INAP
INSTITUTO NACIONAL DE ADMINISTRACIÓN PÚBLICA

# Curso *online*: **Seguridad en Redes WAN e Internet**

## Módulo 4 SERVICIOS DE SEGURIDAD EN REDES

Autores: Daniel Díaz y Andrés Marín

# Índice de contenidos

# CAPÍTULO 1 SERVICIOS Y MECANISMOS DE SEGURIDAD

La recomendación ISO 7498-2, ya obsoleta, al igual que hizo en su día X-800, definían un servicio de seguridad como aquél proporcionado por un sistema de comunicaciones que asegura la adecuada seguridad en una transferencia de datos. Estas arquitecturas definían los servicios de seguridad básicos y su localización en el modelo de referencia OSI, planteando, fundamentalmente, el conjunto de servicios y mecanismos necesarios para proteger los datos durante su transmisión, de las potenciales amenazas, y discutiendo sus interrelaciones. Pese a que el modelo OSI no está en uso actualmente, supuso el primer esfuerzo de dotar a un sistema completo de comunicaciones de seguridad.

Así por ejemplo, el cifrado es un mecanismo que puede ser utilizado para proporcionar total o parcialmente varios servicios de seguridad. Además, un mismo servicio puede ser proporcionado por diferentes mecanismos.

Los servicios de seguridad definidos por OSI se clasifican en cinco tipos:

- Autenticación
- Control de acceso
- Confidencialidad de datos
- Integridad de datos
- No repudio

Aunque hoy en día la arquitectura más común es TCP/IP y es probable que nunca nos encontremos con un sistema diferente, la arquitectura OSI nos ofrece un marco de referencia conceptual, con una separación de niveles que permite enfocar los distintos problemas y funcionalidades requeridas en la comunicación, motivo de muchos quebraderos de cabeza de otras arquitecturas. Por ejemplo, en TCP/IP no existe el concepto de nivel de sesión ni de presentación, lo que ocasiona que la funcionalidad asociada dependa fuertemente de los protocolos y aplicaciones que se usen y sus requisitos, baste citar que en la web se tuvo que incorporar el concepto de sesión como un mecanismo en el protocolo de aplicación.

Los servicios de seguridad definidos por OSI se clasifican en cinco tipos (y no existe variación con la actualidad):

- Autenticación
- Control de acceso
- Confidencialidad de datos
- Integridad de datos

- No repudio

## 1.1. SERVICIOS DE SEGURIDAD

Las normas OSI definen un servicio de seguridad como: "una función suministrada por un sistema de comunicación, para garantizar la seguridad del mismo y de las transferencias de datos". La definición de OSI es consistente con el uso actual.

Los Servicios de Seguridad que se pueden proporcionar en la arquitectura OSI son:

- Autenticación. Es un servicio ofrecido para acreditar fehacientemente a los participantes en una comunicación. Puede ser de dos tipos:

Autenticación de la pareja de entidades que se comunican. Se trata de acreditar dos aspectos: primero, que en el momento de iniciarse la comunicación, la pareja de entidades son las que alegan ser; y segundo, que ninguna tercera suplanta la identidad de una de las entidades de la pareja durante la conexión o pretende repetir una conexión previa. Dos entidades parejas son dos procesos ubicados en el mismo nivel de comunicaciones pero en diferentes sistemas

Se suele utilizar en el establecimiento de, o a veces durante, la fase de transferencia de una conexión para verificar la identidad de una o más entidades. Para su implementación se suelen utilizar mecanismos basados en esquemas de autenticación unidireccional o entre pares.

Autenticación del origen de los datos. Para garantizar que el mensaje proviene de la fuente que realmente lo emitió. Este servicio, cuando se proporciona en algún nivel, garantiza a una entidad de dicho nivel que la fuente del mensaje recibido es la entidad pareja del mismo nivel del otro lado de la comunicación.

- Control de acceso. Es un servicio destinado a regular el acceso a los recursos disponibles a través de un sistema de interconexión. Estos recursos pueden ser dispositivos físicos, programas o datos. Actúa tras la autenticación, una vez que ésta ha concluido satisfactoriamente, y permite o deniega el acceso a un recurso dado a tenor de la identidad fehacientemente autenticada del demandante. Esta identidad del demandante, en la terminología OSI identidad autenticada, puede ser un usuario u otro recurso, como por ejemplo, un programa en ejecución que requiere el acceso a ciertos recursos.

Al ser el control de acceso un servicio suministrado tras la autenticación del demandante se diseña según el perfil de éste, permitiendo unos tipos de accesos u otros a un determinado recurso. Por ejemplo, dada una información (supóngase almacenada en una base de datos) y la identidad de un demandante, se puede autorizar sólo la lectura, o la lectura y escritura, o el borrado, etc. de dicha información.

Los mecanismos para la implementación de este servicio varían desde las simples listas de control de acceso (ACL, *Access Control List*) a los procedimientos de control multinivel.

- Confidencialidad (llamada en la norma confidencialidad de los datos). Protege a los datos de los ataques pasivos y adquiere cuatro modalidades:

- Confidencialidad con conexión. Este servicio proporciona confidencialidad de todos los mensajes en una asociación basada en conexión.
- Confidencialidad sin conexión. Este servicio proporciona confidencialidad de todos los mensajes en una asociación simple sin conexión.
- Confidencialidad en campos seleccionados. Este servicio proporciona confidencialidad en los campos seleccionados de cada mensaje en una asociación con o sin conexión.
- Confidencialidad de Flujo de Tráfico. Este servicio proporciona protección de la información que puede ser derivada de la observación del flujo de tráfico. Esta información puede ser la fuente y el destino, el momento de la transferencia, la frecuencia de las transmisiones, las políticas de encaminamiento, etc.

- Integridad. Garantiza que los mensajes, todos sus campos o sólo algunos, son recibidos sin alteraciones no autorizadas; es decir que son recibidos tal cual fueron emitidos. Lo cual incluye ausencia de duplicaciones (o replicaciones), inserciones, modificaciones o destrucciones.

Hay dos aspectos importantes en relación con la integridad de los datos; por una parte, la integridad de un mensaje o algunos campos del mensaje y por la otra, la integridad de una serie de mensajes (o campos de mensajes) consecutivos. Este servicio admite dos modalidades principales con conexión y sin conexión.

- Integridad con conexión con recuperación o sin recuperación. Este servicio proporciona integridad de todos los mensajes en una asociación y detecta cualquier modificación, inserción, borrado o repetición de cualquier dato en todo el mensaje. Este servicio puede implementarse con o sin recuperación.
- Integridad con conexión en campos seleccionados. Este servicio proporciona integridad de los campos seleccionados en el mensaje de una secuencia completa de mensajes transferidos en una conexión. Puede estar basado en la determinación de cuando los campos seleccionados han sido modificados, insertados, borrados o repetidos.
- Integridad sin conexión. Este servicio proporciona integridad de un mensaje simple sin conexión y puede estar basado en la determinación de cuando un mensaje recibido ha sido modificado. De forma adicional, se puede proporcionar una forma limitada de detección de repeticiones ilegales.
- Integridad sin conexión en campos seleccionados. Este servicio proporciona la integridad de los campos seleccionados en una asociación no orientada a conexión y determina cuando los campos seleccionados del mensaje han sido modificados ilegalmente.

