Lineamientos de Seguridad IoT para los Operadores de Red

Lineamientos de Seguridad IoT para los Operadores de Red

Versión 2.0

26 de Octubre 2017

Non-binding Permanent Reference Document

Clasificación de Seguridad: No Confidencial

El acceso y distribución de este documento está restringido a las personas permitidas por la clasificación de seguridad. Este documento es confidencial para la Asociación y está sujeto a la protección de derechos de autor. Este documento se utilizará únicamente para los fines para los que ha sido suministrado y la información contenida en él no debe divulgarse ni ponerse a disposición en ninguna otra forma posible, en su totalidad o en parte, a personas distintas a las permitidas bajo la clasificación de seguridad sin la aprobación previa por escrito de la Asociación.

Aviso de Copyright

Aviso Legal

La Asociación GSM ("Asociación") no acepta ninguna responsabilidad por la representación, garantía o compromiso (expreso o implícito) con respecto al contenido de este documento, así como por la exactitud o integridad o actualidad de la información. La información contenida en este documento puede estar sujeta a cambios sin previo aviso.

Aviso Antimonopolio

La información aquí contenida es conforme a la política de cumplimiento antimonopolio de la Asociación GSM.

Table of Contents

1 Introducción

1.1 Resumen

Este documento proporciona lineamientos de seguridad de alto nivel para los operadores de red que tienen la intención de proporcionar servicios a los proveedores de servicios de IoT para garantizar la seguridad del sistema y la privacidad de los datos. Las recomendaciones se basan en sistemas y tecnologías fácilmente disponibles que se implementan en la actualidad.

1.2 Estructura del Documento

Este documento es un documento destinado a operadores de red y proveedores de servicios de IoT. Los lectores de este documento también pueden estar interesados en leer los otros documentos contenidos en las Directrices de seguridad de IoT de la GSMA [11], cuya estructura se muestra a continuación.

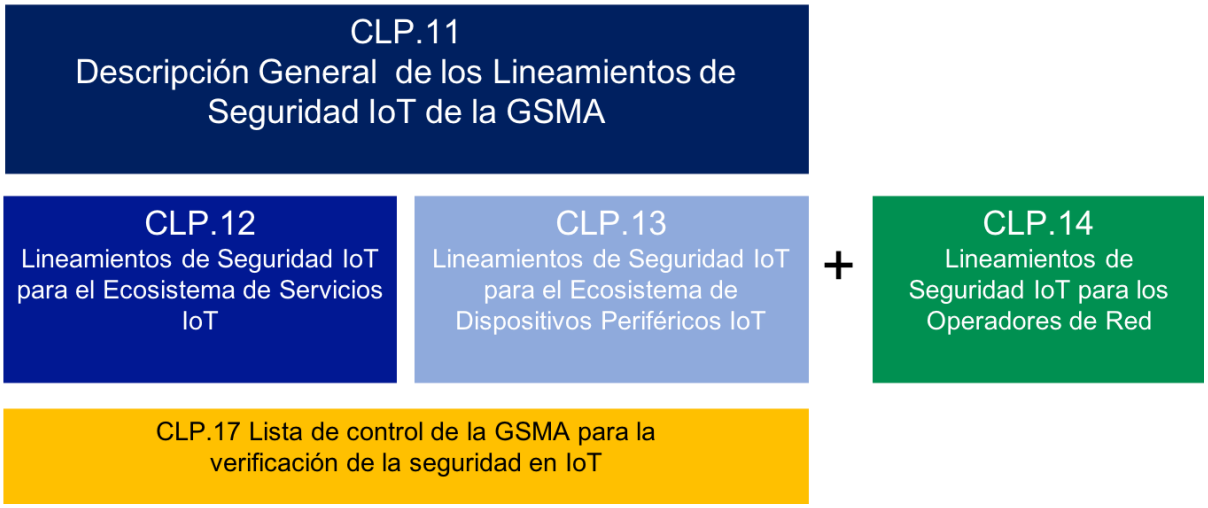

Figura 1- Estructura del Conjunto de Documentos

1.3 Propósito y Alcance del Documento

Este documento debe actuar como una lista de verificación para los acuerdos con los suministradores entre los proveedores de servicios de IoT y los operadores de red que se asocien.

El alcance del documento está limitado a:

- Pautas de seguridad relacionadas con los servicios de IoT.
- Recomendaciones relacionadas con los servicios de seguridad ofrecidos por un operador de red.
- Tecnologías de redes celulares.

Este documento no pretende impulsar la creación de nuevas especificaciones o estándares de IoT, sino que hará referencias a soluciones, estándares y mejores prácticas actualmente disponibles.

Este documento no pretende acelerar la obsolescencia de los servicios de IoT existentes. La compatibilidad con versiones anteriores de los servicios de IoT existentes del operador de Red debe mantenerse cuando se consideren adecuadamente protegidas.

Este documento no aborda los problemas de seguridad asociados con las interfaces y APIs implementadas en las Plataformas de Servicios IoT (o Plataformas de Gestión de la Conectividad IoT) con respecto a la compartición y manejo de datos con los usuarios finales (por ejemplo, para compartir datos con un usuario final a través de una aplicación en un Smartphone o PC) u otras entidades dentro del ecosistema. Dichas interfaces y APIs se deben proteger utilizando las mejores tecnologías y protocolos de seguridad de Internet.

Se hace notar que el cumplimiento de las leyes y reglamentos nacionales para un territorio en particular pueden, en cualquier momento, anular las pautas establecidas en este documento.

1.4 Audiencia a la que se Dirige el Documento

A quien se dirige este documento:

- En primer lugar, a los operadores de red que desean proporcionar servicios a los proveedores de servicios IoT.
- En segundo lugar, a las empresas y organizaciones que buscan desarrollar productos y servicios conectados nuevos e innovadores (dentro del llamado "Internet de las cosas") utilizando redes celulares o redes cableadas (Red Fija). En este documento nos referimos a estas empresas como "Proveedores de servicios IoT".

1.5 Definiciones

Término	Descripción
Reporte del Identificador del dispositivo anfitrión (Host)	Es una función de un dispositivo de Dispositivo Periférico que permite a un operador de red obtener información sobre el dispositivo anfitrión (host). Ver Pautas de Eficiencia de Conectividad GSMA [17]
Diameter	“Diameter” es un protocolo de autenticación, autorización y contabilidad para redes de computadoras. Ver IETF RFC 6733 [18]
Dispositivo Periférico IoT	Un dispositivo con capacidad de computo que realiza una función o tarea como parte de un producto conectado o servicio de Internet. Ver la sección 3 del documento CLP.13 [29] para una descripción de las tres clases comunes de dispositivos de IoT y ejemplos de cada clase de dispositivo periférico.
Pasarela	Un dispositivo periférico complejo que normalmente conecta dispositivos periféricos ligeros (conectados a través de una red local) con una red de acceso tipo WAN. Ver CLP.13 [29] para más información.
Internet de las Cosas	El Internet de las cosas (IoT) describe la coordinación entre múltiples máquinas, dispositivos y aparatos conectados a Internet a través de múltiples redes. Estos dispositivos incluyen objetos cotidianos tales como tabletas y electrónica de consumo y otros dispositivos o máquinas tales como vehículos, monitores y sensores equipados con capacidades de comunicación que les permitan enviar y recibir datos.

Término	Descripción
Plataforma de Gestión de la Conectividad IoT	Un sistema, normalmente gestionado por un operador de red, que permite la autogestión de las suscripciones de IoT y los planes de conectividad y precios por parte del proveedor de servicios IoT.
Servicio IoT	Cualquier programa de computadora que utiliza datos desde dispositivos de IoT para prestar el servicio.
Plataforma de servicios IoT	La plataforma de servicios, alojada en el Proveedor de servicios IoT que se comunica con un Dispositivo Periférico para proporcionar un Servicio IoT.
Proveedor de un Servicio IoT	Las empresas u organizaciones que buscan desarrollar nuevos productos y servicios conectados innovadores.
Dispositivo Periférico Ligero	Típicamente, un dispositivo “restringido” (por ejemplo, un sensor o actuador) que se conecta a un Servicio IoT a través de un dispositivo tipo pasarela.
Operador de Red	El operador y propietario de la red de comunicaciones que conecta un dispositivo periférico de IoT a un ecosistema de servicios IoT.
UICC	Elemento seguro entendido como plataforma especificada en ETSI TS 102 221 que puede soportar múltiples aplicaciones de autenticación estandarizadas para una red o servicio dentro de distintos dominios de seguridad. Puede ser integrada y encapsulada en varios formatos especificados en ETSI TS 102 671.
Red de Área Extendida (WAN)	Una red de telecomunicaciones que se extiende dentro de una gran distancia geográfica.

