Unión Internacional de Telecomunicaciones

# UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

# X.1366

(09/2020)

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

Aplicaciones y servicios con seguridad (2) – Seguridad en la internet de las cosas (IoT)

## Sistemas de autentificación de mensajes combinados en el entorno de Internet de las cosas

Recomendación UIT-T X.1366

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 | |
| Terminologías | X.1700–X.1701 |
| Generador de números aleatorio cuántico | X.1702–X.1709 |
| Marco de seguridad QKDN | X.1710–X.1711 |
| Diseño de seguridad para QKDN | X.1712–X.1719 |
| Técnicas de seguridad para QKDN | X.1720–X.1729 |
| SEGURIDAD DE LOS DATOS | |
| Seguridad de los macrodatos | X.1750–X.1759 |
| SEGURIDAD DE 5G | X.1800–X.1819 |

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

# Recomendación UIT-T X.1366

## Sistemas de autentificación de mensajes combinados en el entorno de Internet de las cosas


### Resumen

El número de dispositivos de Internet de las cosas (IoT) está aumentando y, en un futuro próximo, un ingente número de dispositivos se conectará a la red IoT, incluida la 5G. En la Recomendación UIT-T X.1366 se especifican dos sistemas de autentificación de mensajes. El primero es un sistema de autentificación de mensajes combinados (AMA) para la IoT, que sirve de mecanismo básico. El segundo es un sistema de autentificación interactiva de mensajes combinados (IAMA), dotado de un protocolo interactivo simple y seguro. Estos sistemas de autentificación de mensajes combinados pueden aplicarse para garantizar tanto la "autentificación (de la identidad) de las entidades", como la "autentificación de los mensajes". Cabe la posibilidad de que estos sistemas no sean aplicables en todos los casos de uso de dispositivos IoT, no obstante, resultan bastante eficaces y adecuados en los casos de uso en los que:

- es necesario autenticar mensajes de decenas a decenas de miles de dispositivos IoT;
- se recurre, de manera frecuente e intermitente, a un proceso de autentificación para la gestión de datos o mensajes.

Por ejemplo, las aplicaciones de vigilancia que utilizan datos de imágenes y las aplicaciones de telemetría a distancia, que garantizan funciones tales como la vigilancia de las actividades de plantas o fábricas y el seguimiento médico, son ejemplos típicos de casos de uso de estos sistemas.



### Historia

| Edición | Recomendación | Aprobación | Comisión de Estudio | ID único* |
|---|---|---|---|---|
| 1.0 | UIT-T X.1366 | 2020-09-03 | 17 | 11.1002/1000/14262 |

### Palabras clave

Autentificación de mensajes combinados (AMA), IoT.


* 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.1366

## Sistemas de autentificación de mensajes combinados en el entorno de Internet de las cosas

### 1 Alcance

En la presente Recomendación se especifican dos sistemas de autentificación de mensajes. El primero es un sistema de autentificación de mensajes combinados (AMA) para la IoT, que sirve de mecanismo básico. El segundo es un sistema de autentificación interactiva de mensajes combinados (IAMA), dotado de un protocolo interactivo simple y seguro. Estos sistemas de autentificación de mensajes combinados pueden aplicarse para garantizar tanto la "autentificación (de la identidad) de las entidades", como la "autentificación de los mensajes".

El método de implementación de estos sistemas en un entorno específico de IoT, así como la tecnología de firma combinada, quedan fuera del alcance de esta Recomendación.

### 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 preconiza que los usuarios de esta Recomendación 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 esta Recomendación, la referencia a un documento, en tanto que autónomo, no le otorga el rango de una Recomendación.

Ninguna.

### 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 código de mensaje de autentificación (MAC, *message authentication code*)** [b-ITU-T X.813]: Valor de verificación criptográfica utilizado para garantizar la autentificación del origen de los datos y la integridad de los datos.

#### 3.2 Términos definidos en la presente Recomendación

En la presente Recomendación se definen los siguientes términos:

**3.2.1 autentificación de mensajes**: Propiedad que garantiza que un mensaje no ha sido modificado durante el proceso de tránsito, a fin de asegurar la integridad de los datos, y permite a la parte receptora verificar la fuente del mensaje.

**3.2.2 autentificación de mensajes combinados (AMA, *aggregate message authentication*)**: Propiedad que permite combinar múltiples códigos de autentificación de mensajes, generados por múltiples remitentes, en un código de autentificación más corto, que un destinatario provisto de las claves secretas de los remitentes pueda verificar.

**3.2.3 etiquetas de autentificación**: Conjunto de datos que se utiliza para autenticar el mensaje.

## 4 Abreviaturas y acrónimos

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

AGT Protocolo de pruebas de grupo adaptativas (*adaptive group testing protocol*)

AMA Autentificación de mensajes combinados (*aggregate message authentication*)

AMAC Código de autentificación de mensajes combinados (*aggregate message authentication code*)

IAMA Autentificación interactiva de mensajes combinados (*interactive aggregate message authentication*)

IoT Internet de las cosas (*Internet of things*)

MAC Código de autentificación de mensajes (*message authentication code*)

XOR Operación O exclusivo (*exclusive OR operation*)

## 5 Convenios

Ninguno.

## 6 Introducción y concepto básico

### 6.1 Introducción

El número de dispositivos de Internet de las cosas (IoT) aumenta a un ritmo constante y, en un futuro próximo, un ingente número de dispositivos se conectará a la red IoT, incluida la 5G. En la presente Recomendación se describe un sistema de autentificación sencillo y seguro, que puede aplicarse en esa situación.

Los códigos de autentificación de mensajes (MAC) figuran entre las primitivas criptográficas más básicas y pueden utilizarse como primitiva criptográfica sencilla para la autentificación de mensajes. No obstante, según se ilustra en la Figura 1, en el contexto de los sistemas IoT actuales, las etiquetas de autentificación (véase la cláusula 3.2.3) de los mensajes enviados desde dispositivos IoT se generan a título individual en el lado del dispositivo y cada mensaje dotado de una etiqueta se comprueba básicamente mediante un proceso de verificación en el lado del receptor. El principal problema detectado en este contexto radica en que la carga de los procesos de autentificación y verificación existentes es directamente proporcional al número de dispositivos IoT implicados.

La tecnología de los códigos de autentificación de mensajes combinados (AMAC) permite comprimir múltiples etiquetas MAC de múltiples mensajes generados por diferentes dispositivos en una sola etiqueta combinada sin poner en riesgo la seguridad (véase el Apéndice II). La ventaja de los códigos AMAC consiste en que las etiquetas combinadas son mucho más pequeñas que la suma de todas las etiquetas MAC, lo que resulta útil en aplicaciones de redes móviles o de redes IoT, a las que se conectan numerosos dispositivos para enviar mensajes. Concretamente, los códigos AMAC pueden utilizarse en aplicaciones, a fin de mejorar la eficiencia de las redes que usan códigos MAC. Sin embargo, este método no suele permitir la detección de mensajes no válidos entre múltiples mensajes, si estos últimos se han considerado no válidos utilizando una etiqueta combinada en AMAC. En la presente Recomendación, el sistema AMAC existente se amplía con objeto de incluir tanto la compresión de múltiples etiquetas MAC como la capacidad de detección para la especificación de mensajes no válidos.