- No repudio evita que el emisor o el receptor de un mensaje puedan renegar de su emisión o de su recepción respectivamente. Es un servicio básico en cualquier modalidad de transacción electrónica. Admite dos modalidades:

    - No repudio con prueba de origen. Con este servicio, el receptor de los datos puede demostrar el origen del mensaje. Este servicio protege frente a cualquier intento del emisor de negar falsamente el envío o el contenido de los datos recibidos.

    - No repudio con prueba de recepción. Proporciona al emisor de los datos una prueba de la recepción de los mismos y le protege frente a cualquier intento del receptor de negar, falsamente, la recepción o el contenido de los datos enviados.

El principal mecanismo involucrado en el no repudio es la firma digital. Una mejora del servicio de no repudio se obtiene mediante la intervención de una notaría de firmas digitales, también denominada Autoridad de Certificación.

En la Tabla 1 se relacionan los tipos y subtipos de servicios con los niveles del modelo de interconexión OSI en que se pueden implantar.

## 1.2. MECANISMOS DE SEGURIDAD

Un mecanismo de seguridad como un dispositivo físico o lógico responsable de suministrar un servicio de seguridad. Sin embargo, un servicio de seguridad puede requerir el concurso de más de un mecanismo de seguridad. La norma diferencia los mecanismos de seguridad en específicos y generales.

### 1.2.1. MECANISMOS DE SEGURIDAD ESPECÍFICOS

Los mecanismos de seguridad específicos son aquellos que implementados en alguna capa del modelo suministran algún servicio de seguridad, o complementan otro mecanismo para conjuntamente proporcionar un servicio de seguridad. Los mecanismos específicos más importantes son: cifrado, firma digital, control de accesos, integridad de los datos, intercambio de autenticación.

| SERVICIOS DE SEGURIDAD EN EL MODELO OSI | | | | | | | |
|---|---|---|---|---|---|---|---|
| Servicio | NIVEL | | | | | | |
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| **Autenticación** | | | | | | | |
| - de la pareja de entidades | 0 | 0 | X | X | 0 | X | X |
| - del origen de los datos | 0 | 0 | X | X | 0 | X | X |
| **Control de acceso** | 0 | 0 | X | X | 0 | X | X |
| **Confidencialidad** | | | | | | | |
| - con conexión | X | X | X | X | 0 | X | X |
| - sin conexión | 0 | X | X | X | 0 | X | X |
| - en campos seleccionados | 0 | 0 | 0 | 0 | 0 | X | X |
| - de Flujo de Tráfico | X | 0 | X | 0 | 0 | 0 | X |
| **Integridad** | | | | | | | |
| - con conexión con recuperación | 0 | 0 | 0 | X | 0 | 0 | X |
| - con conexión sin recuperación | 0 | 0 | X | X | 0 | X | X |
| - con conexión en campos seleccionados | 0 | 0 | 0 | 0 | 0 | X | X |
| - sin conexión | 0 | 0 | X | X | 0 | X | X |
| - sin conexión en campos selecionados | 0 | 0 | 0 | 0 | 0 | X | X |
| **No repudio** | | | | | | | |
| - con prueba de origen | 0 | 0 | 0 | 0 | 0 | X | X |
| - con prueba de recepciónen destino | 0 | 0 | 0 | 0 | 0 | X | X |

- Cifrado

La función inmediata del cifrado es el suministro del servicio de confidencialidad sea de los datos o del flujo de los mismos, pero además es una pieza fundamental para el logro de otros servicios. Este mecanismo supone procedimientos y técnicas de gestión de claves, capaces de generarlas y distribuirlas de manera segura a lo largo de la red.

- Firma digital

Este mecanismo comprende dos procesos, la firma del mensaje y la verificación de la misma.

La firma del mensaje se consigue a partir del propio mensaje a firmar o de una transformación precisa del mismo y de una información privada sólo conocida por el signatario, de modo que si éste cambia también lo hace la firma.

La verificación de la firma se consigue aplicando a la firma a comprobar una información pública, que aunque es una función matemática de la citada información privada es computacionalmente imposible obtenerla de ésta. Finalmente, el resultado de este proceso se coteja con el mensaje o con la transformación citada del mismo.

- Control de acceso

Es el responsable de conceder o denegar un cierto tipo de acceso a un recurso determinado. Esta decisión se toma en función de la identificación fehacientemente comprobada (por el mecanismo de autenticación) de la entidad, del recurso al que se pretende acceder, y del tipo

de acceso (lectura, escritura, etc.) demandando. Además, caso de denegarse el acceso, el mecanismo puede desencadenar un aviso del intento de violación de la seguridad o registrar el hecho en un registro de auditoría, o ambas.

- Integridad

Hay dos modalidades integridad: la integridad de la unidad simple de datos y la integridad del flujo completo de datos (mensaje).

La integridad de la unidad simple de datos supone que la fuente emisora de los datos añade una información adicional que es función de dichos datos, como un CRC (código de redundancia cíclica) o una función resumen que puede a su vez ser cifrada. En el caso de una función resumen, el receptor primero recupera la información añadida, descifrándola si corresponde, y, segundo, la recalcula directamente de la unidad de datos recibida. Finalmente, coteja ambos valores aceptando la unidad de datos si son iguales o solicitando su retransmisión caso contrario.

Para la integridad sin conexión se requiere, además de lo anterior, alguna forma de ordenación de los campos, como una numeración de los mismos o un cifrado en modo de encadenamiento de bloques.

En cuanto a la integridad de una sucesión de mensajes consecutivos, se suelen utilizar números de secuencia, *timestamps* o cadenas criptográficas.

- Relleno de tráfico

Estos mecanismos protegen frente al análisis del flujo de tráfico. Suelen basarse en añadir tráfico redundante, protegido con mecanismos de confidencialidad.

- Control de encaminamiento

Estos mecanismos permiten seleccionar el camino que seguirá la información en la red, de forma que circule por la ruta más segura. Se basa en el etiquetado de rutas seguras y de mensajes con niveles de seguridad.

- Registro

Consisten en la introducción de una entidad Notario, capaz de registrar determinadas transferencias de información, con vistas a resolver disputas.

**SERVICIOS Y MECANISMOS DE SEGURIDAD EN EL MODELO OSI**

| SERVICIO | MECANISMO | | | | | | |
|---|---|---|---|---|---|---|---|
| | CIFRA | FIRMA | CTROL ACCE. | INTG DAT | RELL TRAF | CTROL ENCAM | CERTF |
| **Autenticación** | | | | | | | |
| - de la pareja de entidades | X | X | 0 | 0 | 0 | 0 | 0 |
| - del origen de los datos | X | X | 0 | 0 | 0 | 0 | 0 |
| **Control de acceso** | 0 | 0 | X | 0 | 0 | 0 | 0 |
| **Confidencialidad** | | | | | | | |
| - con conexión | X | 0 | 0 | 0 | 0 | X | 0 |
| - sin conexión | X | 0 | 0 | 0 | 0 | X | 0 |
| - en campos seleccionados | X | 0 | 0 | 0 | 0 | 0 | 0 |
| - de Flujo de Tráfico | X | 0 | 0 | 0 | X | X | 0 |
| **Integridad** | | | | | | | |
| - con conexión con recuperación | X | 0 | 0 | X | 0 | 0 | 0 |
| - con conexión sin recuperación | X | 0 | 0 | X | 0 | 0 | 0 |
| - con conex. en campos seleccionados | X | 0 | 0 | X | 0 | 0 | 0 |
| - sin conexión | X | X | 0 | X | 0 | X | 0 |
| - sin conexión en campos selecionados | X | X | 0 | X | 0 | X | 0 |
| **No repudio** | | | | | | | |
| - con prueba de origen | 0 | X | 0 | X | 0 | 0 | X |
| - con prueba de recepciónen destino | 0 | X | 0 | X | 0 | 0 | X |

### 1.2.2. MECANISMOS DE SEGURIDAD GENERALES

Los mecanismos de seguridad generales, no son específicos de ningún servicio particular y no se implementan específicamente en ningún nivel. Estos servicios incluyen:

Funcionalidad Certificada. Se trata de un concepto general que específica que cualquier funcionalidad utilizada directamente para proporcionar seguridad, o que proporciona acceso a un mecanismo de seguridad, debe estar certificada. Se puede utilizar bien para extender a otros mecanismos de seguridad o para establecer su efectividad.

