UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

UIT-T X.813

(10/96)

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

SERIE X: REDES DE DATOS Y COMUNICACIÓN ENTRE SISTEMAS ABIERTOS

Seguridad

Tecnología de la información – Interconexión de sistemas abiertos – Marcos de seguridad en sistemas abiertos: Marco de no rechazo

Recomendación UIT-T X.813

(Anteriormente «Recomendación del CCITT»)

RECOMENDACIONES DE LA SERIE X DEL UIT-T

REDES DE DATOS Y COMUNICACIÓN ENTRE SISTEMAS ABIERTOS

REDES PÚBLICAS DE DATOS	X.1–X.199
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	X.200–X.299
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 declaraciones 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	X.300–X.399
Generalidades	X.300–X.349
Sistemas de transmisión de datos por satélite	X.350–X.399
SISTEMAS DE TRATAMIENTO DE MENSAJES	X.400–X.499
DIRECTORIO	X.500–X.599
GESTIÓN DE REDES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS Y ASPECTOS DE SISTEMAS	X.600–X.699
Gestión de redes	X.600–X.629
Eficacia	X.630–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
Marco y arquitectura de la gestión de sistemas	X.700–X.709
Servicio y protocolo de comunicación de gestión	X.710–X.719
Estructura de la información de gestión	X.720–X.729
Funciones de gestión	X.730–X.799
SEGURIDAD	**X.800–X.849**
APLICACIONES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.850–X.899
Cometimiento, concurrencia y recuperación	X.850–X.859
Tratamiento de transacciones	X.860–X.879
Operaciones a distancia	X.880–X.899
PROCESAMIENTO DISTRIBUIDO ABIERTO	X.900–X.999

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

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.813 se aprobó el 5 de octubre de 1996. Su texto se publica también, en forma idéntica, como Norma Internacional ISO/CEI 10181-4.

_____

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.

ÍNDICE

Resumen

Esta Recomendación | Norma Internacional define un marco general para la prestación del servicio de no rechazo. La finalidad del servicio de no rechazo consiste en obtener, mantener, poner a disposición y validar evidencia irrefutable relativa a la identificación de los originadores y los receptores que participan en las transferencias de datos.

Introducción

La finalidad del servicio de no rechazo consiste en obtener, mantener, poner a disposición y validar evidencia irrefutable relativa a un supuesto evento o acción a fin de resolver las disputas sobre la ocurrencia o no ocurrencia del evento o la acción. El servicio de no rechazo puede aplicarse en diferentes contextos y situaciones. Puede aplicarse a la producción, almacenamiento o transmisión de datos. El no rechazo consiste en la generación de evidencias que puedan utilizarse para probar que ha tenido lugar algún tipo de evento o acción, de modo que ese evento o acción no pueda rechazarse posteriormente.

En un entorno de OSI (véase la Rec. X.800 del CCITT e ISO 7498-2) el servicio de no rechazo tiene dos modalidades:

- no rechazo con prueba de origen que se utiliza para hacer frente a la falsa negación del envío de datos o sus contenidos por parte de un emisor; y
- no rechazo con prueba de entrega que se utiliza para hacer frente a la falsa negación de que no ha recibido los datos o sus contenidos (es decir, la información que representan los datos) por parte de un receptor.

Las aplicaciones que hacen uso de los protocolos de la OSI pueden requerir otras formas del servicio de no rechazo específicas de clases de aplicaciones particulares. Por ejemplo, el MHS (Rec. UIT-T X.402 | ISO 10021-2) define el servicio de no rechazo de depósito, mientras que el sistema de mensajería EDI (véase la Recomendación X.435) define los servicios de no rechazo de recuperación y no rechazo de transferencia.

Los conceptos de este marco no se limitan a las comunicaciones de la OSI sino que pueden interpretarse en términos más amplios para incluir usos tales como la creación y almacenamiento de datos para utilización posterior.

La presente Recomendación | Norma Internacional define un marco general para la prestación de un servicio de no rechazo.

Dicho marco:

- amplía los conceptos de los servicios de no rechazo descritos en la Rec. X.800 del CCITT e ISO 7498-2 y describe cómo pueden aplicarse a los sistemas abiertos;
- describe alternativas para la prestación de estos servicios; y
- explica la relación entre estos servicios y otros servicios de seguridad.

