Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1364

(03/2020)

SERIE X: REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

Aplicaciones y servicios seguros (2) – Seguridad de los sistemas de transporte inteligentes (STI)

Requisitos y marco de seguridad de la Internet de las cosas de banda estrecha

Recomendación UIT-T X.1364

RECOMENDACIONES UIT-T DE LA SERIE X

REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

REDES PÚBLICAS DE DATOS	X.1–X.199
INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.200–X.299
INTERFUNCIONAMIENTO ENTRE REDES	X.300–X.399
SISTEMAS DE TRATAMIENTO DE MENSAJES	X.400–X.499
DIRECTORIO	X.500–X.599
GESTIÓN DE REDES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS Y ASPECTOS DE SISTEMAS	X.600–X.699
GESTIÓN DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.700–X.799
SEGURIDAD	X.800–X.849
APLICACIONES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.850–X.899
PROCESAMIENTO DISTRIBUIDO ABIERTO	X.900–X.999
SEGURIDAD DE LA INFORMACIÓN Y DE LAS REDES	
Aspectos generales de la seguridad	X.1000–X.1029
Seguridad de las redes	X.1030–X.1049
Gestión de la seguridad	X.1050–X.1069
Telebiometría	X.1080–X.1099
APLICACIONES Y SERVICIOS CON SEGURIDAD (1)	
Seguridad en la multidifusión	X.1100–X.1109
Seguridad en la red residencial	X.1110–X.1119
Seguridad en las redes móviles	X.1120–X.1139
Seguridad en la web	X.1140–X.1149
Protocolos de seguridad (1)	X.1150–X.1159
Seguridad en las comunicaciones punto a punto	X.1160–X.1169
Seguridad de la identidad en las redes	X.1170–X.1179
Seguridad en la TVIP	X.1180–X.1199
SEGURIDAD EN EL CIBERESPACIO	
Ciberseguridad	X.1200–X.1229
Lucha contra el correo basura	X.1230–X.1249
Gestión de identidades	X.1250–X.1279
APLICACIONES Y SERVICIOS CON SEGURIDAD (2)	
Comunicaciones de emergencia	X.1300–X.1309
Seguridad en las redes de sensores ubicuos	X.1310–X.1339
Seguridad de las redes eléctricas inteligentes	X.1330–X.1339
Recomendaciones relacionadas con la PKI	X.1340–X.1349
Seguridad en la Internet de las cosas (IoT)	**X.1360–X.1369**
Seguridad en los sistemas de transporte inteligente (ITS)	X.1370–X.1379
Seguridad de tecnología de libro mayor distribuido	X.1400–X.1429
Seguridad de tecnología de libro mayor distribuido	X.1430–X.1449
Protocolos de seguridad (2)	X.1450–X.1459
INTERCAMBIO DE INFORMACIÓN DE CIBERSEGURIDAD	
Aspectos generales de la ciberseguridad	X.1500–X.1519
Intercambio de estados/vulnerabilidad	X.1520–X.1539
Intercambio de eventos/incidentes/heurística	X.1540–X.1549
Intercambio de políticas	X.1550–X.1559
Petición de heurística e información	X.1560–X.1569
Identificación y descubrimiento	X.1570–X.1579
Intercambio asegurado	X.1580–X.1589
SEGURIDAD DE LA COMPUTACIÓN EN NUBE	
Visión general de la seguridad de la computación en nube	X.1600–X.1601
Diseño de la seguridad de la computación en nube	X.1602–X.1639
Prácticas óptimas y directrices en materia de seguridad de la computación en nube	X.1640–X.1659
Aplicación práctica de la seguridad de la computación en nube	X.1660–X.1679
Otras cuestiones de seguridad de la computación en nube	X.1680–X.1699
COMUNICACIÓN CUÁNTICA	X.1700–X.1729

Para más información, véase la Lista de Recomendaciones del UIT-T.

Recomendación UIT-T X.1364

Requisitos y marco de seguridad de la Internet de las cosas de banda estrecha

Resumen

En la Recomendación UIT-T X.1364 se analizan posibles métodos de despliegue y casos de aplicación característicos de la IoT de banda estrecha (NB-IoT). Se especifican los riesgos y requisitos específicos que conlleva el despliegue de la NB-IoT se establece un marco de seguridad que pueden aplicar los operadores para proteger las nuevas aplicaciones de la tecnología NB-IoT.

Los avances actuales de la tecnología de las telecomunicaciones que tienen lugar en la actualidad en el campo de las comunicaciones móviles está transformando las pautas de comunicación entre personas, que pasan a realizarse entre personas y objetos, o entre objetos, y propicia, por ende, la inexorable evolución de la Internet de las cosas (IoT).

Las redes móviles celulares, caracterizadas por su amplia cobertura, movilidad y elevado grado de conectividad, así como por su capacidad para dar soporte a aplicaciones más sofisticadas, pasan a constituir la principal tecnología de interconexión de la IoT, en detrimento de otras tecnologías de comunicación de corto alcance, en particular Bluetooth y ZigBee.

La NB-IoT se basa en la utilización de tecnología de redes móviles celulares que utilizan un ancho de banda de sólo unos 180 kHz. Podría desplegarse directamente en redes del sistema mundial de comunicaciones móviles (GSM) o del sistema universal de telecomunicaciones móviles (UMTS), así como en redes de evolución a largo plazo (LTE), con objeto de reducir costos y facilitar su actualización.

Habida cuenta de su escasa disipación de energía, amplia cobertura, bajo costo y elevada capacidad, cabe esperar que los operadores comiencen a implantar la NB-IoT de forma generalizada, a fin de ofrecer una gran cantidad de aplicaciones en sectores industriales de índole diversa.