Etiquetas de Seguridad. Se utilizan para especificar el nivel de seguridad de elementos de datos particulares. Los recursos del sistema pueden tener asociados etiquetas de seguridad (por ejemplo, para indicar niveles de sensibilidad). A menudo es necesario que los datos en tránsito lleven la etiqueta de seguridad apropiada. Un nivel de seguridad puede implicar datos adicionales que se asocian a los datos transmitidos o puede ser implícito (por ejemplo, por el uso de una clave específica para cifrar los datos o por el contexto de los datos, como su fuente o ruta)

Detección de eventos. Especifica que cualquier violación de la seguridad, así como si es posible, los eventos normales (*login, logout,* acceso a recursos, etc) deben ser detectados,

registrados e informados. Además, el sistema de gestión de eventos también debe incluir acciones de recuperación apropiadas.

Traza de auditoría de seguridad. La auditoría de seguridad es la revisión y examen independiente de los registros y las actividades del sistema para probar la operatividad de los controles, asegurar el cumplimiento de las políticas y de los procedimientos operacionales establecidos y recomendar los cambios adecuados en el control, política y procedimientos.

Recuperación de seguridad. Especifica las acciones de recuperación apropiadas a aplicar según unas reglas. Hay tres tipos de acciones de recuperación:

- Las Inmediatas. Se realizan de forma directa e inmediata, tales como la desconexión de alguien que ha violado la política de seguridad.
- Las acciones temporales, tal como etiquetar una entidad como temporalmente inválida.
- Las acciones a la largo plazo, como pueden ser la inclusión de una entidad en una lista negra de violadores de seguridad o el cambio de alguna clave.

## 1.3. SERVICIOS Y MECANISMOS DE SEGURIDAD POR NIVELES OSI

La implantación de un mecanismo en uno u otro nivel dependerá de los requisitos de seguridad a satisfacer.

De la combinación de las Tablas 1 y 2 obtendremos los mecanismos de seguridad que se pueden implantar en los niveles OSI.

Así, un dispositivo de cifrado a nivel físico o a nivel de enlace es la solución si se desea conectar redes seguras, pero mediante enlaces inseguros. En efecto, aunque las redes de origen y de destino sean seguras, si el camino entre los nodos atraviesa alguna red insegura (por ejemplo, una red pública de datos), se precisa añadir mecanismos de seguridad en el nivel de transporte.

Sin embargo, si los ordenadores que desean comunicarse no tienen la certeza de que las redes a las que pertenecen sean seguras, se precisa que la seguridad se extienda extremo a extremo. Este tipo de seguridad se puede implementar en el nivel de red o de transporte.

Finalmente, algunos usuarios que sólo desean proteger algunas aplicaciones, o algunos campos de ciertas aplicaciones, necesitan implementar la seguridad en el nivel de aplicación (también denominada extremo a extremo).

## 1.4. SERVICIOS Y MECANISMOS DE SEGURIDAD EN TCP

En la actualidad, como hemos comentado, se emplea la pila TCP IP. TCPIP es mucho más flexible que OSI permitiendo el uso de diferentes servicios en multitud de capas e incluso muchas veces empleando cross-layering, es decir, haciendo una capa dependiente de la inferior o la superior por un motivo de seguridad. Estas prácticas de cross-layering rompen la filosofía de las torres de protocolos en las que los niveles son independientes unos de otros.

Existen muchos casos en la actualidad. Haciendo uso de la tabla en la que se mencionan los servicios de seguridad en el modelo OSI y sus respectivos niveles, hagamos un repaso de los servicios y en qué capas se usan en TCP/IP.

La autenticación se utiliza en varios niveles en TCP/IP. Por ejemplo a nivel de enlace (nivel 2) al conectarnos a una WIFI. Si usamos el antiguo WEP en realidad estamos realizando una autenticación implícita. WEP únicamente cifra el enlace, por lo que si no disponemos de la clave, no podemos descifrar los paquetes ni enviarlos. Por lo que no es una autenticación de entidades sino de los los datos y se alcanza mediante confidencialidad (cifrado de datos).

Si usamos en cambio algún protocolo moderno como WPA2 en su versión conocida como "Enterprise", se solicita el uso de un mecanismo de autenticación que será transportado mediante el protocolo 802.1x directamente sobre el nivel de enlace. Posteriormente, se obtendrá una clave para el cifrado del canal. En este caso, existe tanto autenticación como confidencialidad así como comprobación de la integridad de los datos mediante HMAC.

Subiendo a IP (nivel 4) podemos encontrar el protocolo IPSEC, que permite autenticar dos extremos o bien dos aplicaciones en dos extremos y proporcionar confidencialidad mediante un túnel cifrado. Por tanto tendremos autenticación, confidencialidad e integridad de los datos.

Otros protocolos como PANA, permiten realizar la autenticación que haríamos mediante 802.1x, es decir, autenticación de acceso a la red, sobre IP. PANA es un portador de cargas (payloads) EAP sobre el que puede transportarse cualquier mecanismo de autenticación. De esta forma, podríamos conectar a una WIFI con autenticación abierta, obtener una clave de sesión que nos permitiese conectar con el router WIFI, obtener posteriormente una IP mediante DHCP de tipo Link Local (sólo válida entre el router y el dispositivo) y ejecutar PANA para autenticarnos. Como resultado, se obtendría una clave de sesión que se usaría para sustituir la clave previamente obtenida. Este es un buen ejemplo de cross-layering.

Finalmente, la mayoría de los protocolos superiores (sobre TCP) utilizan autenticaciones básicas, como correo (SMTP, POP e IMAP) o HTTP (Basic Authentication) y en algunos casos algo más avanzado como START_TLS para la autenticación o Digest Authentication en el caso de HTTP, pero en general, no fueron diseñados para tener mecanismos de autenticación fuertes y si disponen de éstos es mediante extensiones y no suelen ser utilizados. La razón por las cuales no se utilizan es porque resulta más sencillo utilizar estos protocolos sobre un transporte seguro como TLS sobre TCP.

Un caso muy común es el de HTTPs. HTTP es un protocolo que fue diseñado con autenticación básica o digest muy poco sofisticada. HTTPS no es más que el uso de HTTP sobre TLS sobre TCP. La autenticación se realiza realmente sobre TLS y no sobre HTTP. Sucede de la misma manera en el caso de SMTP, POP o IMAP.

Este tipo de enfoques bien conocidos por todos son parches a un modelo que si bien es cierto que triunfó sobre OSI, no previno la necesidad de incorporar mecanismos de seguridad avanzados.