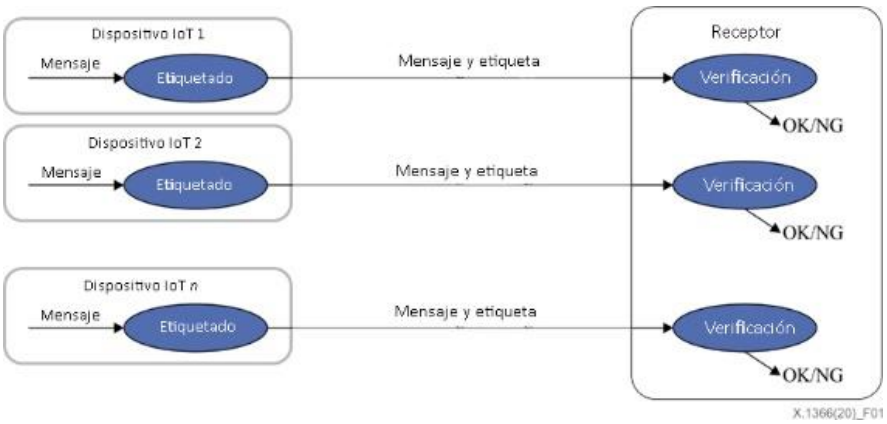


**Figura 1 – Sistema de autentificación individual (sistema convencional)**

## 6.2 Concepto básico de sistema de autentificación de mensajes combinados

### 6.2.1 Consideraciones generales

La Figura 2 ilustra el sistema básico de autentificación de mensajes combinados (AMA) que se propone en la presente Recomendación. En este caso, se instala un nodo de concentración en un sistema de red IoT, a fin de combinar etiquetas de códigos de autentificación de mensajes (MAC) y/o etiquetas de autentificación sin modificar los formatos de entrada o las estructuras de los MAC existentes en la red. El nodo de concentración comprime múltiples etiquetas MAC adjuntas en múltiples mensajes generados por diferentes dispositivos en una sola etiqueta combinada, sin poner en riesgo la seguridad, y la etiqueta combinada se transmite a través de un canal principal a un receptor, que la someterá a un proceso de verificación. El receptor comprueba la validez de los mensajes utilizando la etiqueta combinada, a partir de la cual puede identificar los mensajes o datos no válidos. Esta técnica resulta eficaz para reducir el volumen de datos transmitidos, puesto que la etiqueta combinada es mucho más pequeña que la suma de todas las etiquetas MAC.

En la presente Recomendación se describe un sistema AMA para IoT como mecanismo básico y un sistema IAMA, para especificar el funcionamiento de los procesos de combinación y verificación. En el contexto del sistema AMA, solo se utiliza el canal principal del nodo de concentración al receptor para transmitir la etiqueta combinada. Los algoritmos de combinación y verificación de dicho sistema de detallan en la cláusula 7. En el contexto del sistema IAMA, se utilizan tanto el canal principal como un canal de realimentación, que es un canal autenticado y provisto de un ancho de banda reducido, que va desde el receptor hasta el nodo de concentración. Una vez transmitido el resultado de la verificación del receptor al nodo de concentración a través del canal de realimentación, dicho nodo puede comprimir las etiquetas MAC con mayor eficacia que el sistema AMA de la cláusula 7. Entre el nodo de concentración y el receptor, se ejecuta el protocolo interactivo de verificación especificado en la cláusula 8.

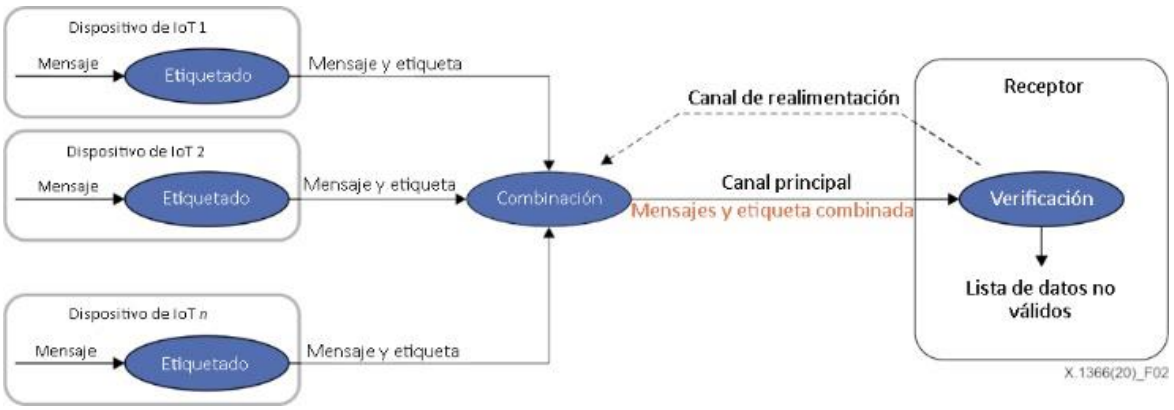


**Figura 2 – Concepto básico de sistema de autentificación de mensajes combinados**

NOTA – La técnica de combinación descrita en esta Recomendación puede aplicarse para comprimir múltiples etiquetas MAC en los casos en que múltiples dispositivos envían datos privados utilizando sistemas de encriptación previa al MAC.

En la presente Recomendación se describen cuatro procesos utilizados para ejecutar sistemas AMA e IAMA, a saber: la generación de claves, el etiquetado, la combinación y la verificación.

1) La generación de claves toma un parámetro de seguridad y un ID como entrada y produce una clave secreta para el ID.
2) El etiquetado toma un mensaje, un ID y la clave secreta correspondiente al ID como entrada y produce una etiqueta.
3) La combinación toma múltiples tuplas de ID, mensajes y etiquetas de múltiples dispositivos como entrada y produce una tupla de etiquetas combinadas como salida.
4) La verificación toma todas las claves secretas, múltiples pares de ID y mensajes de múltiples dispositivos y una tupla de etiquetas combinadas como entrada. A continuación, especifica los mensajes no válidos y produce una lista de ID de dispositivo cuyos mensajes no son válidos.

## 7 Autentificación de mensajes combinados

### 7.1 Consideraciones generales

El sistema de códigos de autentificación de mensajes combinados (AMAC) descrito en la presente Recomendación permite tanto combinar múltiples etiquetas MAC en una etiqueta más corta, como identificar mensajes no válidos a partir de ella. En esta cláusula se detalla el proceso de construcción de los cuatro algoritmos utilizados para generar códigos AMAC, a saber, los algoritmos de generación de claves, etiquetado, combinación y verificación.

