Survey de Protocolos IETF en Seguridad de IoT

Gustavo Mercado[1,3], Marcela Orbiscay [1,2,3], Oscar Giudice[3]
Ana Laura Diedrichs[1], Cristian Pérez Monte[1]

[1] gridTICS, UTN FRM, Mendoza, Argentina
{gmercado,ana.diedrichs,cfperez}@frm.utn.edu.ar

[2] IANIGLA, CCT Conicet, Mendoza, Argentina
morbis@mendoza-conicet.gob.ar

[3] IoT CiberSec LAC, LatinoAmérica y el Caribe
oscar.giudice@gmail.com

Abstract.
El rápido crecimiento de "las cosas conectadas" ha hecho que el IoT (Internet of Things) haya tomado significativa relevancia entre las tecnologías y aplicaciones del ecosistema de Internet. En este aspecto varias instituciones dedicadas a la estandarización de Internet han tomado acciones para fortalecer la "interoperabilidad", uno de los principales valores del ecosistema de Internet, creando protocolos de alcance mundial. Una de estas instituciones es el IETF (Internet Engineering Task Force), y a ella nos referiremos en este artículo.
Una de las características importantes de IoT es que está constituida, mayoritariamente por dispositivos denominados "constrained device", Estos dispositivos de cómputo tienen características de pequeña memoria y bajo poder de cálculo y generalmente se alimentan con baterías, por lo que requieren funcionamiento en bajo consumo. Evidentemente no es posible montar, en ellos, los habituales protocolos de Internet. Por esto, el IETF ha realizado una adaptación de los protocolos de Internet para poder ser usados en los "constrained device". Adicionalmente, se ha considerado que el tema de la "seguridad cibernética" es una cualidad muy importante en el mundo Internet.
En este trabajo se pasa revista actualizada a los protocolos creados por el IETF para el área de seguridad y aplicados al mundo del IoT.

Keywords: Internet de las Cosas, Ciberseguridad, IETF, protocolos de seguridad.

1 Introduccion

El termino de "Internet de los Cosas" (IoT - Internet of Things en inglés) hace referencia a un sistema de dispositivos, a menudo limitados en sus capacidades de comunicación y cálculo, que cada vez están más conectados a Internet, o al menos a una red IP, y a diversos servicios creados a partir de las capacidades que estos dispositivos ofrecen conjuntamente. Se espera que esta evolución dé paso a una mayor comunicación de máquina a máquina a través de Internet sin la participación

activa de un usuario humano.La IoT es un área tecnológica en rápido crecimiento que conecta con otras tecnologías emergentes. Varios grupos de trabajo del IETF [1], que abarcan múltiples áreas, están desarrollando protocolos y mejores prácticas comunes que son directamente relevantes para los aspectos de comunicación y seguridad de la IoT. Estos protocolos son utilizados por diversas empresas, así como por otras organizaciones de desarrollo de normas (SDO) y alianzas de IoT, para construir y especificar sistemas interoperables. Debido a la naturaleza distribuida del desarrollo y uso de protocolos IoT, a menudo es necesaria la coordinación entre los distintos grupos que trabajan en IoT [2].
La Directiva de IoT del IETF es un grupo consultivo de expertos seleccionados por los Directores de Área de Internet del IETF y los Presidentes de la Directiva de IoT [3]. El principal objetivo de la Directiva de IoT es coordinar dentro del IETF el trabajo relacionado con IoT y aumentar la visibilidad y la comunicación entre las actividades de IoT del IETF y otras SDO, alianzas industriales y otras organizaciones. Una entrada del blog del IETF ofrece una visión general del trabajo relacionado con IoT que se está llevando a cabo en el IETF.