1.6 Abreviaciones

Término	Descripción
3GPP	Asociación de proyectos de 3ra generación (“3rd Generation Project Partnership”)
AKA	Autenticación y Acuerdo de Clave (“Authentication and Key Agreement”)
APDU	Unidad de Datos del Protocolo de Aplicación (“Application Protocol Data Unit”)
API	Interfaz del programa de Aplicación (“Application Program Interface”)
APN	Nombre del punto de Acceso (“Access Point Name”)
BGP	Protocolo de la Frontera de la Pasarela (“Border Gateway Protocol”)
CEIR	Registro de la Identidad del Equipamiento Central (“Central Equipment Identity Register”)
CERT	Equipo de Respuesta a Emergencias de Computación (“Computer Emergency Response Team”)
DNS	Sistema de Nombres de Dominio (“Domain Name System”)
DoS	Denegación de Servicio (“Denial of Service”)
DPA	Acuerdo de Procesamiento de Datos (“Data Processing Agreement”)
EAB	Restricción Extendida de Acceso (“Extended Access Barring”)
EAP	Protocolo de Autenticación Extensible (“Extensible Authentication Protocol”)
EID	Identidad del eUICC (“eUICC Identity”)

Término	Descripción
ETSI	Instituto Europeo de Estándares de Telecomunicaciones (“European Telecommunications Standards Institute”)
EU	Unión Europea (“European Union”)
eUICC	UICC Integrado (“Embedded UICC”)
FASG	Grupo de Fraude y Seguridad (“Fraud and Security Group”)
GCF	Foro de Certificación Global (“Global Certification Forum”)
GGSN	Nodo de Soporte de la Pasarela GPRS (“Gateway GPRS Support Node”)
GPRS	Servicio General de Paquetes de Radio (“General Packet Radio Service”)
GRX	Central de Conmutación para el Roaming en GPRS (“GPRS Roaming eXchange”)
GSM	Sistema Global de Comunicaciones Móviles (“Global System for Mobile communication”)
GSMA	Asociación GSM (“GSM Association”)
GTP	Protocolo de Tunelización GPRS (“GPRS Tunnelling Protocol”)
HLR	Registro de Ubicación Base (“Home Location Register”)
HSS	Servidor del Subscriptor Base (“Home Subscriber Server”)
ICCID	Identificador de la Tarjeta del Circuito Integrado (“Integrated Circuit Card Identity”)
IMEI	Identidad Internacional de Equipo Móvil (“International Mobile station Equipment Identity”)
IMSI	Identidad Internacional del Abonado a un Móvil (“International Mobile Subscriber Identity”)
IoT	Internet de las Cosas (“Internet of Things”)
IP	Protocolo de Internet (“Internet Protocol”)
IPSec	Seguridad del protocolo de Internet (“Internet Protocol Security”)
L2TP	Protocolo de Tunelización del Segundo Nivel (“Layer Two Tunnelling Protocol”)
LBO	Ruptura para el Internet Local (“Local Break Out”)
LPWAN	Red de Bajo Consumo para Área Extendida (“Low Power Wide Area Network”)
LTE	Evolución a Largo Plazo (“Long-Term Evolution”)
M2M	Máquina a Máquina (“Machine to Machine”)
MAP	Parte de la Aplicación Móvil (“Mobile Application Part”)
MME	Entidad de Gestión de la Movilidad (“Mobility Management Entity”)
OMA	Alianza Abierta para las Comunicaciones Móviles (“Open Mobile Alliance”)
OSS	Sistema de Soporte a las Operaciones (“Operations Support System”)
OTA	En el Aire (“Over The Air”)
PTCRB	Consejo para la Revisión de Certificación PCS (“A pseudo-acronym, originally meaning PCS Type Certification Review Board, but no longer applicable”)
RAN	Red de Acceso por Radio (“Radio Access Network”)
SAS	Esquema de Acreditación para la Seguridad (“Security Accreditation Scheme”)
SGSN	Nodo de Soporte sirviendo a GPRS (“Serving GPRS Support Node”)
SIM	Módulo de Identificación de Subscriptor (“Subscriber Identity Module”)

Término	Descripción
SMS	Servicio de Mensajes Cortos (“Short Message Service”)
SoR	Manejo del Roaming (“Steering of Roaming”)
SS7	Sistema de Señalización No. 7 (“Signalling System No. 7”)
UMTS	Servicio Universal de Telecomunicaciones Móviles (“Universal Mobile Telecommunications Service”)
USSD	Datos Suplementarios de Servicio sin Estructura (“Unstructured Supplementary Service Data”)
VLR	Registro de Ubicación de la Red Visitada (“Visitor Location Register”)
VPN	Red Privada Virtual (“Virtual Private Network”)
VoLTE	Voz sobre LTE (“Voice over LTE”)
WAN	Red de Área Extendida (“Wide Area Network”)

1.7 Referencias

Ref	Número de Documento	Título
[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/

Ref	Número de Documento	Título
[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

Ref	Número de Documento	Título
[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/JlOlr6
[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 Activos de un Servicio de IoT que los Operadores de Red Pueden Proteger

Las características de seguridad que deben implementarse para proteger adecuadamente los activos de un Servicio de IoT son específicas a cada servicio. Por lo tanto, sigue siendo responsabilidad del proveedor de servicios de IoT utilizar los procesos de evaluación de impacto a la privacidad y de riesgo adecuados para dirimir cuales serán sus necesidades de seguridad específicas. Los operadores de red y los proveedores de servicios de IoT a menudo comparten requisitos de seguridad similares para proteger sus activos, por lo tanto, tiene sentido que aprovechen las soluciones de seguridad comunes en lugar de implementar infraestructuras de seguridad duplicadas (y potencialmente redundantes). Además, en muchos casos, los operadores de red también podrán ser los proveedores de servicios de IoT.

Los servicios de seguridad proporcionados por los operadores de red pueden tener un papel fundamental en la seguridad de los activos utilizados para proporcionar un servicio de IoT. Estos pueden incluir:

- Los datos del servicio IoT enviados entre un dispositivo periférico IoT y la Plataforma de Servicios IoT: esto incluye datos primarios sensibles a la privacidad (por ejemplo, datos relacionados con el usuario final) y comercialmente explotables (p. Ej., Datos de control pertenecientes a un controlador/actuador) que también pueden tener impacto en la privacidad del usuario o servicio.

- Los activos de seguridad (IMSI, conjuntos de claves, etc.) y los ajustes de configuración de red (APN, valores de temporizadores, etc.) utilizados en dispositivos periféricos (incluidos los dispositivos tipo pasarela).
- Información confidencial del negocio del proveedor de servicios de IoT, incluida la reputación de la marca, datos de clientes/usuarios bajo responsabilidad de la compañía, información estratégica, datos financieros y registros de salud, etc.
- Infraestructuras comerciales, plataformas de servicios, redes corporativas y otros elementos de redes privadas del proveedor de servicios de IoT.
- Infraestructuras de centros de datos públicas (es decir, compartidas) proporcionadas por el operador de red y utilizadas por un servicio de IoT. Esto puede incluir servicios públicos, capacidades alojadas, infraestructuras de virtualización, instalaciones de la infraestructura para aplicaciones en la “nube”, etc.
- Infraestructura de red de comunicaciones, que incluye redes de acceso de radio, red central, redes troncales, funciones de servicios básicos (DNS, BGP, etc.), acceso y agregación de redes fijas y celulares, etc.

3 Principios de Seguridad de Red

Los operadores de red deben implementar mecanismos de seguridad adecuados y confiables en sus redes.

En esta sección se describe cómo las redes pueden proporcionar valor dentro del ecosistema de IoT.

Los mecanismos de seguridad más fundamentales provistos por una red de comunicaciones son:

- Identificación y autenticación de las entidades involucradas en un servicio de IoT (es decir, puertas de enlace, dispositivos periféricos, red doméstica, redes en itinerancia, plataformas de servicio).
- Control de acceso a las diferentes entidades que necesitan conectarse para crear un servicio de IoT.
- Protección de datos para garantizar la seguridad (confidencialidad, integridad, disponibilidad, autenticidad) y la privacidad de la información transmitida por la red para un servicio de IoT.
- Procesos y mecanismos para garantizar la disponibilidad de los recursos de la red y protegerlos contra los ataques (por ejemplo, implementando un cortafuegos adecuado, prevención de intrusiones y tecnologías de filtrado de datos)

3.1 Identificación Segura de Usuarios, Aplicaciones, Dispositivos Periféricos, Redes y Plataformas de Servicio

La identificación consiste en proporcionar identificadores únicos a las entidades dentro de un Servicio de IoT, y correlacionar estas identidades electrónicas con identidades legalmente vinculantes del mundo real.

Dentro de un servicio de IoT conectado en una red celular, los dispositivos periféricos se identifican usando una IMSI y/o un IMEI (los EID también se pueden usar para dispositivos tipo eUICCs). Las redes se identifican usando códigos de red y códigos de país. Cada método para proporcionar una identidad tiene niveles variables de seguridad garantizada asociados con él.

La identidad juega un papel crucial en el proceso de autenticación, ya que la autenticación segura solo puede lograrse sobre la base de una identidad segura. Por lo tanto, es esencial que las identidades (por ejemplo, IMSI, IMEI o ICCID) emitidas y utilizadas dentro de un Servicio IoT estén protegidas de forma segura contra modificación, suplantación o cesión no autorizados.

Un problema práctico al que puede enfrentarse un proveedor de servicios de IoT es que su servicio IoT puede requerir comunicaciones con muchas plataformas de servicio IoT, cada una de las cuales puede requerir una identificación única separada. Cada identidad utilizada para establecer un enlace de comunicaciones a cada plataforma de servicios IoT deberá ser aprovisionada, almacenada y gestionada de forma segura por el servicio IoT.