### 7.2 Notación específica

En la presente Recomendación, se utilizan las siguientes notaciones específicas:

$n$ Número de dispositivos

$d$ Número de mensajes no válidos de dispositivos

$id$ ID de un dispositivo. El $ID = \{id_1, id_2, \ldots, id_n\}$ será el conjunto de todos los ID.

$m$ Mensaje

$k_{id}$ Clave secreta de un dispositivo *id.* A modo de simplificación, $k_i$ denota la clave secreta correspondiente a $id_i$ en lugar de $k_{id_i}$

$F()$ Función MAC que toma una clave secreta y un mensaje como entrada y produce una etiqueta MAC

$G = (g_{i,j})$ Matriz disyunta *d* con *u* filas y *n* columnas. La matriz *G* tiene entradas en {0,1}, y las columnas están indexadas por ID, $id_1, id_2, \ldots, id_n$. Se entiende que $G$ es disyuntiva *d*, si las sumas booleanas de cualquiera de las columnas *d* de $G$ no contienen ninguna otra columna, donde $x = (x_1, x_2, \ldots, x_u)$ contiene $y = (y_1, y_2, \ldots, y_u)$ si $x_i \geq y_i$ para cada $1 \leq i \leq u$

$I(G, i)$ El conjunto de *j* ($1 \leq j \leq n$), de tal manera que $g_{i,j} = 1$ para cada *i* = 1,2 ..., *u*

$\oplus$ Funcionamiento de XOR (O exclusivo) a nivel de bits

*H*() Función *hash*.

## 7.3 Especificación del algoritmo

Para cubrir aplicaciones más amplias, se proporcionan dos tipos de MAC combinados con una funcionalidad de detección. El primero se basa en el cifrado XOR (véase la cláusula 7.3.1) y el segundo en una función *hash* (véase la cláusula 7.3.2).

### 7.3.1 Construcción basada en XOR

#### 7.3.1.1 Generación de claves

Para cada $id$, este proceso genera una clave aleatoria, cuya notación es $k_{id}$.

#### 7.3.1.2 Etiquetado

El algoritmo de etiquetado toma un mensaje, un ID y la clave secreta correspondiente a dicho ID, cuya notación es $id, m, k_{id}$, respectivamente, como entrada, y produce una etiqueta MAC *t*, que se calcula mediante $F(k_{id}, m)$.

#### 7.3.1.3 Combinación

El algoritmo de combinación toma los ID, los mensajes y las etiquetas MAC correspondientes de *n* dispositivos, cuya notación es $(id_1, m_1, t_1), \ldots, (id_n, m_n, t_n)$, como entrada. Para cada *i* ($1 \leq i \leq u$), toma el XOR a nivel de bits de las etiquetas MAC, cuyos ID correspondientes se incluyen en $I(G, i)$, y lo define como $T_i$, esto es $T_i = \oplus_{j \in I(G,i)} t_j$. A continuación, produce una etiqueta combinada $(T_1, T_2, \ldots, T_u)$.

#### 7.3.1.4 Verificación

El algoritmo de verificación toma todas las claves secretas, cuya notación es $(k_1, \ldots, k_n)$, múltiples pares de ID y mensajes de *n* dispositivos, cuya notación es $(id_1, m_1), \ldots, (id_n, m_n)$, y una etiqueta combinada, cuya notación es $(T_1, T_2, \ldots, T_u)$, como entrada. A continuación, produce una lista *J*, aplicando el siguiente procedimiento:

Paso 1: $J \leftarrow \{id_1, id_2, \ldots, id_n\}$

Paso 2: Para $i = 1,2, \ldots, u$, procede como sigue:

Si $T_i = \oplus_{j \in I(G,i)} t_j$, entonces $J \leftarrow J \setminus \{id_j\}$ para todos los $j \in I(G, i)$.

### 7.3.2 Construcción basada en una función hash

#### 7.3.2.1 Generación de claves

Para cada $id$, este proceso genera una clave aleatoria, cuya notación es $k_{id}$.

#### 7.3.2.2 Etiquetado

El algoritmo de etiquetado toma un mensaje, un ID y la clave secreta correspondiente a dicho ID, cuya notación es $id, m, k_{id}$, respectivamente, como entrada, y produce una etiqueta MAC *t*, que se calcula mediante $F(k_{id}, m)$.

#### 7.3.2.3 Combinación

El algoritmo de combinación toma los ID, los mensajes y las etiquetas MAC correspondientes de *n* dispositivos, cuya notación es $(id_1, m_1, t_1), \dots, (id_n, m_n, t_n)$, como entrada. Para cada $i$ $(1 \leq i \leq u)$, calcula un valor hash de etiquetas MAC, cuyos ID correspondientes se incluyen en $I(G, i)$, y lo define como $T_i$, esto es $T_i = H(t_{j_1}, t_{j_2}, \dots)$, siendo $I(G, i) = \{j_1, j_2, \dots\}$ con $1 \leq j_1 < j_2 < \cdots$.

A continuación, produce una etiqueta combinada $(T_1, T_2, \dots, T_u)$.

#### 7.3.2.4 Verificación

El algoritmo de verificación toma todas las claves secretas, cuya notación es $(k_1, \dots, k_n)$, múltiples pares de ID y mensajes de *n* dispositivos, cuya notación es $(id_1, m_1), \dots, (id_n, m_n)$, y una etiqueta combinada, cuya notación es $(T_1, T_2, \dots, T_u)$, como entrada. A continuación, produce una lista *J*, aplicando el siguiente procedimiento:

Paso 1: $J \leftarrow \{id_1, id_2, \dots, id_n\}$

Paso 2: Para $i = 1,2, \dots, u$, procede como sigue:

Si $T_i = H(t_{j_1}, t_{j_2}, \dots)$, siendo $I(G, i) = \{j_1, j_2, \dots\}$ con $1 \leq j_1 < j_2 < \cdots$,

entonces $J \leftarrow J \setminus \{id_j\}$ para todos los $j \in I(G, i)$.

## 8 Autentificación interactiva de mensajes combinados (IAMA)

### 8.1 Consideraciones generales

El sistema IAMA propuesto en la presente Recomendación permite tanto identificar mensajes no válidos, como producir etiquetas más pequeñas que las del sistema AMA descrito en la cláusula 7. Un sistema IAMA consta de dos algoritmos, a saber los de generación de claves y etiquetado, y un protocolo interactivo entre los procesos de combinación y verificación. En esta cláusula se detalla el procedimiento de construcción de los algoritmos y el protocolo en cuestión.