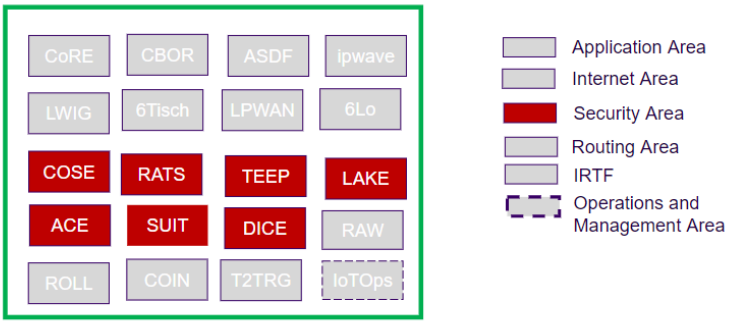

Figura 1: Protocolos del IETF referidos a Seguridad en IoT

Una de las características importantes de IoT es que está constituida, mayoritariamente por dispositivos denominados “constrained device”, Estos dispositivos de cómputo tienen características de pequeña memoria y bajo poder de cálculo y generalmente se alimentan con baterías, por lo que requieren funcionamiento en bajo consumo. Evidentemente no es posible montar, en ellos, los habituales protocolos de Internet. Por esto, el IETF ha realizado una adaptación de los protocolos de Internet para poder ser usados en los “constrained device”.
Los IoT se utilizan ampliamente en aplicaciones sensibles como el ámbito médico y los vehículos autónomos, donde la vida de los seres humanos se ve directamente afectada. De ahí que la seguridad de estos sistemas, tanto del hardware como del software, sea de vital importancia. Los requisitos de seguridad de los sistemas pueden variar en función de las aplicaciones en las que se utilicen. Normalmente, los dispositivos IoT incluyen sensores y actuadores, y microchips para la recogida y transmisión de datos a través de la red. Dado que muchos dispositivos complejos están conectados, la gestión de la seguridad de todo el sistema se vuelve compleja, en

comparación con la gestión de la seguridad de un dispositivo independiente. Los problemas de seguridad en IoT incluyen la autenticación de datos, la fuga de datos, la privacidad del usuario, la seguridad de acceso, etc.
El objetivo del IETF es reutilizar en la mayor medida posible los protocolos y arquitecturas de seguridad ya definidos, adaptándolos al restringido mundo del Internet de las Cosas (IoT).
En la Figura 1 se representan los grupos de tareas del IETF relacionados con IoT y se resaltan aquellos que tratan específicamente la temática de seguridad .[4]
En este trabajo haremos un repaso de los principios y fundamentos de los estándares, protocolos y procedimientos referidos a seguridad para IoT y tratados por el IETF, tales como: DICE – DTLS In Constrained Environments, ACE - Authentication and Authorization for Constrained Environments, COSE - CBOR Object Signing and Encryption, LAKE - Lightweight Authenticated Key Exchange, TEEP - The Trusted Execution Environment ProvisioningM, SUIT - Software Updates for Internet of Things, RATS - Remote ATtestation ProcedureS.

2 Grupos de Tareas y Protocolos del IETF

2.1 DICE – DTLS In Constrained Environments

Iniciado en 2013, el grupo de trabajo del IETF, DTLS en entornos restringidos (DICE) [5] finalizó su trabajo en 2016. DICE se centró en la definición de directrices y mecanismos para el soporte del protocolo DTLS (Datagram Transport Layer Security) [6] en el contexto de entornos limitados (incluyendo dispositivos redes restringidas). El principal producido del GT DICE fue el doc denominado "*Transport Layer Security (TLS)/Datagram Transport Layer Security (DTLS) Profiles for the Internet of Things"* (ver Tabla 1) *y* que fue estandarizado con el RFC 7925 [7]

RFC Número y Título	Descripción
RFC 7925: Transport Layer Security (TLS)/Datagram Transport Layer Security (DTLS) Profiles for the Internet of Things	*Desarrolla dos protocolos de seguridad de Internet ampliamente desplegados para los sistemas de IoT: Transport Layer Security (TLS) y Datagram Transport Layer (DTLS) 1.2.*

Tabla 1: Selección de RFC e I+D relevantes del GT DICE

Permitir que los dispositivos IoT intercambien datos a menudo requiere la autenticación de los dos puntos finales y la capacidad de proporcionar protección de la integridad y confidencialidad de los datos intercambiados. Aunque estos servicios de seguridad pueden proporcionarse en diferentes capas de la pila de protocolos, el uso de Transport Layer Security (TLS) / Datagram Transport Layer (DTLS) ha sido muy popular en muchos protocolos de aplicación, y es probable que también resulte útil en escenarios de IoT.
Adaptar los protocolos de Internet a dispositivos restringidos puede ser difícil, pero gracias a los esfuerzos de estandarización, existen nuevos perfiles y protocolos, como

el Protocolo de Aplicación Restringida (CoAP - Constrained Application Protocol) [8]
Los mensajes CoAP se transportan principalmente sobre UDP/DTLS, pero se pueden utilizar otro transportes como TCP, como se propone actualmente en el documento “COAP over -TCP, TLS and WebSockets" [9]
Esencialmente, DICE proporcionó un perfil de DTLS 1.2 [D2] y TLS 1.2 [10] que ofrece servicios de seguridad de comunicaciones para aplicaciones IoT y es razonablemente implementable en muchos dispositivos con restricciones. De este modo, este perfil permite que las opciones de configuración y extensiones de protocolo disponibles se utilicen para dar el mejor soporte al entorno de IoT.

