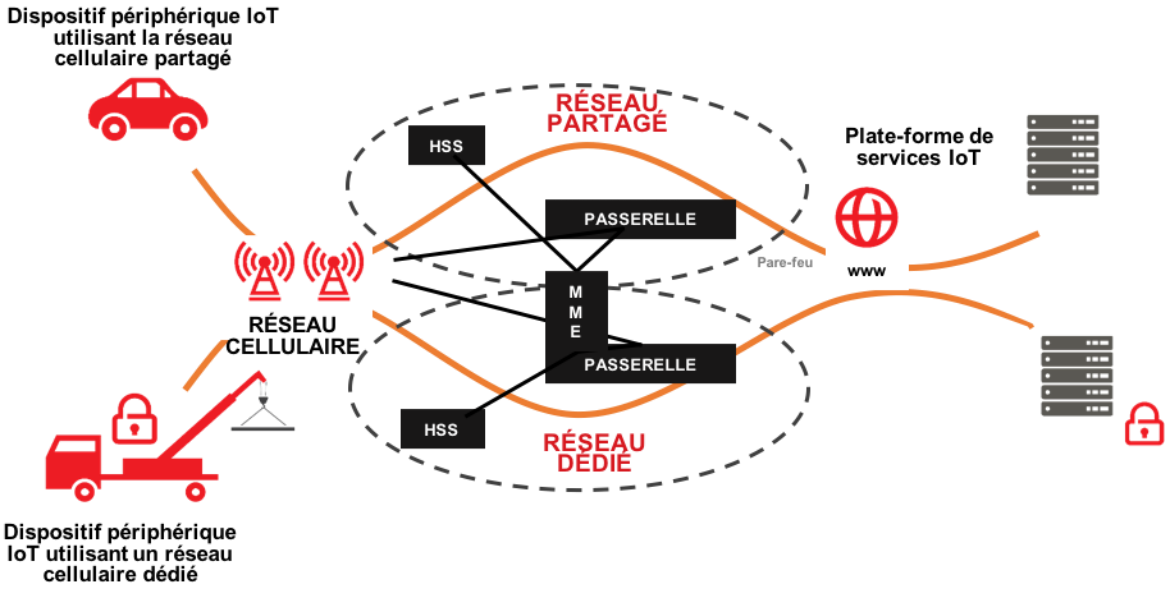

Figure 2 - Exemple de configurations de réseau privé

3.4 Assurer la disponibilité des canaux de communication

Selon le NIST [10], la "disponibilité" est la propriété d'être accessible et utilisable à la demande d'une entité autorisée.

Les opérateurs de réseau peuvent livrer aux fournisseurs de services IoT des réseaux qui assurent la disponibilité. Les mécanismes les plus fondamentaux fournis par les opérateurs de réseau pour garantir la disponibilité du réseau sont énumérer dans les sections ci-dessous.

3.4.1 Utilisation du spectre sous licence

Les opérateurs membres de la GSMA exploiteront des réseaux utilisant un spectre sous licence dédié en vertu des licences délivrées par leurs régulateurs nationaux. L'utilisation d'un spectre sous licence garantit que les interférences provenant d'autres technologies radio sont réduites au minimum, car toute utilisation non autorisée de ce spectre fera l'objet de poursuites. Les opérateurs de réseau ainsi que les régulateurs nationaux rechercheront toute source de brouillage non autorisée afin de s'assurer que la disponibilité du réseau n'est pas affectée.

L'utilisation du spectre sous licence, qui fournit à l'opérateur de réseau des bandes radio dédiées pour exploiter son réseau, garantit qu'une couverture réseau et une planification de la capacité soient pourvues par l'opérateur de réseau d'une manière minutieuse pour assurer une disponibilité maximale du réseau à ses clients.

3.4.2 Mise en œuvre de technologies de réseau normalisées et éprouvées

Les opérateurs mettent en place des technologies de réseau standardisées telles que GSM, UMTS et LTE qui sont spécifiées par des organismes de normalisation tels que le 3GPP. L'utilisation de technologies standardisées assure non seulement l'interopérabilité entre les opérateurs de réseaux, mais garantit également que le standard est soumis à un examen minutieux lors de sa création afin d'assurer la robustesse de la technologie employée.

3.4.3 Mise en œuvre de technologies réseau testées et certifiées

De nombreux composants du réseau d'un opérateur seront testés et certifiés selon les normes d'essai internationales. Les dispositifs périphériques complexes et les modules de communication qu'ils contiennent seront soumis aux spécifications de test 3GPP [13] via les tests d'acceptation des organisations GCF et PTCRB, et en plus chaque opérateur normalement a ses propres tests. Les réseaux d'accès radio (RAN) seront soumis aux spécifications de test 3GPP [14] via les tests d'acceptation des opérateurs de réseau. Les UICC seront soumises aux spécifications de test 3GPP [15] via les tests d'acceptation des opérateurs de réseau et, en outre, pourront être soumises à la certification SAS de la GSMA [16].

3.4.4 Topographies de réseaux résilients et configuration

Les opérateurs de réseau fournissent des réseaux résilients mettant en œuvre et renforçant la redondance géographique et l'isolation nécessaires pour assurer une disponibilité maximale avec un temps d'arrêt minimal. Tous les éléments du réseau sont soigneusement configurés et surveillés pour assurer une qualité de service stricte et que les accords de niveau de service soient respectés.

3.4.5 Surveillance en temps réel et gestion des ressources du réseau

Les opérateurs de réseau construisent des centres d'opérations de réseau de pointe qui surveillent les performances de leurs réseaux 24 heures sur 24, 7 jours sur 7 et en temps réel pour gérer le trafic réseau, répondre à la demande du réseau et corriger les défaillances. Des informations supplémentaires peuvent être trouvées dans la section 4.10.

3.4.6 Gestion des menaces et partage de l'information

Le groupe de sécurité et de lutte contre la fraude de la GSMA (FASG) offre un environnement ouvert, réceptif et fiable à tous les opérateurs de réseau pour partager les informations de fraude et de sécurité et les détails des incidents de manière opportune et responsable. Le groupe évalue le « paysage » global des menaces de fraude et de sécurité, analyse les risques associés pour les opérateurs de réseau et leurs clients et définit et priorise les actions d'atténuation appropriées.

3.4.7 Services d'itinérance

Grâce à l'utilisation de technologies et de services d'interconnexion de réseau et de terminaux standardisés, les opérateurs de réseau peuvent offrir des services d'itinérance entre réseaux différents, améliorant ainsi la couverture et la disponibilité d’une connexion réseau pour leurs clients.