### 8.2 Notación específica

En la presente Recomendación, se utilizan las siguientes notaciones específicas:

| | |
|---|---|
| $n$ | Número de dispositivos |
| $d$ | Número de mensajes no válidos de dispositivos |
| $id$ | ID de un dispositivo. El $ID = \{id_1, id_2, \dots, id_n\}$ será el conjunto de todos los ID. |
| $m$ | Mensaje |
| $k_{id}$ | Clave secreta de un dispositivo *id*. A modo de simplificación, $k_i$ denota la clave secreta correspondiente a $id_i$ en lugar de $k_{id_i}$. |
| $F()$ | Función MAC que toma una clave secreta y un mensaje como entrada y produce una etiqueta MAC |
| AGT | Protocolo de pruebas de grupo adaptativas |
| $\oplus$ | Funcionamiento de XOR (O exclusivo) a nivel de bits |
| $H()$ | Función hash. |

### 8.3 Especificación del protocolo interactivo

Un sistema IAMA puede construirse a partir de una función MAC $F()$ y un protocolo de pruebas de grupo adaptativas (AGT), sobre el que se proporciona más información en el Apéndice III. Estas

construcciones se detallan a continuación utilizando dos tipos de operaciones, a saber, un cifrado XOR o una función *hash* análoga a la utilizada en la construcción de los sistemas AMA.

### 8.3.1 Construcción basada en XOR

#### 8.3.1.1 Generación de claves

Para cada $id$, este proceso genera una clave aleatoria, cuya notación es $k_{id}$.

#### 8.3.1.2 Etiquetado

El algoritmo de etiquetado toma un mensaje, un ID y la clave secreta correspondiente a dicho ID, cuya notación es $id, m, k_{id}$, respectivamente, como entrada, y produce una etiqueta MAC *t*, que se calcula mediante $F(k_{id}, m)$.

#### 8.3.1.3 Combinación y verificación

La combinación y la verificación se construyen a partir de un protocolo AGT, tal y como ilustra la Figura 3. El algoritmo de combinación toma como entrada todo el conjunto de identificadores $ID = \{id_1, id_2, \dots, id_n\}$, mensajes y etiquetas MAC correspondientes de *n* dispositivos, cuya notación es $(m_1, t_1), \dots, (m_n, t_n)$, siendo $(m_i, t_i)$ $(1 \leq i \leq n)$ un par de etiquetas de mensaje corresponde a $id_i$. El algoritmo de verificación toma el conjunto de identificadores $ID$ y todas las claves secretas $k_i$ $(1 \leq i \leq n)$ correspondientes a $id_i$. En primer lugar, el algoritmo de combinación selecciona un subconjunto $S \subseteq ID$, genera una etiqueta combinada $T_S$ comprimiendo las etiquetas MAC de $S$; $T_S$ puede generarse tomando el XOR de las etiquetas MAC $T_S = \oplus_{j \in S} t_j$. Acto seguido, envía $T_S$ con los mensajes $(m_1, \dots, m_n)$ para su verificación. A continuación, el algoritmo de verificación establece $J = ID$, y comprueba la validez de $T_S$ utilizando las claves secretas de $S$. $T_S$ se considera válida si $T_S = \oplus_{j \in S} t_j$, siendo $t_j = F(k_j, m_j)$; de lo contrario, $T_S$ se considera no válida. Si $T_S$ es válida, establece $J \leftarrow J \setminus S$. El algoritmo de verificación envía el resultado de la comprobación de $T_S$ (es decir, la información de un bit) al de combinación. Posteriormente, el algoritmo de combinación selecciona otro subconjunto $S' \subseteq ID$, genera una etiqueta combinada $T_S$ comprimiendo las etiquetas MAC de $S'$, y somete $T_S$ a verificación. El algoritmo de verificación comprueba la validez de $T_S$ utilizando las claves secretas de $S'$; si $T_S$ es válida, $J \leftarrow J \setminus S'$. El algoritmo de verificación envía el resultado de la verificación de $T_S$ al de combinación. Por último, una vez repetidos todos los procedimientos anteriores, el algoritmo de verificación genera una lista *J*, en la que incluye los ID de los dispositivos cuyos mensajes no son válidos.

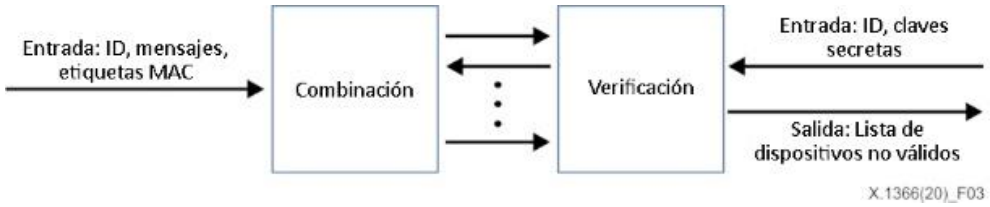


**Figura 3 – Protocolo interactivo entre la combinación y la verificación**

### 8.3.2 Construcción basada en *hash*

#### 8.3.2.1 Generación de claves

Para cada $id$, este proceso genera una clave aleatoria, cuya notación es $k_{id}$.

#### 8.3.2.2 Etiquetado

El algoritmo de etiquetado toma un mensaje, un ID y la clave secreta correspondiente a dicho ID, cuya notación es $id, m, k_{id}$, respectivamente, como entrada, y produce una etiqueta MAC *t*, que se calcula mediante $F(k_{id}, m)$.

#### 8.3.2.3 Combinación y verificación

La combinación y la verificación se construyen a partir de un protocolo AGT, tal y como ilustra la Figura 3. El algoritmo de combinación toma como entrada todo el conjunto de identificadores $D = \{id_1, id_2, \dots, id_n\}$, mensajes y etiquetas MAC correspondientes de *n* dispositivos, cuya notación es $(m_1, t_1), \dots, (m_n, t_n)$, siendo $(m_i, t_i)$ $(1 \leq i \leq n)$ un par de etiquetas de mensaje corresponde a $id_i$. El algoritmo de verificación toma el conjunto de identificadores $ID$ y todas las claves secretas $k_i$ $(1 \leq i \leq n)$ correspondientes a $id_i$. En primer lugar, el algoritmo de combinación selecciona un subconjunto $S \subseteq ID$ y genera una etiqueta combinada $T_S$ calculando un valor *hash* $T_S = H(t_{j_1}, t_{j_2}, \dots)$, siendo $S = \{id_{j_1}, id_{j_2}, \dots\}$ con $1 \leq j_1 < j_2 < \cdots$. Acto seguido, envía $T_S$ con los mensajes $(m_1, \dots, m_n)$ para su verificación. A continuación, el algoritmo de verificación establece $J = ID$, y comprueba la validez de $T_S$ utilizando las claves secretas de $S$. $T_S$ se considera válida si $T_S = H(t_{j_1}, t_{j_2}, \dots)$, siendo $t_j = F(k_j, m_j)$; de lo contrario, $T_S$ se considera no válida. Si $T_S$ es válida, establece $J \leftarrow J \setminus S$. El algoritmo de verificación envía el resultado de la comprobación de $T_S$ (es decir, la información de un bit) al de combinación. Posteriormente, el algoritmo de combinación selecciona otro subconjunto $S' \subseteq ID$, genera una etiqueta combinada $T_S$ comprimiendo las etiquetas MAC de $S'$, y somete $T_S$ a verificación. El algoritmo de verificación comprueba la validez de $T_S$ utilizando las claves secretas de $S'$; si $T_S$ es válida, $J \leftarrow J \setminus S'$. El algoritmo de verificación envía el resultado de la verificación de $T_S$ al de combinación. Por último, una vez repetidos todos los procedimientos anteriores, el algoritmo de verificación genera una lista *J*, en la que incluye los ID de los dispositivos cuyos mensajes no son válidos.