2.2 ACE - Authentication and Authorization for Constrained Environments

El Grupo de Trabajo de Autenticación y Autorización para Entornos Restringidos (ace) ha definido un framework de soluciones estandarizado para la autenticación y autorización que habilite el acceso autorizado a recursos identificados por una URI y alojados en un servidor de recursos en entornos restringidos.[11]
El acceso al recurso está mediado por un servidor de autorización, que no se considera restringido.
Además del trabajo de mantenimiento en curso, el Grupo de Trabajo amplía el marco según sea necesario para su aplicabilidad a las comunicaciones de grupo.

RFC Número y Título	Descripción
RFC 7744 Use Cases for Authentication and Authorization in Constrained Environments	*Este documento incluye una colección de casos de uso representativos para autenticación y autorización en entornos restringidos.*
RFC 9430 Extension of the Datagram Transport Layer Security (DTLS) Profile for Authentication and Authorization for Constrained Environments (ACE) to Transport Layer Security (TLS)	*Este documento actualiza el RFC 9202 "Datagram Transport Layer Security (DTLS) para autenticación y autorización en entornos restringidos (ACE) Constrained Environments (ACE)", especificando que el perfil se aplica tanto a TLS como a DTLS.*
RFC 9482 Constrained Application Protocol (CoAP) Transfer for the Certificate Management Protocol	*Este documento especifica el uso del protocolo de aplicación restringida (CoAP) como mecanismo de transferencia para el Protocolo de Gestión del Protocolo de Gestión de Certificados (CMP)*

RFC 9431 Message Queuing Telemetry Transport (MQTT) and Transport Layer Security (TLS) Profile of Authentication and Authorization for Constrained Environments (ACE) Framework	*Este documento especifica un perfil para el framework de Autenticación y Autorización para Entornos Restringidos (ACE) para permitir la autorización en un sistema de mensajería de publicación-suscripción basado en el protocolo Message Queuing Telemetry Transport (MQTT).*

Tabla 2: Selección de RFC e I+D relevantes del GT ACE

Draft Título	Descripción
The Group Object Security for Constrained RESTful Environments (Group OSCORE) Profile of the Authentication and Authorization for Constrained Environments (ACE) Framework	*Este documento especifica un perfil para el framework de autenticación y autorización para entornos restringidos (ACE). El perfil utiliza la Seguridad de Objetos de Grupo para Entornos RESTful Restringidos (Group OSCORE).*
Using the Constrained RESTful Application Language (CoRAL) with the Admin Interface for the OSCORE Group Manager	*Este documento especifica cómo una entidad Administradora interactúa con la interfaz administrativa en el Gestor de grupos, utilizando el lenguaje de aplicaciones RESTful (CoRAL)*

Tabla 3: Selección de RFC e I+D relevantes del GT ACE

El grupo de trabajo normaliza los procedimientos para solicitar y distribuir material de claves de grupo utilizando el marco ACE, así como las interfaces de gestión adecuadas.[12]

Los protocolos de autenticación y autorización tripartita definidos previamente en el IETF (por ejemplo, la infraestructura de clave pública, PKI -Public Key Infrastructure- y el Protocolo de Autorización Web, OAuth -Open Authorization-) son en su mayoría adecuados para entornos no restringidos y no tienen en cuenta los requisitos adicionales y las limitaciones de los escenarios típicos de IoT; por ejemplo, la conectividad intermitente puede reducir la posibilidad de ponerse en contacto con un servidor de autorización en tiempo real. un servidor de autorización en tiempo real. [5]

También se han normalizado perfiles de este framework para su aplicación a protocolos de seguridad utilizados habitualmente en entornos restringidos, incluidos CoAP+DTLS (Constrained Application Protocol - Datagram Transport Layer Security y CoAP+OSCORE (Object Security for Constrained RESTful Environments) [13].