Cuando corresponda para el servicio IoT, los operadores de red recomiendan el uso de mecanismos basados en una UICC para identificar de manera segura los dispositivos periféricos. Los operadores de red también pueden extender la funcionalidad de

almacenamiento seguro proporcionado por la UICC al proveedor de servicios IoT para permitirles almacenar identidades adicionales relacionadas con un servicio de IoT en la UICC. Esta técnica se puede aplicar a dispositivos periféricos tanto celulares como no celulares (por ejemplo, EAP-AKA [27]).

Los operadores de red también pueden proporcionar servicios de inicio de sesión único (“Single Sign-on”) para permitir que los dispositivos periféricos establezcan y prueben su identidad una vez, y luego se conectan a varias plataformas de servicios IoT sin más inconvenientes. Las ventajas, desventajas y riesgos de seguridad de utilizar dicho servicio se deben analizar a través de todas las plataformas utilizadas.

3.2 Autenticación Segura de Usuarios, Aplicaciones, Dispositivos de Punto Final, Redes y Plataformas de Servicio

Según NIST [10], la "autenticación" significa "verificar la identidad de un usuario, proceso o dispositivo periférico, a menudo como un requisito previo para permitir el acceso a los recursos en un sistema de información".

Los operadores de red pueden proporcionar servicios para garantizar que los usuarios, las aplicaciones, los dispositivos periféricos, las redes y las plataformas de servicio asociadas con un servicio IoT estén autenticados de forma segura.

La autenticación tiene una propiedad relacionada: la de no-repudio. De acuerdo con NIST [10], una definición de no-repudio es: "garantía de que el remitente de la información recibe la prueba de la entrega y se proporciona al receptor una prueba de la identidad del remitente, por lo que ninguno puede negar haber procesado la información”. El no-repudio depende de afirmar que la autenticidad no se ha violado al identificar el origen de esa transacción o mensaje.

3.3 Proporcionar Canales de Comunicación Seguros

Los operadores de red proporcionan mecanismos de seguridad para las comunicaciones en redes móviles y fijas de área extendida (WAN) que proporcionan una seguridad inmejorable de la integridad, confidencialidad y autenticidad de las comunicaciones. Cuando corresponda, los operadores de red pueden proporcionar y administrar conexiones seguras a redes empresariales mediante redes privadas virtuales (VPN) y conexiones de internet cifradas.

El objetivo de un canal de comunicación seguro es garantizar que los datos que se envían a través del canal no se procesen, utilicen, ni transmitan sin el conocimiento y consentimiento del interesado. Las tecnologías de cifrado juegan un papel crucial en la transmisión segura de datos al garantizar las propiedades de confidencialidad, integridad y autenticidad. La encriptación debe ser apropiada para el sistema que se diseña y se implementa teniendo en cuenta los dispositivos ligeros periféricos, los aspectos de red (como las restricciones en redes satelitales troncales) y el servicio que se proporciona.

Los operadores de red pueden proporcionar a los proveedores de servicios de IoT, servicios de encriptación de datos para garantizar la integridad de la comunicación y la resiliencia de la red.

Los operadores de red tradicionalmente proporcionan una infraestructura pública de telecomunicaciones o una combinación de infraestructura de red pública y privada. Muchos operadores de red pueden garantizar que los datos del cliente/usuario que transitan por su infraestructura de red pública estén encriptados entre el punto en que los datos ingresan a la infraestructura de la red pública hasta el punto en que abandonan la red. Cuando sea necesario, los operadores de red también pueden ayudar a los proveedores de servicios de IoT a implementar u obtener sus propias claves de cifrado para garantizar la confidencialidad de los datos de IoT durante el tránsito a través de la infraestructura del operador de red.

Los operadores de red pueden proporcionar a sus clientes redes privadas donde se ofrecen canales de comunicación dedicados para el uso de un solo cliente para garantizar que ningún dato atraviese una red pública como la de Internet. Tales redes privadas podrían ser creadas:

1. Mediante el uso de un protocolo de túnel como el de capa 2 (L2TP) para la red virtual y uno de seguridad como el protocolo de Internet (IPsec) para asegurar los datos, o
2. Proporcionando a los clientes seguridad de extremo a extremo entre el equipo de usuario (UE) y el servidor de aplicaciones usando p. Ej. BEST [36] o
3. Creando una red dedicada para el servicio de IoT mediante la implementación de una instancia separada de la red central con una red de radio compartida, como se muestra a continuación.

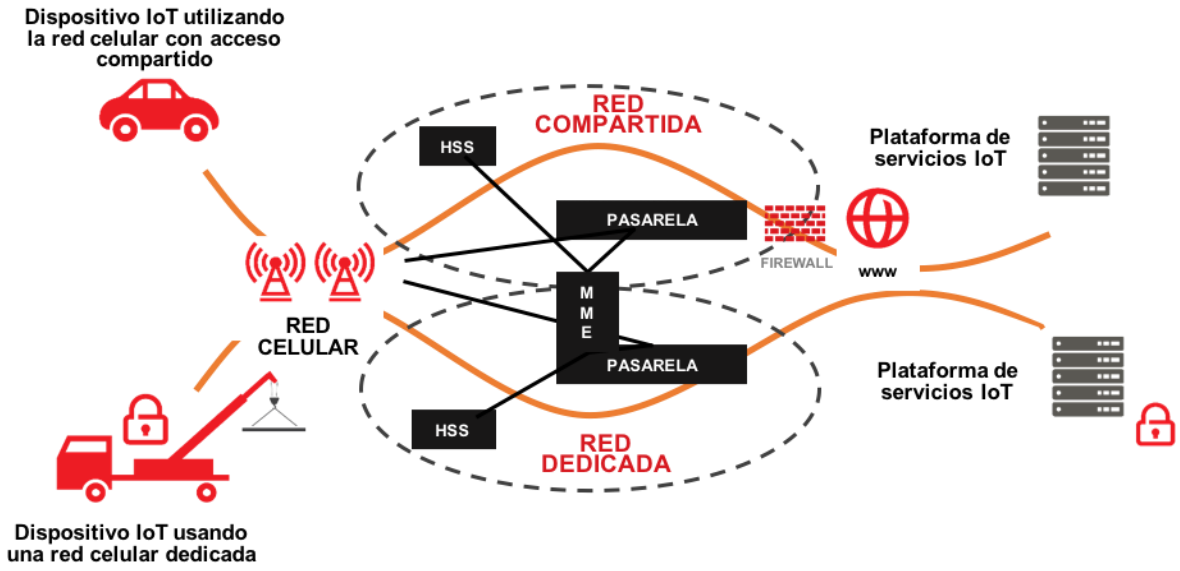

Figura 2 – Ejemplo de una Configuración para una Red Privada

3.4 Asegurar la Disponibilidad de los Canales de Comunicación

Según NIST [10], la "disponibilidad" es la propiedad de ser accesible y utilizable a petición de una entidad autorizada.

Los operadores de red pueden proporcionar a los proveedores de servicios de IoT las redes disponibles. Los mecanismos más fundamentales provistos por los operadores de red para proporcionar disponibilidad de red son los siguientes:

3.4.1 Uso en las Redes del Espectro bajo Licencia

Los operadores de red miembros de la GSMA operarán redes utilizando un espectro dedicado con licencia bajo los términos de las licencias emitidas por sus reguladores nacionales. El uso del espectro con licencia garantiza que la interferencia de otras tecnologías de radio se reduzca al mínimo ya que cualquier uso no autorizado de este espectro estará sujeto a las leyes previstas para un uso ilícito. Los operadores de red junto con los reguladores nacionales buscarán cualquier fuente de interferencia no autorizada para garantizar que la disponibilidad de la red no se vea afectada.

El uso del espectro con licencia, que proporciona al operador de red bandas de radio dedicadas para operar su red, garantiza que el operador de Red pueda realizar una cuidadosa cobertura de la red y planificar la capacidad para garantizar la máxima disponibilidad de red para sus clientes.

3.4.2 Implementación de Tecnologías de Red Estandarizadas y Probadas

Los operadores de red miembros de la GSMA implementan tecnologías de red estandarizadas, como GSM, UMTS y LTE, tal como lo especifican los organismos de estandarización como 3GPP. El uso de tecnologías estandarizadas no solo garantiza la interoperabilidad entre los operadores de red, sino que también garantiza que el estándar esté sujeto a un escrutinio máximo durante su creación para garantizar la solidez de su tecnología.

3.4.3 Implementación de Tecnologías de Red Probadas y Certificadas

Muchas partes de la red de un operador de red serán probadas y certificadas de acuerdo con los estándares internacionales de prueba. Los dispositivos periféricos complejos y los módulos de comunicación que contienen estarán sujetos a las especificaciones de prueba 3GPP [13] a través de las pruebas de certificación de los organismos GCF, PTCRB y las organizaciones internas de los operadores de red. Las redes de acceso de radio (RAN) estarán sujetas a las especificaciones de prueba de 3GPP [14] a través de las pruebas de aceptación del operador de red. Las UICC estarán sujetas a las especificaciones de prueba 3GPP [15] a través de las pruebas de aceptación del operador de red y, adicionalmente, pueden estar sujetos a la certificación SAS de la GSMA [16].