3.4.8 Surveillance et gestion des performances des dispositifs périphérique

Les opérateurs réseau peuvent mesurer les performances des dispositifs périphériques connectés à leurs réseaux pour isoler les dispositifs susceptibles de générer des interférences radio excessives (non conformes aux réglementations nationales, par exemple) ou de trafic de signalisation réseau (par exemple, non conformes à la norme GSMA, lignes directrices pour une connexion efficace [17]) qui, à leur tour, peuvent dégrader les performances du réseau global. Les dispositifs périphériques peuvent ainsi être surveillés, déconnectés ou leur firmware peut être mis à jour lorsqu'un comportement anormal est détecté.

4 Considérations sur la confidentialité

Pour saisir les opportunités qu'offre l'IoT, il est important que les consommateurs fassent confiance aux fournisseurs de services IoT qui collectent des données à leur sujet. La GSMA et ses membres croient que la confiance des consommateurs ne peut être pleinement atteinte que lorsque les utilisateurs estiment que leur vie privée est respectée et protégée de manière appropriée.

Il existe déjà des lois bien établies sur la protection des données et la vie privée dans le monde qui ont été appliquées et respectées par les opérateurs de réseau. Les opérateurs estiment qu'il est possible d'appliquer les réglementations et principes de protection des données existants pour répondre aux besoins de confidentialité dans le contexte des services et des technologies IoT.

Toutefois, les services IoT impliquent généralement les opérateurs travaillant en collaboration avec les partenaires du fournisseur de services IoT. Il est important que les services IoT bénéficient d'une clarté réglementaire et d'une sécurité juridique et que les réglementations en matière de confidentialité et de protection des données s'appliquent de manière cohérente à tous les fournisseurs de services IoT, de manière neutre pour les services et la technologie.

Les opérateurs de réseau doivent savoir que s'ils traitent des données de quelque manière que ce soit, ils doivent signer un accord de traitement de données (DPA) avec le fournisseur de services IoT. Les pratiques de protection et de sécurité des données développées pour un service IoT donné devraient refléter le risque global pour la vie privée d'un individu et le contexte dans lequel les données sur l'individu sont collectées, distribuées et utilisées. Toute intervention réglementaire devrait être limitée aux domaines où les risques identifiés apparaissent et les mesures existantes sont insuffisantes pour arriver à un remède. Par exemple, oneM2M (via TS-0003 [31]) permet à l'opérateur de jouer le rôle de gestionnaire de la confidentialité pour un fournisseur de services.

Les opérateurs de réseaux peuvent s'appuyer sur leur vaste expérience en matière de confidentialité et de sécurité et travailler en collaboration avec les fournisseurs de services IoT pour intégrer la confidentialité et la sécurité dans les technologies IoT et l'expérience globale du consommateur. Grâce à cette collaboration, les fournisseurs de services IoT seront en mesure d'identifier et d'atténuer les risques pour la vie privée des consommateurs dans le contexte du service fourni.

Pour plus d'informations, veuillez consulter les principes de confidentialité de la GSMA : http://www.gsma.com/publicpolicy/mobile-and-privacy/mobile-privacy-principles

5 Services fournis par les opérateurs de réseau

Les opérateurs de réseau peuvent fournir aux fournisseurs de services IoT des réseaux étendus cellulaires et fixes (WAN) sécurisés.

Cette section contient des recommandations sur les meilleures pratiques lors de la connexion de services IoT à des réseaux étendus. Le cas échéant, les recommandations seront indépendantes de la technologie utilisée, mais utiliseront également les meilleures pratiques du réseau cellulaire et d'autres types de réseau.

5.1 Procédures sécurisées de gestion des abonnements

Cette section contient des recommandations sur la façon dont les abonnements du fournisseur de services IoT doivent être gérés par les opérateurs de réseau :

- L'opérateur de réseau ou le fournisseur de services IoT doit effectuer une évaluation continue à travers le temps des services de réseau nécessaires pour activer le service IoT (voix, données, SMS, etc.).
- Sur la base de cette évaluation, l'opérateur de réseau devrait opérer selon le principe du « moindre privilège » et provisionner les abonnements du fournisseur de services IoT uniquement avec les services requis pour le service IoT spécifique. Par exemple :
    - Les services IoT qui utilisent uniquement des supports de données ne doivent pas être fournis avec des services vocaux et SMS.
    - Lorsqu'un dispositif périphérique se connecte uniquement à une plate-forme de service IoT connue, l'abonnement associé à ce périphérique ne doit autoriser que la connexion à une liste blanche connue de plages d'adresses IP (ou de domaines).
    - Si le service IoT utilise la voix ou le SMS, l'utilisation d'une liste de numérotation fixe préconfigurée doit être prise en compte.

- Les opérateurs de réseau doivent mettre en œuvre des processus de gestion des abonnements sécurisés pour les abonnements IoT qui permettent des services IoT critiques (par exemple pour les abonnements associés aux services de soins de santé critiques). Ces services ne doivent pas être déconnectés arbitrairement.
- Les opérateurs de réseau doivent identifier les UICC utilisés pour les services IoT par rapport aux UICC utilisés pour fournir des services traditionnels et, si le fournisseur de services IoT l'exige, les séparer de manière appropriée.
    - Si les UICC utilisés pour les services IoT sont séparés des UICC utilisés pour les services traditionnels, cela constitue une base pour une gestion plus sûre et efficace des abonnements associés par l'opérateur du réseau aux services IoT. Par exemple, un opérateur de réseau peut envisager d'utiliser un HLR et un HSS différents pour les dispositifs périphériques IoT qui ont une durée de vie prolongée et sont mieux configurés pour supporter ces UICC pendant une très longue période (plusieurs années).

5.1.1 Approvisionnement et gestion de l'UICC

5.1.1.1 Gestion à distance de l'UICC (OTA)

Les dispositifs périphériques IoT ne sont pas physiquement accessibles dans certains scénarios. Pour pouvoir effectuer des modifications à distance sur l'UICC, la gestion OTA de l'UICC doit être réaliser par l'opérateur de réseau. Les mécanismes de sécurité OTA de l'UICC doivent suivre les dernières spécifications ETSI [1] [2] et 3GPP [3] et utiliser le niveau de sécurité le plus approprié pour un service IoT.

Les dispositifs périphériques IoT doivent prendre en charge les commandes APDU nécessaires reconnues par l'UICC pour s'assurer que l'exécution de la commande OTA UICC réussira.