El grupo de trabajo se encarga del mantenimiento del framework y de los perfiles existentes del mismo, y puede emprender trabajos para especificar perfiles del marco para protocolos de comunicaciones seguras adicionales y para servicios de soporte

adicionales que proporcionen acceso autorizado a claves criptográficas (que no se limitan necesariamente a puntos finales restringidos, aunque la atención sigue centrada en el despliegue en ecosistemas con una parte sustancial de dispositivos restringidos).[4]
En las Tablas 2 y 3 se describe un subconjunto de los documentos relevantes y actualizados producidos por el GT ACE [14].

2.3 COSE - CBOR Object Signing and Encryption

CBOR Object Signing and Encryption (COSE) [15] describe cómo crear y procesar firmas, códigos de autenticación de mensajes y cifrado utilizando Concise Binary Object Representation (CBOR) [16] para la serialización. COSE describe además una representación para claves criptográficas. [17]
El grupo de trabajo COSE se constituyó en 2015, concluyó en 2016 y se volvió a constituir en 2019.
El grupo utiliza CBOR para los formatos de firma y cifrado de objetos. Una de las motivaciones es reutilizar las claves criptográficas, la autenticación de mensajes (MAC), el cifrado y las firmas digitales que se hicieron para JSON en el ahora concluido JOSE WG, pero esta vez en CBOR. [5].
El GT tiene actualmente dos puntos de trabajo:
1-Documentos que describen el uso de algoritmos criptográficos en COSE Estos algoritmos deben cumplir los requisitos descritos anteriormente.
2- Una codificación en CBOR del perfil de certificado definido en RFC 5280 [18] . Se espera que la codificación funcione con RFC 7925 [19] y tenga en cuenta cualquier actualización en draft-ietf-uta-tls13-iot-profile-00. La codificación también puede incluir otros perfiles de certificado IoT importantes como IEEE 802.1AR [20].
El grupo de trabajo colaborará y se coordinará con otros GT del IETF como TLS, UTA, LAKE para comprender y validar los requisitos y la solución.
En las Tablas 4 y 5 se describe un subconjunto de los documentos relevantes y actualizados producidos por el GT COSE [21].

RFC Número y Título	Descripción
RFC 8152 CBOR Object Signing and Encryption (COSE)	*Define los mecanismos de seguridad de COSE para el formato de datos CBOR, como la creación y el procesamiento de firmas, códigos de autenticación de mensajes, representación de claves criptográficas mediante CBOR, etc.*

RFC 9052 CBOR Object Signing and Encryption (COSE): Structures and Process	*Esta especificación describe cómo crear y procesar firmas, códigos de autenticación de mensajes y cifrado mediante CBOR para la serialización. Esta especificación describe además cómo representar claves criptográficas utilizando CBOR.*
RFC 9459 CBOR Object Signing and Encryption (COSE): AES-CTR and AES-CBC	*Este documento especifica las convenciones para utilizar AES-CTR y AES-CBC como algoritmos de contenido con COSE.*

Tabla 4: Selección de RFC e I+D relevantes del GT COSE

Draft Título	Descripción
CBOR Object Signing and Encryption (COSE): Header Parameters for Carrying and Referencing Chains of CBOR Web Tokens (CWTs)	La estructura de mensajes de COSE utiliza referencias a claves y define parámetros de cabecera para transportar cadenas de certificados X.509. Esta especificación amplía esta funcionalidad a los CBOR Web Tokens (CWT).
COSE Header Parameter for Carrying OpenID Federation 1.0 Trust Chain	*Este documento define un nuevo parámetro de cabecera COSE para identificar y transportar una cadena de confianza OpenID Federation 1.0.*
CBOR Web Token (CWT) Claims in COSE Headers	*Este documento describe cómo incluir las reivindicaciones CBOR Web Token (CWT) en los parámetros de cabecera de cualquier estructura COSE.*