3.4.4 Topografías y Configuraciones de Red Resilientes

Los operadores de red proporcionan redes resistentes que implementan y construyen la redundancia geográfica y el aislamiento necesarios para garantizar la máxima disponibilidad con un tiempo de inactividad mínimo. Todos los elementos de la red están cuidadosamente configurados y monitorizados para asegurar que se cumplan estrictos acuerdos de calidad de servicio y de nivel de servicio.

3.4.5 Monitorización en Tiempo Real y Gestión de Recursos de Red

Los operadores de red implementan centros de operaciones de red de última generación que monitorean el rendimiento de sus redes las 24 horas del día, los 7 días de la semana y en tiempo real para administrar el tráfico de la red, responder a la demanda de la red y corregir fallos. Se puede encontrar información adicional en la sección 4.10.

3.4.6 Gestión de Amenazas e Intercambio de Información

El Grupo de Fraude y Seguridad de la GSMA (FASG) proporciona un entorno abierto, receptivo y confiable para que todos los operadores de Red compartan información de fraude y seguridad y detalles de incidentes de manera oportuna y responsable. El grupo evalúa el panorama mundial de amenazas de seguridad y fraude, analiza los riesgos asociados para los operadores de red y sus clientes, y define y prioriza las acciones de mitigación apropiadas.

3.4.7 Servicios de Itinerancia

Debido al uso de tecnologías estandarizadas de red y dispositivos periféricos y servicios de interconexión, los operadores de red pueden ofrecer servicios de itinerancia de red, mejorando aún más la cobertura de red y la disponibilidad para sus clientes.

3.4.8 Monitorización y Gestión del Rendimiento de Dispositivos Periféricos

Los operadores de red pueden medir el rendimiento de los dispositivos periféricos que se conectan a sus redes para aislar dispositivos periféricos que pueden crear interferencias de radio excesivas (por ejemplo, cuando no cumplen con las regulaciones nacionales) o tráfico de señalización de red (por ejemplo, cuando no cumplen con los lineamientos de Eficiencia de Conexión GSMA [17]) que, a su vez, pueden estar degradando el rendimiento de la red global. Los dispositivos periféricos se pueden supervisar, desconectar o su firmware se puede actualizar cuando se detecta un comportamiento anormal.

4 Consideraciones de Privacidad

Para darse cuenta de las oportunidades que ofrece IoT, es importante que los consumidores confíen en los proveedores de servicios de IoT que brindan servicios de IoT y recopilan datos sobre ellos. La GSMA y sus miembros creen que la fiabilidad y la confianza de los consumidores solo pueden lograrse plenamente cuando los usuarios sienten que su privacidad se respeta y protege de manera apropiada.

Ya existen leyes sobre la privacidad y protección de datos bien establecidas en todo el mundo que han sido aplicadas y cumplidas por los operadores de red. Los operadores creen que es posible aplicar las normas y principios de protección de datos existentes para abordar las necesidades de privacidad en el contexto de los servicios y tecnologías de IoT.

Sin embargo, los Servicios de IoT generalmente involucran operadores que trabajan junto con socios proveedores de servicios de IoT. Es importante que exista claridad normativa y seguridad jurídica en torno a los Servicios de IoT y que las normas de privacidad y protección de datos se apliquen sistemáticamente a todos los proveedores de servicios de IoT de forma neutral en términos de servicio y tecnología.

Los operadores de redes deben ser conscientes de que si procesan datos de alguna manera, deben firmar un Acuerdo de Procesamiento de Datos (DPA) con el Proveedor de servicios de IoT. Las prácticas de seguridad y protección de datos desarrolladas para un servicio de IoT determinado deben reflejar el riesgo general para la privacidad de una persona y el contexto en el que se recopilan, distribuyen y utilizan los datos sobre la persona. Cualquier intervención reguladora debe limitarse a las áreas donde surgen riesgos identificados y cuando las medidas existentes son insuficientes para abordarlos. Por

ejemplo, oneM2M (a través de TS-0003 [31]) permite al operador desempeñar el rol de administrador de la privacidad para un proveedor de servicios.

Los operadores de red pueden aprovechar su amplia experiencia para abordar cuestiones de privacidad y seguridad y trabajar en colaboración con los proveedores de servicios de IoT, para incorporar privacidad y seguridad a las tecnologías IoT y a la experiencia de usuario en general del servicio IoT para el consumidor. Dicha colaboración garantizará que los proveedores de servicios IoT puedan identificar y reducir los riesgos de privacidad del consumidor relevantes en el contexto del servicio que se está proporcionando.

Para obtener más información, consulte los principios de privacidad móvil de la GSMA: http://www.gsma.com/publicpolicy/mobile-and-privacy/mobile-privacy-principles

5 Servicios Provistos por Operadores de Red

Los operadores de red pueden proporcionar a los proveedores de servicios de IoT redes seguras de área extendida (WAN) celulares y fijas.

Esta sección contiene recomendaciones sobre las mejores prácticas a tener en cuenta a la hora de conectar servicios de IoT a redes WAN. Cuando corresponda, las recomendaciones serán independientes de la tecnología utilizada, pero también harán referencia a las mejores prácticas empleadas en las redes celulares y en otros tipos de redes.

5.1 Procedimientos de Gestión de Suscripción Segura

Esta sección contiene recomendaciones sobre cómo las suscripciones del proveedor de servicios de IoT deben ser administradas por operadores de red:

- El operador de red o el proveedor de servicios de IoT debe realizar una evaluación de los servicios de red necesarios para habilitar el servicio de IoT (voz, datos, SMS, etc.) tanto ahora como en el futuro.
- Basándose en esta evaluación, el operador de red debe aplicar el "principio de privilegio mínimo" y proporcionar suscripciones al proveedor de servicios con sólo aquellos servicios requeridos para el servicio de IoT específico. Por ejemplo:
    - Los servicios IoT que solo usan portadoras de datos no deben aprovisionarse con servicios de voz, ni SMS.
    - Cuando un dispositivo periférico solo se conecta a una plataforma de servicios de IoT conocida, la suscripción asociada con el dispositivo solo debe permitir la conexión a una “lista blanca” conocida de rangos de direcciones IP (o dominios).
    - Si el servicio IoT usa voz o SMS, se debe considerar el uso de una lista de marcación fija preconfigurada.
- Los operadores de red deberían implementar procesos de gestión segura de suscripciones para las suscripciones de IoT que estén involucradas en servicios de IoT críticos (por ejemplo, para las suscripciones asociadas a la atención médica). Estos servicios no se deben desconectar arbitrariamente.
- Los operadores de red deben identificar las UICC utilizadas para servicios de IoT a partir de UICC tradicionales utilizadas para proporcionar servicios tradicionales

y, si así lo requiere el proveedor de servicios de IoT, segregarlas adecuadamente.

- Si las UICC utilizadas para los servicios de IoT están separadas de las UICC utilizadas para los teléfonos celulares tradicionales, esto proporciona una base para una gestión más segura y eficiente de las suscripciones asociadas a IoT por parte del operador de red, que de otra manera sería más compleja. Por ejemplo, un operador de red podría considerar usar un HLR/HSS adicional y diferente para dispositivos periféricos que tengan una vida útil larga y así estaría mejor configurado para soportar estos UICC durante un período de tiempo muy largo (es decir, muchos años).

5.1.1 Suministro y Gestión de las UICCs

5.1.1.1 Gestión Remota de las UICCs (OTA)

Los dispositivos IoT periféricos no son físicamente accesibles en algunos escenarios. Para poder realizar cambios en la UICC de forma remota, la gestión OTA de una UICC debe ser compatible y soportada por el operador de red. Los mecanismos de seguridad OTA UICC deben seguir las últimas especificaciones ETSI [1] [2] y 3GPP [3] y utilizar el nivel de seguridad más apropiado para el servicio de IoT en concreto.

Los dispositivos IoT periféricos deben admitir los comandos APDU necesarios reconocidos por la UICC para garantizar que la ejecución del comando OTA de UICC tenga éxito.

5.1.1.2 UICC no extraíble

El operador de red debe proporcionar UICCs no extraíbles, es decir que debe utilizar uno de los encapsulados (factores de forma para máquinas) definidos en los estándares de las UICC) para los servicios de IoT, donde el modelo de amenaza para estos servicios sugiere que el dispositivo IoT periférico puede ser vulnerable a la manipulación física. Se deben aplicar medidas de seguridad adicionales para poder detectar y reaccionar ante tal amenaza.

5.1.1.3 Gestión Remota de las UICCs Embebidas (eUICCs)

El operador de red debe proporcionar una gestión remota segura de las UICCs embebidas y no extraíbles (es decir, eUICCs) para los servicios de IoT que requieren que los dispositivos periféricos estén instalados en ubicaciones remotas o de difícil acceso.

Por ejemplo, para los proveedores de servicios IoT que necesitan administrar una gran cantidad de eUICCs integrados en dispositivos periféricos de los cuales no es el dueño y no puede acceder fácilmente a estos (por ejemplo, dentro de un automóvil en una central de comunicaciones y servicios multimedia).

Normalmente, los operadores utilizan las Plataformas de gestión de la conectividad IoT para supervisar y controlar los servicios de comunicación ofrecidos a los dispositivos IOT a través de las (e)UICCs.

