UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

UIT-T X.811

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

(04/95)

REDES DE DATOS Y COMUNICACIÓN ENTRE SISTEMAS ABIERTOS

SEGURIDAD

TECNOLOGÍA DE LA INFORMACIÓN – INTERCONEXIÓN DE SISTEMAS ABIERTOS – MARCOS DE SEGURIDAD PARA SISTEMAS ABIERTOS: MARCO DE AUTENTICACIÓN

Recomendación UIT-T X.811

(Anteriormente «Recomendación del CCITT»)

PREFACIO

La UIT (Unión Internacional de Telecomunicaciones) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones. El UIT-T (Sector de Normalización de las Telecomunicaciones de la UIT) es un órgano permanente de la UIT. En el UIT-T, que es la entidad que establece normas mundiales (Recomendaciones) sobre las telecomunicaciones, participan unos 179 países miembros, 84 empresas de explotación de telecomunicaciones, 145 organizaciones científicas e industriales y 38 organizaciones internacionales.

Las Recomendaciones las aprueban los Miembros del UIT-T de acuerdo con el procedimiento establecido en la Resolución N.° 1 de la CMNT (Helsinki, 1993). Adicionalmente, la Conferencia Mundial de Normalización de las Telecomunicaciones (CMNT), que se celebra cada cuatro años, aprueba las Recomendaciones que para ello se le sometan y establece el programa de estudios para el periodo siguiente.

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. El texto de la Recomendación UIT-T X.811 se aprobó el 10 de abril de 1995. Su texto se publica también, en forma idéntica, como Norma Internacional ISO/CEI 10181-2.

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.

RECOMENDACIONES UIT-T DE LA SERIE X

REDES DE DATOS Y COMUNICACIÓN ENTRE SISTEMAS ABIERTOS

(Febrero de 1994)

ORGANIZACIÓN DE LAS RECOMENDACIONES DE LA SERIE X

Dominio	Recomendaciones
REDES PÚBLICAS DE DATOS	
Servicios y facilidades	X.1-X.19
Interfaces	X.20-X.49
Transmisión, señalización y conmutación	X.50-X.89
Aspectos de redes	X.90-X.149
Mantenimiento	X.150-X.179
Disposiciones administrativas	X.180-X.199
INTERCONEXIÓN DE SISTEMAS ABIERTOS	
Modelo y notación	X.200-X.209
Definiciones de los servicios	X.210-X.219
Especificaciones de los protocolos en modo conexión	X.220-X.229
Especificaciones de los protocolos en modo sin conexión	X.230-X.239
Formularios para enunciados de conformidad de implementación de protocolo	X.240-X.259
Identificación de protocolos	X.260-X.269
Protocolos de seguridad	X.270-X.279
Objetos gestionados de capa	X.280-X.289
Pruebas de conformidad	X.290-X.299
INTERFUNCIONAMIENTO ENTRE REDES	
Generalidades	X.300-X.349
Sistemas móviles de transmisión de datos	X.350-X.369
Gestión	X.370-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	
Gestión de redes	X.600-X.649
Denominación, direccionamiento y registro	X.650-X.679
Notación de sintaxis abstracta uno	X.680-X.699
GESTIÓN DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.700-X.799
SEGURIDAD	X.800-X.849
APLICACIONES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	
Cometimiento, concurrencia y recuperación	X.850-X.859
Tratamiento de transacciones	X.860-X.879
Operaciones a distancia	X.880-X.899
TRATAMIENTO ABIERTO DISTRIBUIDO	X.900-X.999

ÍNDICE

Introducción

Muchas aplicaciones necesitan medidas de seguridad que las protejan contra las amenazas que sufre la comunicación de información. Algunas de las amenazas más conocidas, así como los servicios y mecanismos de seguridad que pueden utilizarse para la protección contra esas amenazas, se describen en la Rec. X.800 del CCITT | ISO 7498-2.

Muchas aplicaciones de sistemas abiertos exigen medidas de seguridad que dependen de la identificación correcta de los participantes principales (brevemente, los principales). Entre esas exigencias puede citarse la protección de activos y recursos contra el acceso no autorizado, para lo cual pudiera utilizarse un mecanismo de control de acceso basado en la identidad, acompañado quizás de un régimen de responsabilización que se basaría en el mantenimiento de cuadernos de auditoría (audit logs) en que se registrarían los sucesos relevantes, lo que también serviría para fines de contabilidad y tarificación.

El proceso de corroborar una identidad se denomina autenticación. Esta Recomendación | Norma Internacional define un marco para la prestación de servicios de autenticación.

NORMA INTERNACIONAL

RECOMENDACIÓN UIT-T

TECNOLOGÍA DE LA INFORMACIÓN – INTERCONEXIÓN DE SISTEMAS ABIERTOS – MARCOS DE SEGURIDAD PARA SISTEMAS ABIERTOS: MARCO DE AUTENTICACIÓN

1 Alcance

La serie de Recomendaciones | Normas Internacionales sobre marcos de seguridad para sistemas abiertos tratan la aplicación de servicios de seguridad en un entorno de sistemas abiertos, donde el término «sistemas abiertos» ha de entenderse que incluye sectores tales como base de datos, aplicaciones distribuidas, procesamiento distribuido abierto, y OSI. Los marcos de seguridad se ocupan de la definición de medios para dar protección a sistemas y a objetos dentro de los sistemas, así como de las interacciones entre los sistemas. Los marcos de seguridad no se ocupan de la metodología para construir sistemas o mecanismos.

Los marcos de seguridad tratan tanto los elementos como las secuencias de operaciones (pero no los elementos de protocolo) que se utilizan para obtener servicios de seguridad específicos. Estos servicios de seguridad pueden aplicarse a las entidades comunicantes de sistemas, así como a los datos intercambiados entre sistemas y a los datos gestionados por sistemas.

Esta Recomendación | Norma Internacional:

- define los conceptos básicos de la autenticación;
- identifica las posibles clases de mecanismos de autenticación;
- define los servicios para estas clases de mecanismos de autenticación;
- identifica los requisitos funcionales que deben cumplir los protocolos para soportar estas clases de mecanismos de autenticación; e
- identifica los requisitos generales de gestión que deben cumplirse para la autenticación.

Diferentes tipos de normas pueden utilizar este marco, incluidas:

1) normas que incorporan el concepto de autenticación;
2) normas que proporcionan un servicio de autenticación;
3) normas que utilizan un servicio de autenticación;
4) normas que especifican los medios para proporcionar autenticación dentro de una arquitectura de sistemas abiertos;
5) normas que especifican mecanismos de autenticación.

[Obsérvese que el servicio de 2), 3) y 4) podría incluir autenticación, pero puede tener una finalidad primaria diferente.]

Estas normas deben utilizar este marco como sigue:

- las normas de los tipos 1), 2), 3), 4) y 5) pueden utilizar la terminología de este marco;
- los tipos de normas 2), 3), 4) y 5) pueden utilizar los servicios definidos en la cláusula 7 de este marco; y
- los tipos de normas 5) pueden basarse en los mecanismos definidos en la cláusula 8 de este marco.

Al igual que otros servicios de seguridad, la autenticación sólo puede proporcionarse dentro del contexto de una política de seguridad definida para una aplicación determinada. Las definiciones de políticas de seguridad están fuera del alcance de esta Recomendación | Norma Internacional.

Esta Recomendación | Norma Internacional no incluye la especificación de los detalles de los intercambios de protocolo que deben realizarse para lograr la autenticación.

Esta Recomendación | Norma Internacional no especifica mecanismos determinados para soportar estos servicios de autenticación. Otras normas (tales como ISO/CEI 9798) establecen métodos de autenticación específicos de una manera más detallada. Además, en otras normas (tales como la Rec. UIT-T X.509 | ISO/CEI 9594-8) se presentan ejemplos de esos métodos para tratar exigencias de autenticación específicas.

Algunos de los procedimientos descritos en este marco obtienen la seguridad mediante la aplicación de técnicas criptográficas. Este marco no depende de la utilización de un determinado algoritmo criptográfico o de otro tipo, aunque ciertas clases de mecanismos de autenticación pueden depender de ciertas propiedades de ese algoritmo, por ejemplo, de sus propiedades asimétricas.

NOTA – La ISO no normaliza algoritmos criptográficos, pero sí normaliza los procedimientos aplicados para registrarlos en ISO/CEI 9979.

2 Referencias normativas

Las siguientes Recomendaciones y Normas Internacionales contienen disposiciones que, mediante referencia en este texto, constituyen disposiciones de la presente Recomendación | Norma Internacional. Al efectuar esta publicación estaban en vigor las ediciones indicadas. Todas las Recomendaciones y Normas son objeto de revisiones, por lo que se preconiza que los participantes en acuerdos basados en la presente Recomendación | Norma Internacional investiguen la posibilidad de aplicar las ediciones más recientes de las Recomendaciones y las Normas citadas a continuación. Los miembros de la CEI y de la ISO mantienen registros de las Normas Internacionales actualmente vigentes. La Oficina de Normalización de las Recomendaciones de la UIT mantiene una lista de las Recomendaciones UIT-T actualmente vigentes.

2.1 Recomendaciones | Normas Internacionales idénticas

– Recomendación UIT-T X.810[1)] | ISO/CEI 10181-1:...[1)], *Tecnología de la información – Interconexión de sistemas abiertos – Marcos de seguridad para sistemas abiertos: Visión general.*

2.2 Pares de Recomendaciones | Normas Internacionales de contenido técnico equivalente

– Recomendación X.800 del CCITT:1991, *Arquitectura de seguridad de la interconexión de sistemas abiertos para aplicaciones del CCITT.*

ISO 7498-2:1989, *Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture.*

2.3 Referencias adicionales

– ISO/CEI 9979:1991, *Data cryptographic techniques – Procedures for the registration of cryptographic algorithms.*

– ISO/CEI 10116:1991, *Information technology – Modes of operation for an n-bit block cipher algorithm*.

3 Definiciones

Esta Recomendación | Norma Internacional utiliza los siguientes términos generales, relacionados con la seguridad, definidos en la Rec. X.800 del CCITT | ISO 7498-2:

– auditoría;

– camino de auditoría;

– información de autenticación;

– confidencialidad;

– criptografía;

– valor de comprobación criptográfico;

– autenticación del origen de datos;

---

1) Actualmente en estado de proyecto.

- integridad de los datos;
- descifrado;
- firma digital;
- cifrado;
- clave;
- gestión de claves;
- suplantación (o impostura);
- contraseña;
- autenticación de entidad par;
- política de seguridad.

Esta Recomendación | Norma Internacional utiliza el siguiente término definido en ISO/CEI 10116:

- encadenamiento de bloques.

Esta Recomendación | Norma Internacional utiliza los siguientes términos definidos en la Rec. UIT-T X.810 | ISO/CEI 10181-1:

- impronta digital;
- función de condensación;
- función unidireccional;
- clave privada;
- clave pública;
- sello;
- clave secreta;
- autoridad de seguridad;
- certificado de seguridad;
- dominio de seguridad;
- testigo de seguridad;
- confianza;
- tercero de confianza.

Para los fines de esta Recomendación | Norma Internacional se aplican las siguientes definiciones:

3.1 **método de autenticación asimétrico**: Método de autenticación en el que no toda la información de autenticación es compartida por ambas entidades.

3.2 **identidad autenticada**: Identificador distintivo de un principal que ha sido confirmado por autenticación.

3.3 **autenticación**: Confirmación de la identidad declarada de una entidad.

3.4 **certificado de autenticación**: Certificado de seguridad garantizado por una autoridad de autenticación, y que puede utilizarse para confirmar la identidad de una entidad.

3.5 **intercambio de autenticación**: Secuencia de una o más transferencias de información de autenticación de intercambio destinadas a efectuar una autenticación.

3.6 **información de autenticación**: Información utilizada con fines de autenticación.

3.7 **iniciador de autenticación**: Entidad que comienza un intercambio de autenticación.

3.8 **puesta a prueba**: Parámetro variante en el tiempo generado por un verificador.

3.9 **información de autenticación de declaración (AI de declaración)**: Información utilizada por un declarante para generar la información de autenticación de intercambio necesaria para autenticar un principal.

3.10 **declarante**: Entidad que es o representa a un principal para fines de autenticación. Un declarante incluye las funciones necesarias para intervenir en intercambios de autenticación en nombre de un principal.

3.11 **identificador distintivo**: Datos que distinguen inequívocamente una entidad en el proceso de autenticación. Esta Recomendación | Norma Internacional exige que dicho identificador sea inequívoco al menos dentro de un dominio de seguridad.

3.12 **información de autenticación de intercambio (AI de intercambio)**: Información intercambiada entre un declarante y un verificador durante el proceso de autenticación de un principal.

3.13 **certificado de autenticación fuera de línea**: Certificado de autenticación que vincula un identificador distintivo a AI de verificación, disponible para todas las entidades.

3.14 **certificado de autenticación en línea**: Certificado de autenticación utilizado en un intercambio de autenticación, y obtenido directamente por el declarante de la autoridad que lo garantiza.

3.15 **principal**: Entidad cuya identidad puede ser autenticada.

3.16 **método de autenticación simétrico**: Método de autenticación en el que ambas entidades comparten información de autenticación común.

3.17 **parámetro variante en el tiempo**: Ítem de datos utilizado por una entidad para verificar que un mensaje no es una reproducción.

3.18 **número único**: Parámetro variante en el tiempo generado por un declarante.

3.19 **información de autenticación de verificación (AI de verificación)**: Información utilizada por un verificador para confirmar una identidad declarada mediante AI de intercambio.

3.20 **verificador**: Entidad que es o representa a la entidad que requiere una identidad autenticada. Un verificador incluye las funciones necesarias para intervenir en intercambios de autenticación.

4 Abreviaturas

A los efectos de esta Recomendación | Norma Internacional, se aplican las abreviaturas siguientes:

AI información de autenticación (*authentication information*)

OSI interconexión de sistemas abiertos (*open systems interconnection*)

5 Discusión general de la autenticación

5.1 Conceptos básicos de la autenticación

La autenticación confirma la identidad declarada de una entidad. La autenticación sólo tiene significado en algún contexto. Dos casos importantes son:

- el contexto de una relación de comunicación entre un principal y un verificador (autenticación de entidad); y
- el principal que pretende ser la fuente de un ítem de datos disponibles para otra entidad (autenticación del origen de datos).

Esta Recomendación | Norma Internacional distingue dos formas determinadas de autenticación.

La autenticación de entidad corrobora la identidad de un principal, dentro del contexto de una relación de comunicación. La identidad autenticada del principal sólo es confirmada cuando se invoca este servicio. La seguridad de la continuidad de la autenticación sólo puede obtenerse como se indica en 5.2.7. Ejemplo de esto es la autenticación de entidades homólogas de OSI definida en la Rec. X.800 del CCITT | ISO 7498-2.

La autenticación del origen de datos corrobora la identidad del principal responsable de una unidad de datos concreta.

NOTAS

1 Cuando se utiliza autenticación del origen de datos es también necesario tener seguridad adecuada de que los datos no han sido modificados, lo cual puede realizarse de una de las siguientes maneras:

a) utilizando entornos en los que no puedan alterarse los datos;

b) comprobando que los datos recibidos corresponden a una impronta digital de los datos enviados;

c) por autenticación del origen de datos utilizando un mecanismo de firma digital;

d) utilizando un algoritmo criptográfico simétrico.

2 El término relación de comunicaciones utilizado al definir la autenticación de entidad puede interpretarse en sentido amplio y podría referirse, por ejemplo, a una conexión de OSI, comunicación entre procesos, o interacción entre un usuario y un terminal.

5.1.1 Identificación y autenticación

Un principal es una entidad cuya identidad puede ser autenticada. Un principal tiene asociados uno o más identificadores distintivos. Las entidades pueden utilizar servicios de autenticación para verificar las identidades declaradas de los principales. Una identidad de principal que ha sido verificada de esta forma se denomina identidad autenticada.

Ejemplos de principales que pueden ser identificados y, por ende, autenticados, son:

- usuarios humanos;
- procesos;
- sistemas abiertos reales;
- entidades de capas OSI; y
- empresas.

Los identificadores distintivos deben ser inequívocos dentro de un dominio de seguridad dado. Los identificadores distintivos distinguen un principal de otros en el mismo dominio, lo cual hacen de una de estas dos maneras:

- en un nivel grueso de granularidad, por el hecho de pertenecer a un grupo de entidades consideradas equivalentes a los fines de la autenticación (en este caso, se considera que todo el grupo es un principal y tiene un solo identificador distintivo); o
- en el nivel más fino de granularidad, identificando una entidad y sólo una.

Cuando la autenticación se produce entre dominios de seguridad diferentes, un identificador distintivo puede no ser suficiente para identificar inequívocamente una entidad, ya que autoridades de dominios de autoridad diferentes pueden utilizar los mismos identificadores distintivos. En este caso, los identificadores distintivos tienen que ir acompañados de un identificador del dominio de seguridad para que el identificador de la entidad sea inequívoco.

Ejemplos de identificadores distintivos típicos son:

- nombres de directorio (Rec. UIT-T X.509 | ISO/CEI 9594-8);
- direcciones de red (Rec. UIT-T X.213 | ISO/CEI 8348);
- títulos AP y títulos AE (Rec. UIT-T X.207 | ISO/CEI 9545);
- identificadores de objeto (Rec. UIT-T X.208 | ISO 8824);
- nombres de personas (inequívocos en el contexto del dominio);
- número de pasaporte o de seguridad social.

5.1.2 Entidades que intervienen en la autenticación

El término declarante se utiliza para designar la entidad que es o representa a un principal para fines de autenticación. Un declarante incluye las funciones necesarias para intervenir en intercambios de autenticación en nombre de un principal.

El término verificador se utiliza para designar la entidad que es o representa a la entidad que requiere una identidad autenticada. Un verificador incluye las funciones necesarias para intervenir en intercambios de autenticación.

Una entidad que interviene en la autenticación mutua (véase 5.2.4) asumirá los papeles de declarante y de verificador.

El término tercero de confianza se utiliza para designar una autoridad de seguridad o agente de la misma en la que otras entidades depositan confianza en actividades relacionadas con la seguridad. En el contexto de esta Recomendación | Norma Internacional, un declarante y/o un verificador depositan su confianza en un tercero en las actividades de autenticación.

NOTA – El declarante o el verificador puede descomponerse en múltiples componentes funcionales, que posiblemente se encuentren en sistemas abiertos diferentes.