Como todas las nuevas tecnologías, la NB-IoT posee características propias que pueden conllevar problemas de seguridad. Con el fin de garantizar la seguridad de la implantación de la NB-IoT, así como la de sus aplicaciones, es necesario examinar los riesgos y requisitos de seguridad que guardan una relación específica con la NB-IoT, y establecer para esta un marco de seguridad general adecuado.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	ITU-T X.1364	2020-03-26	17	11.1002/1000/14088

Palabras clave

Banda estrecha, Internet de las cosas, marco de seguridad, requisitos de seguridad

* Para acceder a la Recomendación, sírvase digitar el URL http://handle.itu.int/ en el campo de dirección del navegador, seguido por el identificador único de la Recomendación. Por ejemplo, http://handle.itu.int/11.1002/1000/11830-en.

PREFACIO

La Unión Internacional de Telecomunicaciones (UIT) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones y de las tecnologías de la información y la comunicación. El Sector de Normalización de las Telecomunicaciones de la UIT (UIT-T) es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución 1 de la AMNT.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI.

NOTA

En esta Recomendación, la expresión "Administración" se utiliza para designar, en forma abreviada, tanto una administración de telecomunicaciones como una empresa de explotación reconocida de telecomunicaciones.

La observancia de esta Recomendación es voluntaria. Ahora bien, la Recomendación puede contener ciertas disposiciones obligatorias (para asegurar, por ejemplo, la aplicabilidad o la interoperabilidad), por lo que la observancia se consigue con el cumplimiento exacto y puntual de todas las disposiciones obligatorias. La obligatoriedad de un elemento preceptivo o requisito se expresa mediante las frases "tener que, haber de, hay que + infinitivo" o el verbo principal en tiempo futuro simple de mandato, en modo afirmativo o negativo. El hecho de que se utilice esta formulación no entraña que la observancia se imponga a ninguna de las partes.

PROPIEDAD INTELECTUAL

La UIT señala a la atención la posibilidad de que la utilización o aplicación de la presente Recomendación suponga el empleo de un derecho de propiedad intelectual reivindicado. La UIT no adopta ninguna posición en cuanto a la demostración, validez o aplicabilidad de los derechos de propiedad intelectual reivindicados, ya sea por los miembros de la UIT o por terceros ajenos al proceso de elaboración de Recomendaciones.

En la fecha de aprobación de la presente Recomendación, la UIT no ha recibido notificación de propiedad intelectual, protegida por patente, que puede ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los usuarios que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar la base de datos sobre patentes de la TSB en la dirección http://www.itu.int/ITU-T/ipr/.

ÍNDICE

Recomendación UIT-T X.1364

Requisitos y marco de seguridad de la Internet de las cosas de banda estrecha

1 Alcance

En la presente Recomendación se examinan varios métodos de despliegue de la Internet de las cosas de banda estrecha (NB-IoT), incluidas sus aplicaciones frecuentes. También se determinan los riesgos y requisitos específicos en materia de seguridad asociados al despliegue de la NB-IoT, y habida cuenta de ello, se establece un marco de seguridad que pueden aplicar los operadores para proteger las aplicaciones de esta nueva tecnología NB-IoT.

2 Referencias

Las siguientes Recomendaciones del UIT-T y otras referencias contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de la presente Recomendación. Al efectuar esta publicación, estaban en vigor las ediciones indicadas. Todas las Recomendaciones y otras referencias son objeto de revisiones por lo que se alienta a los usuarios de esta Recomendación a que investiguen la posibilidad de aplicar las ediciones más recientes de las Recomendaciones y otras referencias citadas a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T actualmente vigentes. En la presente Recomendación, la referencia a un documento no confiere a este último, como documento autónomo, la categoría de una Recomendación.

[ETSI TS 123 401] ETSI TS 123 401 V15.8.0 (2019-10), *LTE; General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access (3GPP TS 23.401 version 15.8.0 Release 15)*.

[ETSI TS 123 501] ETSI TS 123 501 V15.6.0 (2019-10), *5G; System architecture for the 5G System (5GS) (3GPP TS 23.501 version 15.6.0 Release 15)*.

3 Definiciones

3.1 Términos definidos en otros documentos

En la presente Recomendación se utilizan los siguientes términos definidos en otros documentos:

3.1.1 autenticación [b-UIT-T X.1141]: Proceso para determinar si alguien o algo es en realidad, con cierto grado de confianza, la persona o cosa que pretende ser.

3.1.2 capacidad [b-UIT-T X.1145]: Idoneidad de un sistema o de un equipo para prestar un servicio determinado.

3.1.3 IoT celular (CIoT) [ETSI TS 123 401]: Red celular que soporta la utilización de dispositivos sencillos de bajo caudal en una red de objetos. La IoT celular admite tráfico IP y no IP.

3.1.4 integridad de los datos [b-UIT-T X.800]: Propiedad que evita la alteración o supresión de los datos de forma no autorizada.

3.1.5 cifrado [b-UIT-T X.800]: Transformación criptográfica de datos (criptografía) que da lugar a criptogramas o a texto cifrado.

NOTA – El cifrado puede ser irreversible, en cuyo caso no puede realizarse el correspondiente proceso de descifrado.

3.1.6 entidad [b-UIT-T X.1252]: Cualquier cosa que tenga una existencia autónoma y bien definida y pueda ser identificada en contexto.