El operador de red debe soportar una plataforma de este tipo que sea compatible con la especificación técnica de la arquitectura de aprovisionamiento remoto de la GSMA para eUICCs [7].

5.1.1.4 Servicios Basados en UICC

Un operador de red puede proporcionar a un proveedor de servicios de IoT, servicios basados en UICCs. Esto hace posible que el proveedor de servicios de IoT use UICCs como una plataforma segura y resistente a alteraciones para sus Servicios de IoT. Dichos servicios basados en UICCs generalmente se desarrollan en JavaCard™ y son interoperables con todas las tarjetas UICC compatibles con JavaCard™. Un ejemplo de una aplicación de este tipo para un dispositivo periférico IoT podría ser la supervisión y la generación de informes de calidad de red. La resistencia a la manipulación provista por la plataforma UICC es una característica muy valiosa para los dispositivos IoT periféricos a los cuales los atacantes/hackers tangan un fácil acceso (en lugares sin supervisión, por ejemplo). Sacar provecho y utilizar una UICC como un elemento seguro común para todas las partes interesadas también puede hacer que los dispositivos periféricos IoT seguros se vuelvan más rentables.

La UICC también se puede usar para el almacenamiento, a prueba de manipulaciones, de datos confidenciales para los Servicios de IoT, incluidas las claves de seguridad controladas por el proveedor de servicios de IoT. ETSI TS 102 225 [1] aprovecha la función de gestión confidencial de contenidos en tarjetas de la especificación de las tarjetas existente en la plataforma global (“Global Platform”) para permitir a los proveedores de servicios de IoT gestionar de forma independiente su propio dominio de seguridad en un UICC.

Un proveedor de servicios de IoT o un operador de red puede solicitar al proveedor de UICCs que cree dichos dominios de seguridad dentro de las UICCs. El emisor de la tarjeta UICC debe asegurarse de que esté protegida por claves de seguridad adecuadas y el dispositivo IoT periférico pueda ejecutar los comandos APDU necesarios para acceder a ella y a los dominios incluidos en la tarjeta.

Además, la UICC también podría usarse para cifrar (utilizando sus claves almacenadas de forma segura) y enviar contenido confidencial para servicios de IoT, o proporcionar servicios de seguridad para aplicaciones basadas en dispositivos periféricos a través de servicios como Open Mobile API [4] o oneM2M TS-0003 [31].

5.1.1.5 Fabricación y Aprovisionamiento Seguro de una UICC

Un operador de red debe obtener sus UICCs de fabricantes cuyos procesos de fabricación y aprovisionamiento estén acreditados de acuerdo con el Esquema de Acreditación de Seguridad de la GSMA (SAS) [16].

5.2 Autenticación de Red y Algoritmos de Encriptación

Esta sección contiene recomendaciones y mejores prácticas para la autenticación de red y el cifrado de enlaces para diferentes redes WAN.

El operador de red debe implementar algoritmos de autenticación de red que cumplan con las expectativas para toda la vida útil de los dispositivos periféricos del proveedor de servicios de IoT.

Los operadores de red proporcionan varios tipos de servicios de comunicación que pueden ser utilizados por un servicio IoT para sus datos, como la utilización de las siguientes portadoras: USSD, SMS y/o conectividad de datos IP. Para los fines de este documento, solo se analiza la conectividad de datos IP, ya que es la forma de servicio de comunicación más utilizada por los Servicios de IoT en la actualidad.

Muchos servicios existentes de IoT utilizan USSD y SMS, por lo que cabe destacar que USSD y SMS tienen capacidades de soporte a la seguridad limitadas en comparación con la conectividad de datos IP. En general, el tráfico de USSD y SMS no están protegidos de forma criptográfica en las comunicaciones -extermo a extremo- por defecto en los servicios ofrecidos por los operadores. Los mecanismos de protección criptográfica para garantizar la confidencialidad y la integridad no están disponibles para los mensajes SMS. Los proveedores de servicios de IoT que usan USSD o SMS para su comunicación deben ser conscientes de las vulnerabilidades asociadas con USSD y SMS y, cuando sea posible, implementar un cifrado adicional en la capa de servicio.

5.2.1 Seguridad de los sistemas GSM / GPRS (2G)

Los operadores de red que proporcionan redes GSM / GPRS deben:

- Usar un cifrado de secuencia A5/3 de 128 bits como mínimo para proteger el enlace entre el dispositivo periférico IoT y la estación base. Los operadores de red deben evitar A5/1 y A5/2 o el uso de enlaces no encriptados cuando sea posible.
- Usar el algoritmo de autenticación MILENAGE. Los operadores de red deben evitar COMP128-1 y COMP128-2. Además deben considerar la compatibilidad con el algoritmo de autenticación TUAK
- Tomar las medidas apropiadas para abordar y mitigar los ataques de estaciones base falsas.

En sistemas GSM/GPRS, los dispositivos periféricos NO antentican a la red a la que se conectan, en cambio la red si que autentica a los dispositivos . Por lo tanto, se recomienda el cifrado de extremo a extremo en la capa de servicio cuando se utilizan sistemas GSM/GPRS. Se debe tener en cuenta las capacidades de procesamiento en la práctica, las limitaciones de los dispositivos periféricos y las restricciones de ancho de banda de la red en las soluciones proporcionadas como servicios de IoT.

En los sistemas GSM/GPRS, el túnel GTP entre SGSN y GGSN creado a través de la red GRX no está encriptado. El operador de red debe garantizar la seguridad de este enlace asegurando que la red GRX se administre como una red privada.

5.2.2 Seguridad de los Sistemas UMTS (3G)

Las redes UMTS permiten la autenticación mutua, donde el dispositivo periférico no solo es autenticado por la red, sino que también la red es autenticada por el dispositivo.

Los operadores de red que proporcionan redes UMTS deben admitir la autenticación MILENAGE y el algoritmo de generación de claves. Los operadores de red deben admitir los algoritmos de cifrado de confidencialidad e integridad de Kasumi.

Los operadores de red deben considerar la compatibilidad con el algoritmo de autenticación TUAK.

5.2.3 Seguridad de los Sistemas LTE (4G)

Los operadores de red que proveen una red LTE deben soportar el algoritmo de autenticación MILENAGE. Los operadores de red deben soportar los algoritmos de encriptación LTE EEA1, EEA2 o EEA3.

Los operadores de red deben considerar la compatibilidad con el algoritmo de autenticación TUAK.

Se recomienda a los operadores de red que revisen el documento técnico de la GSMA "Seguridad Inalámbrica en Redes LTE" [30].

5.2.4 Seguridad de Redes de Área Extendida de Baja Potencia

Varios operadores de red han implementado varias tecnologías de red de área extendida de baja potencia (LPWA). Se puede encontrar una lista completa y actualizada de las implementaciones de redes LPWA en el sitio web de GSMA: www.gsma.com/iot

Las guías de implementación para NB-IoT [34] y LTE-M [35] se pueden encontrar en el portal de la GSMA para ayudar a garantizar el despliegue consistente con las normas de estas tecnologías desde la perspectiva de la red y del dispositivo.

En mayo de 2017, los analistas de seguridad de la información Franklin Heath publicaron un informe independiente titulado "Comparación de Seguridad Tecnológica LPWA" [33] que compara y contrasta las características de seguridad de cinco diferentes tecnologías de red de área extendida de baja potencia (LPWA) para varios casos típicos de uso de IoT como la agricultura Inteligente, el alumbrado público inteligente, los detectores de humo, los contadores de agua y contadores inteligentes para la energía/electricidad. Evalúa las características de seguridad de tres tecnologías de IoT móvil estandarizadas 3GPP que operan en espectro con licencia, LTE-M, NB-IoT y EC-GSM-IoT, así como las tecnologías de espectro sin licencia LoRaWAN y Sigfox. El informe se puede descargar desde: https://goo.gl/JIOlr6 [33].

El informe sostiene que las organizaciones deben determinar qué nivel de seguridad necesitan además de otras consideraciones como el costo, la duración prolongada de la batería y la cobertura de la red cuando se considera una solución LPWA. Resalta cómo las necesidades de seguridad de IoT son impulsadas principalmente por cuestiones de privacidad y seguridad, y cualquier implementación que utilice tecnologías LPWA debe estar sujeta a una evaluación de riesgos de seguridad utilizando herramientas como la evaluación de seguridad GSMA para IoT [32].

Algunos factores importantes para la seguridad de la red destacados en el informe que deberían considerarse como parte de dicha evaluación incluyen:

- Ancho de banda, incluidas las velocidades de datos máximas de enlace descendente y enlace ascendente: esto puede limitar las características de seguridad que pueden ser admitidas por la red LPWA o implementadas en la capa de aplicación.