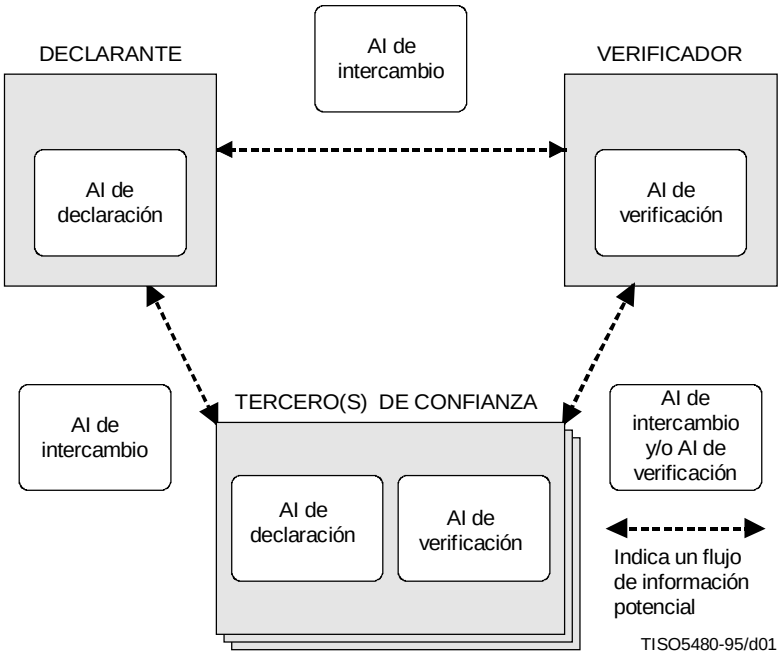
5.1.3 Información de autenticación

Los tipos de información de autenticación son:

- información de autenticación de intercambio (AI de intercambio);
- información de autenticación de declaración (AI de declaración);
- información de autenticación de verificación (AI de verificación).

El término intercambio de autenticación se utiliza para designar una secuencia de una o más transferencias de AI de intercambio destinadas a efectuar una autenticación.

La Figura 1 ilustra la relación entre declarante, verificador, tercero de confianza, y los tres tipos de información de autenticación.



NOTAS

1 En algunos escenarios no pueden intervenir terceros de confianza.

2 La AI de verificación puede ser la del principal o la del tercero de confianza (para más detalles, véase 5.5).

Figura 1 – Ilustración de las relaciones entre pretendiente, verificador, tercero de confianza, y tipos de información de autenticación

En algunos escenarios, para generar AI de intercambio, un declarante puede tener que interactuar con un tercero de confianza. Análogamente, para verificar AI de intercambio, un verificador puede tener que interactuar con un tercero de confianza. En estos casos, el tercero de confianza puede poseer AI de verificación correspondiente a un principal.

También es posible que se utilice un tercero de confianza en la transferencia de AI de intercambio.

Las entidades pueden también tener que poseer la información de autenticación que se utilizará en la autenticación del tercero de confianza.

En 6.1 se presentan ejemplos de los tres tipos de información de autenticación.

NOTA – Como el término credenciales no siempre se utiliza de manera coherente en otras Recomendaciones | Normas Internacionales, este marco de seguridad no lo utiliza. El término credenciales, que se define en la Rec. X.800 del CCITT | ISO 7498-2, podría ser un ejemplo de AI de intercambio.

5.2 Aspectos del servicio de autenticación

5.2.1 Amenazas a la autenticación

El objetivo de la autenticación es confirmar la identidad de un principal. Los mecanismos que permiten la autenticación deben normalmente eliminar las amenazas de suplantación (o impostura) y de reproducción.

Suplantación (o impostura) designa la pretensión de una entidad de hacerse pasar por una entidad diferente, es decir, la entidad pretende hacerse pasar por otra entidad relacionada con el verificador de una manera concreta (por ejemplo, por el origen de los datos, o por una relación de comunicaciones). Entre estos tipos figuran la reproducción, la retransmisión y el compromiso de AI de declaración.

Una amenaza de suplantación se produce en el contexto de una actividad (por ejemplo, origen de los datos, una relación de comunicación) iniciada por el declarante o por el verificador. La protección contra las amenazas a una actividad relativa a la suplantación depende de la relación entre la autenticación y esa actividad. Para hacer frente a amenazas de tipo suplantación, debe utilizarse autenticación en unión de alguna forma de servicio de integridad, que vincule la identidad autenticada a la actividad.

La reproducción designa la repetición de una AI de intercambio, para producir un efecto no autorizado. La reproducción suele utilizarse en combinación con otros ataques, tales como la modificación de datos. No todos los mecanismos de autenticación son igualmente resistentes a la reproducción. La reproducción puede constituir una amenaza a otros servicios de seguridad. La autenticación puede utilizarse para combatir la reproducción, ya que brinda un medio de determinar el origen de la información intercambiada.

5.2.2 Reenvío de autenticación

En algunas circunstancias un principal puede tener que actuar indirectamente dentro de un sistema. En tales casos habrá que crear su representación dentro de ese sistema. Además, antes de crear la representación de un principal dentro del sistema, el principal debe ser autenticado.

Cuando actúa en nombre del principal, la representación será autenticada en lugar de la entidad del principal. Dado que la representación actúa como si fuera el principal, las acciones del principal pueden efectuarse dentro del sistema sin que se requiera la participación directa del principal. Véase un ejemplo en el Anexo A.

Además de soportar representaciones de duraciones independientes, cuando el principal es un usuario humano pueden también utilizarse representaciones con mecanismos adicionales que hagan la duración de las representaciones dependientes de la presencia del usuario.

Un declarante, al actuar en nombre de su principal, puede acceder a otro sistema que cree su propia representación del principal tras la autenticación. La creación de esta representación se denomina reenvío de autenticación.

La aptitud para reenviar autenticación de esa manera puede ser afectada por la política de seguridad.

5.2.3 Autenticación unilateral y mutua

La autenticación puede ser unilateral o mutua. La autenticación unilateral solamente confirma la identidad de un principal. La autenticación mutua confirma las identidades de ambos principales.

La autenticación de entidad puede ser mutua o unilateral. Por su propia naturaleza, la autenticación del origen de datos es siempre unilateral.

5.2.4 Iniciación de un intercambio de autenticación

Un intercambio de autenticación puede ser iniciado por el declarante o por el verificador. La entidad que comienza el intercambio se denomina iniciador de la autenticación.

5.2.5 Revocación de la información de autenticación

Revocación de la información de autenticación designa la invalidación permanente de AI de verificación.

La política en vigor puede exigir la revocación de la información de autenticación en determinadas situaciones. La decisión de revocar información de autenticación puede basarse en la detección de eventos de violación de seguridad, cambio de política u otras razones. La revocación de información de autenticación puede o no implicar revocación del acceso existente, o tener otros efectos derivados.

Además, pueden ejecutarse las siguientes acciones relacionadas con la gestión:

a) registro del evento en el camino de auditoría;

b) informe local del evento;

c) informe a distancia del evento; y/o

d) desconexión de una relación de comunicación.

La acción concreta a ejecutar con cada evento depende de la política de seguridad en vigor.

5.2.6 Garantía de continuidad de la autenticación

La autenticación de entidad sólo garantiza una identidad en un instante dado. Una forma de obtener garantía de continuidad de la autenticación es vincular el servicio de autenticación a un servicio de integridad de datos.

Se dice que un servicio de autenticación y un servicio de integridad están vinculados cuando el principal es inicialmente autenticado mediante un servicio de autenticación, y éste junto con otra información está utilizando un servicio de integridad. Se asegura así que la información posterior no puede ser alterada por cualquier otra entidad, y que por tanto debe proceder del principal inicialmente autenticado. Es importante que el servicio de integridad se proporcione en la totalidad del trayecto que la información sigue para ir del principal al verificador. Por ejemplo, la suplantación es posible si parte de la información puede ser producida por principales que no sean el autenticado.

Otra forma de garantizar que la entidad distante sigue estando presente en un momento posterior es efectuar otros intercambios de autenticación de vez en cuando. Sin embargo, esto no evita intrusiones durante los intervalos, por lo que no se obtiene garantía de continuidad. Por ejemplo, es posible el siguiente ataque: un intruso, cuando se le pide que presente más autenticación, permite a la parte válida efectuar las acciones de autenticación; una vez concluidas éstas, el intruso toma el relevo.

Si el mecanismo de integridad requiere una clave, dicha clave podrá derivarse de parámetros especificados durante el intercambio de autenticación. Habiendo así establecido que la clave está asociada con el principal autenticado, su utilización en el mecanismo de integridad servirá para enlazar los dos servicios prestados de la manera antes descrita.

La forma de derivar una clave para un servicio de integridad puede especificarse como parte de los parámetros que determinan los métodos y algoritmos que deben utilizarse para el intercambio de autenticación global.

NOTA – Cuando se utilizan otros servicios de seguridad, es también posible derivar información de servicio de parámetros especificados durante el intercambio de autenticación, por ejemplo, una clave de confidencialidad.

5.2.7 Distribución de componentes de autenticación a través de múltiples dominios

Cabe la posibilidad de que dominios de seguridad entren en una relación tal que el declarante perteneciente a un dominio pueda ser autenticado por un verificador perteneciente a otro dominio. Pueden estar involucrados múltiples dominios de seguridad, a saber:

– el dominio de seguridad en el que reside el iniciador;

– el dominio de seguridad en el que reside el verificador;

– los dominios de seguridad en los que residen los terceros de confianza.

Estos dominios no tienen porqué ser todos distintos.

Antes de que tenga lugar la autenticación entre diferentes dominios de seguridad, es necesario establecer una política de interacción segura.

5.3 Principios aplicados en la autenticación

En general, un método de autenticación determinado se basará en una serie de supuestos o expectativas relacionados con uno o más principios.

Estos principios son:

a) algo que se conoce, por ejemplo, una contraseña;

b) algo que se posee, por ejemplo, una tarjeta magnética o una tarjeta inteligente;

c) alguna característica inmutable, por ejemplo, identificadores biométricos;

d) aceptación de que una tercera entidad (tercero de confianza) ha establecido la autenticación; y

e) contexto, por ejemplo, dirección del principal.

Debe señalarse que todos los principios tienen sus puntos débiles. Por ejemplo, la autenticación de algo que se posee es a menudo la autenticación del objeto poseído, más bien que la de su poseedor. En algunos casos el inconveniente puede superarse por combinación de varios principios. Por ejemplo, cuando se utiliza una tarjeta inteligente (algo que se posee), puede superarse por adición de un número de identidad personal (PIN) (algo que se conoce) a fin de autenticar al usuario de la tarjeta. Además, el principio e) es particularmente endeble y se aplica prácticamente siempre en combinación con otro principio.

Obsérvese que en d) hay dos tipos de recursión:

– para ser identificada, la tercera entidad tendría a su vez que ser autenticada; y

– la autenticación que la tercera entidad establece puede utilizar una cuarta entidad, etc.

El análisis de los métodos de autenticación reales que incorporan estos principios conducirá a una indicación de las entidades que intervienen, los principios que se aplican, y los principales que son autenticados.

5.4 Fases de la autenticación

La autenticación puede comprender las siguientes fases:

– fase de instalación;

– fase de información de autenticación de cambio;

– fase de distribución;

– fase de adquisición;

– fase de transferencia;

– fase de verificación;

– fase de inhabilitación;

– fase de rehabilitación;

– fase de desinstalación.

Las fases aquí descritas no necesariamente tienen que producirse en periodos de tiempo distintos, es decir, pueden estar superpuestas.

Un determinado esquema de autenticación no necesita todas estas fases. Además, en algunos casos, la secuencia de las fases puede ser diferente de la que se desprende de la descripción siguiente.

5.4.1 Instalación

En la fase de instalación se define la AI de declaración y la AI de verificación.

5.4.2 Información de autenticación de cambio

En la fase de información de autenticación de cambio, un principal o un gestor hace que cambie una AI de declaración o una AI de verificación (por ejemplo, se cambia una contraseña).

5.4.3 Distribución

En la fase de distribución, la AI de verificación se distribuye a una entidad (por ejemplo, un pretendiente) o un verificador para utilizarla al verificar AI de intercambio. Por ejemplo, en los procedimientos fuera de línea, unas entidades pueden obtener certificados de autenticación, listas de renovación de certificados y listas de revocación de autoridades. La fase de distribución puede tener lugar, antes, durante o después de la fase de transferencia.

5.4.4 Adquisición

En la fase de adquisición, un declarante o un verificador puede obtener la información local requerida para generar AI de intercambio específica para una instancia de autenticación. Diferentes procedimientos pueden adquirir AI de intercambio por interacción con un tercero de confianza o por intercambio de mensajes entre entidades autenticantes.

Por ejemplo, cuando se utiliza un centro de distribución de claves en línea el declarante o el verificador puede obtener alguna información, tal como un certificado de autenticación (véase 6.1.3), del centro de distribución de claves, para habilitar la autenticación ante la otra entidad.

5.4.5 Transferencia

En la fase transferencia se transfiere AI de intercambio entre un declarante y un verificador.

5.4.6 Verificación

En la fase de verificación, la AI de intercambio se confronta con la AI de verificación. En esta fase, una entidad que no puede verificar por sí misma AI de intercambio podrá contactar a un tercero de confianza que efectuará la verificación de AI de intercambio. En este caso, el tercero de confianza retornará una respuesta positiva o negativa.

5.4.7 Inhabilitación

En la fase de inhabilitación, se establece un estado en el cual un principal que antes podía ser autenticado está temporalmente incapacitado para ser autenticado.

5.4.8 Rehabilitación

En la fase de rehabilitación se termina el estado establecido en la fase de inhabilitación.

5.4.9 Desinstalación

La fase de desinstalación consiste en retirar un principal de una población de principales.

5.5 Intervención de terceros de confianza

Los mecanismos de autenticación pueden ser caracterizados por el número de terceros de confianza que intervienen.

5.5.1 Autenticación sin intervención de terceros de confianza

En la situación más simple, ni el declarante ni el verificador es soportado por ninguna otra entidad en la generación y verificación de AI de intercambio. En este caso, la AI de verificación para el principal tiene que estar ya instalada en el verificador.

A menos que la mayor parte de las entidades estén limitadas a un pequeño número de posibles interlocutores de comunicación, este método es de uso limitado en los entornos de comunicaciones en gran escala. En el caso peor, cada verificador deberá tener AI de verificación sobre todos los principales en un dominio de seguridad, aumentando la información total requerida en proporción al cuadrado del número de entidades que intervienen (véase la Figura 2).

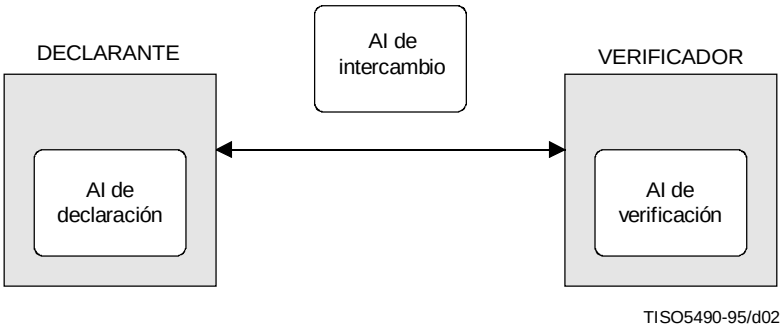


Figura 2 – Autenticación sin intervención de un tercero de confianza

5.5.2 Autenticación con intervención de terceros de confianza

Un tercero de confianza puede tener disponible la AI de verificación de los principales que se encuentren en su propio dominio de seguridad y, opcionalmente, su propia AI de declaración y AI de verificación de algunos otros terceros de confianza. La integridad de esta información debe ser garantizada. También es necesario mantener la confidencialidad de la AI de declaración del tercero de confianza, así como de la AI de verificación si de esta información puede deducirse la AI de declaración.

La confianza multientidad exige una cadena de entidades de confianza, tal como se define en el principio d) de 5.3. La cadena está formada por todos los puntos de confianza mutuos entre un par de entidades autenticantes. La introducción de terceros de confianza adicionales permite la autenticación entre una gran población de entidades, cada una de las cuales sólo mantiene información sobre un número limitado de ellas (y no sobre las demás). Así, la información total podrá aumentar proporcionalmente al número de entidades que intervienen.

Las relaciones multientidad pueden determinarse según las exigencias de comunicaciones (número de enlaces activos que intervienen) y según el grado de control de gestión que tienen, por ejemplo, el retardo inherente a la revocación de la información de autenticación.

5.5.2.1 Autenticación con corte de línea

En el caso de autenticación con corte de línea, una entidad de confianza (un intermediario) interviene directamente en un intercambio de autenticación entre el declarante y el verificador. El intermediario autentica a un principal y, seguidamente, garantiza la identidad en un subsiguiente intercambio de autenticación con corte de línea.

La autenticación con corte de línea requiere que el verificador confíe en que el intermediario haya autenticado debidamente al principal, y que se garantice al verificador la identidad del intermediario mediante autenticación.

La revocación de la aptitud para autenticar puede controlarse hasta la granularidad del siguiente intento de autenticación. Si se le revocase al declarante su información de autenticación, el intermediario podría actualizar inmediatamente el estatus del declarante y rechazar cualesquiera intentos futuros de autenticación.

Ocasionalmente, esto puede ampliarse de modo que pueda recibirse una garantía que comprenda una cadena de intermediarios de confianza. Corresponde al verificador determinar la validez de la cadena de intermediarios.

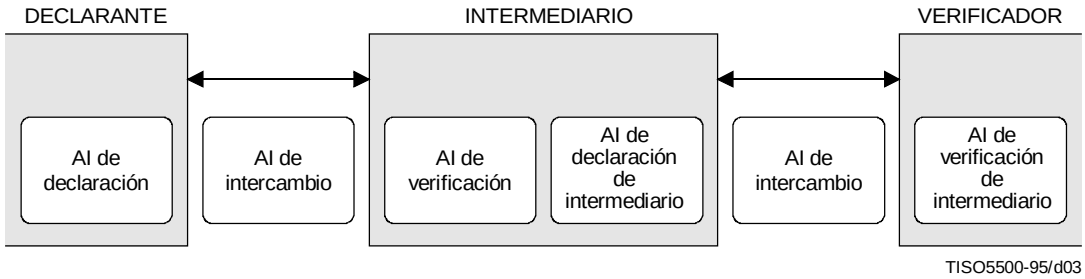


Figura 3 – Autenticación con corte de línea

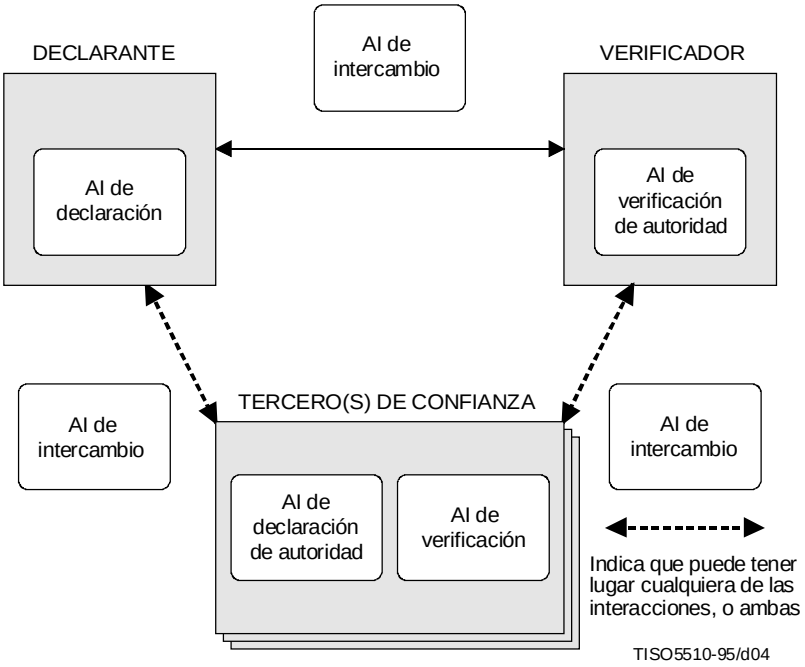
5.5.2.2 Autenticación en línea

En el caso de autenticación en línea, uno o más terceros de confianza intervienen activamente en cada instancia de un intercambio de autenticación. Sin embargo, a diferencia de la autenticación con corte de línea, los terceros de confianza en línea no están directamente en el trayecto del intercambio de autenticación entre el declarante y el verificador. Los terceros de confianza en línea pueden recibir una petición de un declarante para que generen AI de intercambio y pueden ayudar al verificador en la verificación de AI de intercambio. Un tercero de confianza en línea puede generar certificados de autenticación en línea (véase 6.1.3).