NOTA – Una entidad puede ser una persona física, un animal, una persona jurídica, una organización, una cosa activa o pasiva, un dispositivo, una aplicación informática, un servicio, etc., o un grupo de estos elementos. En el contexto de las telecomunicaciones, como ejemplos de entidades cabe mencionar puntos de acceso, abonados, usuarios, elementos de red, redes, aplicaciones informáticas, servicios y dispositivos, interfaces, etc.

3.1.7 núcleo de paquetes evolucionado (EPC) [b-UIT-T Q.1743]: Marco para la evolución o migración de un sistema 3GPP a un sistema optimizado para paquetes, de mayor velocidad de transmisión de datos y menor latencia, que soporta varias tecnologías de acceso radioeléctrico (RAT).

3.1.8 sistema de paquetes evolucionado (EPS) [b-UIT-T Q.1743]: Sistema UMTS de tercera generación (3G) evolucionado que se caracteriza por un sistema optimizado para paquetes, de mayor velocidad de transmisión de datos y menor latencia, que soporta varias RAT. El sistema de paquetes evolucionado comprende el núcleo de paquetes evolucionado y la red de acceso radioeléctrico evolucionada (E-UTRA y E-UTRAN).

3.1.9 gestión de claves [b-UIT-T X.800]: Generación, almacenamiento, distribución, supresión, archivo y utilización de claves con arreglo a una política de seguridad determinada.

3.1.10 IoT de banda estrecha [ETSI TS 123 401]: Tecnología de acceso radioeléctrico 3GPP que forma parte de la IoT celular. Brinda acceso a los servicios de red por medio de la red de acceso terrenal universal evolucionado (E-UTRA), con arreglo a un ancho de banda de canal limitada a 180 kHz (correspondiente a un bloque de recursos físicos). A menos que se indique lo contrario en casos específicos, la IoT de banda estrecha es un subconjunto de la red E-UTRAN.

3.1.11 amenaza [b-UIT-T X.800]: Posible riesgo de seguridad.

3.2 Términos definidos en la presente Recomendación

En la presente Recomendación se definen los siguientes términos

3.2.1 nodo de pasarela de servicio de la CIoT (C-SGN): El nodo de pasarela de servicio de la Internet de las cosas celular (C-SGN) constituye un método de implementación del núcleo de paquetes evolucionado (EPC) mediante nodos combinados para minimizar la cantidad de entidades físicas por medio de la ubicación de entidades del sistema de paquetes evolucionado (EPS) en trayectos de los planos de control y de usuario (por ejemplo, la entidad de gestión de la movilidad (MME), la pasarela de servicio (S-GW) o la pasarela de red de datos por paquetes (P-GW)), que podría ser adecuada para los despliegues de la CIoT.

NOTA – Las funciones que se enumeran en esta definición figuran en [ETSI TS 123 401].

3.2.2 nodo B evolucionado (eNodeB): Nodo de acceso inalámbrico que incorpora funciones de gestión de recursos radioeléctricos, descompresión de datos en el enlace ascendente, cifrado del flujo de datos de usuario y encaminamiento de datos del plano de usuario, entra otras.

NOTA – Las funciones que se enumeran en esta definición figuran en [ETSI TS 123 401].

3.2.3 red de acceso radioeléctrico terrenal universal evolucionado (E-UTRAN): Red de acceso radioeléctrico que incorpora funciones de compresión de encabezamiento y cifrado del plano de usuario, selección de MME, establecimiento de la velocidad de transmisión a nivel de portadora en los enlaces ascendente y descendente, control de admisión a nivel de portadora y control de congestión, entre otras.

NOTA – Las funciones que se enumeran en esta definición figuran en [ETSI TS 123 401].

3.2.4 servidor del abonado de origen (HSS): Elemento de la red troncal móvil que incorpora funciones de almacenamiento y gestión de la información relativa al abono del usuario.

NOTA – Las funciones que se enumeran en esta definición figuran en [ETSI TS 123 401].

3.2.5 entidad de gestión de la movilidad (MME): Elemento de la red troncal móvil que incorpora funciones de gestión de la lista de zonas de seguimiento, determinación de la localización del equipo del usuario (UE), selección de S-GW y P-GW, selección de traspaso, autenticación, autorización y gestión de portadoras, entre otras.

NOTA – Las funciones que se enumeran en esta definición figuran en [ETSI TS 123 401].

3.2.6 pasarela de red de datos por paquetes (P-GW): Elemento de la red troncal móvil que incorpora funciones de filtrado de paquetes por usuario, asignación de direcciones del protocolo de Internet (IP) a UE, marcado de paquetes a nivel de transporte y tarificación a nivel de servicio, entre otras.

NOTA – Las funciones que se enumeran en esta definición figuran en [ETSI TS 123 401].

3.2.7 función de detección de capacidades de servicio (SCEF): Elemento de una red troncal móvil que incorpora funciones de autenticación y autorización, detección de capacidades de servicio disponibles, gestión de políticas y configuración de parámetros de red, entre otras.

NOTA – Las funciones que se enumeran en esta definición figuran en [ETSI TS 123 401].

3.2.8 pasarela de servicio (S-GW): Elemento de una red troncal móvil que incorpora funciones de punto de anclaje de movilidad a nivel local a los efectos de traspaso entre nodos B evolucionados, establecimiento de redes de anclaje móvil 3GPP, encaminamiento y reenvío de paquetes, marcado de paquetes a nivel de transporte y contabilidad y tarificación entre operadores, entre otras.

NOTA – Las funciones que se enumeran en esta definición figuran en [ETSI TS 123 401].