- Rendimiento diario del enlace descendente y del enlace ascendente: los dispositivos LPWA generalmente no transmiten ni reciben datos todo el tiempo, lo que puede afectar a las funciones de seguridad, como en las actualizaciones de seguridad de manera inalámbrica.
- Autenticación para dispositivos, suscriptores y la red: la conectividad de red segura requiere que los diferentes actores en un servicio IoT se autentiquen entre sí, como el dispositivo, el suscriptor y el proveedor de la red. La tecnología de red debe protegerse contra la posible "falsificación" de estos actores por parte de entes o hackers malintencionados.
- Confidencialidad de los datos: el cifrado generalmente se usa para evitar que los datos sean interceptados por un atacante. La confianza en esto se puede aumentar al establecer seguridad de extremo a extremo en la capa de aplicación.
- Aprovisionamiento de claves: las técnicas criptográficas para autenticación, confidencialidad e integridad dependen de que las claves criptográficas se compartan de forma segura entre las partes.
- Equipo certificado: en muchos mercados, existen requisitos legales para que los dispositivos con transmisión por radio cuenten con una aprobación o certificación determinada antes de ser vendidos. Esta es una oportunidad para verificar las características de seguridad.
- Red IP: el uso de IP puede abrir la posibilidad de ataques a dispositivos desde Internet y se deben considerar las características de seguridad IP.

El informe concluye que varias características de seguridad potencialmente importantes de las tecnologías LPWA son de alguna manera opcionales, ya que pueden ser habilitadas directamente por el operador de red, o dependen de otras elecciones hechas por el operador de red. Los operadores de red deben asegurarse de conocer las consecuencias con respecto a la seguridad de las elecciones que realizan en la configuración de su red y asegurarse de que las opciones disponibles en su red se comuniquen claramente a sus clientes. Algunas opciones existen también para tener un control del fabricante del dispositivo (como si se incluye un elemento de seguridad fijo-soldado como un eUICC) y se aplica el mismo deber de comunicar las implicaciones y requisitos de seguridad de esto a sus clientes.

Consideraciones específicas de seguridad cuando se utiliza una tecnología LPWA incluyen:

Para todas las tecnologías de red LPWA,

- Si una capa de red IP se implementa sobre la capa de enlace.
- Si un elemento seguro está presente, y si es así, si es extraíble.
- En qué medida se garantiza la integridad de los datos.
- Si los algoritmos o las longitudes de clave admitidas por la tecnología están en la lista negra para la prácticas actuales de seguridad o son obsoletas (como las claves de cifrado de 64 bits para GPRS).

Para las Tecnologías de red LPWA definidas por 3GPP (es decir, NB-IoT y LTE-M),

- Si se admite la gestión remota del aprovisionamiento de las SIM (“Remote SIM Provisioning-RSP “).

- Qué algoritmos de integridad (EIAx / GIAx) y algoritmos de confidencialidad (EEAx / GEAx) son implementados y permitidos.

Para LoRaWAN:

- Si se implementa ABP (activación por personalización) o OTAA (activación inalámbrica) y para OTAA si se puede compartir una AppKey entre dispositivos.

Para SigFox:

- Al usar la red SigFox, se debe tener en cuenta que el cifrado del Payload es opcional, pero está disponible por defecto. Por lo tanto, se debe utilizar un chip criptográfico certificado por Sigfox para habilitar el cifrado AES 128 y mantener los datos confidenciales en las transmisiones inalámbricas.

Para todos los dispositivos LPWA:

- Qué forma (si ha existido alguna) de certificación de seguridad se ha llevado a cabo.

5.3 Seguridad de las Redes Fijas

Las recomendaciones para la configuración predeterminada de redes Wifi bajo el control de un operador de red o un proveedor de servicios IoT incluyen la autenticación EAP-SIM [28] o EAP-AKA [27] y pueden basarse en el marco EAP de UICC de ETSI TS 102 310 [8].

5.4 Priorización del Tráfico

Los operadores de red pueden proporcionar niveles de calidad de servicio apropiados para el servicio de IoT que se proporciona.

5.5 Seguridad de la Red Troncal

Los estándares 3GPP que especifican GSM, UMTS y LTE no requieren el uso de enlaces a la red troncal cifrados. Además, la RAN y la compartición de la red troncal entre diferentes operadores de red pueden introducir vulnerabilidades de seguridad adicionales.

El operador de red debe implementar el cifrado de retorno para las redes GSM, UMTS y LTE tanto para el tráfico de datos del usuario final como del tráfico de datos perteneciente a la capa de señalización.

5.6 Itinerancia

Los operadores de red pueden proporcionar a los proveedores de servicios de IoT una huella internacional en sus redes celulares mediante el uso de servicios en itinerancia.

Las redes que soportan itinerancia pueden ser vulnerables a distintas brechas de seguridad debido a la relativa transparencia de las funciones de interfuncionamiento de SS7/Diameter utilizadas para conectar las redes locales con aquellas donde se proporciona itinerancia. Esto es de particular relevancia para los servicios IoT debido a la proporción potencialmente alta de dispositivos IoT periféricos que residirán en redes intenacionales en itinerancia. Hay algunas razones para el alto porcentaje de dispositivos periféricos itinerantes. En primer

lugar, muchos dispositivos periféricos se fabrican en un solo lugar y se distribuyen globalmente. Por lo tanto, en muchos casos, la sustitución de una UICC en dichos equipos no es una solución práctica o no es posible en el caso de una UICC embebida. En segundo lugar, en muchos casos, el estado en itinerancia del dispositivo es preferible a utilizar la conectividad local, debido a la cobertura global que puede ofrecer el hecho de tener varias redes con conectividad asegurada en itinerancia. La formación de alianzas globales entre operadores con UICCs globales y acuerdos dedicados de itinerancia IoT facilitan el estado en los dispositivos de “itinerancia permanente”, donde lo permita la legislación local.

Los operadores de red deben considerar cómo proteger sus HLR y VLR contra los ataques de denegación de servicio (incluidos los ataques DoS involuntarios), con respecto a las solicitudes de fuentes no autorizadas y contra el uso indebido de los servicios de "control de itinerancia".

La itinerancia es posible gracias a los protocolos de señalización entre operadores de red que se comparten entre los principales elementos de las redes móviles:

1. Entre el VLR o el SGSN en la red itinerante (visitada) y el HLR en la red doméstica: el protocolo MAP (parte de aplicación móvil) (para redes CDMA, IS41 es similar a MAP).
2. Entre el MME en la red itinerante LTE y el HSS en la red LTE doméstica: el protocolo Diameter (ciertas variantes como S6a).
3. Entre el SGSN / S-GW en la red visitada y GGSN / P-GW en la red doméstica: la transferencia de datos itinerantes usando GTP (Protocolo de túnel GPRS).

Esta sección se concentrará en los problemas de seguridad en itinerancia relacionados con los Servicios de IoT. Los problemas generales de seguridad en itinerancia están cubiertos por el grupo GSMA FASG (“Fraud and Security Group”) y sus subgrupos. Por lo tanto, cuestiones como el doble registro en itinerancia, recibidas de dos VLR diferentes ubicados en diferentes países (un escenario clásico de fraude en itinerancia) están fuera del alcance de este documento.

5.6.1 Tormentas y Ataques de Señalización en Itinerancia

IoT tiene requisitos de seguridad adicionales con respecto a la red móvil, debido a la naturaleza diferente de los dispositivos periféricos y al alto potencial de que los servicios sean críticos. Cómo la red móvil da servicios a una gran cantidad de dispositivos periféricos, está expuesta a tormentas de señalización. Un ataque de denegación de servicio malintencionado es sólo una de las razones para que se registren tormentas de señalización. Un problema en la red eléctrica, en la cobertura de la red celular o un desastre natural dentro de un área determinada de una red celular puede ser común en muchos países y, por lo tanto, puede causar problemas muy parecidos a las tormentas de señalización. Todos los contadores inteligentes itinerantes y otros dispositivos periféricos ubicados en esa área intentarán “moverse” a otra red itinerante, de forma simultánea. Tal escenario crea una tormenta de señalización e impone un riesgo severo en el HLR/HSS local. 3GPP TS 23.122 [9] define un servicio de restricción de acceso extendido (EAB) para abordar tales escenarios: los operadores de red pueden restringir el acceso a la red a los dispositivos periféricos configurados para EAB, además de los mecanismos de control de acceso comunes y específicos de dominio. La configuración de EAB se puede realizar en la UICC o en el dispositivo periférico. Las pasarelas de seguridad de red deben configurarse

para evitar ataques intencionados de denegación de servicio y prohibirlos, descartándolos completamente si se producen.

También puede ser necesario que el operador de red local (junto con el proveedor de servicios de IoT) distinga entre dispositivos periféricos de baja prioridad y dispositivos periféricos críticos. Por ejemplo, puede ser necesario que los dispositivos de un servicio de salud continúen manteniendo el servicio bajo tormentas de señalización y ataques de denegación de servicio. Puede haber una necesidad de que la red rechace el registro de dispositivos periféricos itinerantes de "baja prioridad" en condiciones de tormenta de señalización, pero debe permitir el registro de dispositivos periféricos de "alta prioridad". El mecanismo de rechazo implementado puede ir acompañado de un temporizador de retroceso para ayudar al dispositivo periférico a conectarse en un nuevo intento de registro posterior, después de la tormenta de señalización.

La recomendación general sería que los operadores de red rastreen todos los mensajes itinerantes recibidos de las redes locales de los socios de itinerancia. Además de bloquear mensajes de redes locales no autorizadas o falsificadas de los socios de itinerancia, existe la necesidad de filtrar los mensajes de acuerdo con la prioridad del dispositivo periférico. En ataques de tormenta de señalización o denegación de servicio, existe la necesidad de permitir mensajes desde dispositivos periféricos críticos con alta prioridad o rechazar mensajes desde dispositivos periféricos no críticos. Se requieren métodos de rechazo para posponer los intentos de registro y otras actividades durante un período determinado.