La autenticación en línea exige que haya una cadena de terceros de confianza que participen en la generación de AI de intercambio, entre el verificador y el tercero de confianza que puede validar la AI de declaración del principal. En el caso más sencillo un solo tercero de confianza tiene que interactuar directamente con el declarante o el verificador. Esto puede no obstante ampliarse a una cadena de terceros de confianza que comuniquen directa o indirectamente con el declarante o el verificador.

La revocación de la aptitud para autenticar puede controlarse hasta la granularidad del siguiente intento de autenticación.

Ejemplos de terceros de confianza en línea son los servidores de autenticación en línea y los centros de distribución de claves.



NOTA – El intercambio real que se produce entre las tres diferentes entidades representadas en la Figura 4 no es el mismo.

Figura 4 – Autenticación en línea

5.5.2.3 Autenticación fuera de línea

La autenticación fuera de línea se caracteriza por la necesidad de utilización de listas certificadas o certificados revocados, listas certificadas de certificados revocados, temporizaciones de certificados u otros medios no inmediatos para la revocación de AI de verificación.

En el caso de autenticación fuera de línea, uno o más terceros de confianza soportan la autenticación sin intervenir en cada instancia de autenticación. El tercero de confianza fuera de línea genera y distribuye por adelantado certificados de autenticación fuera de línea que el verificador podrá utilizar ulteriormente para validar un intercambio de autenticación. Así, el intercambio de autenticación se efectúa autónomamente, sin intervención de la autoridad.

Como los terceros de confianza no tienen que poder interactuar directamente con el declarante o el verificador en el momento que se produce la autenticación, este método puede ser más eficiente en cuanto al número de interacciones requeridas.

La revocación deberá basarse en disposiciones adicionales como son las relativas a la expiración y renovación de certificados, y listas certificadas de certificados revocados.

Ejemplos de terceros de confianza fuera de línea son las autoridades de certificación que emiten certificados de autenticación fuera de línea (véase 6.1.3).

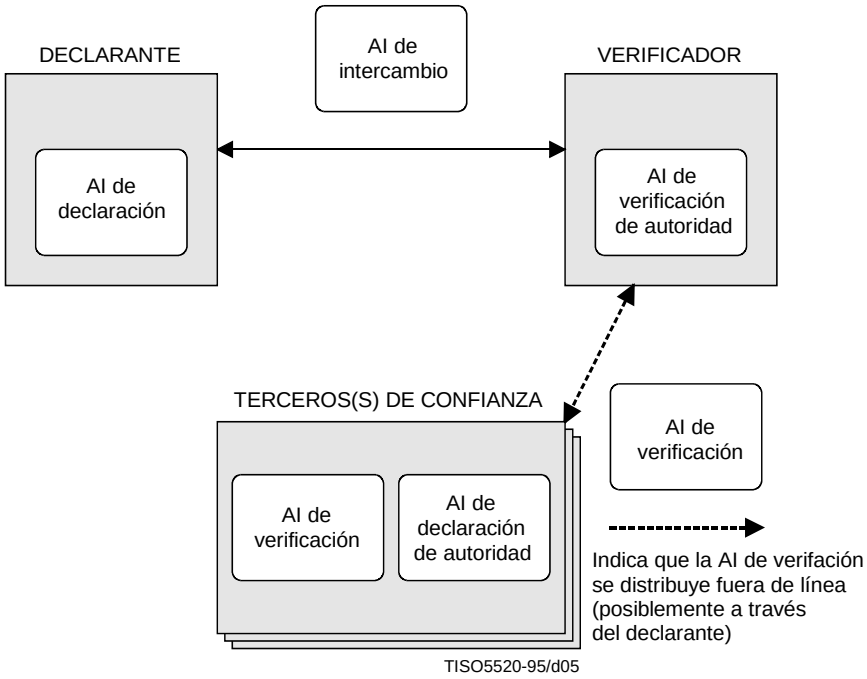


Figura 5 – Autenticación fuera de línea

5.5.3 Confianza de un declarante en un verificador

Los mecanismos en los cuales es necesario confiar en un verificador son inadecuados, a menos que se pueda confiar en todos los verificadores posibles. Esto se debe a que si la identidad del verificador no ha sido autenticada, no puede saberse si es digno de confianza. Por ejemplo, con la simple utilización de contraseñas para la autenticación, es necesario confiar en que un verificador no mantiene y reutiliza una contraseña.

5.6 Tipos de principal

Los principales pueden clasificarse en categorías de diversas maneras, según tengan:

a) una o más características pasivas, por ejemplo, improntas digitales, características retinales;

b) capacidad de intercambio y procesamiento de información;

c) capacidad de almacenamiento de información; y

d) ubicación fija única.

Los principales pueden encajar en más de una categoría [por ejemplo, las entidades humanas tienen cabida en a), b) y c)]. En cada caso se aplica un método de autenticación diferente:

a) medición de la o las características pasivas;

b) evaluación compleja de puesta a prueba y respuesta;

c) memorización de un secreto (por ejemplo, una contraseña);

d) determinación de posición.

5.7 Autenticación de usuarios humanos

En una instancia de autenticación, puede ser necesario autenticar al usuario humano que interviene en último término, más bien que al proceso que actúa en nombre del usuario humano. El diálogo entre usuarios humanos y computadores puede aumentar el potencial de intrusión por suplantación.

Los métodos para la autenticación de usuarios humanos deberán ser aceptables por éstos, además de económicos y seguros. Métodos inaceptables pueden incitar a los usuarios humanos a encontrar maneras de evitar los procedimientos, con lo cual aumenta el potencial de intrusión.

Los métodos de autenticación de usuarios humanos se basan en los principios descritos en 5.3. Los procedimientos para la autenticación de usuarios humanos se basan en las fases descritas en 5.4.

El Anexo A da más información sobre la autenticación de usuarios humanos y sobre los procesos que actúan en nombre de un usuario humano.

5.8 Tipos de ataques a la autenticación

Se consideran tres formas de ataques:

- *ataques de reproducción*, en los que se lee la AI de intercambio y se reproduce posteriormente;
- *ataques de retransmisión* iniciados por un intruso; y
- *ataques de retransmisión* en los que responde un intruso.

Un ataque de retransmisión es un ataque en el que se intercepta AI de intercambio, que es inmediatamente reproducida.

5.8.1 Ataques de reproducción

Hay que considerar dos casos de reproducción. Son éstos la reproducción de alguna AI de intercambio:

- en el mismo verificador; o
- en otro verificador.

Este último caso es posible cuando varios verificadores conocen la (misma) AI de verificación de un principal. Cuando puede conseguirse una reproducción, se produce un caso específico de suplantación (o impostura).

Ambos casos de reproducción pueden combatirse mediante puestas a prueba. Las puestas a prueba son generadas por el verificador. El mismo verificador no debe nunca emitir dos veces la misma puesta a prueba. Esto puede conseguirse de varias maneras (véase el Anexo C).

5.8.1.1 Reproducción en el mismo verificador

La reproducción en el mismo verificador puede combatirse mediante números únicos o puestas a prueba.

Los números únicos son generados por el declarante. El mismo verificador no debe nunca aceptar dos veces el mismo número único. Esto puede conseguirse de varias maneras (véase el Anexo C).

5.8.1.2 Reproducción en un verificador diferente

La reproducción en un verificador diferente puede combatirse utilizando puestas a prueba. Otra posibilidad es combatirla utilizando, en la computación de la AI de intercambio, cualquier característica exclusiva del verificador. Dicha característica puede ser el nombre del verificador, su dirección de red o en general cualquier atributo único con respecto a los verificadores que comparten la misma información de autenticación de verificación.

5.8.2 Ataques de retransmisión

5.8.2.1 Ataques de retransmisión iniciados por intrusos

En este tipo de ataque el intruso es el iniciador de la autenticación. Este ataque es posible sólo si el declarante y el verificador pueden ambos iniciar la autenticación. Con este ataque, el declarante y el verificador intercambian información de autenticación por mediación de un intruso sin ser conscientes de ello, es decir, el intruso pretende ser un cierto verificador para un declarante y ser este declarante para ese verificador.

Por ejemplo, supongamos que el intruso C desea hacer creer al verificador B que es el declarante A. C comienza una interacción con A y B. C dice a A que es B, pide a A que se autentique a B, y también dice a B que es A y que desea autenticarse él mismo (véase la Figura 6).

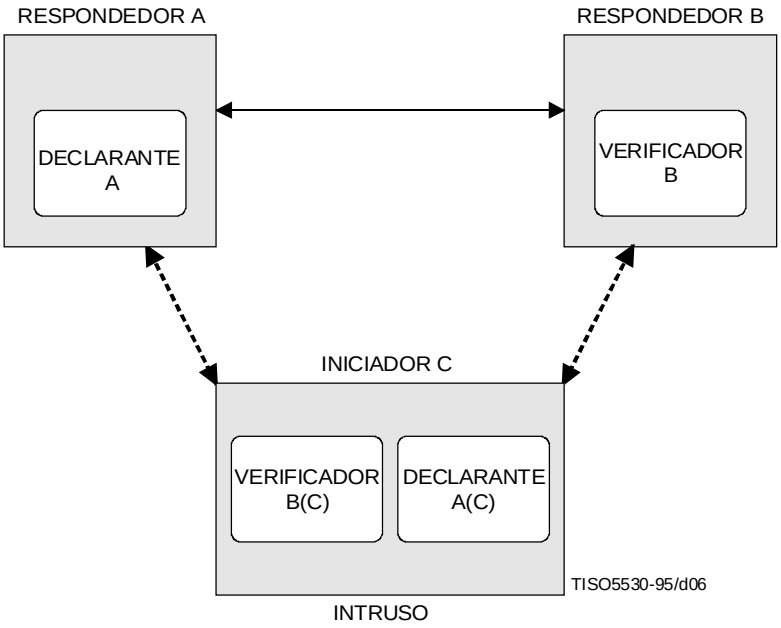


Figura 6 – Ataque de retransmisión iniciado por un intruso

Durante el proceso de autenticación, A actúa como declarante para con B (en realidad para con C actuando como B) y, por tanto, suministra información que C puede utilizar para autenticarse a B. B actúa como el verificador, y también suministra la información que se necesita para desempeñar el papel de verificador. Tras la autenticación, el intruso C aparecerá a B como el A autenticado.

Este tipo de ataque puede combatirse si:

a) la entidad que comienza una interacción es siempre el declarante o siempre el verificador (obsérvese que esto no es posible cuando se utiliza autenticación mutua); o

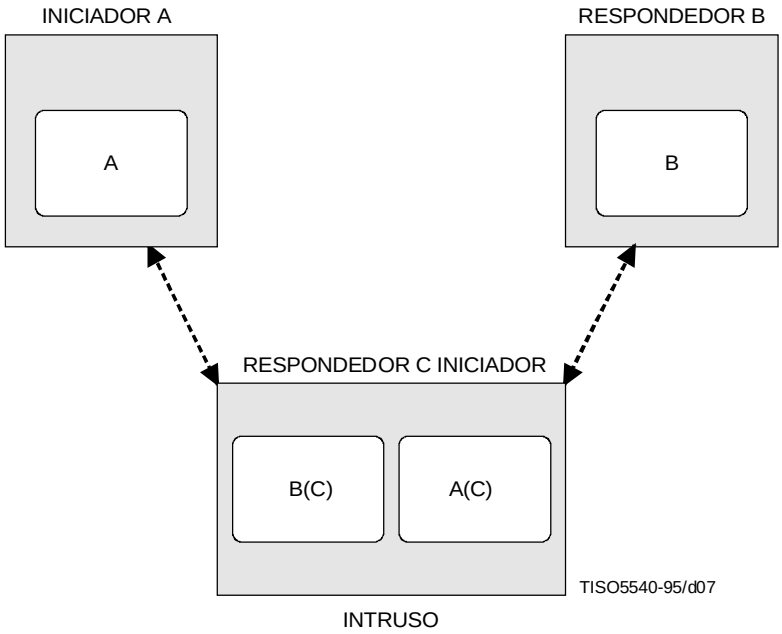
b) la AI de intercambio proporcionada por el declarante difiere según su papel como iniciador de una petición de autenticación o respondedor a una invitación de autenticación. Esta diferencia permite al verificador detectar la interceptación descrita. Véanse más detalles en el Anexo D.

5.8.2.2 Ataques de retransmisión en los que responde un intruso

En este tipo de ataque, el intruso se inmiscuye en un intercambio de autenticación, intercepta la información de autenticación y la reenvía, asumiendo el papel de iniciador. Este tipo de ataque puede producirse ya sea de manera oportunista, en cuyo caso el intruso (o intrusos) espera a que lo confundan con el respondedor, o sistemáticamente, en cuyo caso el intruso se presenta él mismo como el respondedor (por ejemplo, en una tabla de ubicación de recursos centrales).

La forma general de combatir este tipo de ataque exige el uso de un servicio complementario (integridad o confidencialidad). La AI de intercambio se combina con alguna otra información que habilite al declarante y al verificador, siempre que sean las partes legítimas, a derivar una clave. La clave derivada puede entonces utilizarse como clave para un mecanismo de integridad o de confidencialidad de carácter criptográfico.

Otra forma de combatir este tipo de ataque es aplicable cuando la red de comunicaciones no está sujeta a interceptaciones internamente, es decir, siempre entrega datos invariables a la dirección correcta. En esta situación, el ataque puede combatirse integrando las direcciones de red en la AI de intercambio (por ejemplo, firmando la dirección de red).



NOTAS

1 Aun si se combaten los ataques iniciados por el intruso utilizando los métodos a) o b) de 5.8.2.1, un método de autenticación seguirá siendo vulnerable a un ataque de respuesta de un intruso.

2 La notación X(Y) indica que Y intenta hacerse pasar por X.

Figura 7 – Ataques de retransmisión en los que responde el intruso

6 Información de autenticación y servicios

6.1 Información de autenticación

6.1.1 Información de autenticación de declaración

AI de declaración es la información utilizada para generar la AI de intercambio que se necesita para autenticar al principal.

Ejemplos de AI de declaración son:

a) *Contraseña*.

b) *Clave secreta* – Se utiliza con mecanismos de autenticación que emplean algoritmos simétricos.

c) *Clave privada* – Se utiliza con mecanismos de autenticación que emplean algoritmos asimétricos.

6.1.2 Información de autenticación de verificación

La AI de verificación se utiliza para verificar una identidad declarada mediante AI de intercambio.

Ejemplos de AI de verificación son:

a) *Contraseña* – Relacionada con la identidad de un principal.

b) *Clave secreta* – Relacionada con la identidad de un principal o autoridad. Se utiliza con mecanismos de autenticación que emplean algoritmos simétricos.

c) *Clave pública* – Relacionada con la identidad de un principal o autoridad. Se utiliza con mecanismos de autenticación que emplean algoritmos asimétricos.

La AI de verificación puede proporcionarse en forma de una tabla de autenticación y/o un certificado de autenticación fuera de línea (véase 6.1.4.2).

Una tabla de autenticación es un conjunto de entradas directamente accesible por el verificador. El trayecto utilizado para acceder a la tabla está protegido en cuanto a su integridad, y también en cuanto a su confidencialidad si se trata de mecanismos simétricos.

Ejemplos de elementos que pueden estar contenidos en una entrada a una tabla de autenticación son:

- la identidad del principal;
- la información a utilizar para verificar una identidad en un intercambio de autenticación, por ejemplo, una contraseña, una clave secreta, o una clave pública;
- periodo de validez de la entrada;
- política de seguridad aplicable a la entrada;
- autoridad responsable de la entrada.

6.1.3 Información de autenticación de intercambio

Ejemplos de información de autenticación de intercambio son:

- identificador distintivo declarado;
- contraseña;
- puesta a prueba;
- respuesta a puesta a prueba;
- número único;
- identificador distintivo de verificador;
- el resultado de una función de transformación aplicada a (o que utilice) AI de declaración u otros datos (por ejemplo, sello de tiempo, número aleatorio, contador, puesta a prueba, identidad del verificador, impronta digital, identidad del declarante); ejemplos de funciones de transformación son una función unidireccional, una función de cifrado asimétrico, y una función de cifrado simétrico;
- certificado en línea;
- certificado fuera de línea.

Algunas o todas las AI de intercambio transportadas en una misma transferencia pueden tener la forma de un testigo de seguridad.

6.1.4 Certificados de autenticación

Una forma común de información de autenticación es un certificado de autenticación, que es un tipo determinado de certificado de seguridad, expedido por una autoridad de confianza, que puede utilizarse para autenticación.

Diferentes tipos de certificados de autenticación son:

- certificados de autenticación en línea;
- certificados de autenticación fuera de línea;
- certificados de autenticación de revocación; y
- listas de certificados de autenticación de revocación.

Los certificados fuera de línea (véase 6.1.4.2) sólo son aplicables a AI de verificación relacionada con claves públicas. La validez de un certificado fuera de línea puede revocarse por medio de un certificado de revocación o de una tabla de revocación.

Ejemplos de elementos que pueden estar contenidos en cualquier certificado de autenticación son:

- Identificación del método y/o clave que se han utilizado para generar un valor de comprobación criptográfico.
- La identidad de la autoridad de autenticación y la identidad del agente que ha emitido el certificado de autenticación (cuando una autoridad está representada por varios agentes, la identidad del agente permite saber con precisión qué clave de agente se ha utilizado).