# Anexo A

# Orientaciones y limitaciones

(Este anexo forma parte integrante de la presente Recomendación.)

## A.1 Orientaciones relativas al uso de la autentificación de mensajes combinados

En la presente Recomendación se aborda la aplicabilidad de la integración de un nodo de concentración en los protocolos de código de autentificación de mensaje (MAC) existentes, sin modificar los formatos de entrada o las conexiones de red de los MAC subyacentes. El procedimiento de combinación no prevé el uso de claves, ni requiere el mantenimiento de una clave secreta en el nodo de concentración. Además, se ejecuta únicamente mediante el cálculo de operaciones XOR a nivel de bits o de funciones *hash*, por lo que los sistemas de autentificación de mensajes combinados (AMA) descritos en esta Recomendación son aptos para llevar a cabo la autentificación de forma sencilla.

En el proceso de combinación descrito en la cláusula 7, es necesario generar y almacenar una matriz disyuntiva *d*. Existen varios métodos, como los descritos en [b-TM05], para generar matrices disyuntivas *d*. Además, cabe la posibilidad de utilizar una versión comprimida de una matriz disyuntiva *d*, como la descrita en [b-MK19]. En la presente Recomendación, se propone utilizar dichas técnicas incluso en los sistemas AMA. En el caso de una matriz disyuntiva $d$ con $u$ filas y $n$ columnas, el sistema AMA es más eficaz que el sistema tradicional de autentificación individual, si $u < n$ y si $d \ll \sqrt{n}$.

NOTA – En este documento, los niveles de seguridad de los sistemas AMA (o IAMA) basados en el cifrado XOR a nivel de bits o en funciones *hash* se describen de acuerdo con los esquemas previstos en [b-HS18] y [b-SS19]. La seguridad se articula en torno a tres conceptos: la "infalsificabilidad", la "integridad de la identificabilidad" y la "solidez (limitada) de la identificabilidad". La infalsificabilidad garantiza que ningún mensaje pueda ser falsificado, la integridad de la identificabilidad que el sistema considere válido todo mensaje válido y la solidez de la identificabilidad que el sistema considere no válido todo mensaje no válido, mientras que la solidez limitada de la identificabilidad es un concepto similar al de la solidez de la identificabilidad, con la diferencia de que, en principio, los adversarios no deben obtener ninguna etiqueta MAC válida, ni corromper ningún dispositivo, antes de atacar. La solidez limitada sigue siendo útil en el contexto de las aplicaciones, ya que engloba la manipulación de mensajes.

A continuación, se describen los niveles de seguridad de los sistemas AMA (o IAMA) previstos en esta Recomendación. Las construcciones basadas en XOR cumplen la infalsificabilidad, la identificabilidad plena y la solidez limitada de la identificabilidad, si el MAC subyacente cumple la infalsificabilidad. Las construcciones basadas en *hash* cumplen la infalsificabilidad, la identificabilidad plena y la solidez de la identificabilidad, si el MAC subyacente cumple la infalsificabilidad y la función *hash* se considera una función aleatoria.

## A.2 Limitaciones del uso de la autentificación de mensajes combinados

En la presente Recomendación, se supone que el número de mensajes no válidos es como máximo *d* en los sistemas AMA y este parámetro se incluye entre los parámetros de sistema, lo que entraña la necesidad de calcular el número *d* previamente.

Si el número de mensajes no válidos excede el valor *d* supuesto, el algoritmo de verificación genera una lista *J* que contiene más de *d* ID de dispositivos. En este caso, la lista *J* puede comprender no solo los ID de los dispositivos que han enviado mensajes no válidos, sino también los ID de algunos dispositivos que han enviado mensajes válidos. En consecuencia, se recomienda volver a establecer un valor *d* mayor para el sistema AMA.

# Anexo B

## Combinación con los actuales protocolos de autentificación individual

(Este anexo forma parte integrante de la presente Recomendación.)

Los sistemas AMA (o IAMA) descritos en la presente Recomendación pueden combinarse con los sistemas tradicionales de autentificación individual. Al igual que en los AMA, los sistemas tradicionales de autentificación individual son sistemas en los que la matriz disyuntiva subyacente es la matriz de identidad. En el caso de los dispositivos $n = n_1 + n_2$, si se prefiere combinar solo $n_1$ etiquetas MAC entre $n$ etiquetas MAC, cabe proceder como sigue: por un lado, se utiliza un sistema AMA (o IAMA) para los dispositivos $n_1$ y, por otro, se utiliza un sistema de autentificación individual para los dispositivos $n_2$ restantes, según se indica en Figura B.1.

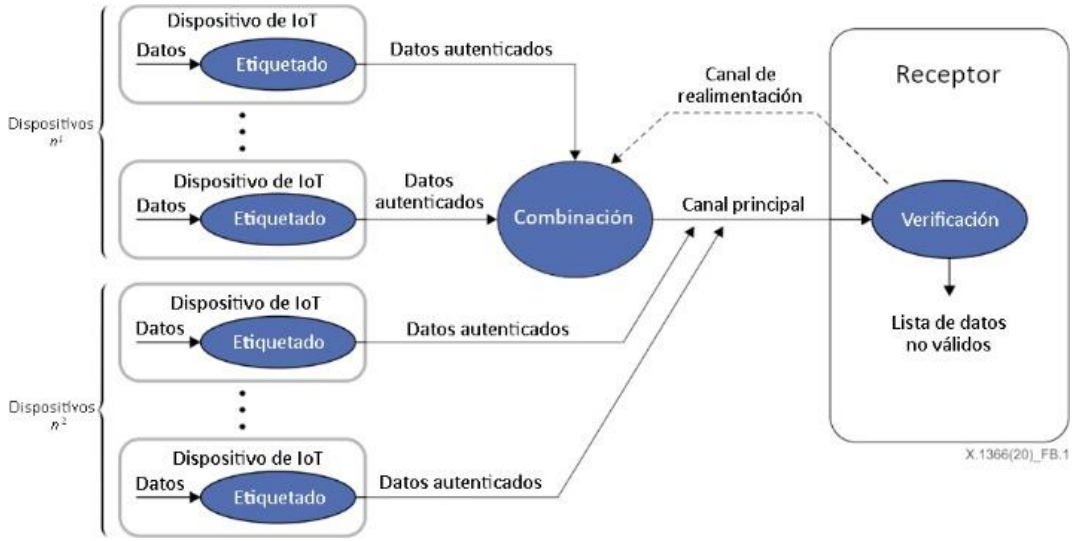


**Figura B.1 – Combinación con protocolos de autentificación individual**

# Apéndice I

## Casos de uso de sistemas de autentificación de mensajes combinados

(Este apéndice no forma parte integrante de la presente Recomendación.)