Los servicios de no rechazo pueden requerir:

- árbitros que medien en las disputas que puedan surgir a resultas de eventos o acciones rechazadas; y
- terceros de confianza que aseguren la autenticidad e integridad de los datos que se han de utilizar para la verificación de la evidencia.

NORMA INTERNACIONAL

RECOMENDACIÓN UIT-T

TECNOLOGÍA DE LA INFORMACIÓN – INTERCONEXIÓN DE SISTEMAS ABIERTOS – MARCOS DE SEGURIDAD EN SISTEMAS ABIERTOS: MARCO DE NO RECHAZO

1 Alcance

La presente Recomendación | Norma Internacional sobre marcos de seguridad para sistemas abiertos aborda la aplicación de los servicios de seguridad en un entorno de sistemas abiertos, donde la expresión «sistemas abiertos» incluye ámbitos tales como bases de datos, aplicaciones distribuidas, el procesamiento distribuido abierto y la OSI. Los marcos de seguridad tienen por objeto la definición de los medios con los que prestar protección a los sistemas y objetos de los sistemas, y las interacciones entre sistemas. Los marcos de seguridad no entran a considerar la metodología para construir sistemas o mecanismos.

Los marcos de seguridad tienen en cuenta tanto los elementos de datos 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.

La presente Recomendación | Norma Internacional:

- define los conceptos básicos del no rechazo;
- define los servicios generales de no rechazo;
- identifica los posibles mecanismos para prestar servicios de no rechazo;
- identifica los requisitos generales de gestión de los servicios y mecanismos de no rechazo.

Al igual que otros servicios de seguridad, el de no rechazo únicamente puede prestarse en el contexto de una política de seguridad definida para una aplicación determinada. Las definiciones de las políticas de seguridad quedan fuera del alcance de la presente Recomendación | Norma Internacional.

El alcance de esta Recomendación | Norma Internacional no incluye la especificación de los detalles de los intercambios de protocolo que han de realizarse para conseguir el no rechazo.

La presente Recomendación | Norma Internacional no describe con detalle los mecanismos particulares que pueden utilizarse para soportar los servicios de no rechazo ni ofrece detalles de los servicios y protocolos de gestión de la seguridad que dan soporte.

Algunos de los procedimientos descritos en este marco consiguen la seguridad mediante la aplicación de técnicas criptográficas. Este marco no depende del uso de una criptografía determinada o de otros algoritmos o técnicas criptográficas particulares (es decir, simétricas o asimétricas) aunque ciertas clases de mecanismos de no rechazo pueden depender de propiedades de algoritmos particulares. De hecho, es probable que, en la práctica, se utilicen varios algoritmos diferentes. Dos entidades que deseen utilizar datos protegidos criptográficamente deben admitir el mismo algoritmo criptográfico.

[NOTA – Aunque la ISO no normaliza algoritmos criptográficos, sí normaliza los procedimientos utilizados para registrarlos en ISO/CEI 9979.]

Normas de tipos diferentes pueden utilizar este marco, por ejemplo:

1) normas que incorporan el concepto de no rechazo;
2) normas que especifican servicios abstractos que incluyen el no rechazo;
3) normas que especifican usos de un servicio de no rechazo;
4) normas que especifican los medios de prestación del servicio de no rechazo dentro de una arquitectura de sistemas abiertos; y
5) normas que especifican mecanismos de no rechazo.

Tales normas pueden hacer uso de este marco como a continuación se indica:

- las normas de tipo 1), 2), 3), 4) ó 5) pueden utilizar la terminología del marco;
- las normas de tipo 2), 3), 4) ó 5) pueden utilizar las facilidades definidas en la cláusula 7 del marco; y
- las normas de tipo 5) pueden basarse en las clases de mecanismo definidas en la cláusula 8 del marco.

2 Referencias normativas

Las siguientes Recomendaciones y Normas Internacionales contienen disposiciones que, mediante su 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 las 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 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 Telecomunicaciones de la UIT mantiene una lista de las Recomendaciones UIT-T actualmente vigentes.