- La hora de creación del certificado de autenticación (la hora de creación puede utilizarse para fines de auditoría o cuando no aparece el periodo de validez del certificado de autenticación; una vez transcurrido un periodo de tiempo dependiente de la política de seguridad, los certificados de autenticación excesivamente antiguos podrán ser rechazados).
- El periodo de validez (ni antes, ni después) del certificado de autenticación [este periodo de tiempo puede ser considerado si lo permite la política de seguridad del receptor; de no ser así, el tiempo (u hora) de expiración se derivará del tiempo (u hora) de creación según la política de seguridad del receptor].
- La política de seguridad aplicable al certificado de autenticación.
- Un número de referencia de certificado que, para cada certificado de autenticación, es único con respecto a todos los certificados de autenticación del mismo agente de autoridad.
- Tipo de certificado.
- La identidad o los atributos del verificador al que está destinado el certificado de autenticación (las entidades pueden comprobar este valor si aparece y rechazar los que sean incorrectos. Identidades/atributos pueden ser, por ejemplo, nombres de usuarios humanos, procesos de aplicación y/o identidades de máquinas físicas).

En las subcláusulas siguientes se identifican elementos adicionales para los diferentes tipos de certificado de autenticación.

Pueden definirse perfiles, en normas de aplicación, para especificar los elementos que son obligatorios y los que son opcionales.

6.1.4.1 Certificados de autenticación en línea

Un certificado de autenticación en línea es creado por un tercero de confianza a petición directa de un declarante. Un certificado en línea suele transferirse al verificador como parte de la AI de intercambio.

Ejemplos de elementos adicionales que pueden estar contenidos en un certificado de autenticación en línea son:

- Identificador distintivo del principal.
- Impronta digital de los datos cuando se utiliza la autenticación del origen de datos.
- Una clave simétrica asignada al principal para autenticación, junto con identificación del algoritmo que habrá de utilizarse en combinación con esa clave. Será necesario mantener la confidencialidad de esta información.
- El método de autenticación utilizado para obtener este certificado de autenticación.
- El método o métodos de autenticación con los que puede utilizarse este certificado de autenticación.
- Identificación del método que debe utilizarse para proteger el certificado de autenticación mientras se encuentra en tránsito y cualesquiera parámetros asociados necesarios para obtener esta protección. (Ejemplos de esos parámetros de protección son una puesta a prueba, un número único o una clave de protección.)

6.1.4.2 Certificados de autenticación fuera de línea

Un certificado de autenticación fuera de línea vincula una identidad a una clave criptográfica. Es creado por una autoridad sin que el declarante ni el verificador tengan que interactuar directamente con ella. Los certificados fuera de línea se aplican normalmente a mecanismos de autenticación que utilizan algoritmos asimétricos. Puede transferirse al verificador un certificado fuera de línea como parte de la AI de intercambio.

Ejemplos de elementos adicionales que pueden estar contenidos en un certificado de autenticación fuera de línea son:

- identificador distintivo del principal;
- una clave pública asignada al principal por la autoridad de autenticación, junto con la identificación del algoritmo a utilizar en combinación con esta clave pública.

Un certificado de autenticación fuera de línea puede revocarse antes del fin de su periodo de validez mediante un certificado de revocación o una lista de certificados de revocación.

6.1.4.3 Certificados de revocación

Un certificado de revocación es un certificado de seguridad emitido por una autoridad de seguridad para indicar que ha sido revocado un determinado certificado de autenticación fuera de línea. Esta información es almacenada, remitiéndose a la misma siempre que se presente un certificado para determinar si el certificado de autenticación presentado sigue siendo válido.

Ejemplos de elementos adicionales que pueden estar contenidos en un certificado de revocación son:

- la identidad de un principal, grupo de principales o autoridad;
- la hora y fecha en que se revocó el certificado de autenticación fuera de línea;
- el número de referencia del certificado revocado.

6.1.4.4 Listas de certificados de revocación

Una lista de certificados de revocación es una lista certificada de todos los certificados de autenticación revocados por una determinada autoridad de seguridad, en unión de la hora y la fecha de emisión de la lista. Esta información es almacenada, remitiéndose a la misma siempre que se presente un certificado para determinar si el certificado de autenticación presentado sigue siendo válido.

Un lista de certificados de revocación puede comprender lo siguiente:

- certificados de revocación;
- identificadores de referencia de certificados de revocación;
- los certificados de autenticación revocados;
- identificadores de referencia de los certificados de autenticación revocados;
- la fecha en que se emitió la lista;
- la fecha en que se emitirá la lista siguiente.

6.1.4.5 Cadenas de certificados

Los certificados de autenticación están siempre protegidos de modo que proporcionen autenticación del origen de datos procedente de un tercero de confianza. Si el verificador no posee la AI de verificación para comprobar el origen del certificado, puede utilizarse una cadena de certificados. Un certificado procedente de otra autoridad certifica la AI de verificación utilizada para validar el origen del primer certificado.

Recursivamente, puede utilizarse una cadena de certificados, cada uno de los cuales certifica una AI de verificación utilizada para validar el origen del certificado precedente. La cadena proporciona un *trayecto de certificación* de autoridades desde el verificador hasta el declarante. El verificador, basándose en la información que posea o que pueda obtener de un tercero de confianza, deberá decidir por sí mismo si cada certificado de la cadena es o no digno de confianza.

6.2 Servicios

Esta subcláusula proporciona un modelo general de autenticación basado en primitivas de servicio genéricas.

6.2.1 Información de estado de autenticación

La información de estado de autenticación representa el estado de autenticación retenido entre invocaciones de los servicios de autenticación. La información de estado de autenticación puede incluir:

- claves criptográficas de sesión;
- estado de autenticación mutua.

La información de estado de autenticación tiene que estar almacenada de manera segura. Esta información es mantenida por los proveedores de estos servicios.

6.2.2 Servicios relacionados con la gestión

Los servicios relacionados con la gestión de autenticación pueden exigir la distribución de información descriptiva, contraseñas o claves (mediante gestión de claves) a entidades que deben efectuar la autenticación. Puede exigir también la utilización de un protocolo entre entidades comunicantes y otras entidades que proporcionen servicios de autenticación. La gestión de autenticación puede también incluir la revocación de información de autenticación.

6.2.2.1 Instalar

El servicio instalar instala AI de declaración y AI de verificación. Este servicio puede perfeccionarse más aún mediante los servicios enrolar, validar y confirmar.

6.2.2.1.1 Enrolar

El servicio enrolar hace que una autoridad de seguridad registre información de autenticación asociada con un principal. Esta información incluye un identificador distintivo proporcionado sea por el principal o por la autoridad de seguridad. El servicio es invocado por el principal, por otra entidad, o por una autoridad de seguridad. (La autoridad de seguridad de registro puede exigir al principal que dé garantías de la validación del enrolamiento.) En ese momento, el principal es un candidato para penetrar en un dominio de seguridad, pero aún no es reconocido como miembro del mismo. No es posible ningún intercambio de autenticación en ese momento.

6.2.2.1.2 Validar

El servicio validar, proporcionado en nombre de la autoridad de dominio de seguridad, introduce un principal en un dominio de seguridad.

La validación de la AI de verificación asociada con un principal puede exigir la comunicación entre la autoridad de seguridad y otra entidad, lo cual no necesariamente se efectúa mediante comunicaciones OSI. El servicio validar hace que un identificador distintivo se vincule a AI de verificación.

6.2.2.1.3 Confirmar

El servicio confirmar se invoca después del servicio validar. Retorna información específica al principal o a otras entidades. La forma más simple de información retornada es un acuse de recibo o un rechazo de la instalación. Otras formas son:

- certificado de autenticación fuera de línea;
- el identificador distintivo aceptado; o
- AI de declaración.

Después de la confirmación, el principal puede ser autenticado.

6.2.2.2 Cambiar AI

El servicio cambiar AI se invoca en nombre de un principal o un gestor para provocar un cambio de la información de autenticación.

6.2.2.3 Distribuir

El servicio distribuir habilita a cualquier entidad a obtener AI de verificación suficiente para verificar AI de intercambio.

6.2.2.4 Inhabilitar

El servicio inhabilitar, que se invoca en nombre de una autoridad de seguridad, hace que se establezca un estado por el cual un principal queda inhabilitado temporalmente para ser autenticado.

6.2.2.5 Rehabilitar

El servicio rehabilitar, que se invoca en nombre de una autoridad de seguridad, provoca la terminación del estado establecido por el servicio inhabilitar.

6.2.2.6 Desinstalar

El servicio desinstalar provoca la supresión de un principal de una población de principales autenticables. Este servicio puede perfeccionarse más aún mediante los servicios invalidar, notificar y desenrolar.

6.2.2.6.1 Invalidar

El servicio invalidar es una acción efectuada por un administrador de seguridad, compuesta por la revocación de la AI de verificación y/o un cambio de la información de estatus asociado con un principal. El servicio invalidar impide a un principal autenticar.

6.2.2.6.2 Notificar

El servicio notificar puede ser invocado por la autoridad de seguridad después del servicio invalidar. Retorna al principal una notificación de su invalidación y posiblemente información sobre cómo reenrolar.

6.2.2.6.3 Desenrolar

El servicio desenrolar provoca la supresión de un principal de un dominio de seguridad. Corresponde a la supresión de la identidad del principal y la AI de verificación asociada. El servicio es invocado por una autoridad de seguridad.

6.2.3 Servicios de carácter operacional

6.2.3.1 Adquirir

El servicio adquirir permite a un declarante o verificador obtener la información requerida para generar AI de intercambio específica para una instancia de autenticación. Esto puede exigir la interacción con un tercero de confianza (por ejemplo, un servidor de autenticación).

Posibles entradas son:

- tipo de intercambio de autenticación;
- identificador distintivo de principal;
- identidad del verificador;
- tipo de AI de declaración (por ejemplo, contraseña, clave);
- AI de declaración (por ejemplo, valor de contraseña);
- tipo de AI de intercambio;
- validez (tiempos de comienzo/expiración).

Posibles salidas son:

- estatus (éxito o fracaso);
- información requerida para generar AI de intercambio;
- validez (tiempos de comienzo/expiración).

6.2.3.2 Generar

El servicio generar lo invoca un declarante para generar AI de intercambio y/o procesar AI de intercambio recibida.

Posibles entradas son:

- tipo de intercambio de autenticación;
- identificador distintivo de principal;
- información requerida para generar AI de intercambio como salida de un servicio adquirir;
- referencia a información de estado de autenticación retenida;
- AI de intercambio recibida del verificador;
- tipo de AI de intercambio;
- identidad del verificador;
- AI de declaración.

Posibles salidas son:

- estatus (éxito, ulteriores transferencias requeridas, o fracaso);
- referencia a información de estado de autenticación retenida;
- AI de intercambio para transferirla al verificador.

El tipo de intercambio de autenticación puede proporcionarse como entrada, en la primera invocación del servicio generar en un intercambio de autenticación, cuando el declarante es el iniciador de la autenticación. En la misma invocación se retorna, como salida, una referencia a información de estado de autenticación retenida. En invocaciones subsiguientes del servicio generar para el mismo intercambio de autenticación, esta entrada o salida no estará presente, pero la referencia a información de estado de autenticación retenida se puede proporcionar como entrada.

La información de estado de autenticación se retiene dentro del servicio para ulterior utilización en autenticación, hasta que se retorne éxito o fracaso.

Si se retorna «ulteriores transferencias requeridas», el declarante tendrá necesidad de invocar el servicio generar después de que haya recibido la AI de intercambio de la otra entidad. Es posible que el declarante deba efectuar varias de esas operaciones (es decir, invocar el servicio generar con la anterior información de estado de autenticación y la AI de intercambio recibida) hasta que se indique éxito o fracaso. De esta forma, este servicio permite la utilización de muchos esquemas, incluidos intercambios puesta a prueba-respuesta n-direccionales, así como los múltiples intercambios requeridos por esquemas basados en un conocimiento nulo.

6.2.3.3 Verificar

Un verificador invoca el servicio verificar para verificar AI de intercambio procedente del declarante y/o para generar AI de intercambio que transferirá al declarante.

Posibles entradas son:

- tipo de intercambio de autenticación;
- información requerida para generar AI de intercambio como salida de un servicio adquirir;
- referencia a información de estado de autenticación retenida;
- AI de intercambio recibida del declarante;
- AI de verificación.

Este servicio puede producir las siguientes salidas:

- estatus (éxito, ulteriores transferencias requeridas, o fracaso);
- referencia a información de estado de autenticación retenida;
- AI de intercambio para transferirla al declarante (si el estatus es «ulteriores transferencias requeridas»);
- identificador distinguidor de principal (si el estatus es «éxito»);
- validez (tiempo de comienzo/expiración);
- indicador de autenticación mutua.

El tipo de intercambio de autenticación puede proporcionarse como una entrada, en la primera invocación del servicio verificar en un intercambio de autenticación, cuando el verificador sea el iniciador de la autenticación. En la misma invocación se retorna, como salida, una referencia a información de estado de autenticación retenida. En invocaciones subsiguientes del servicio verificar para el mismo intercambio de autenticación, esta entrada o salida no estará presente, pero la referencia a información de estado de autenticación retenida podrá proporcionarse como entrada.

La información de estado de autenticación se retiene dentro del servicio para ulterior utilización en autenticación, hasta que se retorne éxito o fracaso.

Si se retorna estatus de «éxito», se retornará también el identificador distintivo del principal.

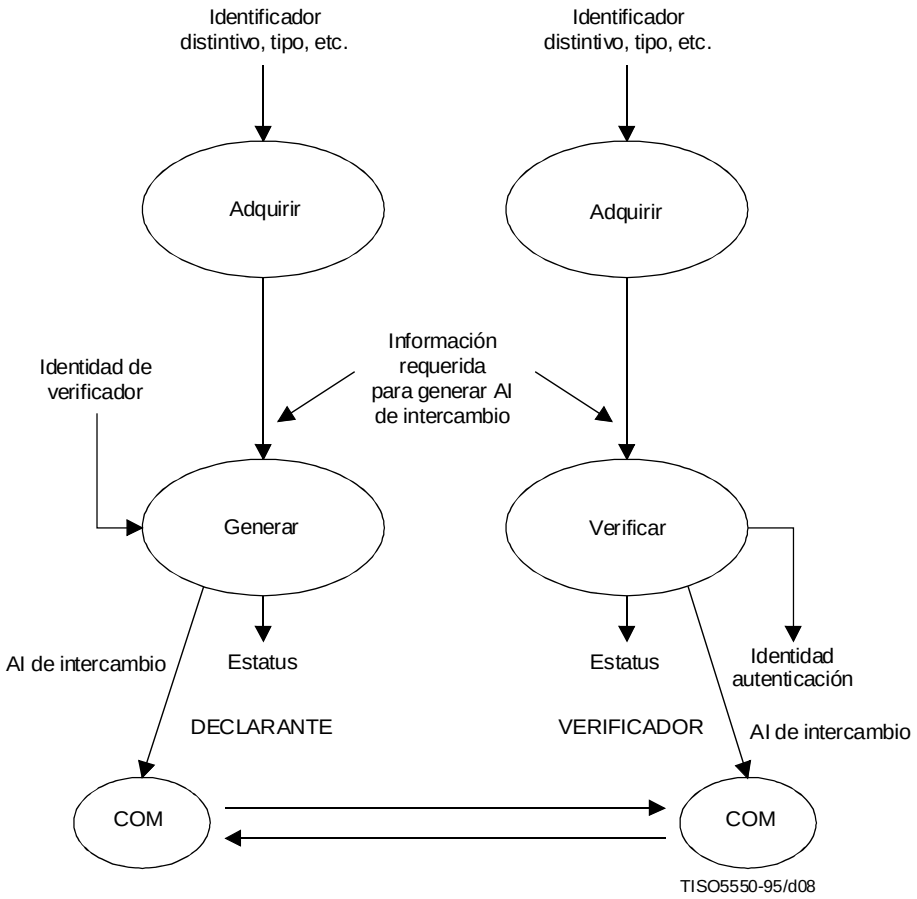
6.2.3.4 Generar y verificar

En el caso de autenticación mutua, los servicios generar y verificar pueden ser fusionados en un solo servicio. Las posibles entradas y las salidas de estos dos servicios fusionados son la unión de las entradas y las salidas de cada uno de ellos.

NOTA – El servicio generar y el servicio verificar no transfieren datos. La transferencia de datos depende del entorno en que se utiliza la autenticación. Este aspecto cae fuera del alcance de esta Recomendación | Norma Internacional.

6.2.3.5 Ejemplo de flujos de información

La Figura 8 presenta un ejemplo de los flujos de información asociados con la invocación de los servicios adquirir, generar y verificar, utilizados para modelar el suministro de autenticación (por ejemplo, a procesos de aplicación).



NOTA – En este ejemplo se muestra el servicio adquirir invocado por el declarante y el verificador. En la práctica, este servicio por lo general lo invoca una sola de las dos entidades, o no se invoca en absoluto. Aunque haya flujos de información entre generar y verificar, ninguno de estos servicios está destinado a invocar primitivas de comunicaciones.

Figura 8 – Ejemplo de flujos de información en servicios de carácter operacionales

7 Características de los mecanismos de autenticación

Los mecanismos de autenticación en el ámbito de esta Recomendación | Norma Internacional pueden basarse en los principios a), d) y e) de 5.3. El principio d) exige la utilización de un tercero de confianza como se describe en 5.5.2, pero estos mecanismos se basarán, en último término, en los principios a) o e). De no ser así, en sistemas abiertos, la autenticación de principales distantes se basa a menudo en el principio a), en el cual se utilizan secretos en forma de clave o contraseña.

7.1 Simetría/asimetría

La autenticación de principales distantes se basa a menudo en secretos en forma de contraseña o clave. La autenticación exige la demostración del conocimiento del secreto. Los métodos de demostración pertenecen a dos grandes categorías:

– *simétricos*, en los cuales ambas entidades comparten información de autenticación común; y

– *asimétricos*, en los cuales no toda la información de autenticación es compartida por ambas entidades.

Ejemplos de métodos de autenticación simétricos son:

- contraseña; y
- una puesta a prueba cifrada mediante una técnica de clave simétrica.

Ejemplos de métodos de autenticación asimétricos son:

- técnicas de clave asimétrica; y
- técnicas con las que puede verificarse la posesión de información sin que se revele ninguna parte de la misma.

7.2 Utilización de técnicas criptográficas/no criptográficas

Los mecanismos de autenticación basados en algo que se conoce (véase 5.3) pueden caracterizarse aún más según utilicen o no algoritmos criptográficos para proteger la información de autenticación. Pueden utilizarse técnicas simétricas, asimétricas, o una combinación de técnicas criptográficas para garantizar la integridad y, en algunos casos, la protección de la confidencialidad de la información de autenticación.

Las técnicas no criptográficas incluyen la utilización de contraseñas o tablas de puesta a prueba y respuesta. Los ejemplos de técnicas criptográficas incluyen la utilización de cifrado para proteger las contraseñas durante la transmisión.