4 Abreviaturas y acrónimos

En la presente Recomendación se utilizan las abreviaturas y acrónimos siguientes:

3G	Tercera generación
3GPP	Proyecto de asociación tercera generación (*the 3rd generation partnership project*)
CDMA	Acceso múltiple por división del código (*code-division multiple access*)
CIoT	Internet de las cosas celular (*cellular Internet of things*)
C-SGN	Nodo de pasarela de servicio de la CIoT (*CIoT serving gateway node*)
DDoS	Denegación de servicio distribuida (*distributed denial of service*)
EPC	Núcleo de paquetes evolucionado (*evolved packet system*)
eNodeB	Nodo B evolucionado (*evolved node B*)
EPS	Sistema de paquetes evolucionado (*evolved packet system*)
E-UTRAN	Red de acceso radioeléctrico terrenal universal evolucionado (*evolved universal terrestrial access network*)
GSM	Sistema mundial de comunicaciones móviles (*global system for mobile communications*)
HSS	Servidor del abonado de origen (*home subscriber server*)
IMEI	Identidad internacional del equipo móvil (*international mobile equipment identity*)
IP	Protocolo Internet (*Internet protocol*)
LTE	Evolución a largo plazo (*long term evolution*)
MME	Entidad de gestión de la movilidad (*mobility management entity*)
NB-IoT	Internet de las cosas de banda estrecha (*narrowband Internet of things*)
P-GW	Pasarela de red de datos por paquetes (*packet data network gateway*)

RAT	Tecnología de acceso radioeléctrico (*radio access technology*)
SCEF	Función de detección de la capacidad de servicio (*service capability exposure function*)
S-GW	Pasarela de servicio (*serving gateway*)
SMS	Servicio de mensajes cortos (*short message service*)
SIM	Módulo de identificación de abonado (*subscriber identification module*)
UE	Equipo del usuario (*user equipment*)
UMTS	Sistema de telecomunicaciones móviles universales (*universal mobile telecommunications system*)
UTRA	Acceso radioeléctrico terrenal universal (*universal terrestrial radio access*)

5 Convenios

Ninguno.

6 Visión general de la NB-IoT

El desarrollo de la tecnología de las telecomunicaciones que tiene lugar en la actualidad, en particular con respecto a las comunicaciones móviles, está transformando las pautas de comunicaciones entre personas, que pasan a realizarse entre personas y objetos, o entre objetos, y propicia, por ende, la inexorable evolución de la Internet de las cosas (IoT).

Las redes móviles celulares, caracterizadas por su amplia cobertura, movilidad y elevado grado de conectividad, así como por su capacidad para dar soporte a aplicaciones más abundantes, pasan a constituir la principal tecnología de interconexión de la IoT, en detrimento de las tecnologías de comunicación de corto alcance, en particular Bluetooth y ZigBee.

La IoT de banda estrecha (NB-IoT) se basa en la utilización de redes móviles celulares que requieren un ancho de banda de sólo unos 180 KHz. Podría desplegarse directamente en redes del sistema mundial de comunicaciones móviles (GSM) o del sistema universal de telecomunicaciones móviles (UMTS), así como en redes de evolución a largo plazo (LTE), con objeto de reducir costos y facilitar su actualización.

Entre las propiedades habituales de la NB-IoT cabe destacar:

– escasa disipación de energía: la duración del periodo de utilización de los dispositivos de la NB-IoT oscila entre cinco y diez años;
– amplia cobertura: para la misma banda, la NB-IoT posee una ganancia de 15 a 20 dB superior a la de una red actual, y ofrece una zona de cobertura hasta 100 veces mayor;
– elevada capacidad: cada sector de la NB-IoT puede soportar alrededor de 100 000 dispositivos; y
– bajo costo: el precio de un dispositivo de la NB-IoT es de 5 dólares de Estados Unidos aproximadamente.

Habida cuenta de la escasa disipación de energía, la amplia cobertura, el bajo costo y la elevada capacidad de la NB-IoT, cabe esperar que los operadores comiencen a implantarla de forma generalizada para ofrecer una gran cantidad de aplicaciones en sectores industriales de índole diversa.

7 Métodos de despliegue y aplicaciones habituales

7.1 Métodos de despliegue

7.1.1 Despliegue mediante redes troncales móviles implantadas

Con arreglo a este método, los operadores pueden desplegar la NB-IoT por medio de redes troncales móviles 2/3/4G ya implantadas.

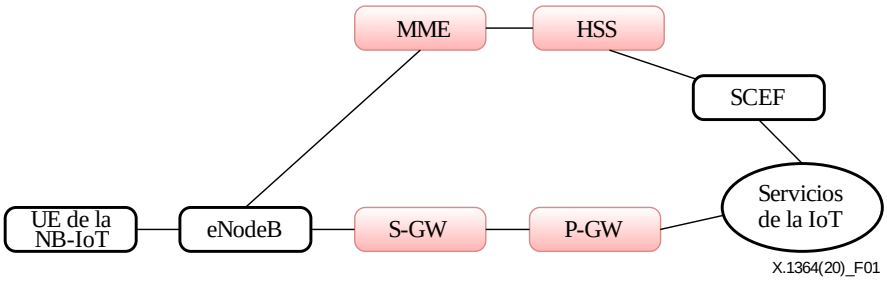
Los elementos de las redes troncales móviles implantadas, en particular la entidad de gestión de la movilidad (MME), la pasarela de servicio (S-GW) y la pasarela de red de datos por paquetes (P-GW) deben optimizarse para que la NB-IoT pueda ofrecer las siguientes propiedades [ETSI TS 123 401]:

– minimización del consumo energético del equipo del usuario (UE);

– capacidad para soportar una gran cantidad de dispositivos por célula;

– utilización de tecnologías de acceso radioeléctrico (RAT) para espectro de banda estrecha, en particular la red de acceso radioeléctrico terrenal universal evolucionado (E-UTRAN), el acceso radioeléctrico terrenal universal (UTRA), GSM, CDMA2000; y

– aumento de cobertura.