De forma práctica TLS es el mejor comodín para montar otros protocolos no seguros, de forma que usar un protocolo inseguro sobre un túnel cifrado no provoque problema alguno. Pero esto no es siempre así, existen numerosos problemas por el uso de túneles para portar protocolos inseguros, pero, en la práctica, no es tan importante. Se recomienda al lector que profundice en https://tools.ietf.org/html/draft-puthenkulam-eap-binding-04 y http://www.opus1.com/www/whitepapers/8021xbindingproblem.pdf

# CAPÍTULO 2 AUTENTICACIÓN CRIPTOGRÁFICA

Antes de acceder a una red para utilizar sus recursos, los usuarios (entidades) deben identificarse fehacientemente. Se entiende por Autenticación la verificación de la supuesta entidad de un principal. La autenticación tiene como resultado la autenticidad, lo que quiere decir que el principal que verifica (verificador) puede estar seguro de que el principal verificado (solicitante) es quien es o quien dice ser.

La autenticación es el primer control de seguridad al que se enfrenta cualquier persona que desea trabajar con un sistema conectado a una red, por lo que su importancia es, si cabe, mayor que la de los restantes. Por ello, estos mecanismos han sido objeto de una atención preferente, llegando, sobre todo en los primeros años de implantación de las redes, a ser los únicos mecanismos de seguridad implementados.

Es práctica común dividir las técnicas utilizadas para la autenticación en tres categorías dependiendo de en qué se basan:

- Algo que el solicitante sabe, prueba por conocimiento. Ejemplo los números de identificación personales PIN (*Personal Identification Numbers)*, los números de identificación de transacción TAN (*Transaction Authentication Numbers*).
- Algo que el solicitante posee. Ejemplo las tarjetas de identificación y otros dispositivos físicos o elementos personales
- Algunas características biométricas del solicitante, prueba por propiedad: huellas dactilares, imágenes faciales, imágenes de la retina y patrones de voz.

La mayor parte de los mecanismos de autenticación que se utilizan hoy en día, en redes de ordenadores y sistemas distribuidos, se basan en la prueba por conocimiento.

Cualquier mecanismo de autenticación o de firma digital puede dividirse en dos niveles fundamentales. El nivel inferior debe ser algún tipo de función que produzca un autenticador: un valor que será usado para autenticar el mensaje. Esta función de nivel inferior se utiliza como primitiva en el protocolo de autenticación del nivel superior que permite al receptor

verificar la autenticidad del mensaje. El nivel superior será el encargado de aplicar la función de autenticación, para proporcionar el servicio requerido.

Tradicionalmente, en los sistemas informáticos convencionales, la identidad fehaciente de los usuarios se obtenía, normalmente, mediante un código llamado de identificación, y posterior verificación mediante una contraseña. Sin embargo, la situación actual recomienda el uso de técnicas de cifrado para esta transmisión.

La idea básica de la autenticación criptográfica es que el solicitante A pruebe su identidad al verificador B realizando una operación criptográfica sobre una cantidad que ambos conocen o que B suministra. La operación criptográfica realizada por A se basa en una clave criptográfica, que puede ser una clave secreta o una clave privada de un criptosistema de clave pública.

En general, la autenticación criptográfica puede hacerse más segura que la autenticación basada en contraseña. Además, existen nuevas técnicas basadas en pruebas de conocimiento cero, que pueden proporcionar mecanismos de autenticación que permiten que el solicitante pruebe que conoce el secreto de identificación correcto, sin transferir realmente al verificador ningún conocimiento sobre ese secreto.

## 2.1. TIPOS DE AUTENTICACIÓN CRIPTOGRÁFICA

Por su amplia aceptación, se expondrá el tratamiento que se hace en la norma OSI/IEC 9594-8, equivalente a la recomendación X.509 del ITU-T, conocida como Marco de Autenticación del Directorio. Este estándar considera dos tipos generales de autenticación: simple y fuerte. El primero se basa en las contraseñas usuales, opcionalmente encubiertas mediante una función irreversible, mientras el segundo se apoya en las claves públicas de los usuarios certificadas por una Autoridad de Certificación.

### 2.1.1. AUTENTICACIÓN SIMPLE

Estos procedimientos se han venido empleando y considerando aceptablemente seguros para la autenticación ante ordenadores locales en entornos protegidos. Sin embargo, para la autenticación ante ordenadores remotos los procedimientos que se usaban inicialmente son inadecuados. Por ello, la norma ISO/IEC 9594-8 (e ITU-T X.509) contempla una autenticación, que denomina simple, mucho más segura basada en funciones irreversibles.

La autenticación simple de un usuario A ante un ordenador B se puede instrumentar en los siguientes pasos:

- El usuario A aplica una función irreversible f, a un argumento, que llamaremos $X_A$ constituido por su código de identificación, ID(A), su contraseña $c_A$, y, opcionalmente, el tiempo t y un número aleatorio r, o sea $f(X_A) = f(ID(A),c_A,t,r)$. Los dos últimos parámetros se incluyen para evitar replicaciones.

- El usuario A remite al ordenador B, una información (denominada autenticador en la norma citada), constituida por: ID(A), t, r, $f(X_A)$

El ordenador B, a partir de ID(A) recupera de su tabla de contraseñas $c_A$ (o en caso más general del directorio de la red) y aplica la misma función, f, a esta $c_A$ junto con el ID(A), t, r recibidos. Si el resultado coincide con el $f(X_A)$ recibido, acepta a A como el legítimo usuario. Caso contrario le rechaza. En ambos casos, B comunica a A la decisión tomada.

### 2.1.2. AUTENTICACIÓN FUERTE

La autenticación fuerte (*strong authentication)* establecida en la norma citada se basa en el uso de técnicas criptográficas asimétricas. Además, esta autenticación comporta que cada usuario posea una identificación indubitable, conocida como nombre discriminante, cuya aceptación y almacenamiento es responsabilidad de la Autoridad de Certificación.

Se distinguen tres tipos de autenticación fuerte, que conllevan un número diferente de intercambios de información entre las entidades implicadas: la autenticación en un sólo sentido (o unidireccional), en dos sentidos (o bidireccional) y de tres sentidos, de ellas sólo expondremos la primera.

La autenticación en un sólo sentido (o unidireccional), supone un único paso, mediante el cual A (entidad que desea identificarse) transmite a B (entidad autenticadora) una información a partir de la cual ésta verifica fehacientemente la identidad de aquella. Los pasos pormenorizados son los siguientes:

- A genera un número irrepetible $r_1$, usado para prevenir falsificaciones.
- A remite a B un mensaje formado por ID(A), $t_1$,$r_1$ ID(B), E(Kva, ($t_1$,$r_1$, ID(B))

Donde $t_1$, indica el día y hora de remisión del mensaje e ID ( ) la identificación de la entidad correspondiente.

Caso de precisarse el intercambio posterior de mensajes cifrados, A también podría enviar firmado a B, E($k_{uB}$, $K_s$), siendo $K_s$ la clave secreta a emplear en dichos intercambios.

- B procede de la siguiente forma:

a) Comprueba que el certificado que A le debe hacer remitido (acción no indicada anteriormente) no está caducado. Si ello es así, obtiene mediante este certificado la clave pública de A.

b) Verifica la firma y consiguientemente la integridad de $t_1$,$r_1$ e ID(B).

c) Comprueba que él es el destinatario pretendido.

d) Verifica que la fecha y hora son válidas.

e) Constata que $r_1$ no está repetido.

Si todas estas acciones concluyen satisfactoriamente acepta al usuario, caso contrario rechaza la autenticación.