5.1.1.2 UICC non amovible

L'opérateur de réseau doit fournir des UICC non amovibles (c'est-à-dire avec un facteur de forme pour machine, par ex. « QNF8 ») pour les services IoT lorsque le modèle de menace de service suggère que le terminal IoT peut être vulnérable à une altération physique. Des mesures de sécurité supplémentaires doivent être appliquées pour pouvoir détecter et réagir à une telle menace.

5.1.1.3 Gestion à distance des UICC embarquées (eUICC)

L'opérateur de réseau doit fournir une gestion à distance sécurisée des UICC non amovibles (c'est-à-dire des puces eUICC) pour les services IoT qui requièrent que les dispositifs périphériques soient situés dans des emplacements distants ou d'accès difficile.

Par exemple, pour les fournisseurs de services IoT qui doivent gérer un grand nombre d'eUICC intégrés dans des dispositifs périphériques pour lesquels le fournisseur de services IoT n'est pas le propriétaire et ne peut pas y accéder facilement (par exemple, une voiture).

Généralement, les opérateurs utilisent les plates-formes de gestion de la connectivité IoT pour surveiller et contrôler les services de communication offerts aux dispositifs IOT par eUICC.

L'opérateur de réseau devrait supporter sur sa plate-forme la spécification technique de l'architecture d'approvisionnement à distance de la GSMA pour l'UICC embarqué [7].

5.1.1.4 Services basés sur l'UICC

Un opérateur de réseau peut faciliter à un fournisseur de services IoT des services basés sur UICC. Cela permet au fournisseur de services IoT d'utiliser l'UICC comme plate-forme sécurisée et inviolable pour ses services IoT. De tels services basés sur UICC sont généralement développés en JavaCardTM et sont interopérables entre toutes les cartes UICC compatibles JavaCardTM. Un exemple d'une telle application pour un dispositif périphérique IoT pourrait être la surveillance et le rapport de la qualité du réseau. La fonctionnalité de protection anti-sabotage fournie par la plate-forme UICC est très utile pour les dispositifs périphériques IoT auxquels les attaquants peuvent accéder physiquement. Tirer parti de l'UICC en tant qu'élément de sécurité commun pour toutes les parties prenantes peut également rendre les dispositifs IoT sécurisés plus rentables.

L'UICC peut également être utilisé pour le stockage infalsifiable de données sensibles pour les services IoT, y compris les clés de sécurité contrôlées par le fournisseur de services IoT. L'ETSI TS 102 225 [1] exploite la fonction de gestion de contenu confidentielle de la spécification de la carte comme une plate-forme globale pour permettre aux fournisseurs de services IoT de gérer de manière indépendante leur propre domaine de sécurité sur une UICC.

Un fournisseur de services IoT ou un opérateur de réseau peut demander au fournisseur UICC de créer de tels domaines de sécurité à l'intérieur de l'UICC. L'émetteur de l'UICC doit s'assurer qu'il est protégé par des clés de sécurité appropriées et que le dispositif périphérique IoT peut exécuter les commandes APDU nécessaires pour y accéder.

En outre, l'UICC pourrait également être utilisée pour crypter (en utilisant ses clés sécurisées) et envoyer du contenu confidentiel pour les services IoT, ou fournir des services

de sécurité pour les applications basées sur les terminaux via des services tels que « Open Mobile API » [1] ou « oneM2M TS-0003 » [31].

5.1.1.5 Sécurisation de la fabrication et de l'approvisionnement de l'UICC

Un opérateur de réseau devrait s'approvisionner leurs UICC auprès de fabricants dont les processus de fabrication et d'approvisionnement sont accrédités conformément au système d'accréditation de sécurité (SAS) de la GSMA [16].

5.2 Algorithmes d'authentification et de chiffrement de réseau

Cette section contient des recommandations et une description des bonnes pratiques pour l'authentification réseau et le cryptage des connexions pour différents réseaux étendus.

L'opérateur de réseau devrait supporter des algorithmes d'authentification de réseau qui répondent aux exigences liées à la durée de vie des dispositifs périphériques du fournisseur de services IoT.

Les opérateurs de réseau fournissent plusieurs types de services de communication pouvant être utilisés par un service IoT, tels que la connectivité USSD, SMS et IP. Aux fins du présent document, seule la connectivité des données IP est discutée car il s'agit du service de communication le plus utilisé par les services IoT.

USSD et SMS sont utilisés par de nombreux services IoT existants, il est donc intéressant de souligner que USSD et SMS ont des capacités de support de sécurité limitées par rapport à la connectivité de données IP. En général, le trafic USSD et SMS n'est pas protégé de manière cryptographique par défaut par l'opérateur de réseau et les mécanismes de protection cryptographique pour assurer la confidentialité et l'intégrité ne sont pas disponibles pour les messages SMS. Les fournisseurs de services IoT qui utilisent USSD ou SMS pour leur communication doivent être conscients des vulnérabilités associées à USSD et SMS et, si possible, implémenter un chiffrement supplémentaire à la couche de service.

5.2.1 Securité des systèmes 2G – GSM / GPRS

Les opérateurs de réseau qui fournissent des réseaux GSM / GPRS devraient :

- Utiliser un chiffrement de flux A5 / 3 de 128 bits minimum pour protéger la connexion entre un dispositif périphérique IoT et une station de base. Les opérateurs de réseau devraient éviter A5 / 1 et A5 / 2 ou utiliser des connexions non cryptées lorsque cela est possible.
- Utiliser l'algorithme d'authentification MILENAGE. Les opérateurs de réseau devraient éviter COMP128-1 et COMP128-2. Les opérateurs de réseau devraient envisager de prendre en charge l'algorithme d'authentification TUAK
- Prendre les mesures appropriées pour traiter et atténuer les attaques de fausses stations de base.

Dans les systèmes GSM / GPRS, le réseau n'est pas authentifié par le dispositif périphérique, seul le dispositif est authentifié par le réseau. Le cryptage de bout en bout sur la couche de service est donc recommandé lors de l'utilisation de systèmes GSM ou GPRS. Une attention particulière doit être accordée au traitement pratique, aux limitations des dispositifs périphériques et aux contraintes de bande passante réseau dans les solutions fournies en tant que services IoT.

Dans les systèmes GSM / GPRS, le tunnel GTP entre SGSN et GGSN qui est créé sur le réseau GRX n'est pas crypté. L'opérateur de réseau doit assurer la sécurité de ce tunnel en s'assurant que le réseau GRX est géré comme un réseau privé.