### I.1 Introducción

Los sistemas de autentificación de mensajes combinados pueden aplicarse para garantizar tanto la "autentificación (de la identidad) de las entidades", como la "autentificación de los mensajes". Cabe la posibilidad de que estos sistemas no sean aplicables en todos los casos de uso de dispositivos de Internet de las cosas (IoT), no obstante, resultan bastante eficaces y adecuados en los casos de uso en los que:

- es necesario autenticar mensajes de decenas a decenas de miles de dispositivos IoT;
- se recurre, de manera frecuente e intermitente, a un proceso de autentificación para la gestión de datos y/o mensajes.

A continuación se exponen ejemplos concretos de aplicaciones que, en principio, podrían utilizar la tecnología de autentificación combinada:

a) Aplicaciones para el envío conciso y frecuente de datos y/o mensajes, como datos de imágenes de cuasivídeo (imágenes fijas):
   - aplicaciones de vigilancia que utilizan datos de imágenes.

b) Aplicaciones de la telemetría a distancia:
   - aplicaciones para la vigilancia de las actividades de las fábricas;
   - aplicaciones para el estudio de las dinámicas de las audiencias;
   - aplicaciones para el seguimiento sanitario, como *Citizen Marathon*;
   - aplicaciones para la gestión de instalaciones, por ejemplo, el alumbrado público de zonas urbanas;
   - aplicaciones para la vigilancia del tráfico; y
   - aplicaciones para la vigilancia del nivel de los ríos.

La integración de la tecnología de autentificación combinada en estas aplicaciones de IoT puede mejorar drásticamente la eficiencia de los procesos de transmisión y autentificación de mensajes en todo el sistema IoT.

Los siguientes casos de uso constituyen ejemplos de utilización del sistema de autentificación combinada descrito en la presente Recomendación.

### I.2 Caso de uso 1: Parques temáticos y centros de ocio

En espacios de la índole de parques temáticos y centros de ocio, cabe suponer una densidad de entre 1 000 y 10 000 visitantes al mismo tiempo, lo que equivale a miles de personas dotadas de los privilegios necesarios para hacer uso de las atracciones del parque/centro, que quizás deban someterse a verificación de forma simultánea. En este caso, un sistema de autentificación combinada puede resultar perfectamente apto para gestionar las autorizaciones de forma eficiente. Según se ilustra en la Figura I.1, cada atracción puede contar con una serie de servidores combinados, encargados de recopilar y combinar etiquetas de autentificación para solicitar la verificación del servidor de autentificación de soporte.

En concreto, los visitantes compran por adelantado una entrada con una serie de chips integrados, en los que se almacena la información relativa a los eventos, la admisión a las atracciones y los servicios web prestados. Esta tecnología suele utilizarse en los maratones. En lugar de las entradas, también podrían utilizarse pulseras con chips integrados.

En la puerta principal del lugar de celebración del evento o a la entrada de cada atracción, el contenido de la entrada se lee, se combina mediante tecnología de autentificación combinada y se envía al servidor de autentificación combinada.

El centro del servidor de autentificación combinada analiza el contenido y los requisitos del servicio prestado a los visitantes, informa a las diversas atracciones y a los proveedores del servicio web, y utiliza la información para analizar y predecir la congestión. Una vez efectuada la verificación, los visitantes pueden utilizar diversos servicios web registrados empleando sus propios teléfonos inteligentes o dispositivos ponibles con forma de gafas, entre otros sistemas.

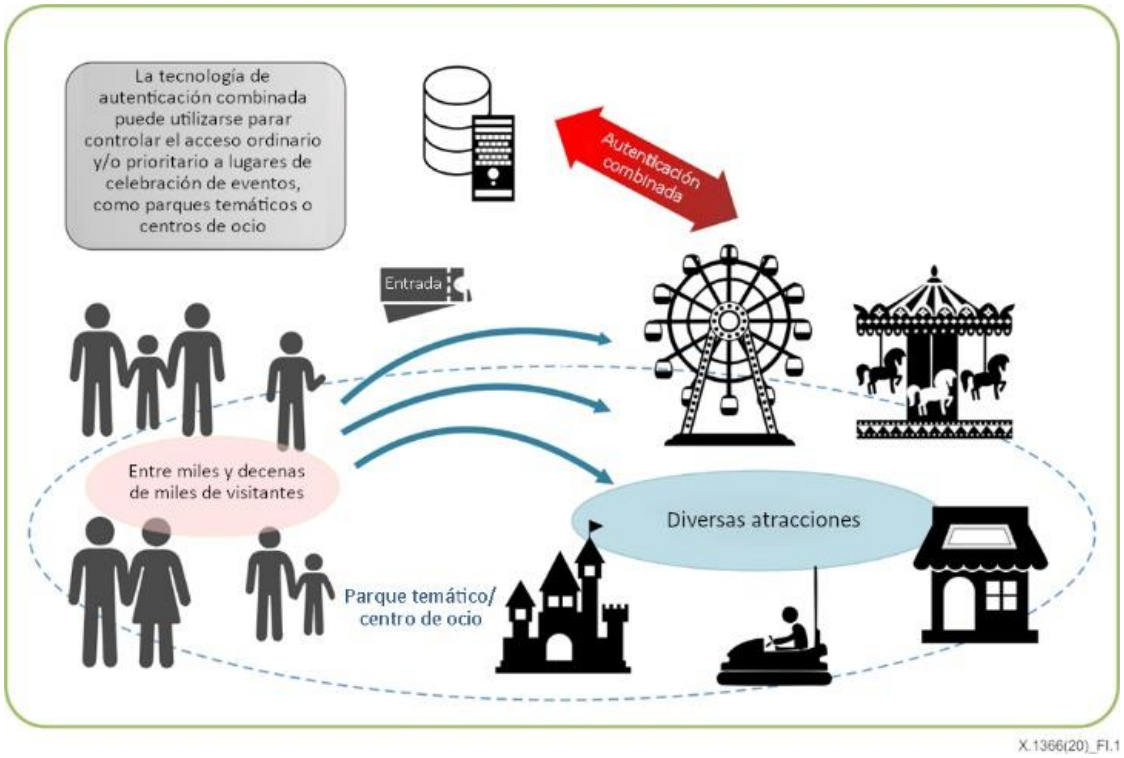


**Figura I.1 – Sistema de autentificación combinada en parques temáticos y centros de ocio**

## I.3 Caso de uso 2: Sensores de vigilancia

### I.3.1 Consideraciones generales

El seguimiento de las actividades mediante sensores de vigilancia, como cámaras de dispositivos IoT, a fin de garantizar la alerta y la intervención tempranas en situaciones de catástrofe natural y accidentes y/o incidentes, puede integrar un caso de uso de los sistemas de autentificación combinada descritos en la presente Recomendación. En este caso, las imágenes fijas o de cuasivídeo captadas por varias cámaras de vigilancia se envían a un centro de vigilancia prácticamente en tiempo real (o de forma periódica), pero es importante velar por la fiabilidad e integridad de los datos que se envían.