7.3 Tipos de autenticación

En la autenticación de entidad intervienen dos entidades. En la autenticación unilateral, una entidad actúa como declarante y la otra como verificador. En la autenticación mutua, cada entidad actúa al mismo tiempo como declarante y como verificador. La autenticación mutua puede obtenerse utilizando mecanismos de autenticación idénticos o diferentes en ambos sentidos.

7.3.1 Autenticación unilateral

Puede obtenerse autenticación unilateral utilizando:

- una sola transferencia de información de autenticación, por ejemplo, cuando se utilizan números únicos; o
- tres transferencias de información de autenticación cuando se utilizan puestas a prueba; o
- más de tres transferencias de información de autenticación. Este caso es aplicable a algunos mecanismos que utilizan técnicas de conocimiento nulo.

En estos casos se ha supuesto que el declarante es el iniciador de la autenticación. Si el verificador es el iniciador de la autenticación, el número de transferencias es diferente; para más detalles, véase 8.2.

7.3.2 Autenticación mutua

La autenticación mutua no implica necesariamente que se duplique el número de transferencias, ni que se utilice el mismo mecanismo de autenticación en ambos sentidos.

Con los mecanismos de autenticación que utilizan tres transferencias de información de autenticación para la autenticación unilateral, la autenticación mutua no requiere ningún intercambio ulterior; la petición de una puesta a prueba puede combinarse con el envío de otra utilizada por el verificador (que en ese momento actúa como declarante) para autenticar al declarante (que actúa entonces como verificador).

7.3.3 Acuse de autenticación

En algunos casos es útil un acuse del hecho de que la autenticación de una entidad ha sido aceptada o rechazada. Este acuse puede estar garantizado o ser simplemente una respuesta de tipo sí o no, sin ninguna garantía. Esto exigirá una transferencia adicional.

8 Mecanismos de autenticación

8.1 Clasificación según las vulnerabilidades

Los propios mecanismos de autenticación pueden ser vulnerables a ataques, lo que limita su eficacia (véase 5.8).

En esta subcláusula, los mecanismos de autenticación que pueden emplearse para soportar autenticación en la fase de transferencia se clasifican según las amenazas a las que son resistentes. Todos los mecanismos descritos se basan en el principio de autenticación de «algo que se conoce» [véase 5.3 a)].

Todos los mecanismos descritos son aplicables a la autenticación de entidad, y algunos también lo son a la autenticación del origen de datos, por ejemplo, una impronta digital de los datos en el intercambio de autenticación.

Se definen las siguientes clases de mecanismos de autenticación:

- clase 0: no protegido;
- clase 1: protegido contra revelación;
- clase 2: protegido contra revelación y reproducción en verificadores diferentes;
- clase 3: protegido contra revelación y reproducción en el mismo verificador;
- clase 4: protegido contra revelación y reproducción en el mismo verificador o en verificadores diferentes.

NOTA – En las clases 1 a 4, «protegido contra revelación» significa protegido contra AI de declaración.

Pueden definirse otras clases si así conviene. Para algunas clases de mecanismos se identifican subclases. La enumeración de esas subclases no es necesariamente exhaustiva.

La AI de intercambio para cada clase de mecanismo es la indicada en los diagramas.

Cuando se utiliza una función de cifrado como parte del servicio generar, se emplea para formar la clave AI de declaración, posiblemente junto con otra información. Cuando se utiliza una función de descifrado como parte del servicio verificar, se emplea para formar la clave AI de verificación, posiblemente junto con otra información recibida en el intercambio de autenticación.

Los siguientes intercambios de autenticación se describen desde la perspectiva del declarante, y son siempre iniciados por éste. Para intercambios iniciados por el verificador, véase 8.2. Los intercambios descritos son aplicables a la autenticación unilateral. Para intercambios aplicables a la autenticación mutua, véase 8.4. En algunos casos, se necesita un acuse de recibo de que la autenticación tuvo éxito o no lo tuvo. Para ello puede ser necesaria una transferencia adicional de datos, la cual no se describe en esta cláusula. Los servicios aludidos en esta cláusula se definen en 6.2.

En los diagramas que siguen, la notación de un par de corchetes [ ] indica un componente opcional de la información transferida, incluido sólo en algunas condiciones.

El componente opcional [impronta digital] está presente en el caso de autenticación del origen de datos, y ausente en otro caso. Puede conseguirse una impronta digital, por ejemplo, utilizando un algoritmo de cifrado asimétrico, sea simplemente cifrando los datos o bien proporcionando un valor de comprobación criptográfico de los datos utilizando la clave privada del firmante. Para la autenticación del origen de datos, la transferencia de los datos a los que se refiere la impronta digital puede producirse de manera completamente independiente del medio de comunicación utilizado para los mecanismos siguientes, o puede compartir la utilización de dicho medio.

8.1.1 Clase 0 (no protegido)

En los mecanismos de la clase 0, la AI de declaración se envía simplemente, junto con el identificador distintivo, como AI de intercambio de declarante a verificador. Un ejemplo típico es el envío de una contraseña. La clase 0 es un caso de autenticación simétrica. Esta clase de mecanismo es vulnerable a los ataques de revelación de información de autenticación, y de reproducción.

El servicio generar produce AI de intercambio, como se muestra en la Figura 9, directamente de sus entradas.

El servicio verificar verifica que la AI de declaración recibida (por ejemplo, una contraseña) se corresponde con la AI de verificación asociada con el identificador distintivo recibido.

Los mecanismos de clase 0 son aplicables tanto a la autenticación del origen de datos como a la autenticación de entidad.

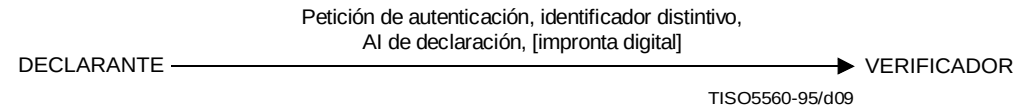


Figura 9 – Mecanismo de clase 0 (no protegido)

8.1.2 Clase 1 (protegido contra revelación)

Esta clase de mecanismo da protección contra la revelación de AI de declaración. Los mecanismos de clase 1 son aplicables tanto a la autenticación del origen de datos como a la autenticación de entidad.

Estos mecanismos emplean una función de transformación en la cual la AI de declaración, posiblemente combinada con el identificador distintivo, es transformada según la función y transferida junto con el identificador distintivo. La AI de declaración real no se transmite por el canal de comunicaciones. Ejemplos son:

- envío de una contraseña transformada según una función unidireccional (por ejemplo, un valor de comprobación criptográfico o una función de condensación);
- envío de una impronta digital cifrada según una clave secreta;
- envío de una contraseña encriptada según una clave de confidencialidad; y
- envío de una impronta digital firmada utilizando una clave privada.

Los mecanismos de este tipo son aplicables tanto a la autenticación del origen de datos como a la autenticación de entidad. Son vulnerables a los ataques por reproducción, pero dan protección contra la revelación de la AI de declaración. Por ejemplo, la contraseña transformada puede ser reproducida a nivel de intercambio de protocolo, pero la contraseña en texto claro, que es utilizable a nivel de interfaz del sistema, no es revelada.

El servicio generar utiliza la AI de declaración y, si es necesario, el identificador distintivo y/o una impronta digital, como entradas a una transformación criptográfica para generar la AI de intercambio, como muestra la Figura 10.

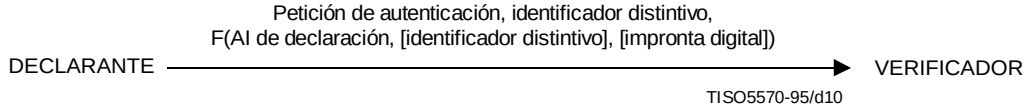


Figura 10 – Mecanismo de clase 1 protegido contra revelación

Tres ejemplos de funciones de transformación (F) son los siguientes:

a) En el caso de una función unidireccional, el servicio verificar repite la función unidireccional utilizando AI de verificación en lugar de AI de declaración, y la confronta con la AI de intercambio recibida.

b) En el caso de empleo de cifrado simétrico, el servicio de verificación utiliza la AI de verificación para descifrar la AI de intercambio recibida, y verifica luego la corrección del descifrado comprobando que contiene características distintivas tales como el identificador distintivo del declarante, la impronta digital correcta, una contraseña o un valor constante.

c) En el caso de una firma digital, la función verificar vuelve a calcular la impronta digital a partir de los datos recibidos y utiliza la verificación AI para controlar que la firma recibida es una firma válida para esa impronta.

Además, para la autenticación del origen de datos, se confronta la impronta digital de la AI de intercambio con una impronta digital de los datos que requieren autenticación.

NOTA – Cuando el identificador distintivo esté combinado con la AI de declaración, un ataque global será más difícil. En este caso sólo podrá efectuarse un ataque aislado contra un principal específico en vez de un ataque contra todos los principales juntos.

Para garantizar la confidencialidad, la función de transformación debe no tener inversa o, si la tiene, la inversa debe resultar computacionalmente insoluble a las partes con respecto a las cuales la AI de declaración (y la impronta digital) ha de mantenerse confidencial.

8.1.3 Clase 2 (protegido contra revelación y reproducción en verificadores diferentes)

Esta clase de mecanismo brinda protección contra la revelación de AI de declaración y la reproducción en verificadores diferentes, pero no contra una reproducción en el mismo verificador. Esta clase de mecanismo es idéntica a la clase 1, de la que sólo se diferencia en que como entrada de la función de transformación se incluye un ítem de datos que contiene una característica exclusiva del verificador deseado. Esto brinda protección adicional.

8.1.4 Clase 3 (protegido contra revelación y reproducción en el mismo verificador)

Este mecanismo brinda protección contra la revelación de AI de declaración y contra la reproducción en el mismo verificador.

Los mecanismos de número único introducen funciones de transformación en combinación con información única para dar protección contra la reproducción en un solo verificador. La AI de declaración y el número único, posiblemente combinados con la identidad, son transformados y transferidos, junto con el identificador distintivo.

Cuatro ejemplos de fuentes de número único son:

a) *Número aleatorio o seudoaleatorio* – Dicho número no se repite involuntariamente durante el tiempo de vida de la AI de intercambio. Un número aleatorio o seudoaleatorio de una gama suficientemente grande puede reducir el riesgo (probabilidad) de que ya se haya usado el mismo número;

b) *Sello de tiempo* – El número único es un sello de tiempo, obtenido de una fuente de confianza, que es exclusivo durante el tiempo de vida de la AI de reclamación. Se rechazarán los sellos de tiempo antiguos y los que hayan sido utilizados antes;

c) *Contador* – El número único es el valor de un contador que es continuamente incrementado mientras se esté utilizando la misma AI de declaración;

d) *Encadenamiento criptográfico* – El número único es el valor derivado del contenido de los intercambios de datos anteriores entre el reclamante y el verificador por encadenamiento de bloques.

La unicidad de este número fuera del declarante puede asegurarse por concatenación del mismo con datos únicos para el declarante (tales como su propio identificador distintivo).

También es posible utilizar una combinación de estas técnicas para producir un número único.

Tres ejemplos de funciones de transformación (F) son:

a) *Función unidireccional* – El número único, la AI de declaración y, opcionalmente, el identificador distintivo son transformados según una función unidireccional. El número único también es transmitido a fin de que el verificador pueda efectuar la misma transformación;

b) *Cifrado asimétrico* – Cuando la AI de declaración es una clave privada, el número único se firma según esa clave privada;

c) *Cifrado simétrico* – Cuando la AI de declaración es una clave secreta, el número único se cifra según esa clave secreta.

Esta subclase es aplicable a la autenticación del origen de datos y a la autenticación de entidad.

El servicio generar genera un número único. Después efectúa el cifrado utilizando las siguientes entradas:

– número único;

– AI de declaración;

– identificador distintivo (opcional);

– impronta digital (en caso de autenticación del origen de datos);

y produce la AI de intercambio como se muestra en la Figura 11.

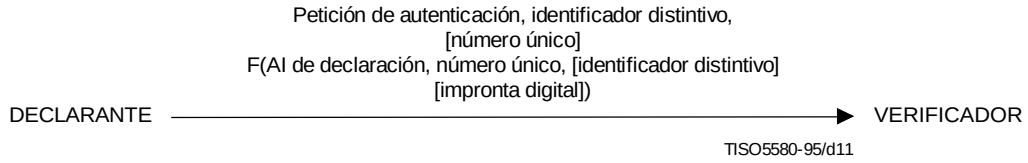


Figura 11 – Subclase 3b – Mecanismo de número único

El servicio verificar descifra la AI de intercambio y comprueba su validez confrontándola con la AI de verificación, como se indica en la clase 1. También comprueba que el número único recibido no se ha recibido con anterioridad. Si el número se ha recibido anteriormente, es señal de que ha habido una reproducción. Además, para la autenticación del origen de datos, se confronta la impronta digital de la AI de intercambio con una impronta digital regenerada de los datos recibidos.

NOTA – El empleo del término *encadenamiento criptográfico* corresponde aquí a la definición de *encadenamiento de bloques* que figura en ISO/CEI 10116.

8.1.5 Clase 4 (protegido contra revelación y reproducción en el mismo verificador o en verificadores diferentes)

8.1.5.1 Subclase 4a – Mecanismos de número único

Esta subclase de mecanismo es idéntica a la clase 3, salvo en que se incluye un ítem de datos que contiene una característica exclusiva del verificador deseado como entrada a la función de transformación en el intercambio. Esto brinda protección adicional.

8.1.5.2 Subclase 4b – Mecanismos de puesta a prueba

Los mecanismos de puesta a prueba tienen por finalidad combatir ataques de reproducción, es decir, asegurar que no tenga éxito ningún intento de autenticar mediante una reproducción de AI de intercambio. En respuesta a una petición de autenticación, el verificador envía una puesta a prueba al declarante en forma de ítem de datos con un valor único. El declarante transforma la información de puesta a prueba y la AI de declaración según alguna función, y retorna el resultado de esta transformación al verificador.

Los mecanismos de puesta a prueba, por lo tanto, exigen una transferencia tridireccional de información:

- envío de una petición de autenticación;
- emisión de una puesta a prueba; y
- envío de una respuesta que contiene un valor obtenido de la AI de declaración, posiblemente combinado con el identificador distintivo, y la información de desafío, transformados según una función (F) apropiada.

En el caso general, el identificador distintivo puede enviarse con la petición de autenticación o con la respuesta final.

Tres ejemplos de funciones (F) de transformación utilizadas en mecanismos de puesta a prueba son:

a) *Función unidireccional* – La puesta a prueba y la AI de declaración son transformadas según una función unidireccional;

b) *Algoritmo asimétrico* – Cuando la AI de declaración es una clave privada, la puesta a prueba se firma según esa clave privada;

c) *Algoritmo simétrico* – Cuando la AI de declaración es una clave secreta, la puesta a prueba se cifra según esa clave secreta.

Como caso especial de un mecanismo de puesta a prueba, la puesta a prueba generada puede depender de la identidad recibida en la petición de autenticación. Este mecanismo se conoce como mecanismo de puesta a prueba dedicado. En este caso, el identificador distintivo es obligatorio con la petición de autenticación. Además, el ejemplo de algoritmo simétrico difiere en que la puesta a prueba es cifrada por la entidad desafiada. Además, una cuarta función de transformación posible es:

d) *Función no criptográfica* – Un ejemplo es la utilización de una tabla de pares puesta a prueba-respuesta; la entidad que emite la puesta a prueba solicita una respuesta determinada. Otro ejemplo es un esquema biométrico, como lo es un sistema de repetición de la voz.

Esta subclase es aplicable a la autenticación del origen de datos y a la autenticación de entidad.

El servicio generar produce una petición de autenticación (que, en el caso de puesta a prueba dedicada, debe ir acompañada de un identificador distintivo). Al recibirse la petición de autenticación, el servicio verificar genera una puesta a prueba única como AI de intercambio.

Seguidamente, el servicio generar produce AI de intercambio como una transformación de los datos de entrada como se muestra en la Figura 12.

En el caso de una función unidireccional, el servicio verificar repite la transformación utilizando AI de verificación en lugar de AI de declaración y la confronta con la AI de intercambio recibida. A fin de repetir esta función, el verificador debe tener disponible el identificador distintivo y los datos a los que se aplica el servicio. En el caso de otras transformaciones, el servicio verificar repite la transformación o aplica una función inversa y comprueba el contenido utilizando la AI de verificación.

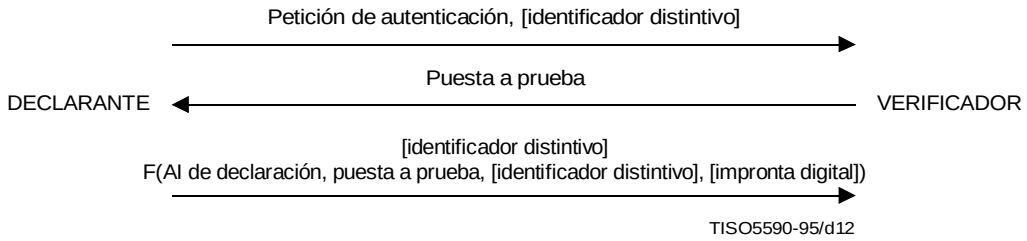


Figura 12 – Subclase 4b: Mecanismo de puesta a prueba

8.1.5.3 Subclase 4c – Mecanismos de puesta a prueba cifrada dedicados

Los mecanismos de puesta a prueba cifrada dedicados también exigen una transferencia tridireccional de información:

- envío de una petición de autenticación y un identificador distintivo;
- emisión de una puesta a prueba y AI de verificación, posiblemente combinados con el identificador distintivo, transformados según alguna función (F) adecuada; y
- envío de una respuesta constituida por la información de puesta a prueba.

Dos ejemplos de mecanismos de puesta a prueba cifrada dedicados son:

a) *Algoritmo asimétrico* – Cuando la AI de declaración es una clave privada, la puesta a prueba se cifra según la clave pública correspondiente;

b) *Algoritmo simétrico* – Cuando la AI de declaración es una clave secreta, la puesta a prueba se cifra según esa clave secreta. El desafío es cifrado por la entidad que hace la puesta a prueba.

Este tipo de mecanismo es aplicable a la autenticación de entidad, pero no a la autenticación del origen de datos.

El servicio generar produce una petición de autenticación. Al recibirse la petición de autenticación y un identificador distintivo, el servicio verificar genera una puesta a prueba única. La función de transformación actúa entonces sobre ésta para producir AI de intercambio, como se muestra en la Figura 13.