5.2.2 Sécurité des systèmes UMTS (3G)

Les réseaux UMTS permettent une authentification mutuelle, où le dispositif périphérique n'est pas seulement authentifié par le réseau, mais le réseau est également authentifié par le dispositif périphérique.

Les opérateurs de réseau qui fournissent des réseaux UMTS doivent supporter l'algorithme d'authentification et de génération de clé MILENAGE. Les opérateurs de réseau doivent supporter aussi les algorithmes de chiffrement de confidentialité et d'intégrité de Kasumi.

Les opérateurs de réseau devraient incorporer de plus l'algorithme d'authentification TUAK.

5.2.3 Sécurité des systèmes LTE (4G)

Les opérateurs de réseau qui fournissent un réseau LTE doivent supporter l'algorithme d'authentification MILENAGE. Les opérateurs de réseau doivent aussi supporter les algorithmes de chiffrement LTE EEA1, EEA2 ou EEA3.

Les opérateurs de réseau devraient envisager d'être compatible avec l'algorithme d'authentification TUAK.

Les opérateurs de réseau sont invités à consulter le livre blanc de la GSMA « Sécurite sans fil dans les réseaux LTE » [30].

5.2.4 Sécurité des réseaux étendus de faible puissance

Plusieurs technologies de réseau à faible puissance et longue portée (LPWA) ont été déployées par divers opérateurs de réseau. Une liste complète et à jour des déploiements du réseau LPWA peut être trouvée sur le site Web de la GSMA : www.gsma.com/iot

Les guides de déploiement pour NB-IoT [34] et LTE-M [35] peuvent être consultés sur le site Web de la GSMA pour assurer le déploiement cohérent de ces technologies du point de vue du réseau et du dispositif IoT.

En mai 2017, les analystes de sécurité informatique Franklin Heath ont publié un rapport indépendant intitulé « LPWA Technology Security Comparison » [33] comparant et contrastant les caractéristiques de sécurité de cinq technologies de réseau LPWA pour plusieurs cas typiques d'utilisation de l'IoT : agriculture, éclairage routier intelligent, détecteurs de fumée, compteurs d'eau et compteurs intelligents. Il évalue les caractéristiques de sécurité de trois technologies IoT mobiles normalisées 3GPP qui opèrent dans les technologies de spectre sous licence, LTE-M, NB-IoT et EC-GSM-IoT ainsi que les technologies de spectre sans licence LoRaWAN et Sigfox. Le rapport peut être téléchargé à partir de : https://goo.gl/JIOlr6 [33].

Le rapport soutient que les organisations doivent déterminer le niveau de sécurité dont elles ont besoin en plus d'autres considérations telles que le coût, la durée de vie nécessaire de la batterie et la couverture du réseau lorsqu'elles envisagent une solution LPWA. Il souligne que les besoins de sécurité IoT sont largement motivés par des préoccupations de sécurité

et de confidentialité et que tout déploiement utilisant les technologies LPWA doit faire l'objet d'une évaluation des risques de sécurité à l'aide d'outils tels que l'évaluation éditée par la GSMA : « GSMA IoT Security Assessment » [32].

Certains facteurs importants de sécurité du réseau mis en évidence dans le rapport qui devraient être pris en compte dans le cadre d'une telle évaluation comprennent :

- Bande passante, y compris les débits de données de liaison descendante et de liaison montante maximale - Ceci peut limiter les fonctions de sécurité pouvant être prises en charge par le réseau LPWA ou implémentées dans la couche d'application.
- Débit journalier de liaison descendante et de liaison ascendante : les périphériques LPWA ne transmettent ou ne reçoivent généralement pas de données tout le temps, ce qui peut avoir un impact sur les fonctions de sécurité telles que les mises à jour OTA de sécurité.
- Authentification - Périphérique, abonné et réseau - La connectivité réseau sécurisée nécessite un certain nombre de parties différentes pour s'authentifier mutuellement, telles que le dispositif périphérique, l'abonné et le fournisseur de réseau. La technologie doit protéger contre l'usurpation de l'identité de ces parties par des logiciels ou acteurs malveillants.
- Confidentialité des données - Le chiffrement est généralement utilisé pour empêcher les données d'être interceptées par un attaquant. La confiance dans ce cas peut être augmentée en établissant la sécurité de bout en bout dans la couche d'application.
- Provisionnement de clés - Les techniques de cryptographie pour l'authentification, la confidentialité et l'intégrité reposent toutes sur le partage sécurisé des clés cryptographiques entre les parties.
- Équipement certifié - Dans de nombreux marchés, les appareils munis d'une transmission radio doivent être homologués ou certifiés avant d'être vendus. Ceci est une opportunité pour vérifier les fonctionnalités de sécurité.
- Réseau IP - L'utilisation du protocole IP peut ouvrir la possibilité d'une attaque sur les appareils à partir d'Internet et les caractéristiques de sécurité IP doivent être prises en compte.

Le rapport conclut que plusieurs caractéristiques de sécurité potentiellement importantes des technologies LPWA sont en quelque sorte optionnelles dans la mesure où elles peuvent être directement activées par l'opérateur de réseau, ou dépendent d'autres choix faits par l'opérateur de réseau. Les opérateurs de réseau doivent s'assurer qu'ils sont conscients des conséquences sur la sécurité des choix qu'ils font dans leur configuration réseau et s'assurer que l'état de ces options est clairement communiqué à leurs clients. Certaines options sont également sous le contrôle du fabricant de l'appareil (comme l'inclusion d'un élément sécurisé fixe tel qu'une eUICC non amovible) et le même devoir de communiquer les implications de sécurité de ces éléments à leurs clients s'applique.

Considérations de sécurité spécifiques lors de l'utilisation d'une technologie LPWA comprennent :

Pour toutes les technologies de réseau LPWA :

- Si une couche réseau IP est implémentée sur la couche liaison.
- Si un élément sécurisé est présent et, dans l'affirmative, s'il est amovible.

- Dans quelle mesure l'intégrité des données est-elle garantie?
- Si des algorithmes ou des longueurs de clé supportés par la technologie sont répertoriés dans la liste noire ou doivent être déconseillés (par exemple, des clés de chiffrement 64 bits pour GPRS).

Pour les technologies de réseau LPWA 3GPP (c'est-à-dire NB-IoT et LTE-M) :

- Si le provisionnement à distance de la SIM, RSP (« Remote SIM Provisioning »), est utiliser.
- Quels algorithmes d'intégrité (EIAx / GIAx) et algorithmes de confidentialité (EEAx / GEAx) sont implémentés et autorisés.