NOTA – Los elementos de la red troncal móvil implantada se representan con color rosa.

Figura 1 – Despliegue mediante una red troncal móvil ya implantada

Además de los citados elementos de red optimizados, cabe destacar los siguientes elementos de red representados en la Figura 1 [ETSI TS 123 401]:

– Nodo B evolucionado (eNodeB): nodo de acceso inalámbrico que incorpora funciones de gestión de recursos radioeléctricos, descompresión de datos en el enlace ascendente, cifrado del flujo de datos de usuario y encaminamiento de datos del plano de usuario, entra otras.

– Servidor del abonado de origen (HSS): almacena información relativa al abono del usuario, en particular, parámetros de autenticación y datos de localización.

– Función de detección de capacidades de servicio (SCEF): determina de forma segura los servicios y las capacidades que proporcionan las interfaces de red 3GPP.

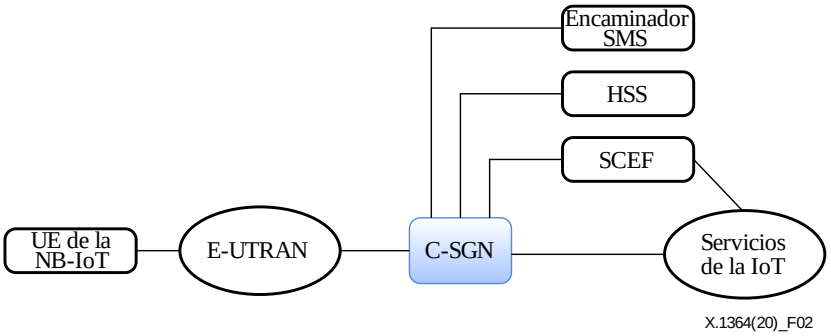
Estos elementos de red, incluidas sus funciones, soportan los servicios de la NB-IoT a través de redes de telecomunicaciones móviles.

7.1.2 Despliegue mediante redes troncales móviles específicas de reciente implantación

Con arreglo a este método, los operadores pueden establecer una red troncal móvil de implantación específica para la prestación de servicios de la NB-IoT.

El nodo de la pasarela de servicio de la Internet de las cosas celular (C-SGN) se define en [ETSI TS 123 401].

El C-SGN soporta las funciones de subconjunto necesarias de los elementos de la red troncal del sistema de paquetes evolucionado (EPS) existentes. Se basa en un nodo combinado de núcleos de paquetes evolucionados (EPC). Por otro lado, permite minimizar la cantidad de entidades físicas EPS y asigna las funciones de las entidades EPS a trayectos de los planos de control y de usuario. El C-SGN conjuga funciones MME, P-GW y S-GW con el fin de ofrecer soluciones CIoT optimizadas. Esas interfaces corresponden a las que incorporan las respectivas entidades EPC, en particular la MME, la S-GW y la P-GW.



NOTA – Los elementos de la red troncal móvil de reciente implantación se representan con color azul.

Figura 2 – Despliegue mediante una red troncal móvil específica de reciente implantación

Además de los elementos de la red de reciente implantación, cabe destacar los siguientes elementos de red representados en la Figura 2 [ETSI TS 123 401]:

– E-UTRAN: incorpora funciones de compresión de encabezamiento y cifrado del plano de usuario, selección de MME, establecimiento de la velocidad de transmisión a nivel de portadora, control de congestión y marcado de paquetes a nivel de transporte en el enlace ascendente, entre otras.

– HSS: almacena y gestiona la información relativa al abono del usuario, en particular, parámetros de autenticación y datos de localización.

– SCEF: determina de forma segura los servicios y las capacidades que proporcionan las interfaces de red 3GPP.

– Encaminador del servicio de mensajes cortos (SMS): permite la transferencia de solicitudes de vinculación sin agrupación EPS (solicitud de servicios EPS o no EPS); esta propiedad la incorporan únicamente los UE compatibles exclusivamente con la NB-IoT.

Estos elementos de red, incluidas sus funciones, soportan los servicios de la NB-IoT a través de redes de telecomunicaciones móviles.

7.2 Aplicaciones habituales

7.2.1 Realización de mediciones a distancia

Esta aplicación permite utilizar dispositivos NB-IoT para recibir los datos proporcionados por contadores que miden el consumo de servicios públicos que realiza una familia, por ejemplo, el consumo de agua o de gas, y transmitirlos posteriormente a los proveedores de dichos servicios por medio de redes inalámbricas.

La utilización de la tecnología de la NB-IoT permite realizar mediciones más eficaces, exactas y eficientes que en el caso de la lectura de contadores manual tradicional.

7.2.2 Estacionamiento inteligente

Esta aplicación permite implantar dispositivos NB-IoT como sensores en plazas de estacionamiento para detectar las que estén libres. Por otro lado, proporciona a los conductores que utilicen aplicaciones de estacionamiento inteligente información sobre plazas de estacionamiento recomendadas y permite abonar las correspondientes tarifas de estacionamiento mediante sistemas de pago en línea.

La utilización de la tecnología NB-IoT puede facilitar la búsqueda de plazas de estacionamiento disponibles y el pago de su correspondiente tarifa.