Tabla 5: Selección de RFC e I+D relevantes del GT COSE

2.4 LAKE - Lightweight Authenticated Key Exchange

Es sabido que uno de los grandes desafíos presentados por los dispositivos de IoT es la capacidad restringida de recursos (memoria, procesador, velocidad, consumo energético).
El GT LAKE [22] especifica un protocolo para el intercambio de claves Diffie-Hellman autenticado muy compacto y liviano con claves efímeras, denominado EDHOC Ephemeral Diffie-Hellman Over COSE) [23]
Como se indica en la tabla Dx, EDHOC proporciona autenticación mutua, secreto de reenvío y protección de identidad. EDHOC está diseñado para su uso en escenarios restringidos como NB-IoT [24], 6TiSCH [25] y LoRaWAN [26].
Su uso principal es establecer un contexto de seguridad de objetos para entornos RESTful restringidos (OSCORE) [27]. Al reutilizar el cifrado y firma de objetos CBOR [28] (COSE) para la criptografía, la representación concisa de objetos binarios

(CBOR) para la codificación y, el protocolo de aplicación restringida (CoAP) para el transporte, el tamaño del código adicional (overload) puede mantenerse muy bajo.

RFC Número y Título	Descripción
RFC 9528 Ephemeral Diffie-Hellman Over COSE (EDHOC)	*Este documento especifica un intercambio de claves Diffie-Hellman autenticado muy compacto y liviano con claves efímeras. EDHOC proporciona autenticación mutua, secreto de reenvío y protección de identidad.*

Tabla 6: Selección de RFC e I+D relevantes del GT LIKE

2.5 TEEP - The Trusted Execution Environment Provisioning

El Grupo de Trabajo sobre el Protocolo de Entorno de Ejecución de Confianza (TEEP) se constituyó en 2018. El concepto de Entorno de Ejecución de Confianza (TEE) está diseñado para ejecutar aplicaciones en un entorno protegido que impone que cualquier código dentro de ese entorno no puede ser manipulado, y que cualquier dato utilizado por dicho código no puede ser leído o adulterado por ningún proceso informático fuera de ese entorno, incluyendo un sistema operativo básico, si estuviera presente. En un sistema con múltiples TEE, esto también significa que el código de un TEE no puede ser leído o manipulado por el código de otro TEE. [4]

El TEE proporciona características de seguridad tales como la ejecución aislada y la integridad de las aplicaciones de confianza, junto con disposiciones para mantener la confidencialidad de sus activos. En términos generales, el TEE ofrece un espacio de ejecución que proporciona un mayor nivel de seguridad que un sistema operativo "rico" y más funcionalidad que un elemento seguro. Por ejemplo, las implementaciones del concepto TEE han sido desarrolladas por ARM e Intel, utilizando la tecnología TrustZone y SGX, respectivamente. [29]

El protocolo Trusted Execution Environment Provisioning se ejecuta como un servicio dentro del TEE en un dispositivo determinado, una aplicación de retransmisión o un punto de acceso al servicio en la pila de red del dispositivo y una infraestructura del lado del servidor que interactúa con las aplicaciones y, opcionalmente, las mantiene. Lo antedicho sirve para instalar, actualizar y eliminar mediante programación de aplicaciones en un TEE. [30]

El grupo elaborará los siguientes documentos. El primer documento versará sobre la arquitectura y describirá las entidades implicadas, sus relaciones, supuestos, el marco de codificación y los casos de uso pertinentes. En segundo lugar, se elaborará un documento de solución que incluya la funcionalidad descrita en un protocolo. La elección del formato o formatos de codificación se decidirá en el grupo de trabajo. El grupo podrá documentar varias tecnologías de atestación (testimonio/alegación)

teniendo en cuenta las diferentes capacidades de hardware, rendimiento, privacidad y propiedades operativas.
En las tablas 7 y 8 se describe un subconjunto de los documentos relevantes y actualizados producidos por el GT TEEP. [31]

RFC Número y Título	Descripción
RFC 9397 Trusted Execution Environment Provisioning (TEEP) Architecture	*This architecture document discusses the motivation for designing and standardizing a protocol for managing the lifecycle of Trusted Applications running inside such a TEE.*

Tabla 7: Selección de RFC e I+D relevantes del GT TEEP

Draft Título	Descripción
TEEP Usecase for Confidential Computing in Network	*This document is a use case and extension of TEEP architecture and could provide guidance for cloud computing, MEC and other scenarios to use confidential computing in network.*
Trusted Execution Environment Provisioning (TEEP) Protocol	*This document specifies a protocol that installs, updates, and deletes Trusted Components in a device with a Trusted Execution Environment (TEE). This specification defines an interoperable protocol for managing the lifecycle of Trusted Components*