No obstante, en los casos en que se registra un número muy elevado de sensores de vigilancia, el procedimiento consistente en verificar los códigos de autentificación vinculados a los datos de las imágenes de las cámaras comprobando el código de autentificación de las cámaras uno por uno ya no resulta eficiente. En un contexto como este, el sistema de autentificación combinada es eficaz. Los códigos de autentificación vinculados a los datos pueden combinarse en los servidores combinados antes de su envío al centro de vigilancia, de modo que todo el sistema IoT pueda proporcionar una función de autentificación y unas comunicaciones eficientes. El número de servidores combinados depende del número de sensores de vigilancia. La Figura I.2 ilustra una serie de sensores de vigilancia en el marco de un sistema de autentificación combinada.

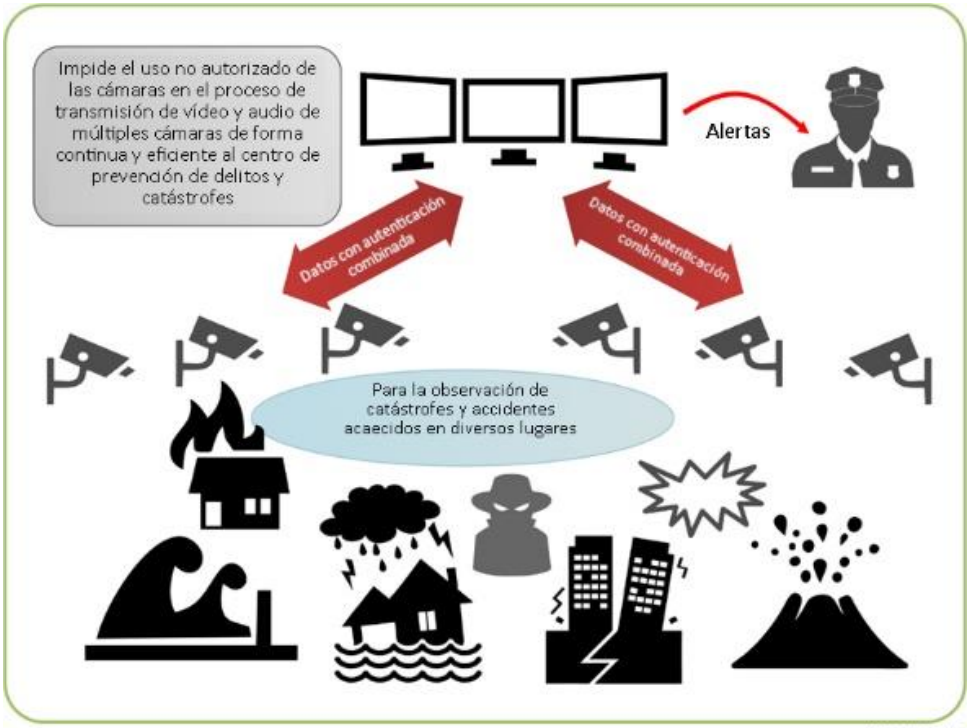


**Figura I.2 – Sensores de vigilancia en un sistema de autentificación combinada**

### I.3.2 Casos de uso específicos

1) Vigilancia de entornos de vida, tales como comunidades y viviendas

La información relativa al entorno vital procedente de diversos sensores, en especial cámaras de vigilancia instaladas en edificios de apartamentos, comunidades inteligentes, casas particulares, etc., se combina en una pasarela (concentrador IoT) y se transmite a un servidor central mediante tecnología de autentificación combinada.

El centro analiza la información recibida y la utiliza para facilitar la vigilancia del entorno, predecir anomalías y fallos, responder con prontitud y prevenir delitos y catástrofes.

En concreto, los datos recopilados a través de dispositivos tales como sensores ambientales, sensores de electrodomésticos, cámaras de vigilancia, sensores de apertura y/o cierre de puertas y/o ventanas, sensores de funcionamiento de la infraestructura de gas y/o agua y/o electricidad o sensores de vigilancia de ascensores se envían a centros externos. Los sistemas de autentificación combinada que engloban tanto la autentificación del terminal, como la autentificación de los datos, son eficaces como medio de autentificación para reunir cantidades grandes y diversas de datos y transmitirlas de manera eficiente.

2) Mantenimiento y vigilancia de la infraestructura social y respuesta a las catástrofes

La IoT está empezando a utilizarse en diversos ámbitos a efectos del mantenimiento y la gestión de la infraestructura social, por ejemplo puentes, túneles y carreteras, y, con toda probabilidad, los servicios IoT desempeñarán un papel sumamente importante en la construcción de una sociedad segura y protegida en un futuro próximo. Por ejemplo, en infraestructuras como puentes y carreteras elevadas obsolescentes, diversos sensores captan en detalle datos pertinentes (véanse las tensiones, las vibraciones, el desplazamiento, la inclinación, etc.) e información de vídeo. Así, los volúmenes de datos destinados a los centros están alcanzando proporciones ingentes.

Actualmente, el método de autentificación combinada se está revelando sumamente eficaz para mejorar la eficiencia de los circuitos inalámbricos de Internet y evitar la congestión. Además del mantenimiento y la gestión de estas infraestructuras sociales, el método de autentificación combinada

también puede aplicarse a las pasarelas de los sistemas IoT empleados para la vigilancia constante de los niveles hídricos y los cambios en el caudal de ríos y lagos en entornos agrícolas.

3) Sistemas de prevención de catástrofes que utilizan cámaras de vigilancia

Las cámaras de vigilancia se instalan y explotan con diversos fines, entre ellos la prevención de delitos y catástrofes en diversos lugares del mundo. En el contexto de una red que gestiona imágenes e información de audio, suele ser necesario transmitir continuamente una gran cantidad de datos a los centros y, en aras de una transmisión eficiente, resulta eficaz aplicar una técnica de autentificación combinada. Es decir, cabe la posibilidad de mejorar la eficiencia de la comunicación entre el dispositivo IoT y la pasarela IoT y entre la pasarela IoT y el centro correspondiente aplicando el sistema de autentificación combinada.

4) Vigilancia logística y mejora de la eficiencia de los sistemas de transporte

En los sistemas empresariales de logística y transporte, los sistemas IoT se utilizan cada vez más para mejorar la eficiencia y la elevada funcionalidad comercial. Por ejemplo, actualmente, se está poniendo en práctica en varios ámbitos una solución que permite gestionar con precisión la información relativa al estado de las mercancías y los paquetes desde el envío hasta la entrega. En un sistema de ese tipo, se puede lograr una gestión logística más estable y eficiente aplicando la tecnología de autentificación combinada al sistema que envía al centro la información recopilada por los diversos sensores en relación con los paquetes. También se podría proporcionar una pasarela de IoT para vehículos, tales como automóviles equipados con un gran número de sensores, y aplicar la tecnología de autentificación combinada a la pasarela del vehículo para los sistemas de transporte.