## 2.2. FUNCIONES CRIPTOGRÁFICAS DE AUTENTICACIÓN

En este apartado se describen los tipos de funciones que pueden ser utilizados para construir un autenticador:

- Cifrado de mensajes: El texto cifrado del mensaje completo puede servir como autenticador.
- *Checksum* criptográfico: Una función pública del mensaje y una clave secreta generan un valor de longitud fija que sirve de autenticador.
- Función *hash*: Una función pública transforma un mensaje de cualquier longitud en un valor de longitud fija, para obtener el autenticador ese valor se cifra con una clave privada.

## 2.3. CIFRADO DE MENSAJES

El cifrado de un mensaje puede proporcionar por si mismo una medida de autenticación. Supongamos dos principales A y B que se comunican y que se quieren autenticar. El análisis difiere para los esquemas de cifrado de clave secreta (simétricos) de los de clave pública.

Cifrado de clave secreta (simétricos)

A cifra el mensaje M a enviar a B con una clave secreta K, que sólo conocen A y B. B descifra el mensaje M' con la misma clave K, entonces B sabe que el mensaje proviene de A porque nadie mas conoce esa clave, por esta misma razón también proporciona confidencialidad.

Cifrado de clave pública

El uso directo del cifrado de clave pública proporciona confidencialidad, pero no autenticación. La fuente A, usa la clave pública $Ku_b$ del destino (B), para cifrar M. Dado que sólo B conoce la clave privada correspondiente $Kr_b$, solamente B puede descifrar el mensaje. Este esquema no proporciona autenticación, porque cualquier oponente también puede utilizar la clave pública de B, para cifrar un mensaje y afirmar que lo ha enviado A.

Para proporcionar ambas características a la vez, confidencialidad y autenticidad, A puede cifrar M en primer lugar utilizando su clave privada, para construir la firma digital, y posteriormente cifrar con la clave pública de B, para dar secreto. La principal desventaja de este esquema es que se debe ejecutar cuatro veces el algoritmo de cifrado de clave pública por cada transmisión, y los algoritmos de clave pública son bastante complejos.

## 2.4. CHECKSUM CRIPTOGRÁFICO

El checksum criptográfico, o código de autenticación de mensaje (MAC, *Messages Authentication Code*), se obtiene de aplicar una clave secreta a un pequeño bloque de datos de tamaño fijo, compendio, obtenido a partir del mensaje a enviar. El objetivo es que los MAC no puedan recrearse por alguien que tenga la misma entrada de datos, a menos que también se posea la clave de acceso secreta.

Esta técnica parte de que las dos partes de una comunicación, A y B, comparten una clave secreta K. Cuando A tiene que enviar un mensaje M a B, calcula el MAC como una función del mensaje y de la clave: $C_K(M)$. Transmite el mensaje más el MAC al receptor. El receptor realiza el mismo cálculo sobre el mensaje recibido, usando la misma clave secreta, para generar un nuevo MAC. Compara ambos el recibido con el calculado y si coinciden, entonces:

1. El receptor puede estar seguro de que el mensaje no ha sido alterado. Si un atacante altera el mensaje, pero no altera el MAC, el receptor lo detectará al comparar ambos MAC's. El atacante no puede alterar el MAC, para que refleje los cambios que ha introducido en el mensaje original, porque no conoce la clave secreta K.

2. El receptor puede estar seguro de que el mensaje proviene del emisor. Dado que nadie más conoce la clave secreta, nadie más puede construir un mensaje con el MAC apropiado.

Una forma simple de calcular el MAC es añadir la clave al mensaje y después generar el compendio. Debido a que la clave es parte de la entrada de datos, ésta altera el compendio y no permite recrear el MAC a no ser que se conozca el mensaje y la clave secreta.

Otra forma de MAC es utilizar algún método de cifrado en cadena, como RC4, o DES en el modo CFB. La clave en este caso es la clave de acceso del cifrado y el MAC es el último bloque de bits del algoritmo de cifrado. Como la salida del cifrado depende de todos los bits de entrada y de la clave secreta, el último bloque de salida será diferente para cada entrada de datos distinta o para cada clave de acceso diferente.

Las funciones de *checksum* criptográfico son similares al cifrado, pero al no tener que ser reversibles, son menos vulnerables que las de cifrado.

## 2.5. FUNCIÓN HASH

Como en el MAC, una función *hash* acepta como entrada un mensaje M de longitud variable, y produce como salida un código de longitud fija, H(M), a veces también llamado resumen o huella digital o *MIC* (*Message Integrity Code*).

La norma ISO/IEC 10181-2, define una función de este tipo como: función matemática que transforma valores de un conjunto, posiblemente muy grande, en un conjunto de valores más pequeños.

El código *hash* es función de todos los bits del mensaje, y proporciona capacidad de detección de errores. El cambio en cualquiera de los bits del mensaje, significaría un cambio en el código *hash.*

Requerimientos de una función *hash*

Un valor *hash* se genera por una función H de la forma *h = H(M)* donde M es un mensaje de longitud variable, y H(M) es el valor *hash* de longitud fija.

El propósito de una función *hash* es construir una "huella digital" de un fichero, un mensaje, o de un bloque de datos. Para que sea útil para la autenticación, una función *hash*, H, debe poseer las siguientes propiedades:

1. Poderse aplicar a un bloque de datos de cualquier tamaño.
2. Producir una salida de longitud fija.
3. Ser fácil de calcular *H(x)* para cualquier *x*, de forma que tanto la implementación hardware como software sean prácticas.
4. Efecto avalancha: pequeños cambios de pocos bits en la entrada, deben producir grandes cambios en la salida.
5. **Unidireccional (***preimage resistance***)**. Para cualquier mensaje *m*, debe ser imposible computacionalmente encontrar un valor *x,* tal que *H(x)=m*.
6. **Colisión simple** (2nd preimage resistance). Para cualquier mensaje *x*, debe ser imposible computacionalmente encontrar un *y* tal que *H(y)=H(x).* Dicho de otra forma, dado el hash de un mensaje, es computacionalmente imposible encontrar otro mensaje diferente cuya función *hash* sea la misma.
7. **Colisión fuerte** (collision resistance). Dada una función de hash H, debe ser computacionalmente imposible encontrar dos mensajes x, *y* tales que *H(y)=H(x).* Dicho de otra forma, que al atacante, le resulte computacionalmente imposible encontrar dos mensajes diferente cuya función *hash* sea la misma.

Una función *hash* que satisfaga las seis primeras propiedades, se dice que es una función *hash* débil. Si además satisface la séptima propiedad, entonces se dice que es una función *hash* fuerte.

Las funciones *hash*, se utilizan en los servicios de autenticación y de firma digital para:

1. No tener que cifrar todo el texto, ya que este proceso es lento con los algoritmos asimétricos. El resumen sirve para comprobar si la clave privada del emisor es auténtica, no es necesario cifrar todo el texto si no se quiere confidencialidad.

2. Comprobar automáticamente la autenticidad. Si se cifra todo el texto, al descifrar sólo se puede comprobar la autenticidad mirando si el resultado es inteligible, evidentemente este proceso debe realizarse de forma manual. Utilizando un resumen del texto, se puede comprobar si es auténtico comparando automáticamente el resumen realizado en el receptor con el descifrado.

3. Comprobar la integridad del texto. Si el texto ha sido alterado durante la transmisión, no coincidirá el resumen del texto recibido con el descifrado.