Pour LoRaWAN :

- Si ABP (« Activation By Personalization », Activation à distance) ou OTAA (« Over-The-Air Activation ») sont implémentés, et pour OTAA si une AppKey peut être partagée entre les périphériques.

Pour SigFox :

- Lors de l'utilisation du réseau SigFox, il doit être observé que le cryptage des données utiles est facultatif mais disponible. Par conséquent, une puce cryptographique certifiée Sigfox doit être utilisée pour activer le cryptage AES 128 et protéger les données confidentielles qui sont transmises sur les ondes.

Pour tous les dispositifs LPWA :

- Quelle forme (le cas échéant) de certification de sécurité a été entreprise.

5.3 Sécurité des réseaux fixes

Les recommandations pour la configuration par défaut des réseaux Wi-Fi sous le contrôle d'un opérateur de réseau ou d'un fournisseur de service IoT comprennent l'authentification EAP-SIM [28] ou EAP-AKA [27] et peuvent s'appuyer sur le cadre EAP de l'ETSI TS 102 310 [8].

5.4 Priorisation du trafic

Les opérateurs de réseau peuvent fournir des niveaux de qualité de service appropriés aux services IoT fournis.

5.5 Sécurité du réseau de liaison secondaire (Backhaul)

Les normes 3GPP qui spécifient GSM, UMTS et LTE n'imposent pas l'utilisation de connexions cryptés pour ce type de réseaux. De plus, le partage du réseau radio (RAN) et backhaul entre différents opérateurs de réseau, peut introduire des vulnérabilités de sécurité supplémentaires.

L'opérateur de réseau devrait fournir un cryptage de liaison pour les réseaux GSM, UMTS et LTE pour les données d'utilisateur final et le trafic de données du plan de signalisation.

5.6 Roaming

Les opérateurs de réseau peuvent faciliter aux fournisseurs de services IoT une empreinte mobile internationale grâce à l'utilisation de services d'itinérance.

Les réseaux d'itinérance peuvent être vulnérables aux failles de sécurité en raison de l'ouverture relative des fonctions d'interfonctionnement SS7 / Diamètre utilisées pour connecter les réseaux domestiques et d'itinérance. Ceci est particulièrement important pour les services IoT en raison de la proportion potentiellement élevée de dispositifs périphériques IoT qui résideront sur les réseaux itinérants. Il y a quelques raisons pour le pourcentage élevé de dispositifs itinérants. Tout d'abord, de nombreux dispositifs sont fabriqués en un seul endroit et distribués globalement. Par conséquent, dans de nombreux cas, le remplacement d'une carte UICC n'est pas pratique ou impossible dans le cas de l'eUICC. Deuxièmement, dans de nombreux cas, le statut d'itinérance est préférable à la connectivité locale, en raison de la couverture potentielle par plusieurs réseaux d'itinérance. La formation d'alliances globales avec une UICC global et des accords d'itinérance dédiés à l'IoT facilitent la situation d'itinérance permanente lorsque la législation locale le permet.

Les opérateurs de réseau devraient envisager comment protéger leurs HLR et VLR contre les attaques par déni de service (y compris les attaques par déni de service involontaires), les demandes provenant de sources non autorisées et l'exploitation des services de pilotage des services itinérants.

L'itinérance est facilitée par les protocoles de signalisation inter-réseaux qui sont échangés entre les principales entités du réseau mobile principal :

1. Entre le VLR ou le SGSN dans le réseau itinérant (visité) et le HLR sur le réseau domestique - le protocole MAP (Mobile Application Part) (pour les réseaux CDMA, IS41 est similaire à MAP).
2. Entre le MME dans le réseau d'itinérance LTE et le HSS sur le réseau LTE à domicile - le protocole Diameter (certaines variantes telles que S6a).
3. Entre le SGSN / S-GW dans le réseau visité et GGSN / P-GW sur le réseau domestique - le transfert de données itinérantes utilisant GTP (GPRS Tunneling Protocol).

Cette section se concentrera sur les problèmes de sécurité liés à l'itinérance pour les services IoT. Les questions générales de sécurité en matière d'itinérance sont couvertes par le groupe de la GSMA, FASG (Fraude et sécurité) et ses sous-groupes. Par conséquent, des questions telles que la double inscription en itinérance, realisée par deux VLR différents situés dans des pays différents - un scénario classique de fraude en itinérance - sortent du cadre de ce document.

5.6.1 « Tempêtes » et attaques de signalisation en itinérance

L'Internet des objets présente des exigences de sécurité supplémentaires à partir du réseau mobile, en raison de la nature différente des dispositifs périphériques et du faite que beaucoup des services IoT sont critiques. Tout en desservant un grand nombre de dispositifs périphériques, le réseau mobile est exposé à des « tempêtes de signalisation ». Une attaque de déni de service intentionnellement malveillante n'est qu'une des raisons de ces « tempêtes ». Une panne de courant, un désastre naturel ou un problème de couverture dans une certaine zone géographique d'un réseau mobile peut être courant dans de nombreux pays et donc causer de tels problèmes. Tous les compteurs intelligents itinérants

et autres dispositifs périphériques situés dans cette zone tenteront de se connecter simultanément à un autre réseau itinérant. Un tel scénario crée de multiples essais de connexion (signalisation) et impose un risque sévère sur le HLR / HSS dans le réseau d'origine. 3GPP TS 23.122 [9] définit un service EAB (« Extended Access Barring ») pour traiter de tels scénarios : Les opérateurs de réseau peuvent limiter l'accès réseau aux dispositifs périphériques configurés avec EAB, en plus des mécanismes de contrôle d'accès communs et spécifiques au domaine. La configuration EAB peut être effectuée sur l'UICC ou sur le dispositif lui-même. Les passerelles de sécurité de réseau doivent être configurées pour «gâcher» des attaques de déni de service intentionnelles.

L'opérateur de réseau domestique (avec le fournisseur de services IoT) peut également avoir besoin de faire la distinction entre les dispositifs périphériques de faible priorité et ceux qui sont critiques. Par exemple, il peut être nécessaire pour les dispositifs dédiés à la santé des utilisateurs de continuer à maintenir le service sous les tempêtes de signalisation et les attaques de déni de service. Il se peut que le réseau doive rejeter l'enregistrement des dispositifs périphériques en itinérance avec une faible priorité dans ces conditions, mais autoriser les dispositifs périphériques avec une haute priorité à s'enregistrer. Le mécanisme de rejet mis en œuvre peut être accompagné d'une minuterie de recul, afin d'assister le dispositif périphérique dans une nouvelle tentative d'enregistrement, après la tempête de signalisation.