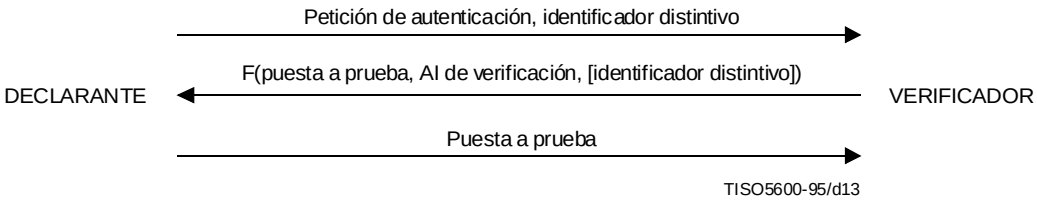


Figura 13 – Subclase 4c: Mecanismo de puesta a prueba cifrada dedicado

El servicio generar efectúa entonces la transformación inversa utilizando AI de declaración en lugar de AI de verificación para obtener la puesta a prueba que es retornada para ser utilizada como AI de intercambio. Obsérvese que sólo son de interés para este esquema las transformaciones de cifrado.

Por último, el servicio verificar confronta la puesta a prueba con la generada anteriormente.

8.1.5.4 Subclase 4d – Mecanismos de respuesta computados

Este tipo de mecanismo también exige una transferencia tridimensional de información:

- envío de una petición de autenticación con diversos valores para seleccionar e información de identidad;
- emisión de una puesta a prueba que indique qué valores fueron seleccionados por el verificador; y
- envío de una respuesta compuesta por el número único, la puesta a prueba, o los valores seleccionados para computar la respuesta, y la AI de declaración, transformada según alguna función apropiada.

Un ejemplo de este mecanismo es una técnica de conocimiento nulo, en la que el verificador selecciona uno de entre un conjunto de «problemas» que el declarante debe resolver sin revelar exactamente cómo.

Los intercambios pueden repetirse para dar un nivel más alto de seguridad de la identidad. Esto protege contra los ataques de suplantación (o impostura) de un intruso que puede computar la respuesta correcta para algunos (no todos) de los valores que un verificador podría seleccionar. Si hay sólo un intercambio, el verificador podría, al azar, seleccionar un valor para el cual el intruso conozca la respuesta correcta. Aumentando el número de intercambios disminuye la probabilidad de éxito de dicho ataque.

El servicio generar genera primeramente un número único y un grupo de valores para seleccionar, y después los coloca en la AI de intercambio como muestra la Figura 14.

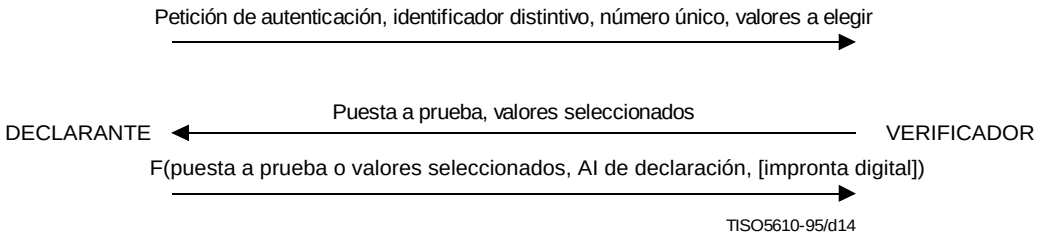


Figura 14 – Subclase 4d: Mecanismo de respuesta computado

El servicio verificar selecciona entonces valores de ese grupo y genera una puesta a prueba para formar la segunda AI de intercambio.

El servicio generar efectúa una transformación sobre la puesta a prueba o los valores seleccionados utilizando AI de declaración.

Por último, el servicio verificar efectúa una transformación inversa utilizando la AI de verificación y comprueba los valores recibidos.

8.2 Iniciación de transferencia

En 8.1 se describen los intercambios siendo el declarante quien inicia el intercambio mediante una *petición de autenticación*. Sin embargo, en el caso de autenticación de entidad, las mismas subclases de mecanismos podrían exigir que el verificador iniciara el intercambio mediante una *invitación de autenticación*. En este caso, el número de transferencias será diferente. El Cuadro 1 de 8.5 da el número de transferencias en cada uno de estos casos.

8.3 Utilización de certificados de autenticación

Los mecanismos de autenticación pueden clasificarse según el medio utilizado para adquirir la AI de verificación. Posibles medios son:

- certificados de autenticación en línea;
- certificados de autenticación fuera de línea; y
- AI de verificación proporcionada por adelantado, por ejemplo, utilizando canales seguros.

Un certificado de autenticación puede utilizarse para proporcionar una prueba de autenticación aplicando el principio descrito en 5.3, d). El certificado de autenticación ofrece la prueba de que un tercero de confianza ha asociado un identificador distintivo con AI de verificación específica.

8.4 Autenticación mutua

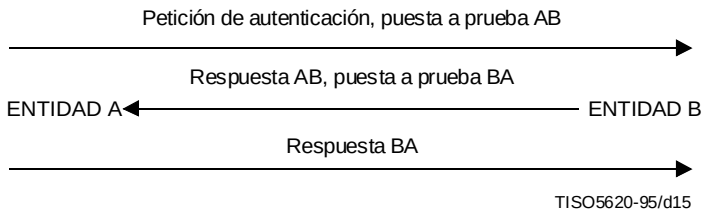
En el caso de las subclases de mecanismos que exigen un intercambio unidireccional (es decir, en las subclases 1, 2, 3 y 4a) puede utilizarse un intercambio de la misma forma en los dos sentidos para la autenticación mutua.

En el caso de la subclase 4b puede usarse el mismo tipo de mecanismo en ambos sentidos. La primera prueba puede enviarse junto con la petición de autenticación, y la transformación de la primera puesta a prueba puede enviarse junto con la segunda puesta a prueba (véase la Figura 15). Esto requiere el mismo número de intercambios que en la autenticación unilateral.

Análogamente, en el caso de la subclase 4c, la transformación de la primera puesta a prueba puede enviarse junto con la petición de autenticación, y la transformación de la segunda puesta a prueba puede enviarse junto con la primera.

La subclase 4b puede utilizarse junto con un mecanismo 4c. Las dos se colocan dentro de los datos transformados. En el caso de cifrado simétrico, las AI de declaración y de verificación en cada extremo son idénticas, y la transformación sólo se efectúa una vez. En el caso de cifrado asimétrico, las dos transformaciones se efectúan en cada extremo.

En el caso de la subclase 4d se necesitan tres o más transferencias para autenticación unilateral. Según el nivel de confianza solicitado para la autenticación en el sentido opuesto, serán necesarios cero, uno, o más intercambios adicionales.



ENTIDAD A Iniciador de la autenticación
ENTIDAD B Respondedor de la autenticación

NOTA – Para detalles de las respuestas y la transferencia de identificadores distintivos, véase la descripción de las subclases y las Figuras.

Figura 15 – Autenticación mutua mediante mecanismos de puesta a prueba

8.5 Sumario de características de las clases

El Cuadro 1 sumariza las vulnerabilidades y las características de las diferentes clases y subclases. Las características se describen en la cláusula 7.

Cuadro 1 – Vulnerabilidades y características de los mecanismos

Subclase	0	1	2	3	4a	4b	4c	4d
Vulnerabilidades								
Revelación	Sí	No	No	No	No	No	No	No
Reproducción en verificadores diferentes	Sí	Sí	No	Sí	No	No	No	No
Reproducción en el mismo verificador	Sí	Sí	Sí	No	No	No	No	No
Intruso inició ataque de reproducción	No	No	No	No	No	No	No	No
Intruso respondiendo al ataque de reproducción	Sí	No	No	No	No	No	No	No
Características								
Simetría/asimetría	Sim	Cualq	Cualq	Cualq	Cualq	Cualq	Cualq	Asim
Criptográfico (Sí)/ no criptográfico (No)	No	Cualq	Cualq	Cualq	Cualq	Cualq	Sí	Sí
Número de transferencias – iniciador declarante – iniciador verificador	 1 2	 1 2	 1 2	 1 2	 1 2	 3 2	 3 4	 3 4
Soporte de la autenticación del origen de datos	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí

8.6 Clasificación según la configuración

Cuando las entidades desean autenticar, pueden tener que hacer intervenir uno o más terceros de confianza. La naturaleza de la confianza entre cada entidad y cualquier tercero de confianza tiene que ser definida. De los modelos en que intervienen terceros de confianza, el más simple es aquél en que interviene un solo tercero. En otros modelos hay un conjunto de terceros de confianza, cada uno de los cuales confía en todos los demás, mientras que el modelo más general exige un conjunto de terceros de confianza que confían entre sí.

8.6.1 Principios de modelación cuando intervienen sólo terceros de confianza

En algunos casos, el verificador sólo puede estar convencido de la identidad del principal si múltiples terceros de confianza le garantizan esta identidad.

Cuando intervienen tres o más terceros de confianza, es necesario protegerse contra la corrupción de uno o más terceros de confianza. Con algunas políticas de seguridad puede aplicarse una regla de mayoría.

Se describe aquí el caso más simple, que es cuando interviene un solo tercero de confianza.

Las relaciones entre el declarante, el verificador y el único tercero de confianza pueden modelarse en términos de:

- fases, como las indicadas en 5.4 (en particular, las fases de distribución, adquisición, transferencia y verificación); y
- conocimiento de información inicial.

8.6.1.1 Modelo de fase

Las fases se relacionan con las diversas entidades de la manera siguiente:

- la fase de distribución es aplicable entre el declarante o el verificador y el tercero de confianza;
- la fase de adquisición es aplicable entre el declarante y el tercero de confianza o entre el verificador y el tercero de confianza;
- la fase de transferencia es aplicable entre cualquier pareja formada por el declarante, el verificador o el tercero de confianza;
- la fase de verificación es aplicable entre el verificador y el tercero de confianza.

Las fases de adquisición, transferencia, y verificación pueden utilizar un mecanismo de autenticación de una clase identificada en 8.1.

La fase de distribución puede ser en línea o fuera de línea. Cuando es fuera de línea, tendrá lugar por lo general antes del intercambio de autenticación. En estos casos no se garantiza que la AI de declaración sea todavía válida (es decir, no haya sido revocada).

Puede identificarse un número de esquemas de autenticación diferentes, que se ilustran en la Figura 16. En esta figura, la entidad A corresponde al declarante y la entidad B corresponde al verificador. Esta figura es puramente ilustrativa y no es necesariamente exhaustiva.

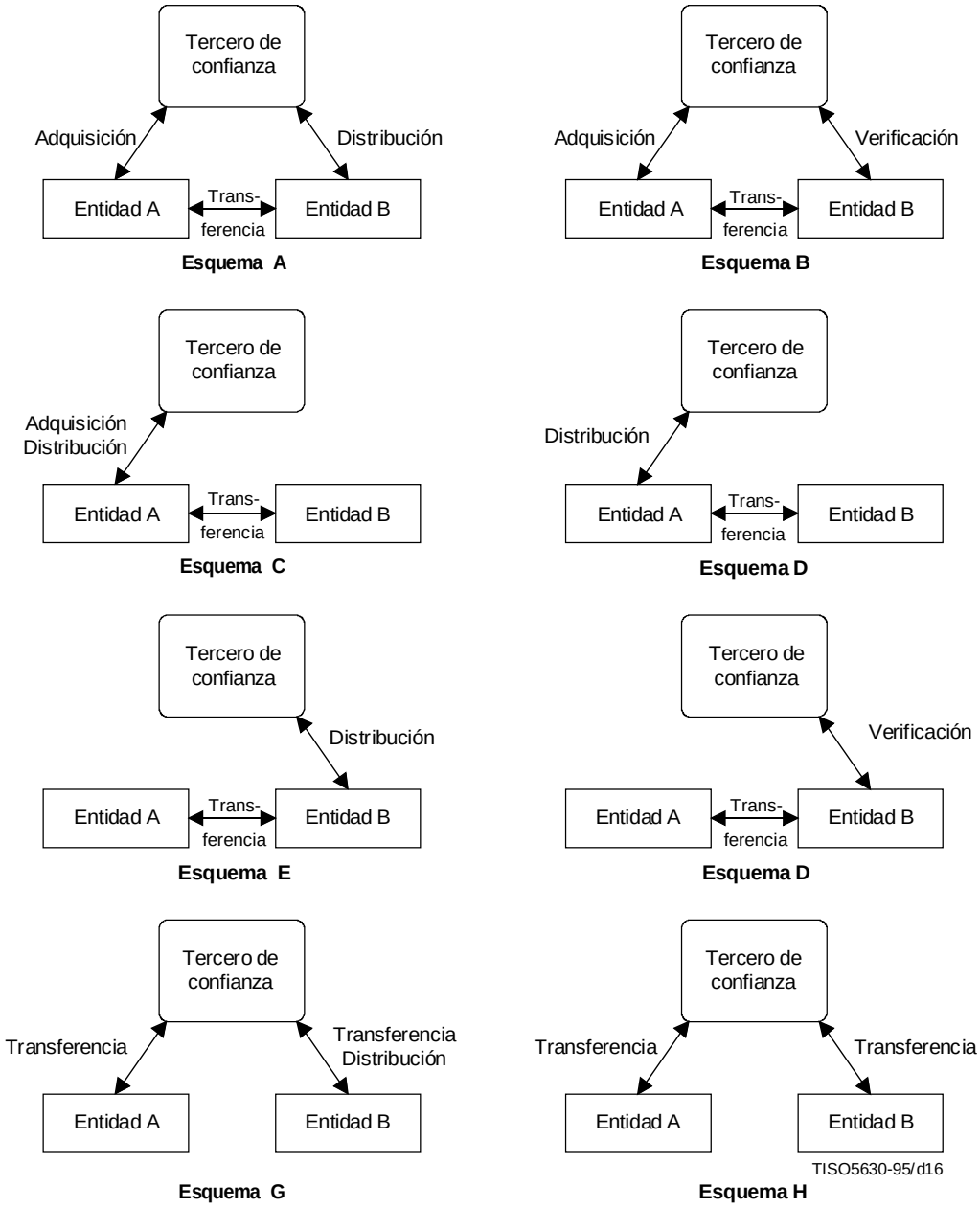


Figura 16 – Esquema de autenticación

En el esquema A, la entidad A obtiene su AI de declaración del tercero de confianza tras un intercambio de autenticación con éste, y la entidad B obtiene la AI de verificación del tercero de confianza. La entidad B efectúa la verificación localmente.

En el esquema B, la entidad A obtiene su AI de declaración del tercero de confianza tras un intercambio de autenticación con éste, y la entidad B presenta la AI de intercambio recibida de la entidad A al tercero de confianza para verificación.

En el esquema C, la entidad A obtiene su AI de declaración del tercero de confianza tras un intercambio de autenticación con éste, así como la AI de verificación que la entidad B necesita para efectuar la verificación localmente.

En el esquema D, la entidad A obtiene la AI de verificación que la entidad B necesita para efectuar la verificación localmente, y genera localmente la AI de intercambio. La AI de intercambio y la AI de verificación son presentadas juntas a la entidad B.

En el esquema E, la entidad A genera localmente su AI de intercambio y la presenta a la entidad B, tras lo cual la entidad B obtiene del tercero de confianza la AI de verificación que necesita para efectuar la verificación localmente.

En el esquema F, la entidad A genera localmente su AI de intercambio y la presenta a la entidad B, tras lo cual la entidad B presenta la AI de intercambio recibida de la entidad A al tercero de confianza para verificación.

En el esquema G, que es una relación de confianza en línea, la entidad A genera localmente su AI de intercambio y la presenta al tercero de confianza, tras lo cual el tercero de confianza envía a la entidad B un certificado de autenticación con la AI de verificación necesaria para efectuar la verificación localmente.

En el esquema H, que es otro caso de relación de confianza en línea, la entidad A genera localmente su AI de intercambio y la presenta al tercero de confianza, tras lo cual el tercero de confianza notifica a la entidad B que la identidad de la entidad A ha sido verificada.

8.6.1.2 Modelación utilizando conocimiento de información inicial

El declarante (entidad A) y el verificador (entidad B) tienen que utilizar alguna información inicial antes de que pueda tener lugar un intercambio. Si interviene un tercero de confianza, ello significa que el declarante no conoce directamente una clave pública o una clave secreta utilizable por el verificador. Pueden considerarse diferentes clases de conocimiento inicial, las cuales se describen a continuación.

8.6.1.2.1 Información inicial compartida entre el declarante y el tercero de confianza

Pueden darse diversos casos:

a) clave secreta compartida entre el declarante y el tercero de confianza, conocida por el declarante y por el tercero de confianza (técnicas de clave secreta);

b) clave privada del declarante conocida solamente por el declarante (entidad A); clave pública del declarante conocida por el tercero de confianza (técnicas asimétricas);

c) clave privada del declarante conocida por el declarante y por el tercero de confianza (técnicas de conocimiento nulo).

8.6.1.2.2 Información inicial compartida entre el verificador y el tercero de confianza

Pueden darse diversos casos:

a) clave secreta compartida entre el verificador (entidad B) y el tercero de confianza conocida por el verificador y por el tercero de confianza (técnicas de clave secreta);

b) clave pública del tercero de confianza, conocida por el verificador (entidad B) (técnicas asimétricas y de conocimiento nulo).

8.6.2 Relaciones entre terceros de confianza que intervienen en una autenticación

8.6.2.1 Tercero de confianza en línea

Es posible que se necesiten terceros de confianza en línea para que pueda tener lugar una autenticación. Terceros de confianza en línea del mismo dominio de seguridad pueden estar en posesión de la AI de declaración y/o la AI de verificación de las entidades que hayan sido previamente registradas en ese dominio.

Se requieren protocolos y/o procedimientos para asegurar que, dentro de un dominio de seguridad dado, no puedan registrarse principales diferentes con el mismo nombre.

La disponibilidad de terceros de confianza en línea es una cuestión importante ya que, en otro caso, los intercambios de autenticación a través de terceras entidades en línea serían objeto de denegaciones de servicio. La replicación de la información de autenticación en un número de terceras entidades diferentes puede minimizar este problema. Se necesitan

también protocolos para replicar esa información de autenticación. Cuando hay que intercambiar AI de verificación, se necesita un servicio de integridad, y en algunos casos, un servicio de confidencialidad, entre los terceros de confianza de la autenticación. Cuando hay que intercambiar AI de declaración, se necesita un servicio de integridad y un servicio de confidencialidad entre los terceros de confianza.

Además, puede ser necesario considerar el intercambio de los caminos de auditoría mantenidos por los diferentes terceros de confianza de la autenticación en línea del dominio de seguridad. Se requieren protocolos para enviar y recibir caminos de auditoría.

8.6.2.2 Terceros de confianza fuera de línea

Los terceros de confianza fuera de línea suelen llamarse autoridades de certificación, ya que pueden emitir certificados de autenticación fuera de línea. No se necesita una protección específica para proteger un certificado de autenticación fuera de línea, ya que este tipo de certificado está protegido por su propia naturaleza. La disponibilidad de terceros de confianza fuera de línea es una cuestión importante ya que, de no estar disponibles, los intercambios de autenticación mediante certificados de autenticación fuera de línea serían objeto de denegaciones de servicio. La replicación de esta información en un número de depositarios (por ejemplo, el Directorio) diferentes puede minimizar este problema.