Tabla 8: Selección de RFC e I+D relevantes del GT TEEP

2.6 SUIT - Software Updates for Internet of Things

Las vulnerabilidades de los dispositivos de Internet de las Cosas (IoT) han planteado la necesidad de un mecanismo seguro de actualización del firmware que, también sea adecuado para dispositivos con limitaciones, del tipo Clase 1 (~10 KiB de RAM y ~100 KiB de FLASH). Expertos en seguridad, investigadores y reguladores recomiendan que todos los dispositivos IoT estén equipados con tales mecanismos. Actualmente se utilizan mecanismos propietarios de actualización de firmware, no existe un enfoque interoperable y moderno que permita actualizar, de forma segura, el firmware de los dispositivos IoT.
El GT SUIT (Software Updates for Internet of Things) [32] ha completado el trabajo produciendo los documentos que describen una solución de actualización de firmware.
Los documentos entregables del SUIT WG son:

* Una especificación de formato de manifiesto SUIT utilizando CBOR. [16] (Concise Binary Object Representation)
* Extensiones al manifiesto SUIT para capacidades opcionales, que incluyen:
  - Cifrado de firmware,
  - Dominios de confianza,
  - Gestión de actualizaciones, y
  - Inclusión de un archivo en formato MUD (Manufacturer Usage Description Specification) [33].
* Un método seguro para que un dispositivo IoT informe sobre el estado de actualización del firmware.

El WG SUIT ha seleccionado el formato de serialización CBOR y los mecanismos criptográficos COSE [c1] asociados para codificar el manifiesto SUIT.
El WG busca mantener una mínima cantidad de formatos de actualización de forma tal de reducir la complejidad de una solución de gestión de firmware. Otros de los motivos por los cuales se prefiere una cantidad muy pequeña de formatos de actualización es la de permitir la mayor integración e interoperabilidad de SUIT con otras tecnologías y ecosistemas de IoT.

RFC Número y Título	Descripción
RFC 9019 *A Firmware Update Architecture for Internet of Thing*	*Las vulnerabilidades en los dispositivos de IoT han aumentado la necesidad de un mecanismo de actualización de firmware confiable, seguro y adecuado para dispositivos con limitaciones de recursos. Incorporar dicha actualización* *El mecanismo es un requisito fundamental para corregir vulnerabilidades, pero también permite otras capacidades importantes como la actualización, ajustes de configuración y agregar nuevas funciones.*

Tabla 9: Selección de RFC e I+D relevantes del GT SUIT

2.7 RATS - Remote ATtestation ProcedureS

El grupo de trabajo sobre procedimientos de atestación remota (RATS) se formaliza para elaborar una arquitectura, unos protocolos y unos modelos de datos que permitan, a varias contrapartes, evaluar la fiabilidad de los componentes que se conectan a distancia.
La cuestión de cómo un sistema puede saber que otro sistema es de fiar ha cobrado relevancia en un mundo en el que los elementos informáticos de confianza están madurando en las arquitecturas de los procesadores.
Los sistemas, de los que se ha atestiguado y verificado que están en buen estado, pueden mejorar la confianza general del sistema. [4]

A la inversa, los sistemas cuyo buen estado no pueda certificarse ni verificarse su buen aspecto, se les puede reducir el acceso o los privilegios, ponerlos fuera de servicio o ser señalados para su remediación. [34]

En los intercambios de protocolos de red, a menudo se da el caso de que una entidad (una Parte que Confía) necesita pruebas sobre el par remoto, con el fin de evaluar la fiabilidad del par. Los procedimientos de atestación remota (RATS) determinan si las partes que confían pueden establecer un nivel de confianza en la fiabilidad de los pares remotos, denominados Attesters. El objetivo se logra mediante un procedimiento de evaluación en dos etapas facilitado por un tercero de confianza, denominado Verificador, con vínculos de confianza con la cadena de suministro.