La recommandation générale serait que les opérateurs de réseau examinent tous les messages d'itinérance reçus des réseaux domestiques et partenaires d'itinérance. En plus de bloquer les messages provenant de réseaux itinérants non autorisés ou truqués, il est nécessaire de filtrer les messages en fonction de la priorité du dispositif périphérique. Sous ce type de problèmes de signalisation, il est nécessaire d'autoriser les messages provenant de dispositifs périphériques prioritaires et critiques, ou de rejeter des messages provenant de dispositifs périphériques non critiques. Des méthodes de rejet sont requises afin de reporter les tentatives d'enregistrement et d'autres activités pendant un certain temps.

5.6.2 Pilotage de l'itinérance basé sur la sécurité (SoR)

Un autre cas d'utilisation de la sécurité qui peut être effectué par un opérateur de réseau est la gestion de l'itinérance (SoR) des dispositifs périphériques IoT à des fins de sécurité. Rejeter un emplacement de mise à jour sans minuteur de désactivation provoque une nouvelle tentative du dispositif périphérique, et enfin, une tentative d'enregistrement à partir d'un autre réseau itinérant (visité). Une autre méthode pour SoR est via OTA, en utilisant des listes préférées d'itinérance et d'autres paramètres stockés dans l'UICC. Les capacités de mise à jour OTA de l'UICC permettent au réseau domestique de mettre à jour les listes d'itinérance préférées, qui déterminent la priorité des réseaux pendant le processus de sélection d'un réseau itinérant. Le réseau domestique peut également actualiser la mémoire du dispositif périphérique avec la nouvelle liste et provoquer la recherche instantanée d'un nouveau réseau.

Dans le cas où un risque de sécurité est détecté dans un réseau visité spécifique, le réseau domestique peut décider de transférer ses dispositifs en itinérance vers un autre réseau visité, en utilisant le mécanisme SoR. Un tel transfert actif de périphériques peut être effectué lors de la prochaine tentative d'enregistrement du dispositif, ou d'une manière ad-hoc en utilisant les services SIM OTA. Un risque de sécurité lié à un réseau visité spécifique

peut être détecté si un problème est signalé par un nombre relativement élevé de dispositifs périphériques itinérants sur ce réseau ou des informations reçues par d'autres entrées.

5.6.3 Déni du service de données en itinérance

Les attaques par déni de service ne sont pas limitées à l'espace de signalisation en mobilité, et l'itinérance des données est également un champ potentiel pour une attaque par excès de signalisation. A ce jour, la plupart des données en itinérance sont routées depuis le réseau visité SGSN (S-GW dans le cas de LTE) vers le réseau domestique GGSN (P-GW pour LTE). Le cas du LBO (« Local Breakout »), où les données sont acheminées à partir du réseau visité directement vers Internet est rarement implémenter. La situation dans le futur pourrait changer, en raison de réglementations telles qu'en Europe qui permettent le service LBO depuis juillet 2014, LTE et surtout VoLTE (Voice over LTE), où les appels vocaux effectués dans le réseau d'itinérance peuvent être traités par le P-GW (comme c'est le cas aujourd'hui avec les appels vocaux réguliers à commutation de circuits effectués dans un réseau visité).

Des excès de signalisation peuvent se produire lorsque le domicile GGSN / P-GW est inondé de demandes de nouvelles sessions de données. Le protocole GPRS crée un tunnel sécurisé entre le dispositif périphérique et le GGSN, et une demande de nouvelle session (« Create-PDP-Context ») entraîne la configuration d'un tunnel et l'attribution d'une adresse IP au dispositif périphérique. Lorsque les dispositifs périphériques IoT ne se comportent pas de manière personnalisée, ils peuvent générer des rafales de demandes pour de nouvelles sessions de données, comme indiqué précédemment. Les attaques par déni de service peuvent être générées par un nombre relativement faible de dispositifs, créant plusieurs demandes de nouvelles sessions de données en parallèle. Les serveurs GGSN / P-GW sont limités dans leur capacité et devraient être protégés contre de telles demandes.

Pour éviter les excès de signalisation, les opérateurs réseau peuvent, sur la base d'une politique de sécurité, empêcher certains dispositifs de se connecter à leur réseau en modifiant le profil de communication des dispositifs affectés ou en adoptant des stratégies de sécurité dans le cœur du réseau.

Les dispositifs périphériques critiques doivent également recevoir un service en cas d'attaque par déni de service, tandis que les demandes de ceux qui ont une priorité inférieure sont différées pendant un certain temps.

5.7 Gestion des dispositifs périphériques et des passerelles

Il convient de noter que les mesures de sécurité matérielle et logicielle, y compris les consoles de gestion de configuration locales pour les dispositifs périphériques et les passerelles, dépassent la portée de ce document. Cette section couvre les aspects liés au réseau. Voir le document de la GSMA "CLP.11 IoT Security Guidelines Overview" [11] pour les consignes de sécurité relatives aux dispositifs périphériques IoT.

5.7.1 Gestion des dispositifs périphériques

Les opérateurs de réseau peuvent offrir aux fournisseurs de services IoT des fonctionnalités de base pour configurer et gérer en toute sécurité les dispositifs périphériques et abonnements, en adoptant certains principes et technologies développés pour la gestion des dispositifs mobiles «traditionnels». Les dispositifs périphériques IoT qui utilisent un

UICC pour s'enregistrer et se connecter à un réseau cellulaire peuvent être gérés à l'aide des plates-formes de gestion de connectivité, de gestion de dispositifs et de gestion des UICC existantes.

En plus de cette fonctionnalité de gestion de base de dispositifs périphériques, des fonctionnalités de gestion plus complexes et spécifiques peuvent être fournies par les plate-formes de service IoT.

Un exemple d'architecture de gestion de dispositifs périphériques typique est présenté ci-dessous et est tiré des principes de communication ETSI M2M [19].