9 Interacciones con otros servicios/mecanismos de seguridad

9.1 Control de acceso

Es posible que los usuarios deban ser autenticados antes de que se les permita obtener información de control de acceso que les permita acceder a recursos que están sometidos a una política de control de acceso. En consecuencia, el servicio de autenticación puede pasar los resultados de la autenticación al servicio de control de acceso para que este servicio los utilice.

La revocación de información de autenticación puede implicar la revocación de acceso existente.

9.2 Integridad de los datos

El servicio de autenticación puede utilizarse en conjunción con el de integridad de datos para garantizar la continuidad de la autenticación y corroborar la fuente de los datos.

Pueden utilizarse algunos mecanismos de autenticación para distribuir, implícita o explícitamente, un material clave que pueda utilizarse para un servicio de integridad. Cuando este material clave está implícitamente definido, la forma de derivarlo de los datos transferidos debe ser conocida o especificada durante el intercambio de autenticación. Cuando este material clave está explícitamente definido, deben transferirse datos adicionales en ambos sentidos durante el intercambio de autenticación.

9.3 Confidencialidad de los datos

Pueden utilizarse algunos mecanismos de autenticación para distribuir, implícita o explícitamente, un material clave que pueda utilizarse para un servicio de confidencialidad. Cuando este material clave está implícitamente definido, la forma de derivarlo de los datos transferidos debe ser conocida o especificada durante el intercambio de autenticación. Cuando este material clave está explícitamente definido, deben transferirse datos adicionales en ambos sentidos durante el intercambio de autenticación.

9.4 No repudio

Pueden utilizarse algunos mecanismos de autenticación para distribuir, implícita o explícitamente, material clave que pueda utilizarse para un servicio de no repudio. Cuando este material clave está implícitamente definido, la forma de derivarlo de los datos transferidos debe ser conocida o especificada durante el intercambio de autenticación. Cuando este material clave está explícitamente definido, deben transferirse datos adicionales en ambos sentidos durante el intercambio de autenticación.

9.5 Auditoría

La información relativa a la autenticación que puede utilizarse para auditoría podría ser:

a) los resultados de la autenticación (esto es, identificación garantizada);

b) información relacionada con la revocación de información de autenticación;

c) información sobre garantía de continuidad de la autenticación;

d) otra información relativa al proceso de autenticación.

Anexo A

Autenticación de usuarios humanos

(Este anexo no es parte integrante de esta Recomendación | Norma Internacional)

A.1 Generalidades

La identificación correcta de usuarios humanos puede ser esencial en la seguridad de los sistemas abiertos cuando el sistema abierto soporta las acciones de personas. El diálogo entre usuarios humanos y sistemas de computador puede aumentar las posibilidades de intrusión por suplantación (o impostura). Los métodos de autenticación de usuarios humanos deberán ser aceptables por éstos, además de económicos y seguros. Métodos inconvenientes incitan a veces a los usuarios humanos a encontrar maneras de evitar los procedimientos, con lo cual aumenta el potencial de intrusión.

La autenticación de usuarios humanos se basa en principios de autenticación pertenecientes a una o más de las siguientes categorías:

a) algo que se conoce;

b) algo que se posee;

c) características particulares del usuario humano;

d) aceptación de que un tercero de confianza identificado ha establecido la identidad del usuario humano;

e) contexto (por ejemplo, dirección del origen de la petición).

En general, el proceso de autenticación de usuario humano exige la confrontación de las credenciales presentadas por el usuario con información de autenticación obtenida en la fase de instalación.

A.1.1 Autenticación mediante algo que se conoce

En esta categoría, la información de autenticación más comúnmente utilizada es una contraseña. Al acceder a un sistema, el usuario humano presenta la contraseña y el sistema autenticante la compara con el valor correspondiente en una lista de contraseñas, con el fin de corroborar la identidad del usuario humano. Las contraseñas deben ser difíciles de adivinar y manejarse cuidadosamente. Si así no fuera, están expuestas a ser reveladas involuntariamente.

A.1.2 Autenticación mediante algo que se posee

En esta categoría se utiliza un testigo físico, tal como:

a) una tarjeta de banda magnética; o

b) una tarjeta de circuito integrado (tarjeta IC).

Con las tarjetas de banda magnética, cuando se accede a un sistema, el usuario humano presenta el testigo físico, y el sistema autenticante lee la información de autenticación del testigo físico y para compararla con información de autenticación almacenada, a fin de corroborar la identidad del usuario humano.

Un punto vulnerable de las tarjetas de banda magnética es que son fáciles de copiar. Otro punto débil es que si la tarjeta de banda magnética está indebidamente en posesión de otra persona, el método de autenticación fracasa.

Con las tarjetas IC, cuando se accede a un sistema, el usuario humano presenta el dispositivo físico y el sistema autenticante utiliza información almacenada en el testigo físico para producir la AI de intercambio, a fin de corroborar la identidad del usuario humano. Una ventaja de las tarjetas IC es que no pueden ser copiadas fácilmente.

Pueden considerarse dos variantes, según que la tarjeta de circuito integrado pueda o no autenticar a su titular:

– cuando la tarjeta IC puede identificar a su titular, hay un doble esquema de autenticación en el cual el usuario es identificado por el verificador; esto es equivalente, por transitividad, a la autenticación directa del usuario;

– cuando la tarjeta IC no puede identificar a su titular, y el objeto se halla indebidamente en posesión de otra persona, el método de autenticación fracasa.

A.1.3 Generador de contraseña dependiente del tiempo

Un tipo de mecanismo de autenticación de usuario humano es un dispositivo de mano que funciona como un generador de contraseña dependiente del tiempo. Se genera AI de intercambio utilizando una combinación de:

– información secreta almacenada en el propio dispositivo;

– tiempo;

– un número de identidad personal (PIN) marcado directamente por el usuario en el teclado del dispositivo.

La AI de intercambio así generada se visualiza en el dispositivo. Seguidamente, el usuario la envía (en forma de texto claro) al sistema verificante. Es posible que este sistema tenga que estar sincronizado con la tarjeta. Cuando se emplea este mecanismo de autenticación de usuarios humanos, es necesario que la persona que trate de autenticarse por este medio:

a) posea el dispositivo adecuado; y

b) conozca el PIN.

A.1.4 Autenticación utilizando características particulares de cada usuario humano

Las contraseñas pueden llegar a conocerse indebidamente si no se tratan con cuidado, y los testigos físicos pueden ser robados, o, en el caso de las tarjetas de banda magnética, ser copiadas sin autorización. Hay una clase de método de autenticación de usuarios humanos que no presenta estos inconvenientes, y que se basa en las características particulares de cada usuario tales como:

– firma manuscrita;

– huellas dactilares;

– patrón vocal;

– patrón retinal; o

– características dinámicas de teclado.

Dos clases importantes del método de la firma manuscrita son los sistemas estáticos y dinámicos. En los sistemas dinámicos puede disponerse de información de presión, tiempo y dirección del movimiento.

El análisis de características dinámicas de teclado proporciona una forma continua de autenticación.

En la fase de enrolamiento, un usuario humano registra su identidad en el sistema de enrolamiento. El usuario ejecuta las operaciones del procedimiento prescrito, por ejemplo, estampa su firma en un lugar especificado, oprime con el dedo una zona determinada, o pronuncia determinadas palabras. El procedimiento se repite cuantas veces sea necesario hasta que se obtenga una información de referencia adecuada. El sistema analiza el valor característico de la acción del usuario humano y lo registra como un perfil.

En la fase de transferencia/verificación, el usuario humano presenta su identidad y vuelve a ejecutar las operaciones del procedimiento prescrito. El sistema de verificación compara el patrón obtenido del usuario con el perfil registrado para ese usuario.

A.2 Procesos que actúan en nombre de un usuario humano

En algunas circunstancias un usuario puede desear actuar sin estar presente. En tales casos el usuario tendrá, dentro del sistema, una representación que puede tener un tiempo de vida independiente de la presencia efectiva del usuario.

Dado que la representación actúa como si fuera el usuario, sus acciones pueden ser continuadas sin necesidad de la intervención directa del usuario. Por ejemplo, un usuario humano puede poner en marcha el procedimiento (dícese, efectuar un «log-on») y usar entonces diferentes computadores sin tener que efectuar ulteriores operaciones.

En lugar de soportar representaciones de duraciones independientes, pueden también utilizarse representaciones con mecanismos adicionales que hagan la duración de las mismas dependiente de la presencia del usuario.

Anexo B

Autenticación en el modelo OSI

(Este anexo no es parte integrante de esta Recomendación | Norma Internacional)

Las relaciones de los servicios de seguridad con el modelo de referencia OSI se definen en ISO 7498-2. En este anexo se recapitula todo lo que ofrece interés para la autenticación.

Se consideran dos servicios de seguridad:

- autenticación de entidad par;
- autenticación del origen de datos.

B.1 Autenticación de entidad par

La autenticación de entidad par puede utilizarse en el momento del establecimiento de una conexión o, a veces, durante la fase de transferencia de datos de una conexión, para confirmar las identidades de una o más entidades conectadas a una o más de las otras entidades. Este servicio está disponible tanto en los protocolos orientados a conexión (brevemente, protocolos con conexión), como en los protocolos sin conexión. En los protocolos con conexión son posibles la autenticación unidireccional y la autenticación mutua de entidades pares.

B.2 Autenticación del origen de datos

La autenticación del origen de datos proporciona la corroboración del origen de una unidad de datos. Este servicio no da protección contra la duplicación o modificación de las unidades de datos.

B.3 Utilización de la autenticación dentro de las capas OSI

La autenticación de entidad par y la autenticación del origen de datos sólo son importantes para las siguientes capas OSI:

- capa de red (capa 3);
- capa de transporte (capa 4);
- capa de aplicación (capa 7).

B.3.1 Utilización de la autenticación en la capa de red

La autenticación de entidad par, cuando se utiliza en la capa de red, permite la confirmación de las identidades de red. Este servicio permite la identificación de nodos de red, nodos de subred, o relevadores.

La autenticación del origen de datos, cuando se utiliza en la capa de red, permite la confirmación de las identidades de la fuente de una unidad de datos. El origen puede ser un nodo de red, un nodo de subred, o un relevador.

Los mecanismos utilizados por la capa de red se encuentran en esa capa.

B.3.2 Utilización de la autenticación en la capa de transporte

La autenticación de entidad par, cuando se utiliza en la capa de transporte, permite la confirmación de las entidades de transporte. Este servicio permite la autenticación de sistemas de extremo. Aplicaciones diferentes soportadas por los mismos sistemas de extremo no pueden ser autenticadas.

La autenticación del origen de datos, cuando se utiliza en la capa de transporte, permite la confirmación de las identidades de la fuente de una unidad de datos. La fuente es un sistema de extremo.

Los mecanismos utilizados por la capa de transporte se encuentran dentro de esa capa.

B.3.3 Utilización de autenticación en la capa de aplicación

La autenticación de entidad par, cuando se utiliza en la capa de aplicación, permite la confirmación de las entidades de aplicación soportadas por sistemas de extremo. Este servicio permite la autenticación de entidades de aplicación o de procesos de aplicación. Entidades de aplicaciones diferentes o procesos de aplicación diferentes soportados por el mismo sistema de extremo no pueden ser autenticados.

La autenticación del origen de datos, cuando se utiliza en la capa de aplicación, permite la confirmación de las identidades de la fuente de una unidad de datos. La fuente puede ser una entidad de aplicación o un proceso de aplicación.

Los mecanismos utilizados por la capa de aplicación pueden estar en la capa de aplicación o en la capa de presentación. La autenticación, cuando se invoca en la capa de aplicación, puede también hacer uso de los servicios de autenticación proporcionados por la capa de red o la capa de transporte.

Anexo C

Protección contra la reproducción mediante números únicos o puestas a prueba

(Este anexo no es parte integrante de esta Recomendación | Norma Internacional)

C.1 Números únicos

Los números únicos son generados por el declarante. Un mismo número único no deberá ser nunca aceptado dos veces por el mismo verificador. Esto puede conseguirse de varias maneras. Algunas técnicas que serían válidas en teoría podrían no ser aplicables en la práctica. Un ejemplo que refleja exactamente el uso de esta técnica sería llevar la cuenta de todos los números únicos recibidos que se han utilizado con éxito durante un intercambio de autenticación. Esto conduciría al empleo de una cantidad de memoria que aumentaría con el número de autenticaciones correctas logradas. Esto podría no ser aceptable por razones de costo y/o de rendimiento.

Una manera de reducir la cantidad de memoria requerida en el lado verificador consiste en llevar la cuenta de todos los números únicos que han sido utilizados con éxito, pero sólo durante cierto tiempo. Esto conduce a la introducción de un sello de tiempo como parte del número único, de modo que el verificador sólo tenga que recordar los números únicos «recientes». En la práctica, una ventana de tiempo de varios minutos puede ser suficiente tanto para limitar la cantidad de memoria necesaria, como para minimizar el problema de la sincronización entre las dos diferentes referencias de tiempo utilizadas por el principal y por el verificador.

Para evitar denegaciones de servicio, conviene evitar colisiones involuntarias entre números únicos generados por dos principales diferentes. Para ello, la gama del número único debe ser lo suficientemente grande. La gama del número único está relacionada con el máximo número de autenticaciones por periodo de tiempo (por ejemplo, por segundo) que debe alcanzarse en el verificador en el que se intente la autenticación. Cuando la referencia de tiempo utilizada por el principal no proporcione directamente ese gran número, podrá añadirse un número aleatorio al sello de tiempo para agrandar la gama del número único.

C.2 Puestas a prueba

Las puestas a prueba son generadas por el verificador. Una misma puesta a prueba no deberá ser emitida dos veces por el mismo verificador. Esto puede conseguirse de varias formas.

Algunas técnicas que serían válidas en teoría podrían no ser aplicables en la práctica. Un ejemplo que refleja exactamente el uso de esta técnica sería llevar la cuenta de todas las puestas a prueba emitidas. Esto conduciría al empleo de una cantidad de memoria que aumentaría con el número de autenticaciones correctas logradas usando estas puestas a prueba. Esto podría no ser aceptable por razones de costo y/o de rendimiento.

Hay varias formas de reducir la cantidad de memoria requerida en el lado verificador:

- generar valores secuenciales para los desafíos y llevar la cuenta solamente del último valor secuencial;
- generar números aleatorios para las puestas a prueba. Aunque esto viola la regla de que una misma puesta a prueba no deberá utilizarse dos veces, la probabilidad de que se dé este caso puede hacerse lo suficientemente baja para que sea aceptable, tomando los números aleatorios de una gama suficientemente grande;
- utilizar un sello de tiempo para las puestas a prueba;
- utilizar una combinación de sello de tiempo y número aleatorio.

Anexo D

Protección contra algunas formas de ataque a la autenticación

(Este anexo no es parte integrante de esta Recomendación | Norma Internacional)

D.1 Ataques de escucha y reproducción

Hay que considerar dos casos de reproducción. Son éstos la reproducción de alguna AI de intercambio:

- en el mismo verificador; o
- en otro verificador.

Este último caso es posible cuando varios verificadores conocen la AI de verificación de un principal. Cuando puede conseguirse una reproducción, se produce un caso específico de suplantación (o impostura).

Ambos casos de reproducción pueden combatirse mediante puestas a prueba. Las puestas a prueba son generadas por el verificador. El mismo verificador no debe nunca emitir dos veces la misma puesta a prueba. Esto puede conseguirse de varias maneras (véase el Anexo C).

D.2 Reproducción en el mismo verificador

La reproducción en el mismo verificador puede combatirse mediante números únicos o puestas a prueba.

Los números únicos son generados por el declarante. El mismo verificador no debe nunca aceptar dos veces el mismo número único. Esto puede conseguirse de varias maneras (véase el Anexo C).

D.3 Reproducción en un verificador diferente

La reproducción en un verificador diferente puede combatirse utilizando puestas a prueba. Otra posibilidad es combatirla utilizando, en la computación en la AI de intercambio, cualquier característica exclusiva del verificador. Dicha característica puede ser el nombre del verificador, su dirección de red o en general cualquier atributo único con respecto a los verificadores que comparten la misma información de autenticación de verificación.

D.4 Ataques de interceptación y retransmisión

D.4.1 Ataques directos

En un cierto tipo de ataque (un ataque directo) el intruso es el iniciador de la autenticación. Este ataque es posible sólo si el declarante y el verificador pueden ambos iniciar la autenticación. Con este ataque, el declarante y el verificador intercambian información de autenticación por mediación de un intruso sin ser conscientes de ello, es decir, el intruso pretende ser un cierto verificador para un declarante y ser este declarante para ese verificador.

Por ejemplo, supongamos que el intruso C desea hacer creer al verificador B que es el declarante A. C comienza una interacción con A y B. C dice a A que es B, pide a A que se autentique a B y también dice a B que es A y que desea autenticarse él mismo.

Durante el proceso de autenticación, A actúa como declarante para con B (en realidad para con C actuando como B), y por tanto suministra información que C puede utilizar para autenticarse a B. B actúa como el verificador, y también suministra la información que se necesita para desempeñar el papel de verificador. Tras la autenticación, el intruso C aparecerá a B como el A autenticado.

Posibles formas de combatir este tipo de ataque exigen protección contra la reproducción en un verificador diferente:

a) la entidad que comienza una interacción es siempre el declarante; o

b) la AI de intercambio proporcionada por el declarante difiere según su papel como iniciador de una petición de autenticación o respondedor a una invitación de autenticación. Esta diferencia permite al verificador detectar la interceptación descrita. Véanse más detalles en el Anexo D.

D.4.2 Ataques oportunistas

Hay un tipo de ataque en el que el intruso se inmiscuye en un intercambio de autenticación, intercepta la información de autenticación y la reenvía asumiendo el papel de declarante.

La forma general de combatir este tipo de ataque exige el uso de un servicio complementario (integridad o confidencialidad). La AI de intercambio se combina con alguna otra información que habilite al declarante y al verificador, siempre que sean las partes legítimas, a derivar una clave. La clave derivada puede entonces utilizarse como clave para un mecanismo de integridad o de confidencialidad de carácter criptográfico.

Otra forma de combatir este tipo de ataque es aplicable cuando la red de comunicaciones no está sujeta a interceptaciones internamente, es decir, siempre entrega datos invariables a la dirección correcta. En esta situación, el ataque puede combatirse integrando las direcciones de red firmadas en el intercambio de autenticación.