Según los algoritmos de autenticación la longitud del resumen es de 128 bits, 256, etc. En la actualidad, con los métodos de ataque conocidos y la potencia de cálculo disponible, se

recomienda no usar algoritmos cuyo resumen tenga menos de 128 bits. Los algoritmos más utilizados son:

### 2.5.1. MD5

MD5 es una función *hash* diseñada por Ron Rivest, en 1992. Las siglas MD provienen de *Message Digest*; el algoritmo genera un valor hash de 128 bits y es de libre circulación.

Este algoritmo fue diseñado con los siguientes objetivos:

- Velocidad. poderse utilizar en implementaciones software de alta velocidad
- Simplicidad y compactitud. Se basa en un conjunto de operaciones simples sobre bits, con operandos de 32 bits.
- Favorecer las arquitecturas *pequeñas*. optimizado para las arquitecturas basadas en microprocesadores.

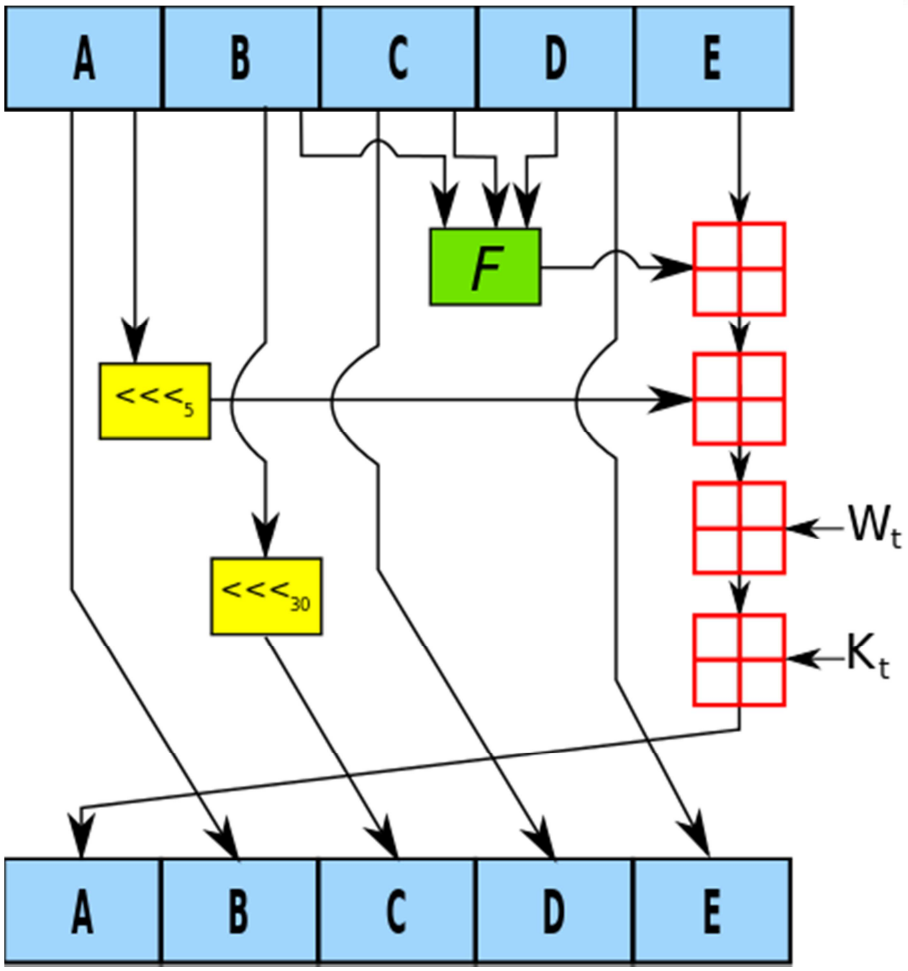
Tras algunos procesos iniciales, MD5 procesa el texto de entrada en bloques de 512 bits, divididos en 16 subbloques de 32 bits. La salida del algoritmo es un conjunto de cuatro bloques de 32 bits, que se concatenan para formar el valor *hash* de 128 bits.

### 2.5.2. SHA

El Algoritmo *Hash* Seguro (SHA *Secure Hash Algorithm*) fue diseñado, en 1994, por el NIST (*National Institute of Standard Techology)*, para su utilización en el Estándar de Firma Digital (DSS *Digital Signature Standard*, también conocido como SHS, *Secure Hash Standard*).

SHA-1 ofrece un tamaño de salida de 160 bits, con un estado interno de 160 bits (mayor que el de MD5 que es de 128 bits). El tamaño de bloque también es de 512 bits y pasa por 80 rondas en lugar de las 64 de MD5. La figura de arriba ilustra el procedimiento seguido en cada una de las 80 rondas de SHA-1 tras las inicializaciones previas para el estado incial y para conseguir que el tamaño de la entrada se pueda trocear en bloques de 512 bits. La notación de la figura es la siguiente:

- A, B, C, D y E son palabras de 32 bits y contienen el estado interno de la función.
- F es una función no lineal que varía,
- $\lll n$ significa rotación de bit a la izquierda n posiciones
- Wt es el mensaje expandido de la ronda anterior t
- Kt es la constante de la ronda t (cada 20 rondas se cambia el valor de la constante)
- $\boxplus$ significa suma en módulo $2^{32}$.




### 2.5.3. Debilidad de MD5 y SHA-1. Las nuevas funciones SHA-2 y SHA-3

Las funciones de hash MD5 y SHA-1 no ofrecen la dificultad computacional en la propiedad de colisión fuerte que en principio se esperaba de ellas. La propiedad de colisión fuerte es la que permite mayor grado de libertad al criptoanalista, pues puede buscar determinados bloques con los que ajustar los estados internos de la función de hash para utilizando dichos bloques construir mensajes distintos pero con el mismo valor de hash.

En la actualidad, en el 2005 se demostró que es más sencillo encontrar colisiones en MD5 de lo que inicialmente se pensaba, y actualmente se pueden generar colisiones (es decir a partir de un mensaje encontrar otro mensaje que produzca el mismo hash) con una complejidad de $2^{21}$ en lugar de las $2^{64}$ inicialmente esperadas. Respecto de la dificultad de conseguir la preimagen, es decir a partir del hash encontrar el mensaje original, actualmente se cifra en $2^{123.4}$ es decir todavía es bastante alta. Sin embargo está totalmente desaconsejado su uso salvo en autenticaciones de mensajes HMAC, y no se debe utilizar ni aceptar su uso en firma de certificados digitales.

También SHA-1 se ha demostrado más débil de lo que inicialmente se pensaba, y teóricamente se pueden encontrar colisiones en $2^{51}$ ejecuciones del algoritmo con lo que su uso en una gran variedad de aplicaciones (nuevamente para certificados digitales) está fuertemente desaconsejado desde el 2010.

La función hash que se utiliza en la actualidad es SHA-2, que permite resúmenes de mayor tamaño, desde 256 bits hasta 512. SHA-2 maneja bloques de 512 bits o de 1024, y el estado interno (de 256 bits o 512 bits), también mayor que el de 160 bits de SHA-1. En realidad bajo el nombre de SHA-2 se hay seis funciones diferentes: SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256. Hay diversas funciones dependiendo del tamaño de la salida , SHA-256/224 y SHA-512/384.

En 2012, tras ganar el concurso para la nueva función SHA-3, keccak resultó ganadora y ya hay implementaciones software. Aunque no se han demostrado ataques contra SHA-2, posiblemente empecemos a ver éste tipo de funciones de hash incorporándose a nuestros protocolos y aplicaciones de seguridad.