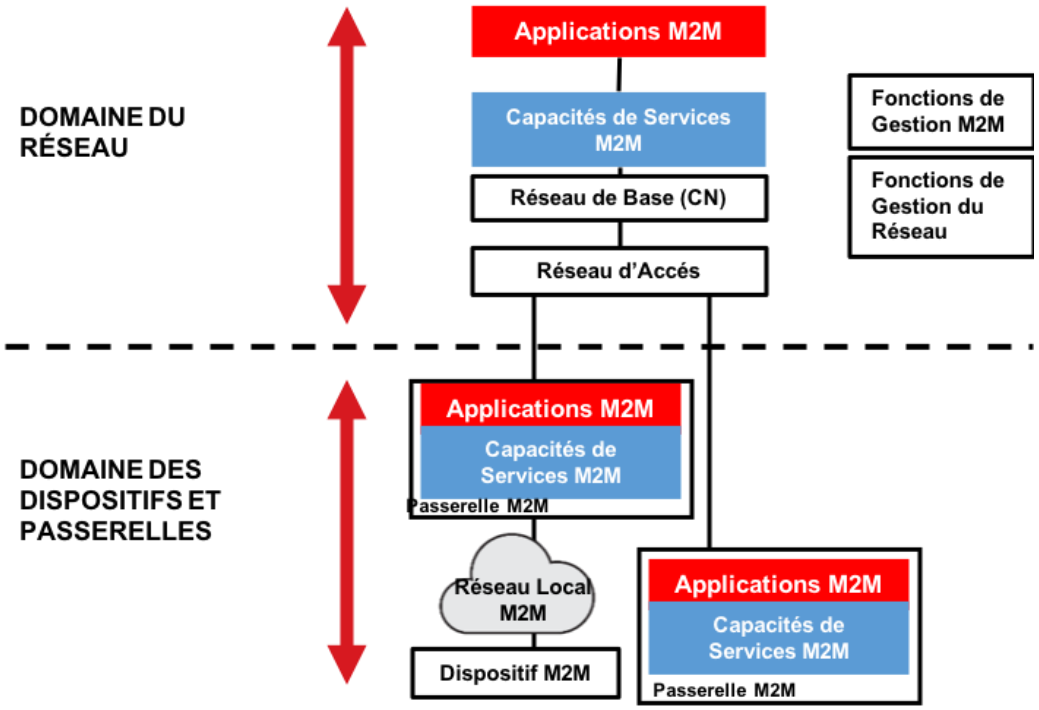

Figure 3 - Architecture de haut niveau ETSI pour la gestion des périphériques M2M

Les blocs bleus indiquent ce qui est traditionnellement géré par les plates-formes de gestion de dispositifs périphériques existantes de l'opérateur de réseau et les blocs rouges indiquent le composant de service géré par la plate-forme de service IoT.

Les opérateurs de réseau peuvent effectuer certaines des fonctions de gestion de périphérique indiquées en rouge à la demande du fournisseur de services IoT.

5.7.2 Gestion des passerelles

L'utilisation de passerelles introduit potentiellement un niveau supplémentaire de complexité de gestion des périphériques pour le fournisseur de services IoT. Dans certains cas, la passerelle IoT peut être un dispositif qui intègre une UICC qui se connecte à un réseau cellulaire, dans d'autres cas, elle se connecte directement au reseau fixe cablé.

La passerelle doit être un objet géré, afin qu'elle puisse être surveillée et mise à jour avec un nouveau micrologiciel ou un nouveau logiciel s'il est nécessaire. Des protocoles pour fournir des mises à jour de logiciels et de micrologiciels sécurisées et des mécanismes sécurisés

d'intégration de logiciels et de systèmes devraient être utilisés pour sécuriser l'interconnexion de la passerelle au cœur du réseau.

Les opérateurs de réseau peuvent fournir et gérer des passerelles sécurisées au nom du fournisseur de services IoT, ce qui permet aux dispositifs périphériques de se connecter de manière sécurisée de manière à s'intégrer au mieux aux mécanismes de sécurité du réseau étendu de l'opérateur réseau.

Les passerelles qui se connectent à l'aide de la connectivité réseau fixe peuvent être gérées à distance à l'aide du protocole de gestion de réseau étendu (WAN) TR-069 du « Broadband Forum CPE » (Customer Premises Equipment) [20].

Les passerelles qui se connectent à l'aide d'un réseau cellulaire peuvent être gérées à distance à l'aide les protocoles DM (« OMA Device Management ») et FUMO (« Firmware Update Management Object ») [5] [6].

5.7.3 Liste noire des dispositifs périphériques IoT

Les opérateurs de réseaux doivent mettre en place la liste noire des dispositifs périphériques IoT et la connexion à la base de données « Central Identity Register » (CEIR) de la GSMA. Le CEIR est une base de données centrale, administrée par la GSMA, qui contient des IMEI associés à des dispositifs périphériques perdus, volés et à des dispositifs qui ne devraient pas bénéficier d'un accès au réseau. Une fois qu'un IMEI est entré dans le CEIR, le dispositif périphérique contenant l'IMEI sera mis sur une liste noire par tous les opérateurs de réseau qui prennent ces données et implémentent une liste noire locale basée sur leur utilisation de registres d'identité d'équipement (EIR).

Les opérateurs de réseaux peuvent également implémenter une *liste grise* (« greylisting ») de dispositifs localisés pour permettre la suspension temporaire des dispositifs «suspects» tandis que l'opérateur de réseau étudie la nature de ces dispositifs avant toute mise en liste noire. Il convient de noter que pour les services critiques tels que ceux qui ont une relation avec la santé, le blocage d'un IMEI peut ne pas être souhaitable ou possible. Il est important que les opérateurs de réseau comprennent clairement les détails des dispositifs périphériques connectés, dans la mesure où la véritable application (ou hôte) d'un dispositif périphérique peut être discernée. Les dispositifs périphériques qui exploitent l'IMEI émis vers un fournisseur de module de communication doivent réaliser le « Device Host Identify Reporting », qui permet au dispositif périphérique de signaler les informations d'hôte à l'opérateur de réseau. Le signalement de l'hôte du dispositif est décrit dans le document des lignes directrices sur l'efficacité de la connexion de la GSMA [17].

5.8 Autres services liés à la sécurité

5.8.1 Services Cloud et de gestion des données

Les opérateurs de réseau peuvent fournir aux clients des plates-formes de services IoT cloud hébergés pour la mise en œuvre de services IoT et fournir également des services de stockage et de gestion des données produites par ces services.

Les opérateurs de réseau peuvent fournir un cloud privé ou une infrastructure de cloud partagé en fonction des besoins du fournisseur de services IoT.