7.2.3 Sistemas de agricultura inteligentes

Esta aplicación permite utilizar dispositivos NB-IoT como sensores para recabar datos agrícolas, por ejemplo, sobre salinidad, humedad o temperatura. Los agricultores pueden utilizar dichos datos para obtener recomendaciones sobre medios de irrigación o fertilización.

La tecnología NB-IoT promueve sistemas agrícolas más inteligentes, puesto que se basa en el análisis de información en tiempo real, no en la experiencia relativa a prácticas agrícolas tradicionales.

8 Riesgos para la NB-IoT

El análisis de los riesgos de seguridad de la NB-IoT abarca dos aspectos, a saber, las características de la NB-IoT y el marco funcional de esta, a tenor de lo establecido en los apartados 8.1 y 8.2 siguientes.

8.1 Características de la NB-IoT

La NB-IoT se caracteriza, en particular, por su baja disipación de energía, elevada capacidad, bajo costo y amplia cobertura.

8.1.1 Disipación de baja energía

1) Descripción de las características

Los dispositivos de la NB-IoT se caracterizan principalmente por su bajo consumo energético, gran durabilidad y, por ende, menor necesidad de recarga, así como por su capacidad de computación limitada. Por otro lado, los sistemas integrados son más ligeros y sencillos.

Por lo general, los sistemas implantados en equipos terminales de la IoT tradicionales poseen una gran capacidad de computación. Utilizan complejos protocolos de transmisión de red y se apoyan en soluciones muy eficaces de aumento de la seguridad. Debido a su elevado consumo energético deben recargarse con frecuencia.

2) Riesgos para la NB-IoT

El mero consumo de los recursos de un dispositivo NB-IoT podría ocasionar una denegación de servicio. Los costos asociados a ese tipo de ataques contra soportes lógicos y físicos son relativamente bajos.

Habida cuenta de las características de los dispositivos NB-IoT, a saber, su poco peso, bajo consumo energético y capacidad de computación limitada, no puede garantizarse el cifrado de los datos durante la transmisión para aumentar la seguridad. En ocasiones, los datos pueden transmitirse como texto sin formato. Ello podría constituir, en consecuencia, un grave riesgo de seguridad a los efectos de autenticación y validación de datos. Por ejemplo, un atacante podría utilizar dispositivos no autorizados para establecer una conexión con la estación de base y enviar datos falsos.

8.1.2 Capacidad elevada

1) Descripción de las características

La capacidad de la NB-IoT es mucho mayor que la de la IoT tradicional; por ejemplo, cada sector de NB-IoT puede soportar alrededor de 100 000 dispositivos.

2) Riesgos para la NB-IoT

Habida cuenta de la gran cantidad de dispositivos que puede soportar la NB-IoT, una pequeña vulnerabilidad podría repercutir de forma crítica en la seguridad de red. Por ejemplo, un virus troyano podría infectar otros equipos terminales e inhabilitar la red.

Si los dispositivos de la NB-IoT pueden utilizar redes troncales móviles ya implantadas, los equipos terminales podrían infectar varios elementos de esas redes, en particular la entidad de gestión de la movilidad y el servidor del abonado de origen, lo que repercutiría adversamente en los usuarios de las redes de comunicaciones móviles. En tal caso, podría denegarse a los usuarios el acceso a la red o modificarse la información de los abonados para dificultar la tarificación de llamadas telefónicas o mensajes breves, o el tráfico de datos.

8.1.3 Bajo costo

1) Descripción de las características

Por lo general, el costo de los dispositivos de la NB-IoT es bajo.

2) Riesgos para la NB-IoT

El reducido costo de los dispositivos es posible gracias, entre otras cosas a la utilización de protocolos simplificados. En consecuencia, se puede aprovechar la vulnerabilidad de dichos protocolos para atacar los dispositivos y la red.

8.1.4 Amplia cobertura

1) Descripción de las características

La cobertura de la NB-IoT es mucho más amplia que la de la IoT tradicional. Por ejemplo, para la misma banda, la NB-IoT posee una ganancia de 15 a 20 dB superior a las redes actuales, y ofrece una zona de cobertura hasta 100 veces mayor.

2) Riesgos para la NB-IoT

Los dispositivos desplegados en emplazamientos lejanos pueden ser suplantados o explotados ilícitamente por atacantes de forma sencilla.

8.2 Capas de la NB-IoT

8.2.1 Capa de dispositivo

Los atacantes podrían perpetrar ataques mediante la duplicación de tarjetas del módulo de identificación del abonado (SIM) con fines ilícitos, por ejemplo, para acceder gratuitamente a la red.

Pueden existir vulnerabilidades de seguridad en las pilas de protocolos de los módulos de los terminales ligeros de desarrollo reciente.

Los fabricantes de equipos terminales de IoT pueden utilizar el soporte físico que soporta los protocolos Wi-Fi, Bluetooth y ZigBee, entre otros, al publicar nuevos equipos compatibles con la NB-IoT. Puesto que sólo podrían incorporar dicha compatibilidad como nueva función, cabe tener en cuenta vulnerabilidades y riesgos de seguridad en el proceso de desarrollo. Por ejemplo, es posible que los puertos destinados a actividades de depuración no estén protegidos adecuadamente, que se hayan utilizado algoritmos de cifrado poco eficaces, que no se haya actualizado el soporte físico o que no se haya llevado a cabo un análisis de integridad necesario de forma oportuna.

8.2.2 Capa de red

La utilización de medios que permiten interceptar las comunicaciones de datos en la red podría vulnerar el acceso a sesiones de conexión entre los equipos terminales y las estaciones de base, con objeto de acceder a paquetes transmitidos entre estos componentes. En consecuencia, al interceptarse la comunicación, el atacante podría analizar las vulnerabilidades de seguridad mediante los datos que contienen los mensajes interceptados.