2.1 Recomendaciones | Normas Internacionales idénticas

- Recomendación UIT-T X.200 (1994) | ISO/CEI 7498-1:1994, *Tecnología de la información – Interconexión de sistemas abiertos – Modelo de referencia básico: El modelo básico*.
- Recomendación UIT-T X.509 (1993) | ISO/CEI 9594-8:1995, *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Marco de autenticación*.
- Recomendación UIT-T X.810 (1995) | ISO/CEI 10181-1:1996, *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 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.*

3 Definiciones

3.1 Definiciones del modelo de referencia básico

La presente Recomendación | Norma Internacional se basa en los conceptos desarrollados en la Rec. UIT-T X.200 | ISO/CEI 7498-1 y utiliza los siguientes términos definidos en ella:

entidad (N).

3.2 Definiciones de la arquitectura de seguridad

La presente Recomendación | Norma Internacional se basa en los conceptos desarrollados en la Rec. X.800 del CCITT e ISO 7498-2 y utiliza los siguiente términos definidos en ella:

- control de acceso;
- auditoría (también auditoría de seguridad);
- autenticación;
- canal;
- valor de comprobación criptográfico;
- criptografía;
- integridad de los datos (también integridad);
- autenticación del origen de los datos;
- descifrado;

- firma digital (también firma);
- cifrado;
- clave;
- gestión de claves;
- notarización;
- rechazo;
- registro de auditoría de seguridad (también auditoría de seguridad, registro fichero, registro cronológico);
- amenaza.

3.3 Definiciones de la visión de conjunto de los marcos de seguridad

La presente Recomendación | Norma Internacional se basa en los conceptos desarrollados en la Rec. UIT-T X.810 | ISO/CEI 10181-1 y utiliza los siguientes términos definidos en ella:

- autoridad de certificación;
- huella digital;
- función de cálculo de clave;
- función unidireccional;
- clave privada;
- clave pública;
- certificado de lista de revocaciones;
- sello;
- sellado;
- clave secreta;
- certificado de seguridad;
- dominio de seguridad;
- testigo de seguridad;
- tercera parte confiable.

3.4 Definiciones adicionales

Para los fines de esta Recomendación | Norma Internacional serán de aplicación las definiciones siguientes:

3.4.1 evidencia comprometida: Evidencia que fue satisfactoria en su momento, pero que ya no dispone de la confianza de la tercera persona confiable o del adjudicador.

3.4.2 contrafirma: Firma digital anexa a una unidad de datos que ya ha sido firmada por una entidad diferente (por ejemplo, una tercera persona confiable).

3.4.3 evidencia: Información que, bien por sí misma o bien cuando se utiliza junto con otra información, puede utilizarse para resolver una disputa.

3.4.4 generador de evidencia: Entidad que produce evidencia de no rechazo.

NOTA – Esta entidad puede ser el peticionario del servicio de no rechazo, el originador, el receptor o múltiples partes que trabajan conjuntamente (por ejemplo, un firmante y un cofirmante).

3.4.5 sujeto de evidencia: Entidad cuya participación en un evento o acción se establece mediante evidencia.

3.4.6 usuario de evidencia: Entidad que utiliza la evidencia de no rechazo.

3.4.7 verificador de evidencia: Entidad que verifica la evidencia de no rechazo.

3.4.8 código de autenticación de mensaje: Valor de comprobación criptográfico utilizado para proporcionar la autenticación del origen de los datos y la integridad de los datos.

3.4.9 peticionario de servicio de no rechazo: Entidad que solicita que se genere la evidencia de no rechazo para un evento o acción particular.

3.4.10 notario: Tercera parte confiable con la que se registran los datos de forma que pueda asegurarse ulteriormente la precisión de las características de los datos.

3.4.11 originador: Entidad que origina los datos en una acción sujeta a un servicio de no rechazo.

3.4.12 receptor: En el contexto de la transferencia de datos, entidad que recibe los datos en una acción sujeta a un servicio de no rechazo.

NOTA – En el modelo lógico de no rechazo, pueden considerarse otras entidades; por ejemplo, el titular es la entidad que emite un mensaje original y el agente de transferencia es la entidad que envía el mensaje. Estas entidades deberían incluirse en la función de los términos originador y receptor en esta Norma.