5.6.2 Manejo de la Itinerancia Basada en la Seguridad (SoR)

Otro caso de uso para la seguridad que puede ser llevado a cabo por un operador de red es el manejo y control de la itinerancia (SoR) de dispositivos IoT periféricos por razones de seguridad. El rechazo de una actualización de localización sin un temporizador de retroceso ocasiona que el dispositivo periférico vuelva a intentarla y, finalmente, intente registrarse desde una red itinerante (visitada) diferente. Otro método para SoR es a través de OTA, usando listas de itinerancia en la UICC preferidas y otros parámetros almacenados en la UICC. Las capacidades de actualización OTA de la UICC permiten a la red local actualizar las listas de redes en itinerancia preferidas, que determinan la prioridad de las redes durante el proceso de selección de una red en itinerancia. La red local también puede actualizar la memoria del dispositivo periférico con la nueva lista y hacer que el dispositivo periférico busque una nueva red al instante.

En caso de que se detecte un riesgo de seguridad en una red visitada específica, la red local puede decidir transferir sus dispositivos periféricos itinerantes salientes a otra red visitada, utilizando el mecanismo SoR. Dicha transferencia activa de dispositivos periféricos se puede realizar en el próximo intento de registro del dispositivo periférico, o de manera ad-hoc utilizando los servicios de la SIM por OTA. Se puede detectar un riesgo de seguridad relacionado con una red visitada específica si un problema es reportado por un número relativamente alto de dispositivos periféricos itinerantes en esa red, o información recibida por otras vías.

5.6.3 Denegación de Servicio en Itinerancia de Datos

Los ataques de denegación de servicio no están limitados al espacio de señalización para soportar la movilidad de los dispositivos, la itinerancia de datos también es un campo

potencial para las tormentas de señalización. Actualmente, la mayoría de los datos en itinerancia se enrutan desde la red visitada SGSN (S-GW en el caso de LTE) a la red doméstica GGSN (P-GW para LTE). El caso de LBO (“Local Breakout”), donde los datos se enrutan desde la red visitada directamente a internet rara vez se implementa. La situación en el futuro podría cambiar, debido a las regulaciones internacionales, como en el caso de la regulación de la UE que permitió el servicio LBO desde julio del 2014, LTE y especialmente VoLTE (Voz sobre LTE), donde las llamadas de voz realizadas en la red en itinerancia pueden ser manejadas por un servicio local en la P-GW (como en el caso hoy en día con las llamadas de voz regulares con conmutación de circuitos realizadas en una red visitada).

Las tormentas de señalización pueden ocurrir cuando el GGSN/P-GW local se llena con solicitudes de nuevas sesiones de datos. El protocolo GPRS crea un túnel seguro entre el dispositivo periférico y el GGSN, y la solicitud de una nueva sesión (“Create-PDP-Context”) da como resultado la configuración de un túnel y la asignación de una dirección IP al dispositivo periférico. Cuando los dispositivos IoT periféricos no se comportan de manera personalizada, pueden generar ráfagas de solicitudes para nuevas sesiones de datos como se señaló anteriormente. Los ataques de Denegación de Servicio pueden ser generados por un número relativamente pequeño de dispositivos periféricos, creando múltiples solicitudes para nuevas sesiones de datos en paralelo. Los servidores GGSN/P-GW tienen una capacidad limitada y deben estar protegidos contra dichas tormentas.

Para evitar las tormentas de señalización, los operadores de red pueden, según una política de seguridad, evitar que ciertos dispositivos se conecten a su red cambiando el perfil de comunicación de los dispositivos afectados o implementando políticas de seguridad dentro del núcleo de la red de paquetes.

Los dispositivos periféricos críticos también deben poder acceder a los servicios de red bajo ataques de denegación de servicio, mientras que las solicitudes de dispositivos periféricos de menor prioridad se posponen durante un determinado período de tiempo.

5.7 Gestión de Dispositivos Periféricos y Pasarelas

Cabe señalar que las medidas de seguridad hardware y software, incluidas las consolas de administración de configuración local para dispositivos periféricos y dispositivos tipo pasarela, están fuera del alcance de este documento. Esta sección cubre aspectos relacionados con la red. Consulte el documento de GSMA "Descripción general de los lineamientos de seguridad IoT de la GSMA CLP.11" [11] para ver las pautas de seguridad relacionadas con los dispositivos periféricos.

5.7.1 Gestión de Dispositivos Periféricos

Los operadores de red pueden ofrecer a los proveedores de servicios de IoT capacidades básicas para configurar y administrar de manera segura los dispositivos periféricos y sus suscripciones a las redes celulares, adoptando algunos de los principios y tecnologías desarrolladas para la administración de dispositivos móviles "tradicionales". Los dispositivos IoT periféricos que usan una UICC para registrarse y conectarse a una red celular se pueden administrar usando las plataformas de gestión de la conectividad, las plataformas de gestión de dispositivos y las plataformas de gestión de las UICC que existen en la actualidad.

Además de esta capacidad básica de gestión de dispositivos periféricos, la plataforma de servicios de IoT puede proporcionar funciones de administración de dispositivos periféricos más específicas y complejas.

A continuación, se muestra un ejemplo de una arquitectura típica de gestión de dispositivos periféricos que se ha tomado de los principios de comunicación ETSI M2M [19].

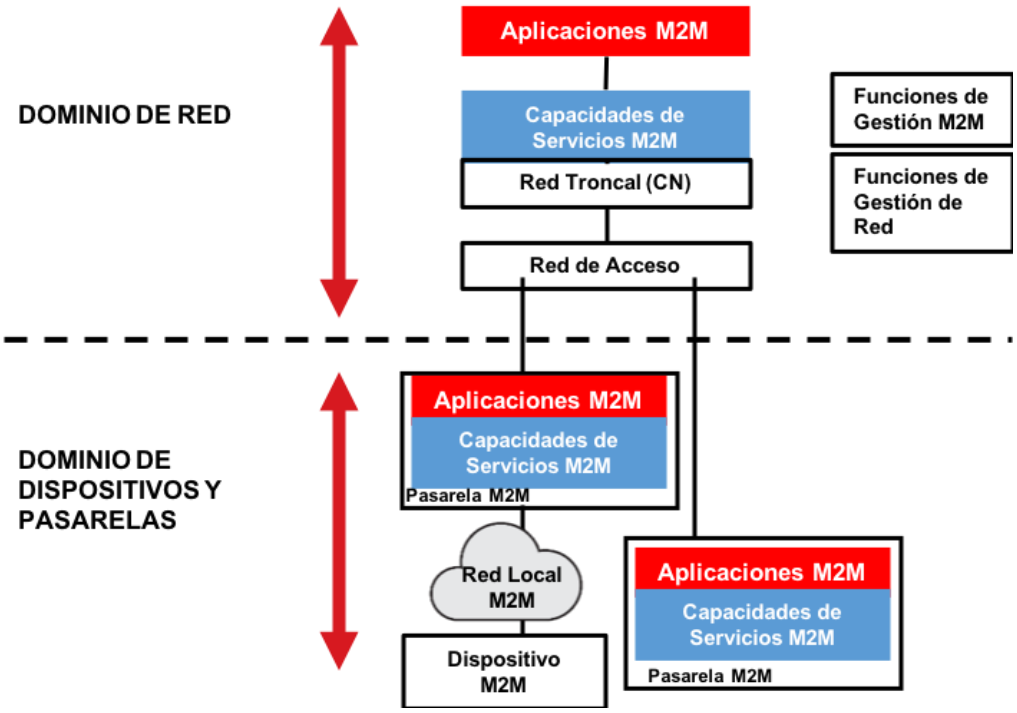

Figura 3– Arquitectura de Alto Nivel para la Gestión de Dispositivos M2M

Los bloques azules indican lo que tradicionalmente es administrado por las plataformas de gestión de dispositivos existentes en el operador de Red y los bloques rojos indican los componentes de servicio que son administrados por la Plataforma de Servicios de IoT.

Los operadores de red pueden llevar a cabo algunas de las funciones de gestión de dispositivos indicadas en rojo a petición del proveedor de servicios IoT.

5.7.2 Gestión de Pasarelas

El uso de los dispositivos tipo pasarela potencialmente introduce un nivel más de complejidad en la gestión de dispositivos para el Proveedor de Servicios IoT. En algunos casos, el dispositivo IoT pasarela puede ser un dispositivo basado en una UICC que se conecta a una red celular, en otros casos se usan líneas fijas cableadas.

La pasarela debe ser un objeto gestionado, para que pueda ser supervisada y actualizada con un nuevo firmware o software en caso de necesidad. Deben utilizarse protocolos para proporcionar actualizaciones seguras de firmware y software y mecanismos seguros de integración de sistemas y funciones para aplicar niveles de seguridad adecuados a la interconexión de la pasarela con la red troncal.

Los operadores de red pueden proporcionar y administrar pasarelas seguras en nombre del proveedor de servicios de IoT, que permiten que los dispositivos periféricos se conecten de forma segura de la manera que mejor se integre con los mecanismos de seguridad de la red de área extendida (WAN) del operador de red.