Habida cuenta de la gran cantidad de dispositivos que comparten acceso a la red de telecomunicaciones móviles con los abonados, los dispositivos NB-IoT alterados podrían provocar errores de señalización generalizados.

Cabe tener en cuenta asimismo el riesgo de divulgación de datos como consecuencia de la gran cantidad de información que recaban los servicios de la NB-IoT, que posteriormente se transmite a través de la red y se procesa en muchos elementos de la misma.

Las señales de la red troncal de la NB-IoT podrían falsificarse, alterarse o retransmitirse varias veces con fines malignos, debido a la falta de un mecanismo de autenticación entre elementos de red.

La realización de múltiples ataques a través de Internet podría repercutir adversamente en la interfaz existente entre la red troncal móvil e Internet; por ejemplo, en los sistemas 5G, dicha interfaz es de tipo N6 [ETSI TS 123 501]; esta interfaz N6 permite conectar la función del plano de usuario e Internet.

8.2.3 Capa de aplicación

La NB-IoT es adecuada para aplicaciones estáticas poco sensibles frente a la latencia, que requieren movimiento discontinuo y transmisión de datos en tiempo real.

Con respecto a las aplicaciones destinadas a la notificación automática de incidencias (por ejemplo, en sistemas de alarma para la detección de humo) o la notificación periódica de información (por ejemplo, en sistemas de supervisión medioambiental) podrían generarse falsas alarmas, o impedirse las señales de alarma. Por ejemplo, si un atacante lograra interceptar los datos de un contador eléctrico inteligente de un usuario, podría alterarlos o falsificarlos, lo que podría tener consecuencias adversas para dicho usuario.

Por otro lado, la transmisión de instrucciones con fines ilícitos podría poner en riesgo determinados sistemas (por ejemplo, los equipos domésticos inteligentes que pueden activar o desactivar los usuarios a distancia).

Las aplicaciones de la NB-IoT están profundamente integradas en varios sectores industriales, y en consecuencia, están expuestas a vulnerabilidades asociadas a la compleja actividad habitual de los mismos y a sus diversos protocolos de aplicación.

Los servicios de la NB-IoT pueden ser objeto de uso abusivo mediante la suplantación de tarjetas de abonado, por ejemplo, al utilizar la tarjeta NB-IoT de un abono específico en dispositivos no destinados a la NB-IoT, o al enviar mensajes cortos no solicitados mediante dicha tarjeta NB-IoT.

9 Requisitos de seguridad

9.1 Requisitos de seguridad de los dispositivos terminales

9.1.1 Seguridad a nivel físico

La protección a nivel físico de la interfaz y del circuito integrado se proporciona a través de los dispositivos terminales de la NB-IoT, que impiden a un atacante acceder a los datos aun si tiene acceso al soporte físico.

Dichos dispositivos terminales de la NB-IoT soportan funciones de autenticación y autorización para diversos tipos de interfaces.

9.1.2 Seguridad de las actualizaciones

Los sistemas y los soportes lógicos y físicos de los dispositivos de la NB-IoT deben permitir su actualización de forma que se garantice la seguridad de los mismos, incluida la de sus aplicaciones.

La protección de la confidencialidad y la integridad de la actualización de archivos permite evitar su alteración.

9.1.3 Protección de la privacidad

Los dispositivos terminales de la NB-IoT deben incorporar mecanismos versátiles de protección de la privacidad, a tenor de los requisitos de servicio de la NB-IoT.

9.2 Requisitos en materia de seguridad de red

9.2.1 Autenticación

La identidad de las entidades de la NB-IoT que utilizan el servicio de la misma debe confirmarse mediante un proceso de autenticación. Este garantiza la validez de la identidad de las entidades e impide a estas hacerse pasar ilegítimamente por entidades autorizadas.

Habida cuenta de las características de la NB-IoT, únicamente puede llevarse a cabo un proceso de autenticación simple.

9.2.2 Prevención de ataques DDoS

La implantación previa de mecanismos de seguridad permite evitar ataques de denegación de servicio distribuida (DDoS) y hacer frente a los mismos de forma oportuna.

9.2.3 Seguridad de las entidades de red

El aumento de la cantidad de entidades de red troncal de la NB-IoT permite garantizar la seguridad e impedir acciones de falsificación o alteración y ataques mediante retransmisión de datos con fines malignos.

9.3 Requisitos en materia de seguridad de las aplicaciones

9.3.1 Supervisión de la conformidad de la utilización y del funcionamiento del servicio

La supervisión de la conformidad de la utilización y del funcionamiento del servicio debe abarcar la comprobación de valores de cresta y flujo total, y permitir la detección de una utilización o de un funcionamiento inusuales del servicio con respecto a las necesidades de los servicios de la NB-IoT.

9.3.2 Prevención de casos abusivos de utilización del servicio

Los casos abusivos de utilización del servicio asociados a la suplantación de tarjetas de abono deben evitarse por medio de la supervisión de las propiedades relativas a la modificación de la identidad internacional del equipo móvil (IMEI).

9.3.3 Determinación de la capacidad para analizar y erradicar riesgos de seguridad

El examen de macrodatos relativos al comportamiento de los dispositivos terminales de la NB-IoT permite determinar, examinar y erradicar riesgos de seguridad.