4 Abreviaturas

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

CA Autoridad de certificación (*certification authority*)

TTP Tercera parte confiable (*trusted third party*)

MAC Código de autenticación de mensaje (*message authentication code*)

5 Presentación general del no rechazo

5.1 Conceptos básicos del no rechazo

El servicio de no rechazo consiste en la generación, verificación y registro de evidencia, y en la recuperación y nueva verificación subsiguientes de esta evidencia para resolver disputas. Las disputas no pueden resolverse a menos que anteriormente se haya registrado la evidencia.

La finalidad del servicio de no rechazo descrito en este marco consiste en proporcionar pruebas sobre un evento o acción particular. Los servicios de no rechazo pueden ser solicitados por entidades distintas de las involucradas en el evento o acción. Algunos ejemplos de acciones que pueden ser protegidas mediante un servicio de no rechazo son:

- el envío de una mensaje X.400;
- la inserción de un registro en una base de datos; y
- la invocación de una operación a distancia.

Cuando participan mensajes, debe confirmarse la identidad del originador y la integridad de los datos para proporcionar prueba de origen. Para proporcionar prueba de entrega, debe confirmarse la identidad del receptor y la integridad de los datos. En algunos casos, también puede requerirse evidencia relativa al contexto (por ejemplo, fecha, hora y ubicación del originador/receptor).

El servicio proporciona las facilidades siguientes que pueden utilizarse en caso de intento de rechazo:

- generación de evidencia;
- registro de evidencia;
- verificación de la evidencia generada;
- recuperación y nueva verificación de la evidencia.

Las disputas pueden ser resueltas directamente por las partes analizando la evidencia. Sin embargo, es posible que una disputa tenga que ser resuelta por un árbitro que evalúe la evidencia y determine si tuvo lugar o no la acción o evento objeto de la disputa. El arbitraje sólo puede ser eficaz si las partes enfrentadas aceptan la autoridad del árbitro. Para que el árbitro acepte la evidencia aportada, debe estar garantizada normalmente por una o más terceras partes confiables. Facultativamente, el árbitro puede ser la tercera parte confiable que garantiza la evidencia. Los mecanismos de no rechazo utilizan varios tipos de terceras partes confiables y formas de evidencia.

5.2 Cometidos de una tercera parte confiable

En el servicio de no rechazo pueden participar una o más terceras partes confiables.

Las terceras partes confiables que soportan el no rechazo sin participar activamente en cada utilización del servicio se conocen como terceras partes confiables fuera de línea. Una TTP que participa activamente en la generación o verificación de evidencia se conoce como TTP en línea. Una TTP en línea que actúa de intermediaria en todas las interacciones se conoce como TTP dentro de la línea.

Una tercera parte confiable puede ser requerida para que registre y/u obtenga evidencia y para que responda de la validez de la misma. Puede haber varias terceras partes confiables participando en diversos cometidos (por ejemplo, los de notario, indicación de tiempo, supervisión, certificación de clave, generación de firma, verificación de firma y autoridad de entrega). Una misma tercera parte confiable puede desempeñar uno o más de estos cometidos.

En un cometido de generación de evidencia, la TTP coopera con un solicitante del servicio de no rechazo para obtener evidencia.

En un cometido de registro de evidencia, la TTP registra la evidencia que luego puede ser recuperada por un usuario de la misma o por un árbitro.

En un cometido de indicación de tiempo, se encarga a la TTP que obtenga evidencia que incluya la hora en que se recibió la petición de indicación de tiempo.

En un cometido de supervisión, la TTP supervisa la acción o el evento y se le encarga que obtenga evidencia sobre lo supervisado.

En un cometido de certificación de clave, la TTP proporciona certificados de no rechazo relativos a un generador de evidencia para asegurar la validez de una clave pública que se ha de utilizar a efectos de no rechazo.

En un cometido de distribución de claves, la TTP proporciona claves a los generadores de evidencia y/o a los verificadores de evidencia. También puede imponer constricciones al uso de las claves, en particular cuando se utilizan técnicas simétricas.