Las pasarelas que se conectan mediante red fija se pueden gestionar de forma remota utilizando el protocolo de gestión de red de área extendida del equipo de cliente (CPE) aplicando el protocolo de Broadband Forum TR-069 [20].

Las pasarelas que se conectan usando la conectividad de una red celular se pueden administrar remotamente usando los protocolos “OMA Device Management” (DM) y el protocolo de administración de actualización de firmware (FUMO) [5] [6].

5.7.3 Listas Negras de Dispositivos Periféricos IoT

Los operadores de red deben implementar una lista negra para los dispositivos periféricos IoT y conectarse a la base de datos del registro central de identidad de equipos (CEIR) de la GSMA. El CEIR es una base de datos central, administrada por la GSMA, que contiene los IMEIs asociados con dispositivos periféricos robados o perdidos, y con dispositivos a los que no se debe otorgar acceso a la red. Una vez que se ingresa un IMEI en el CEIR, el dispositivo periférico que contiene el IMEI quedará en la lista negra de todos los operadores de red que toman esos datos e implementan listas negras locales basadas en el uso de los registros de identidad de equipos (EIR).

Los operadores de red también pueden implementar para dispositivos concretos una “lista gris” para permitir la suspensión temporal de la conectividad de estos dispositivos "sospechosos" mientras el operador de red investiga la naturaleza de dichos dispositivos antes de incluirlos en la lista negra. Cabe señalar que para los servicios críticos, como aquellos destinados a la atención médica, bloquear un IMEI puede no ser deseable o posible. Es importante que los operadores de red entiendan claramente los detalles y funcionalidades de los dispositivos periféricos conectados a su red en la medida en que se pueda discernir la verdadera aplicación (o Host) de un dispositivo periférico. Los dispositivos periféricos que aprovechan el IMEI emitido a un proveedor de módulos de comunicaciones deben soportar en uso de los informes de identificación del host del dispositivo (“Device Host Identify Report”), que es una capacidad que permite que el dispositivo periférico facilite la información del host al operador de red. Como se utiliza el informe arriba mencionado del Host de dispositivos se describe en los “Lineamientos de Eficiencia de la Conectividad de la GSMA” [17].

5.8 Otros Servicios Relacionados con la Seguridad

5.8.1 Servicios en la Nube / Gestión de Datos

Los operadores de red pueden suministrar a los clientes plataformas de servicios de IoT alojadas en la nube para implementar los servicios de IoT y también proporcionar servicios para almacenar y administrar los datos producidos por dichos servicios.

Los operadores de red pueden suministrar una nube privada o una infraestructura de nube compartida según los requisitos del proveedor de servicios de IoT.

5.8.2 Seguridad Basada en el Análisis Estadístico de Datos

Los operadores de red pueden proporcionar servicios de análisis de datos e inspección profunda de paquetes para identificar amenazas y anomalías en los datos generados por los servicios de IoT. Un ejemplo podría ser que un operador de red podría realizar inspecciones profundas en los paquetes de las comunicaciones periódicamente para cadenas de datos o caracteres específicas como números de seguridad social y coordenadas de GPS que podrían sugerir que dicha información no está protegida adecuadamente y alertar al proveedor de servicios de IoT de que la información podría estarse filtrando al exterior sin protección.

Esta es una ventaja para IoT porque los dispositivos y servicios en dispositivos ligeros IoT no pueden proporcionar esta funcionalidad por sí mismos. Los operadores de red pueden proporcionar a los proveedores de servicios de IoT visibilidad del estado de la seguridad en sus productos, amenazas y ataques identificados, así como una verificación general de seguridad. Estos servicios de introspección son vitales para garantizar que las amenazas no se cuelan "dentro de la tubería", particularmente cuando los servicios de datos están encriptados. Los servicios brindados incluyen:

- Uso de detección de anomalías y aprendizaje automático para detectar problemas.
- Construir sistemas de protección contra intrusos haciendo diagnósticos de dispositivos periféricos en tiempo real.
- Proporcionar un tablero (”dashboard”) para visualizar e identificar fácilmente las anomalías.
- Proporcionar medios automatizados para marcar y bloquear conexiones sospechosas.
- Proporcionar análisis de amenazas de servicios implementados en la nube.

5.8.3 Gestión Segura de la Red

Los operadores de red pueden proporcionar redes que se gestionan y mantienen de forma segura, ofreciendo:

- Canales de respaldo en caso de fallos en el enlace físico o lógico
- Identificar fallos de enlace como evidencia de una violación potencial de seguridad
- Implementar políticas de itinerancia que afectan a la seguridad y a la integridad
- Gestión de las UICCs/SIMs
- Gestión segura de la información
- Membresía en la CERT y participación en el intercambio de información sobre amenazas para mitigar y prevenir futuros ataques.
- Protección contra ataques de denegación de servicio
- Realizar escaneos de seguridad periódicos y evaluaciones de vulnerabilidad
- Gestión y manejo de requisitos regulatorios relacionados con la seguridad de la red
- Restringir las opciones de comunicación al mínimo estricto requerido para un determinado servicio de IoT.

5.8.4 Plataforma Segura de Gestión de la Conectividad IoT

Los operadores de red utilizan cada vez más la infraestructura de redes troncales y OSS dedicadas para administrar las suscripciones de IoT y los planes de precios de una manera eficiente y escalable. El acceso a dicha infraestructura a menudo está disponible para el

cliente comercial del operador (es decir, un proveedor de servicios de IoT) para que pueda auto-gestionar sus suscripciones (que incluiría la activación del servicio, la suspensión, etc., individualmente o en bloque).

Las pautas de la plataforma de servicios ofrecidas en CLP 12 "Lineamientos de seguridad de IoT para el Ecosistema de servicios de IoT" [26] ofrecen una valiosa guía que puede beneficiar al operador de red que brinda soporte a las plataformas de gestión de conectividad IoT. Estas pautas contienen las siguientes recomendaciones:

- Los operadores de red deben asegurarse de que el acceso es seguro al portal web de la Plataforma de gestión de la conectividad IoT, que puede ser alojado en el operador de red o en la nube, utilice para esto un cifrado "mejor de su clase" según las últimas guías publicadas de organizaciones como NIST [24] y ECRYPT2 [25].
- Los operadores de red deben asegurarse de que el acceso al portal web de la Plataforma de gestión de la conectividad IoT haga uso de los procedimientos estándar de "mejores prácticas" para la creación, actualización y restablecimiento de contraseñas.

5.8.5 Gestión de Certificados

Los operadores de red pueden proporcionar servicios de gestión de certificados X.509.

5.8.6 Autenticación Multifactorial

Los servicios de autenticación multifactorial generalmente requieren que un usuario se autentique usando un token electrónico además de un nombre de usuario y contraseña. Como tal, la autenticación de factores múltiples puede proporcionar protección adicional contra el acceso a los servicios de IoT de usuarios no autorizados.

La iniciativa Mobile Connect de la GSMA [12], junto con OpenID Connect [21], FIDO [22] y ETSI MSS [23] son ejemplos de habilitadores de autenticación multifactorial que pueden permitir a un proveedor de servicios de IoT obtener autenticación e información adicional de sus usuarios finales. El usuario final en este contexto es un ser humano que puede proporcionar información a una plataforma de servicios de IoT para habilitar diferentes niveles de seguridad. Los ejemplos incluyen meter un PIN y proporcionar una firma biométrica, por ejemplo.

Si bien la mayoría de las soluciones de autenticación multifactorial se utilizan actualmente para habilitar los servicios tradicionales de smartphones, tales tecnologías podrían aplicarse a servicios de IoT que requieren la garantía de autorización por un usuario en concreto para ciertas tareas como realizar una operación de conexión a la red, actualización de software o un restablecimiento completo del dispositivo.

Por ejemplo, al usar autenticación multifactorial, se podría usar una identidad de la red celular (usuario) además de la intrínseca a un dispositivo pasarela dentro de un automóvil conectado. En este caso de uso, la infraestructura de autenticación de múltiples factores podría actuar como una capa de autorización adicional para que los ocupantes del automóvil tengan acceso a los servicios de información y entretenimiento y pago proporcionados dentro del automóvil.

Anexo A Gestión del Documento

A.1 Historia del Documento

Versión	Fecha	Breve Descripción de los Cambios	Aprobación Autoridad	Editor / Compañía
1.0	08-Feb-2016	New PRD CLP.14	PSMC	Ian Smith GSMA
1.1	17-Nov-2016	Se agregaron referencias al esquema de evaluación de seguridad de IoT de GSMA. Correcciones editoriales menores.	PSMC	Ian Smith GSMA
2.0	30 Sep 2017	Cambios Importantes para agregar referencias a	IoT Security Group	Rob Childs GSMA

A.2 Otra Información

Tipo	Descripción
Dueño del Documento	GSMA IoT Programme
Contacto	Rob Childs – GSMA

Es nuestra intención proporcionar un producto de calidad (documento) para su uso. Si encuentra algún error u omisión, contáctenos con sus comentarios. Puede notificarnos a esta dirección: prd@gsma.com.

Sus comentarios o sugerencias y preguntas son siempre bienvenidos.