5.8.2 Sécurité basée sur l'analyse

Les opérateurs de réseau peuvent fournir des services d'analyse de données et d'inspection approfondie des paquets afin d'identifier les menaces et les anomalies dans les données générées par les services IoT. Un exemple pourrait être qu'un opérateur de réseau peut périodiquement effectuer une inspection approfondie des paquets pour chercher des chaînes de caractères spécifiques comme des numéros de sécurité sociale et les coordonnées GPS qui pourraient suggérer que ces informations ne sont pas protégées correctement et alerter le fournisseur de services IoT responsable des fuites d'informations.

Ceci est avantageux pour IoT car les dispositifs périphériques légers et services ne peuvent pas fournir eux-mêmes cette fonctionnalité. Les opérateurs de réseau peuvent fournir aux fournisseurs de services IoT une visibilité de l'état de la sécurité, des menaces identifiées et des attaques, ainsi qu'un contrôle d'intégrité global de la sécurité. Ces services d'introspection sont essentiels pour garantir que les menaces ne sont pas infiltrées «à l'intérieur du pipeline», en particulier lorsque les services de données sont cryptés. Les services fournis incluent :

- L’ utilisation de la détection d'anomalies et de l'apprentissage automatique pour détecter des problèmes.
- Des systèmes de protection contre les intrusions dans les diagnostics de dispositifs périphériques en temps réel.
- Un tableau de bord pour visualiser et identifier facilement les anomalies.
- Des moyens automatisés pour signaler et bloquer les connexions suspectes.
- Une analyse des menaces des services basés sur le cloud.

5.8.3 Gestion sécurisée du réseau

Les opérateurs de réseau peuvent fournir des réseaux gérés et maintenus en toute sécurité. Ces services incluent :

- La sauvegarde des canaux en cas d'échec de liaison physique ou logique
- L’identification d'échec d’une connexion comme preuve d'une violation potentielle de la sécurité
- La mise en œuvre des politiques d'itinérance ayant un impact sur la sécurité et l'intégrité
- La gestion des UICC / SIM
- La gestion de l'information sécurisée
- L'adhésion aux CERTs et la participation au partage d'informations sur les menaces pour atténuer et prévenir les futures attaques.
- La protection contre les attaques par déni de service
- Des analyses de sécurité et évaluations de vulnérabilité périodiques
- La Gestion et traitement des exigences réglementaires liées à la sécurité du réseau
- La restriction des options de communication au strict minimum requis pour un service IoT donné.

5.8.4 Plate-forme sécurisée de gestion de connectivité IoT

Les opérateurs de réseau utilisent de plus en plus une infrastructure réseau et OSS dédiée pour gérer les abonnements IoT et les plans tarifaires de manière efficace et évolutive.

L'accès à une telle infrastructure est souvent exposé au client professionnel de l'opérateur (c'est-à-dire un fournisseur de services IoT) afin qu'il puisse gérer lui-même ses abonnements (activation du service, suspension, etc.) individuellement ou en masse.

Les directives de plate-forme de service proposées dans le document CLP 12 «Directives de sécurité IoT pour l'écosystème de services IoT» [26] offrent des conseils précieux qui peuvent bénéficier à l'opérateur de réseau qui offre les plates-formes de gestion de la connectivité IoT. Ces directives contiennent les recommandations suivantes :

- Les opérateurs de réseau doivent s'assurer que l'accès au portail web de leur plate-forme de gestion de la connectivité IoT, qui peut être hébergé par un opérateur réseau ou par un service dans le cloud, utilise le cryptage de première qualité selon les dernières recommandations publiées par des organisations telles que le NIST [24] [25].
- Les opérateurs de réseau doivent s'assurer que l'accès au portail web de leur plate-forme de gestion de connectivité IoT fait appel aux procédures standard de «meilleures pratiques» pour la création, la mise à jour et la réinitialisation des mots de passe.

5.8.5 Gestion des certificats

Les opérateurs de réseau peuvent fournir des services de gestion de certificats X.509.

5.8.6 Authentification multi-facteurs

Les services d'authentification multi-facteurs exigent généralement qu'un utilisateur s'authentifie en utilisant un token électronique en plus d'un nom d'utilisateur et d'un mot de passe. En tant que tel, l'authentification multi-facteurs peut fournir une protection supplémentaire contre l'accès aux services IoT provenant d'utilisateurs non autorisés.

L'initiative Mobile Connect de la GSMA [12], avec OpenID Connect [21], FIDO [22] et ETSI MSS [23] sont des exemples de facilitateurs d'authentification multi-facteurs qui peuvent permettre à un fournisseur de services IoT d'obtenir une authentification et des informations supplémentaires au sujet de leurs utilisateurs. L'utilisateur final dans ce contexte étant un être humain pouvant apporter des informations à une plate-forme de service IoT pour fournir différents niveaux d'assurance - des exemples incluent la saisie d'un code PIN et une signature biométrique.

Alors que la plupart des solutions d'authentification multi-facteurs sont actuellement utilisées pour les services «intelligents» traditionnels, ces technologies peuvent être appliquées aux services IoT qui requièrent l'autorisation de certaines fonctions telles que l'exécution d'une opération de connexion réseau, la mise à jour d'un logicielle ou la réinitialisation matérielle.

Par exemple, en utilisant l'authentification multi-facteurs, une identité mobile pourrait être utilisée en plus d'une passerelle à l'intérieur d'une voiture connectée. Dans ce cas d'utilisation, l'infrastructure d'authentification multi-facteurs pourrait servir de couche d'autorisation supplémentaire pour que les occupants de la voiture aient accès aux services multimédia et de paiement fournis dans la voiture.

Annexe A Gestion du document

A.1 Historique du document

Version	Date	Brève description du changement	Autorité d'approbation	Éditeur / Société
1.0	08-Feb-2016	Nouvelle Version PRD CLP.14	PSMC	Ian Smith GSMA
1.1	17-Nov-2016	Références au schéma d'évaluation de la sécurité de l'IoT de la GSMA ajoutées. Corrections éditoriales mineures.	PSMC	Ian Smith GSMA
2.0	30 Sep 2017	Modification importante pour ajouter les références à LPWA	IoT Security Group	Rob Childs GSMA

A.2 Autres informations

Type	Description
Propriétaire du document	GSMA IoT Programme
Contact	Rob Childs – GSMA

Nous avons l'intention de fournir un produit de qualité pour votre usage. Si vous trouvez des erreurs ou des omissions, veuillez nous contacter avec vos commentaires. Vous pouvez nous en informer à prd@gsma.com

Vos commentaires ou suggestions et questions sont toujours les bienvenus.