En los procedimientos de ATestado Remoto (RATS), uno de los pares (el "Atestiguador ", Attester en inglés") produce información creíble sobre sí mismo ("Evidencia") para que un sistema par remoto (la "Parte que confía, Relying Party en inglés") decida si puede considerar, al Atestiguador, como un par fiable. Los procedimientos de atestación a distancia son suministrados por una entidad, de vital importancia, denominada el "Verificador" (“Verifier” en inglés). [35]

Se puede mencionar, como metas importantes, que el grupo de trabajo ya ha definido una arquitectura para la certificación a distancia. El grupo de trabajo normalizará los formatos para describir las pruebas y los resultados de la certificación, así como los procedimientos y protocolos asociados para transmitir las evidencias para su evaluación a un verificador y los resultados de la certificación a la parte que confía. Además, el GT estandarizará formatos para endosos y valores de referencia, y podrá aplicar y/o perfilar protocolos existentes (por ejemplo, DTLS, CoAP o MUD) para transmitirlos al verificador.

El GT seguirá cooperando y coordinando con otros GT del IETF, como TEEP, SUIT, CoRE, ACE y CBOR, y trabajando con organizaciones de la comunidad, como el TCG [36], la Plataforma Global [37] y la Alianza FIDO. [38]

En las Tablas 10 y 11 se describe un subconjunto de los documentos relevantes y actualizados producidos por el GT RATS. [39]

RFC Número y Título	Descripción
RFC 9334 Remote ATtestation procedureS (RATS) Architecture	*Este documento ofrece una visión general de la arquitectura de las entidades implicadas que hacen posibles las pruebas mediante el proceso de generación, transmisión y evaluación de Demandas probatorias. Proporciona un modelo neutral con respecto a las arquitecturas de procesador, el contenido de las reclamaciones y los protocolos*

Tabla 10: Selección de RFC e I+D relevantes del GT RATS

Draft Título	Descripción
Attestation Results for Secure Interactions	*En este documento se definen los elementos de información reutilizables. Se pueden evaluar diferentes aspectos del evaluado, cuando estos elementos se ofrecen, como evidencia, a las partes que confían*
Reference Interaction Models for Remote Attestation Procedures	*Este documento describe los modelos de interacción para los procedimientos de atestación remota (RATS). Se exponen y definen tres mecanismos de transmisión: Desafío/Respuesta (Challenge/Response), Uni-Direccional (Uni-Directional), y Streaming Remote Attestation.*

Tabla 11: Selección de RFC e I+D relevantes del GT RATS

References

[1] Ishaq, Isam, et al. "IETF standardization in the field of the internet of things (IoT): a survey." Journal of Sensor and Actuator Networks 2.2 (2013): 235-287.
[2] The Internet of Things, https://www.ietf.org/topics/iot/, Revisado 20 Marzo 2024.
[3] Internet of Things Directorate (iotdir) https://datatracker.ietf.org/group/iotdir/reviews/ , Revisado 20 Marzo 2024.
[4] G. Mercado, M.I. Robles, “Protocolos y Estándares del IETF/IRTF para IoT”, SASE 2023 (Simposio Argentino de Sistemas Embebidos”, Agosto 2023.
[5] R Morabito and J Jiménez, “ IETF Protocol Suite for the Internet of Things: Overview and Recent Advancements”, IEEE Communications Standards Magazine, June 2020
[6] Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security Version 1.2", RFC 6347, DOI 10.17487/RFC6347, January 2012,
[7] H. Tschofenig, Ed.T. Fossati, “Transport Layer Security (TLS)/Datagram Transport Layer Security (DTLS) Profiles for the Internet of Things” Request for Comments: 7925, ISSN: 2070-172, July 2016
[8] Shelby, Z., Hartke, K., and C. Bormann, "The Constrained Application Protocol (CoAP)", RFC 7252, DOI 10.17487/RFC7252, June 2014,
[9] Bormann, C., Lemay, S., Tschofenig, H., Hartke, K., Silverajan, B., and B. Raymor, "CoAP (Constrained Application Protocol) over TCP, TLS, and WebSockets", Work In Progress, draft-ietf-core-coap-tcp-tls-03, July 2016.
[10] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, DOI 10.17487/RFC5246, August 2008,
[11] Authentication and Authorization for Constrained Environments (ace) WG, https://datatracker.ietf.org/wg/ace/about/ Revisado 4 de Abril 2024.
[12] M. Sahni, Ed.S. Tripathi, Ed.”Constrained Application Protocol (CoAP) Transfer for the Certificate Management Protocol” RFC 9482, ISSN: 2070-1721, November 2023