# Apéndice II

## Actividades relacionadas con los sistemas de autentificación de mensajes combinados

(Este apéndice no forma parte integrante de la presente Recomendación.)

En [b-KL08], Katz y Lindell propusieron por primera vez un sistema de autentificación de mensajes combinados (AMA), distinto del descrito en la cláusula 7, que permitía combinar múltiples etiquetas MAC de múltiples mensajes en una etiqueta más corta. Concretamente, Katz y Lindell [b-KL08] formalizaron el modelo y la seguridad de este sistema y definieron una construcción simple tomando el XOR a nivel de bits de todas las etiquetas MAC. En el marco de su sistema AMA, se puede verificar la validez de múltiples mensajes con una sola etiqueta más corta, no obstante, suele ser imposible detectar mensajes no válidos entre múltiples mensajes, si estos últimos si estos últimos se han considerado no válidos con respecto a la etiqueta única. Los sistemas AMA de la presente Recomendación permiten combinar múltiples etiquetas MAC en una etiqueta más corta y detectar mensajes no válidos a partir de esta última. El código AMA previsto en la cláusula 7 de la presente Recomendación se basa en [b-HS18], mientras que el protocolo de autentificación interactiva para la autentificación de mensajes combinados previsto en la cláusula 8 se basa en [b-SS19].

# Apéndice III

## Protocolo de pruebas de grupo adaptativas

(Este apéndice no forma parte integrante de la presente Recomendación.)

Según se indica en [b-DH00], las pruebas de grupo constituyen un método que permite detectar elementos especiales, denominados defectuosos, entre un gran número de elementos enteros llevando a cabo un número reducido de pruebas, en lugar de someter cada elemento a pruebas individuales.

En el ejemplo de protocolo de pruebas de grupo, ilustrado en la Figura III.1, se presupone la existencia de *n* elementos, de los cuales *d* son defectuosos.

En las pruebas de grupo adaptativas los ensayos pueden llevarse a cabo varias veces, de tal manera que, una vez observados los resultados del primer ensayo, se pueda seleccionar un subconjunto de elementos y ponerlo a prueba. Una prueba de grupo competitiva es una prueba de grupo adaptativa para la que no es necesario conocer previamente el número *d* de elementos defectuosos.

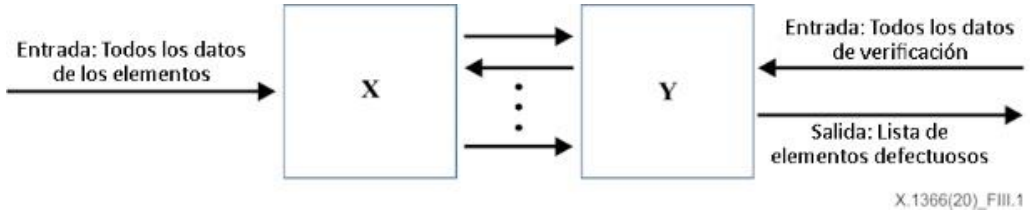


**Figura III.1 – Protocolo de pruebas de grupo adaptativas**

En términos formales, las pruebas de grupo adaptativas son protocolos interactivos entre X e Y, tal y como ilustra la Figura III.1.

*X* toma todo el conjunto de identificadores $ID = \{id_1, id_2, \dots, id_n\}$ y todos los datos de los elementos $\text{data}_i$ $(1 \leq i \leq n)$, correspondientes a $id_i$, e *Y* toma todo el conjunto de identificadores ID y todos los datos de verificación $\text{ans}_i$ $(1 \leq i \leq n)$ correspondientes a $id_i$. En primer lugar, *X* selecciona un subconjunto $S \subseteq ID$, genera $\text{test}_S$ comprimiendo los datos de los elementos de *S* y envía $\text{test}_S$ a *Y*. A continuación, Y establece $J = ID$ y comprueba la validez de $\text{test}_S$ utilizando los datos de verificación de *S*. Si $\text{test}_S$ es válido, se establece $J \leftarrow J \setminus S$. *Y* envía el resultado de la verificación de $\text{test}_S$ (esto es, información de un bit) a *X*. Posteriormente, *X* selecciona otro subconjunto de ID y se repiten los procedimientos entre *X* e *Y*. Por último, una vez repetidos todos los procedimientos anteriores, Y genera una lista *J*, en la que incluye los ID de los dispositivos defectuosos.

Por ejemplo, los protocolos de pruebas de grupo adaptativas incluyen la búsqueda binaria, el algoritmo bifásico denominado *rake and winnow* en [b-EGH07], el algoritmo multietapa de Li de [b-Li62] y el algoritmo de excavación descrito en la cláusula 4.6 de [b-DH00].

# Bibliografía


[b-ITU-T X.813] Recomendación UIT-T X.813 (1996), *Tecnología de la información – Interconexión de sistemas abiertos – Marcos de seguridad en sistemas abiertos: Marco de no rechazo*.

[b-DH00] D. Z. Du and F. K. Hwang, *Combinatorial Group Testing and Its Applications*, Series on Applied Mathematics, vol. 12, 2nd edn. World Scientific, Singapore, 2000.

[b-EGH07] D. Eppstein, M. T. Goodrich, and D. S. Hirschberg, *Improved Combinatorial Group Testing Algorithms for Real-world Problem Sizes*, SIAM J. Comput. 36(5), pp. 1360-1375, 2007.

[b-HS18] S. Hirose and J. Shikata, *Non-adaptive Group-Testing Aggregate MAC Schemes*, The 14th International Conference on Information Security Practice and Experience (ISPEC 2018), LNCS 11125, pp. 357-372, Springer, 2018.

[b-KL08] J. Katz and A.Y. Lindell, *Aggregate message authentication codes*, CT-RSA 2008, LNCS 4964, pp. 155-169. Springer, 2008.

[b-Li62] C. H. Li, *A Sequential Method for Screening Experimental Variables*, J. Am. Stat. Assoc. 57 (298), pp. 455-477, 1962.

[b-MK19] K. Minematsu and N. Kamiya, *Symmetric-key Corruption Detection: When XOR-MACs meet combinatorial group testing*, ESORICS 2019, Part I, LNCS 11735, pp. 595-615, Springer, 2019.

[b-MOV96] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, October 1996, Fifth Printing (August 2001).

[b-SS19] S. Sato and J. Shikata, *Interactive Aggregate Message Authentication Scheme with Detecting Functionality*, The 33rd International Conference on Advanced Information Networking and Applications (AINA-2019), pp. 1316-1328, Springer, 2019.

[b-TM05] N. Thierry-Mieg, *A New Pooling Strategy for High-throughput Screening: the Shifted Transversal Design, BMC Bioinformatics*, vol. 7, no. 28, 2005.

## 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, 2021