10 Funciones de seguridad de la NB-IoT

10.1 Funciones de seguridad de los dispositivos terminales

Los dispositivos terminales de la NB-IoT deben incorporar las siguientes funciones de seguridad:

– SC_terminal device 1: función de gestión de claves;

– SC_terminal device 2: función de negociación de algoritmos de cifrado;

– SC_terminal device 3: función de cifrado de datos;

– SC_terminal device 4: función de mantenimiento de la integridad de los datos;

– SC_terminal device 5: función de actualización segura, en particular a nivel de sistema y de los soportes lógico y físico;

– SC_terminal device 6: función de aplicación de protocolos de cifrado simple seguros.

10.2 Funciones de seguridad de red

La red NB-IoT debe incorporar las siguientes funciones de seguridad:

– SC_network 1: función de gestión de claves;

– SC_network 2: función de negociación de algoritmos de cifrado;

– SC_network 3: función de cifrado de datos;

– SC_network 4: función de mantenimiento de la integridad de los datos;

– SC_network 5: función de control de acceso para garantizar que sólo las entidades autorizadas puedan acceder a los elementos de red de la NB-IoT, en particular la información almacenada, los flujos de datos, los servicios y las aplicaciones;

– SC_network 6: función de detección y/o prevención de alteraciones de datos;

– SC_network 7: función de protección frente a ataques DDoS;

– SC_network 8: función de realización de configuraciones seguras;

– SC_network 9: función de detección de suplantación de tarjetas de abonado.

10.3 Funciones de seguridad de las aplicaciones

Las aplicaciones deben incluir las siguientes funciones de seguridad:

– SC_applications 1: función de protección frente a programas malignos mediante la utilización de soportes lógicos adecuados;

– SC_applications 2: función de supervisión de la conformidad de la utilización y del funcionamiento del servicio mediante indicadores fundamentales de red (por ejemplo, los valores de cresta o el número total de flujos);

– SC_applications 3: función de seguridad a nivel de aplicación para evitar riesgos de seguridad mediante el análisis de macrodatos relativos al comportamiento de los dispositivos terminales de la NB-IoT.

10.4 Relación entre las funciones y los requisitos de seguridad

Las funciones de seguridad que se enumeran y describen en el apartado 10 permiten satisfacer varios requisitos de seguridad especificados en el apartado 9. En el Cuadro 1 se muestra la correspondencia entre las funciones y los requisitos de seguridad.

En dicho cuadro, el símbolo "√" indica que el requisito de seguridad correspondiente guarda relación con una función de seguridad determinada. Ello conlleva que el requisito de seguridad señalado ha de satisfacerse mediante la función correspondiente.

Cuadro 1 – Representación de la relación entre requisitos y funciones de seguridad

Requisitos / Funciones	Seguridad a nivel físico	Seguridad de actualiza-ciones	Protección de la privacidad	Autenti-cación	DDoS Protección frente a ataques DDoS	Supervisión de la conformidad de la utilización y del funcionamiento del servicio	Prevención de casos abusivos de utilización del servicio	Determinación de la capacidad para analizar y erradicar riesgos de seguridad
SC_terminal device 1	√			√				
SC_terminal device 2	√							
SC_terminal device 3			√					
SC_terminal device 4		√						
SC_terminal device 5	√	√						
SC_terminal device 6			√	√				
SC_network 1				√				
SC_network 2		√	√					
SC_network 3		√	√					
SC_network 4		√						
SC_network 5			√	√				
SC_network 6						√		
SC_network 7					√			
SC_network 8		√						
SC_network 9							√	
SC_applications 1		√						
SC_applications 2					√	√	√	
SC_applications 3			√					√

Bibliografía

[b-UIT-T Q.1743] Recomendación UIT-T Q.1743 (2016), *Referencias de las IMT-Avanzadas a la versión 11 de la red básica de paquetes evolucionada de LTE-Avanzada*.

[b-UIT-T X.800] Recomendación UIT-T X.800 (1991), *Arquitectura de seguridad de la interconexión de sistemas abiertos para aplicaciones del CCITT*.

[b-UIT-T X.1141] Recomendación UIT-T X.1141 (2006), *Lenguaje de marcaje de aserción de seguridad (SAML 2.0)*.

[b-UIT-T X.1145] Recomendación UIT-T X.1145 (2017), *Marco y requisitos de seguridad para las capacidades abiertas de servicios de telecomunicación*.

[b-UIT-T X.1252] Recomendación UIT-T X.1252 (2010), *Términos y definiciones de referencia para la gestión de la identidad*.

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie D	Principios de tarificación y contabilidad y cuestiones económicas y políticas de las telecomunicaciones/TIC internacionales
Serie E	Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos
Serie F	Servicios de telecomunicación no telefónicos
Serie G	Sistemas y medios de transmisión, sistemas y redes digitales
Serie H	Sistemas audiovisuales y multimedia
Serie I	Red digital de servicios integrados
Serie J	Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedia
Serie K	Protección contra las interferencias
Serie L	Medio ambiente y TIC, cambio climático, ciberdesechos, eficiencia energética, construcción, instalación y protección de los cables y demás elementos de planta exterior
Serie M	Gestión de las telecomunicaciones, incluida la RGT y el mantenimiento de redes
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Calidad de la transmisión telefónica, instalaciones telefónicas y redes de líneas locales
Serie Q	Conmutación y señalización, y mediciones y pruebas asociadas
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios de telegrafía
Serie T	Terminales para servicios de telemática
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
Serie X	**Redes de datos, comunicaciones de sistemas abiertos y seguridad**
Serie Y	Infraestructura mundial de la información, aspectos del protocolo Internet, redes de próxima generación, Internet de las cosas y ciudades inteligentes
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Impreso en Suiza
Ginebra, 2020