[13] O. Bergmann, J. Preuß Mattsson and G. Selander “Extension of the Datagram Transport Layer Security (DTLS) Profile for Authentication and Authorization for Constrained Environments (ACE) to Transport Layer Security (TLS)”, RFC: 9430, ISSN: 2070-1721, July 2023
[14] Authentication and Authorization for Constrained Environments (ace) Documents, https://datatracker.ietf.org/wg/ace/documents/ , Revisado 4 de Abril 2024
[15] J. Schaad, “CBOR Object Signing and Encryption (COSE)”, RFC 8152, ISSN: 2070-1721, July 2017.
[16] C. Bormann, P. Hoffman, “Concise Binary Object Representation (CBOR), RFC 7049, ISSN: 2070-1721, October 2013.
[17] CBOR Object Signing and Encryption (cose), https://datatracker.ietf.org/wg/cose/about/ Revisado 25 de Marzo 2024
[18] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley and W. Polk, “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”, RFC 5280, May 2008
[19] H. Tschofenig, Ed., T. Fossati, “Transport Layer Security (TLS) / Datagram Transport Layer Security (DTLS) Profiles for the Internet of Things”, RFC 7925, ISSN: 2070-1721, July 2016
[20] IEEE 802.1AR-2009: Secure Device Identity, https://1.ieee802.org/security/802-1ar-2009/, Revisado 22 de Marzo de 2024.
[21] CBOR Object Signing and Encryption (cose) Documents, https://datatracker.ietf.org/wg/cose/documents/ Revisado 25 de Marzo 2024
[22] IETF Working Group. Responsible AD: Paul Wouters. LAKE Lightweight Authenticated Key Exchange (charter-ietf-lake-02) 19 de julio de 2023
[23] Göran Selander, John Preuß Mattsson, Francesca Palombini. “Ephemeral Diffie-Hellman Over COSE (EDHOC)”, RFC 9528, ISSN: 2070-1721,22 de e nero de 2024
[24] GSM Association (Global System for Mobile Communications Association)
[25] Pascal Thubert. “An Architecture for IPv6 over the Time-Slotted Channel Hopping Mode of IEEE 802.15.4 (6TiSCH)”, RFC 9030, ISSN: 2070-172, 29 de mayo de 2021
[26] LoRa Alliance
[27] Jim Schaad, August Cellars. CBOR Object Signing and Encryption (COSE): Structures and Process RFC 9052, versión obsoleta RFC 8152. 30 de agosto de 2022
[28] Göran Selander, John Preuß Mattsson, Francesca Palombini, Ludwig Seitz. “Object Security for Constrained RESTful Environments (OSCORE)”, RFC 8613, ISSN: 2070-1721, July 2019.
[29] Trusted Execution Environment Provisioning (teep) about
https://datatracker.ietf.org/wg/teep/about/ ,Revisado 28 Marzo 2024
[30] M. Pei, H. Tschofenig, D. Thaler, D. Wheeler, “Trusted Execution Environment Provisioning (TEEP) Architecture”, RFC 9397, ISSN: 2070-1721, July 2023
[31] Trusted Execution Environment Provisioning (teep) document
https://datatracker.ietf.org/wg/teep/documents/ ,Revisado 28 Marzo 2024
[32] Software Updates for Internet of Things (suit) about, https://datatracker.ietf.org/wg/suit/about/, Revisado 20/ Marzo 2024
[33] E. Lear, R. Droms, D. Romascanu,”Manufacturer Usage Description Specification-MUD”, RFC 8520, ISSN: 2070-1721, March 2019.
[34] Remote ATtestation ProcedureS (rats) about,

https://datatracker.ietf.org/wg/rats/about/, Revisado 3 de Abril 2024
[35] H. Birkholz, D. Thaler, M. Richardson, N. Smith, W. Pan, “Remote ATtestation procedureS (RATS) Architecture”, RFC 9334, ISSN: 2070-1721, January 2023
[36] Trusted Computing Group, https://trustedcomputinggroup.org/about/ Revisado 3 de Abril 2024
[37] Global Plataform, https://globalplatform.org/ , Revisado 3 de Abril 2024
[38] FIDO Fast IDentity Online, https://fidoalliance.org/, Revisado 3 de Abril 2024
[39] Remote ATtestation ProcedureS (rats) documents,
https://datatracker.ietf.org/wg/rats/documents/ , Revisado 3 de Abril 2024