# CAPÍTULO 3 SISTEMAS DE GESTIÓN DE IDENTIDAD EN INTERNET

En sistemas complejos es necesario mantener un perfil de usuario más allá de mantener un par nombre de usuario y contraseña o cualquier otro tipo de autenticación o autorización. En ellos entra en juego las tecnologías de gestión de identidad.

Anteriormente, el control de acceso ha dado respuesta a muchos de los problemas de la seguridad y sirve de base para la gestión de identidad ¿cómo funciona el control de acceso? Dados:

- un recurso, como un fichero o servicio
- una sensibilidad asociada a dicho recurso: medida de coste económico, moral o de otra categoría,
- unas condiciones de contorno,

El control de acceso permite determinar si una entidad (como sería un usuario) puede acceder a dicho recurso o no.

La gestión de identidad se sirve del control de acceso para parte de sus tareas de gestión de servicios, que veremos más adelante, como son Single Sign On o Single Log Out. La gestión de identidad se sirve de las siguientes funciones de seguridad que engloban al control de acceso:

- Autenticación: Se trata de determinar si una entidad es quien dice ser o no en base a una serie de pruebas criptográficas, de posesión de información o retos.
- Identificación: se trata de autenticar una entidad sobre un espacio de posibles identidades unívocamente a diferencia de la autenticación que no tiene porqué ser univoca
- Autorización: determina, en base a una política, que puede hacer una entidad dada, es decir, cuáles son sus privilegios
- Aplicación de políticas: las políticas son documentos electrónicos en un formato dado que explicitan la sensibilidad sobre los recursos, es decir, qué privilegios son necesarios para acceder a ellos. Las políticas vinculan la sensibilidad a los recursos.

Utilizando estas cuatro funciones de seguridad, los sistemas de gestión de identidad, gestionan la autenticación, autorización e intercambio de información de perfiles en uno o varios dominios administrativos con el objetivo de incrementar la seguridad y disminuir la complejidad de la gestión de estas tareas tanto a los administradores como a los usuarios.

## 3.1. Concepto de identidad digital

La identidad digital responde a varias definiciones. Según la Wikipedia es la representación digital de un conjunto de afirmaciones realizadas por una entidad sobre otra entidad.

Según Dick Hardt en la charla de apertura en OSCON 2005 se trata de la representación digital de lo que digo sobre me (preferencias) y lo que otros dicen sobre mi (información de autenticación, autorización o reputación).

Acorde con lo identificado por Kim Cameron en la publicación "The laws of Identity", la identidad es la representación digital de un conjunto de afirmaciones realizadas por una parte sobre si misma u otra.

En general una identidad digital es:

- Algo que puedo decir sobre mi: colección de atributos
- Algo que otras entidades pueden decir sobre mi: colecciones de atributos y/o credenciales
- La forma de presentarme a mi mismo: preferencias

En lo que se refiere al uso, John Palfrey y Urs Gasser en Digital Identity Interoperability and eInnovation, exponían que la identidad digital podía usarse para múltiples propósitos como autenticación, verificación, unicidad, enlazado, y reputación.

Los usos de la identidad digital son, entre otros, los siguientes:

- Seguridad básica como autenticación, autorización, reputación, verificación
- Para interactuar con servicios dentro de los dominios administrativos autorizados (aunque sean diferentes)
- Para establecer reputación
- Para administración electrónica

Un usuario puede tener varias identidades electrónicas con representación real (para administración electrónica) o ficticia (cuentas o avatares para otros servicios)

## 3.2. Enfoques de gestión de identidad

La identidad corporativa (corporate identity) es aquella en la cual la identidad del usuario consistente en el perfil, atributos y preferencias se encuentran completamente bajo el control de una empresa o prestadora de servicio. Se caracterizan por ser opacas al usuario, el cual, no tiene control de ningún tipo sobre el uso que se hace de dicha información. Los ejemplos son bien conocidos, Google Accounts, MSN .NET Passport, Facebook…

La identidad asociada a telecomunicaciones es aquella en la que la identidad de usuario se asocia a identificadores de dispositivo y suscripción a un servicio, como pueden ser el número de teléfono, el IMEI de dispositivo…

La identidad federada es aquella en la un usuario tiene una cuenta en un servicio que desarrolla un acuerdo con terceras partes para ampliar la prestación de servicio de forma que el usuario puede, usando la misma cuenta, moverse del servicio original a otro conservando sus identificadores. Ejemplos de uso son las cuentas para bibliotecas, el DNI electrónico y los estándares más representativos son SAML, Shibboleth y OpenID.

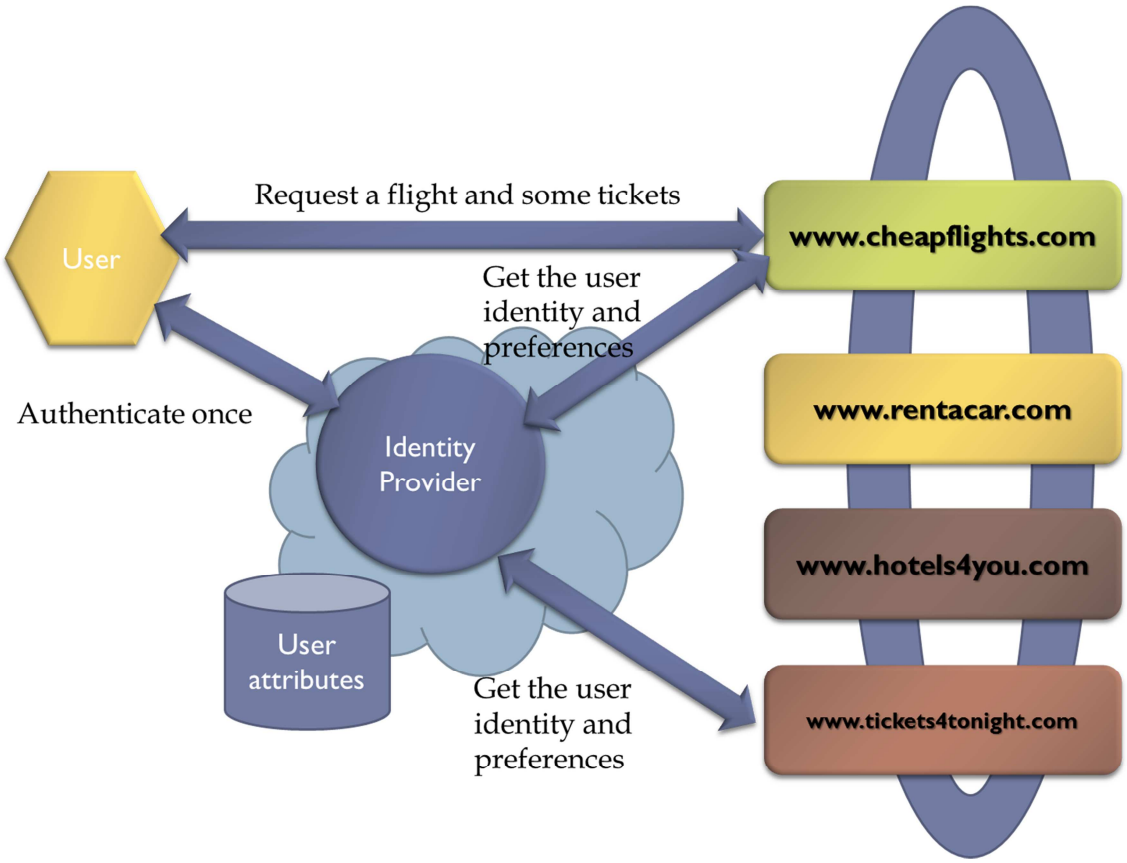
Finalmente, la identidad user centric es aquella en la que el usuario dispone de control absoluto de su identidad y decide cuando liberar y de qué forma filtrar ciertos atributos de su identidad antes de acceder a un servicio. La metáfora más adecuada es la de la cartera física de una persona, la cual contiene diferentes tarjetas (biblioteca, DNI, tarjetas de crédito, del videoclub…) que el usuario decide ante cada situación como usarlas. Ejemplos representativos son Information Cards, Higgings…