D.5 Una forma limitada de protección contra un ataque de intruso

El segundo tipo de ataque descrito en D.4 es posible cuando se utilizan puestas a prueba o cuando se utilizan números únicos. La protección exige la utilización, por el declarante, de un indicador que señale si la respuesta sigue a una invitación de autenticación o a una petición de autenticación. El indicador puede o bien señalar (por ejemplo, cuando está puesto a uno) que la respuesta sigue a una invitación de autenticación o señalar (por ejemplo, cuando está puesto a cero) que la respuesta sigue a una petición de autenticación. Como el indicador es parte de la computación de la respuesta, esto significa que el valor de la respuesta dada por el declarante depende del valor del indicador. En adelante, el indicador se denomina indicador de invitación/petición.

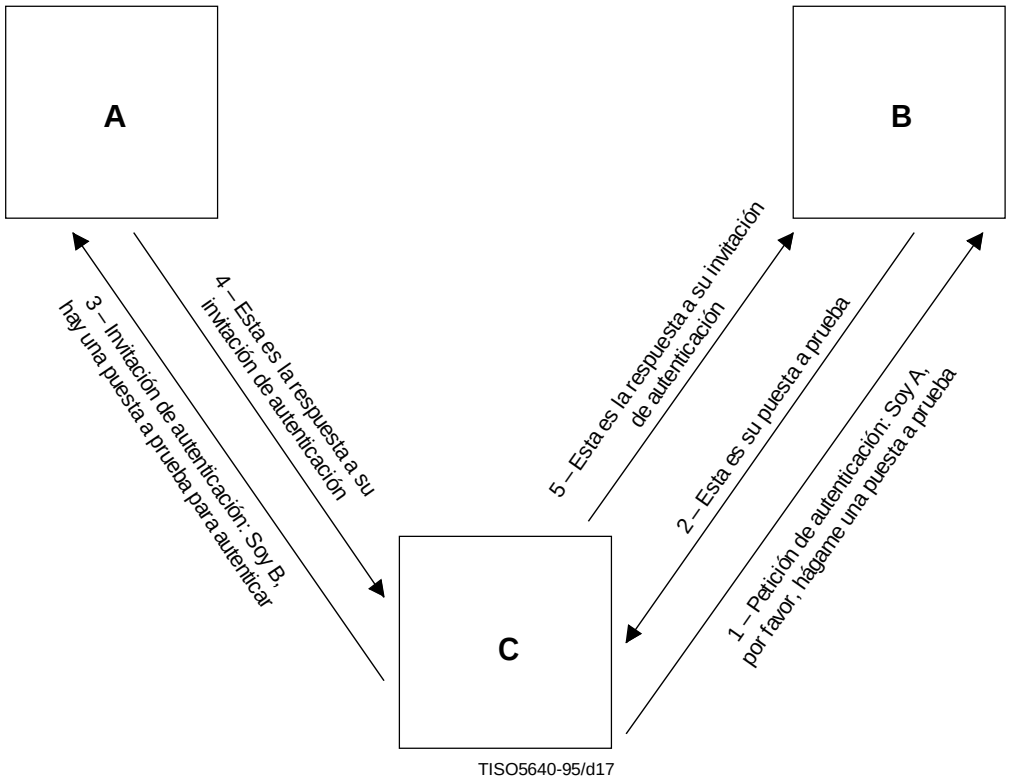
D.6 Protocolo que utiliza protocolos iniciadores de declarante

Cuando se utilizan puestas a prueba, C pretende hacerse pasar por A y envía una petición de autenticación a B (primera transferencia). B envía una puesta a prueba a C (segunda transferencia). C envía una invitación de autenticación a A y reenvía la puesta a prueba recibida de B a A (tercera transferencia). A computa su respuesta utilizando tanto la puesta a prueba recibida de C como el indicador de invitación/petición puesto a «invitación». C reenvía a B la respuesta recibida de A. B comprueba la respuesta. Como ha recibido originalmente de C una petición de autenticación, está esperando un indicador de invitación/petición puesto a «petición». Cuando recibe una respuesta computada con un indicador de invitación/petición puesto a «invitación», rechaza la autenticación (véase la Figura D.1).

Si B soporta tanto peticiones de autenticación como invitaciones de autenticación, debe adoptar una precaución adicional: para cada petición de autenticación emitida por B, B debe recordar a qué declarante se ha dado una determinada puesta a prueba para que C no pueda utilizarla para otro declarante cuando envíe su invitación de autenticación (tercer intercambio).

D.7 Protocolo que utiliza protocolos de iniciadores de declarante

Cuando se utilizan números únicos, C pretende hacerse pasar por B y envía una invitación de autenticación a A (primera transferencia). A computa su respuesta utilizando un número único y el indicador de invitación/petición puesto a «invitación» (segunda transferencia). C reenvía a B la respuesta recibida de A (tercera transferencia). B comprueba la respuesta. Contiene un indicador de invitación/petición puesto a «invitación», pero B no ha emitido ninguna invitación de autenticación, por lo que rechaza la autenticación (véase la Figura D.2).



NOTA – Los ataques directos, que se explican en D.4.1, aun si se combaten con el método a) o b), siguen siendo vulnerables al ataque oportunista.

Figura D.1 – Protección contra un ataque de intruso cuando se emplean puestas a prueba

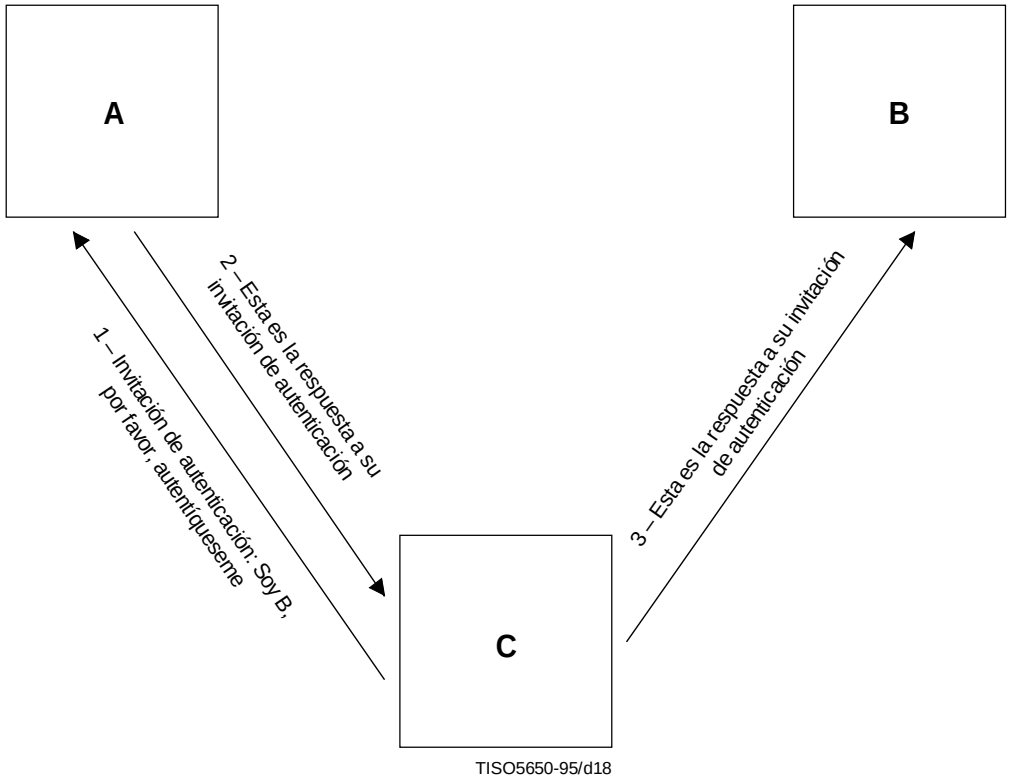


Figura D.2 – Protección contra un ataque de intruso cuando se emplean números únicos

Anexo E

Bibliografía

(Este anexo no es parte integrante de esta Recomendación | Norma Internacional)

ISO/CEI 9798-1:1991, *Information technology – Security techniques – Entity authentication mechanisms – Part 1: General model*.

ISO/CEI 9798-2:1994, *Information technology – Security techniques – Entity authentication – Part 2: Mechanisms using symmetric encipherment algorithms.*

ISO/CEI 9798-3:1993, *Information technology – Security techniques – Entity authentication mechanisms – Part 3: Entity authentication using a public key algorithm.*

ISO/CEI 9798-4:1995, *Information technology – Security techniques – Entity authentication – Part 4: Mechanisms using a cryptographic check function.*

Recomendación UIT-T X.509 (1993) | ISO/CEI 9594-8:1995, *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Marco de autenticación*.

Anexo F

Algunos ejemplos específicos de mecanismos de autenticación

(Este anexo no es parte integrante de esta Recomendación | Norma Internacional)

Este anexo presenta dos ejemplos específicos del empleo de mecanismos de autenticación.

F.1 Ejemplo específico de mecanismo de número único con certificado de autenticación en línea

Este ejemplo ilustra el empleo de un mecanismo de número único que se describe en la clase 3 de 8.1. En este ejemplo, que emplea certificados de autenticación en línea, se incluyen en el certificado de autenticación el identificador distintivo, un método de protección, un parámetro de protección y un periodo de validez. Este ejemplo sólo necesita una transferencia y permite a un certificado de autenticación dado ser utilizado más de una vez.

El método de protección indica la relación entre el parámetro de protección contenido en el certificado y el parámetro de control externo a utilizar para proteger el certificado de autenticación contra su uso no autorizado. El parámetro de control externo puede estar relacionado con el parámetro de protección mediante una relación unidireccional tal como:

- el parámetro de control externo es un valor de validación y el parámetro de protección es el resultado de una función unidireccional aplicada al valor de validación; o
- el parámetro de control externo es una clave privada y el parámetro de protección es la clave pública correspondiente.

Cuando se utiliza un valor de validación como el parámetro de control externo, se envía al verificador como prueba de la posesión del certificado de autenticación. Mientras está en tránsito, debe protegerse la confidencialidad del valor de validación; por ejemplo, es enviado cifrado por el declarante al verificador utilizando una clave de confidencialidad externa asociada con el canal de comunicación o con el extremo receptor del canal de comunicación.

El parámetro de control externo y el número único son transformados y transferidos, junto con el certificado de autenticación. Tres ejemplos de funciones de transformación (F) son:

a) *Función unidireccional* – El número único y el valor de validación se transforman según una función unidireccional. El número único es transmitido de manera que el verificador pueda efectuar la misma transformación;

b) *Algoritmo asimétrico* – Cuando el parámetro de control externo es una clave privada, el número único se firma según esa clave privada;

c) *Algoritmo simétrico* – Cuando el parámetro de control externo es una clave secreta, el número único se cifra o sella según el valor de validación utilizado como clave secreta.

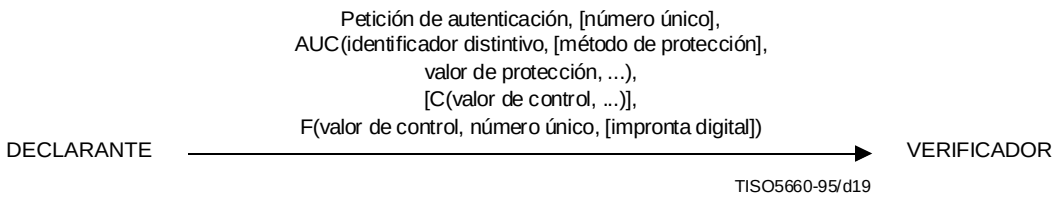
Este ejemplo es aplicable a la autenticación del origen de datos y a la autenticación de entidad. Para la autenticación del origen de datos, los datos, o una impronta digital de los datos, pueden también ser transformados mediante la función F.

El servicio adquirir se utiliza para obtener el certificado de autenticación en línea y un parámetro de control externo. El servicio generar genera entonces un número único y realiza una transformación utilizando lo siguiente como entradas:

- número único;
- parámetro de control externo;
- identificador distintivo (opcional);
- impronta digital (si existe autenticación del origen de datos).

Además, cuando el parámetro de control externo es una clave de validación o una clave de control secreta, el servicio generar envía esta clave cifrada de manera que sólo el verificador destinatario pueda descifrarla, y produce la AI de intercambio como se muestra en la Figura 14.

El servicio verificar comprueba la validez de la AI de intercambio utilizando el valor de protección dentro del certificado de autenticación. Además, cuando se utiliza una clave de validación o una clave de control secreta, el servicio verificar descifra la clave de validación cifrada o la clave de control secreta y verifica que corresponde al valor de protección. También comprueba que el número único no ha sido recibido antes.



NOTAS

1 AUC(...) se utiliza para designar un certificado de autenticación en línea que incluye los parámetros indicados.

2 C(...) se utiliza para designar la aplicación de un servicio de confidencialidad. Es sólo aplicable cuando el parámetro de control es un valor de validación.

Figura F.1 – Mecanismo de número único con certificado de autenticación en línea

F.2 Mecanismo de puesta a prueba con certificado en línea

Este mecanismo utiliza un certificado de autenticación para proporcionar una prueba de autenticación utilizando el principio descrito en 5.3, d) y el mecanismo de puesta a prueba descrito en 8.1.5.2. El certificado de autenticación proporciona la prueba de que un tercero de confianza ha autenticado a su titular con un identificador distintivo específico. El mecanismo proporciona un medio de demostrar que un certificado de autenticación de un determinado identificador distintivo está en posesión del declarante.

En este ejemplo, que emplea certificados de autenticación en línea, se incluyen en el certificado de autenticación el identificador distintivo, un método de protección, un parámetro de protección y un periodo de validez. Este ejemplo permite a un determinado certificado de autenticación ser utilizado más de una vez.

El método de protección indica la relación entre el parámetro de protección contenido en el certificado y el parámetro de control externo a utilizar para proteger el certificado de autenticación contra su uso no autorizado. El parámetro de control externo puede estar relacionado con el parámetro de protección mediante una relación unidireccional tal como:

- el parámetro de control externo es un valor de validación y el parámetro de protección es el resultado de una función unidireccional aplicada al valor de validación;
- el parámetro de control externo es una clave privada y el parámetro de protección es la clave pública correspondiente.

Cuando se utiliza un valor de validación como el parámetro de control externo, se envía al verificador como prueba de la posesión del certificado de autenticación. Mientras está en tránsito, debe protegerse la confidencialidad de la clave; por ejemplo, es enviada cifrada por el declarante al verificador utilizando una clave de confidencialidad externa asociada con el canal de comunicación o con el extremo receptor del canal de comunicación.

El parámetro de control externo y la puesta a prueba, posiblemente combinados con el identificador distintivo, son transformados y transferidos, junto con el certificado de autenticación. Tres ejemplos de funciones de transformación (F) son:

a) *Función unidireccional* – La puesta a prueba y la clave de validación se transforman según una función unidireccional;

b) *Algoritmo asimétrico* – Cuando el parámetro de control externo es una clave privada, la puesta a prueba se firma según esa clave privada;

c) *Algoritmo simétrico* – Cuando el parámetro de control externo es una clave secreta, la puesta a prueba se cifra o sella según el valor de validación utilizado como clave secreta.

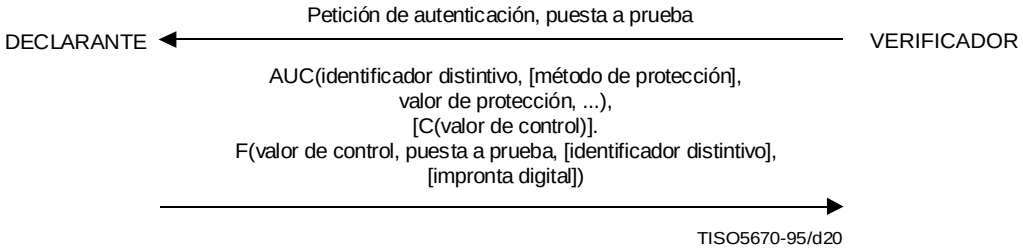
Este ejemplo es aplicable al origen de datos y a la autenticación de entidad.

El servicio adquirir se utiliza para obtener el certificado de autenticación en línea y un parámetro de control externo. El servicio generar produce una petición de autenticación. Al recibir la petición de autenticación, el servicio verificar genera una puesta a prueba AI de intercambio. El servicio generar realiza entonces una transformación utilizando lo siguiente como entradas:

- puesta a prueba;
- parámetro de control externo;
- identificador distintivo (opcional);
- impronta digital (si existe autenticación del origen de datos).

Además, cuando el parámetro de control externo es una clave de validación o una clave de control secreta, el servicio generar envía esta clave cifrada de manera que sólo el verificador destinatario pueda descifrarla, y produce la AI de intercambio como se muestra en la Figura 16.

El servicio verificar comprueba la validez de la AI de intercambio utilizando el valor de protección dentro del certificado de autenticación. Además, cuando se utiliza una clave de validación o una clave de control secreta, el servicio verificar descifra la clave de validación cifrada o la clave de control secreta y verifica que corresponde al valor de protección. También comprueba que la puesta a prueba coincide con la enviada.



NOTAS

1 AUC(...) se utiliza para designar un certificado de autenticación en línea que incluye los parámetros indicados.

2 C(...) se utiliza para designar la aplicación de un servicio de confidencialidad. Es sólo aplicable cuando el parámetro de control es un valor de validación.

Figura F.2 – Mecanismo de puesta a prueba con certificado de autenticación en línea

Anexo G

Compendio de funciones de autenticación

(Este anexo no es parte integrante de esta Recomendación | Norma Internacional)

<table>
<tr><td colspan="2" rowspan="2">Compendio de funciones de seguridad</td><td>Elemento</td><td>Entidad: declarante, verificador, tercero de confianza, principal, gestor</td></tr>
<tr><td></td><td>Objeto info: información de autenticación</td></tr>
<tr><td colspan="2"></td><td colspan="2">Objeto de la entidad: garantizar la identidad declarada de una entidad</td></tr>
<tr><td rowspan="6">ACTIVIDAD</td><td>Entidad</td><td colspan="2">Autoridad de seguridad, principal, gestor</td></tr>
<tr><td>Función</td><td colspan="2"></td></tr>
<tr><td>Actividad relativa a la gestión</td><td colspan="2">– Instalar
– Rehabilitar
– Cambiar AI
– Desinstalar
– Distribuir</td></tr>
<tr><td>Entidad</td><td colspan="2">– declarante
– verificador
– TTP</td></tr>
<tr><td>Función</td><td colspan="2"></td></tr>
<tr><td>Actividad de tipo operacional</td><td colspan="2">– Adquirir
– Generar
– Verificar
– Generar
– Verificar</td></tr>
<tr><td rowspan="3">INFORMACIÓN</td><td>Entrada/salida Elemento de datos gestionado por SDA</td><td colspan="2">Información descriptiva, por ejemplo, contraseña, claves, uso de un protocolo, tabla de puesta a prueba y respuestas, acuse de recibo o rechazo, certificado fuera de línea, información de situación, AI</td></tr>
<tr><td>Tipo de información utilizado en la operación</td><td colspan="2">AI de declaración
AI de intercambio
AI de verificación</td></tr>
<tr><td>Información de control</td><td colspan="2">Validez
Información de estado de autenticación</td></tr>
</table>