## 3.3. Evolución contextual de la gestión de identidad

En cuanto a la aparición de estas tecnologías de identidad en tiempo, debemos partir de lo que se conoce, en diversas clasificaciones como identidad 1.0. Se trata del mencionado enfoque corporativo, y presenta las siguientes características:

- El usuario se asocia con un identificador como un nombre de usuario y contraseña o certificado PKI. Esto lo configura el administrador o dueño del sistema y el usuario no puede seleccionar el tipo de credencial.
- Las decisiones de confianza (es decir, qué usuarios usan el sistema) son tomadas por una única entidad, por lo que existe una asimetría y dichas decisiones son opacas al usuario.
- El usuario no tiene control de su privacidad al no conocer quien accede a la información y de qué manera se usa
- Corresponde a un modelo "silo" en el cual es necesaria una identidad o nombre de usuario por servicio, no es portable y por tanto escala muy mal (al ser necesario recordar una gran cantidad de identificadores y contraseñas)
- En general no es interoperable dado que cada organización utiliza sus propios sistemas de autenticación.

Para mejorar la experiencia de usuario y evitar que sea necesario recordar una gran cantidad de identificadores y contraseñas, se desarrolló lo que se conoce como identidad federada, que correspondería a una evolución de la corporativa, en la que la identidad se comparte con más servicios permitiendo a un usuario moverse entre ellos con la misma cuenta.




Un ejemplo característico es el de un vendedor de vuelos que permite alquilar un coche con una compañía diferente (con la que mantiene un acuerdo), reservar un hotel e incluso tickets para espectáculos, una vez comprado un vuelo, con unas condiciones especiales. Este proceso, no suele necesitar registro en los sitios web de los socios (pertenecientes a la federación).

La federación se orquesta a través de lo que se conoce como círculo de confianza, que es la metáfora del acuerdo entre los participantes, que se consigue técnicamente mediante el intercambio de información criptográfica. La creación de una federación es un proceso en el que intervienen las personas y que por tanto no es dinámica.

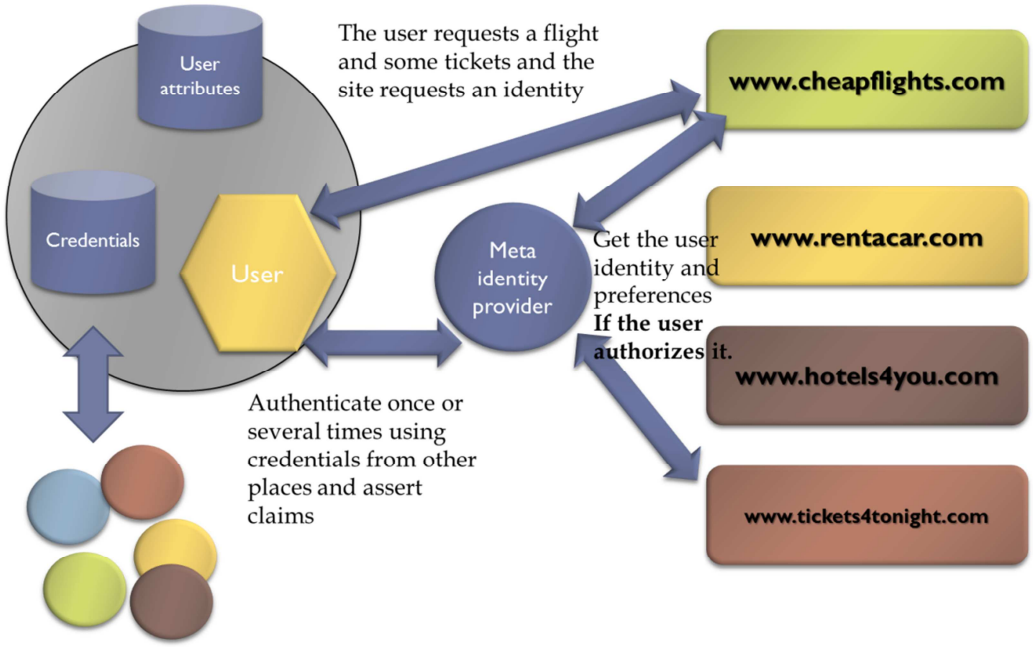
Ejemplos significativos de protocolos son los siguientes: SAML SSO, Shibboleth, OpenID, ID-WSF/liberty.

Las características son las siguientes:

- El usuario se asocia con un identificador en el sistema origen, como un nombre de usuario y contraseña o certificado PKI. No puede seleccionar el tipo de credencial pero como parte de la federación se acuerda el enlazado de cuentas (entre servicios) evitando la necesidad de un identificador por servicio.

- Las decisiones de confianza (es decir, qué usuarios usan el sistema) son tomadas por la federación, por lo que sigue existiendo una asimetría y dichas decisiones son opacas al usuario.
- El usuario no tiene control de su privacidad al no conocer quien accede a la información y de qué manera se usa
- Corresponde a un modelo más descentralizado que en el caso anterior y por tanto escala mejor
- Mejora la experiencia de usuario al no requerir recordar tanta información
- Es interoperable y suele estar basada en estándares lo que facilita que nuevos miembros pasen a formar parte de la federación.

Finalmente, el modelo más prometedor, aún en implantación, es el modelo user-centric, en el que el usuario se convierte en el protagonista mediando en toda transacción. Al acceder a cualquier servicio en estas condiciones, el usuario obtiene del servicio los atributos que dicho servicio necesita conocer para permitir el acceso. El usuario puede decidir qué atributos proporcionar (elegir identificadores, preferencias, nombres de usuario…) y combinar las credenciales a su gusto teniendo control absoluto de la información que proporciona y a quién lo hace.




En el caso visto anteriormente del vendedor de vuelos, la información sobre el usuario ya no reside en la red, sino que está en poder del usuario y éste decide cómo combinarla para acceder a los diferentes servicios.

Las características son las siguientes:

- El usuario decide qué atributos proporciona. En los casos en los que se requiera autenticación o verificación de rasgos de identidad, las credenciales pueden combinarse con otra información a gusto del usuario.
- Las decisiones de confianza (es decir, qué usuarios usan el sistema) son absolutamente transparentes al usuario.
- El usuario tiene control completo de su privacidad y conoce quien accede a la información y de qué manera se usa
- Corresponde a un modelo aún más descentralizado que en el caso anterior y por tanto escala mejor
- La experiencia de usuario es similar al caso de la federación, aunque puede ser complejo de manejar para usuarios no expertos. Por esa razón se recurre a conceptos trasladables a la vida real, como el de la cartera llena de carnés y tarjetas. Ese rol sería asumido por el meta-idp.
- Es interoperable y está basada en estándares lo que facilita la adopción del sistema por nuevos servicios.