En un cometido de generación de firma, se encarga a la TTP que obtenga evidencia en forma de una firma digital en favor del sujeto de la evidencia.

En un cometido de verificación de evidencia, la TTP verifica la evidencia a petición de una entidad.

En un cometido de verificación de firma el usuario de la evidencia encarga a la TTP que verifique la evidencia en forma de una firma digital.

NOTA – Los cometidos de certificación de clave y generación de firma son casos particulares del cometido de generación de evidencia. El cometido de verificación de firma es un caso particular del cometido de verificación de evidencia.

En un cometido de notario, la TTP asegura las propiedades de los datos comunicados entre dos o más entidades, por ejemplo, la integridad, el origen, la hora o el destino de los datos.

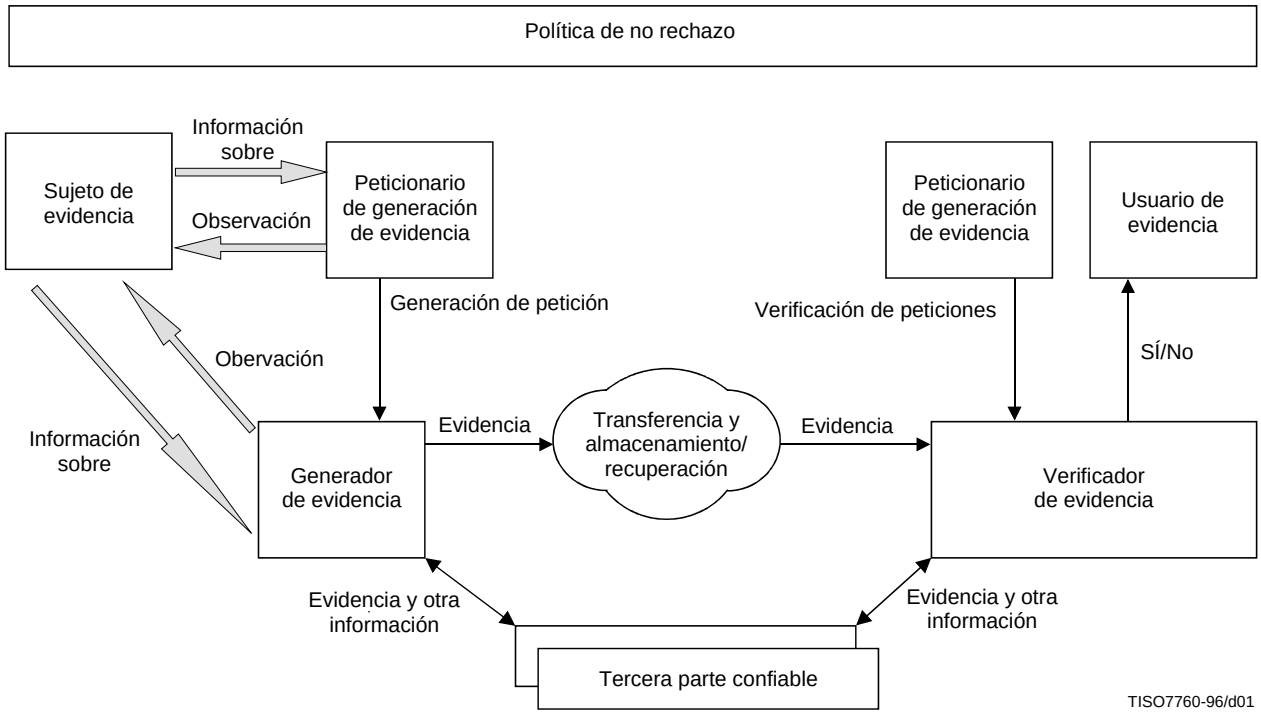
En un cometido de autoridad de entrega, la TTP interactúa con el receptor de los datos pretendido y libera los datos si, y sólo si, el receptor proporciona evidencia de que los datos fueron entregados. Este cometido sólo es necesario cuando se requiere no rechazo con prueba de entrega y cuando el procedimiento de no rechazo requiere una TTP semejante.

5.3 Fases del no rechazo

El no rechazo se compone de cuatro fases diferenciadas:

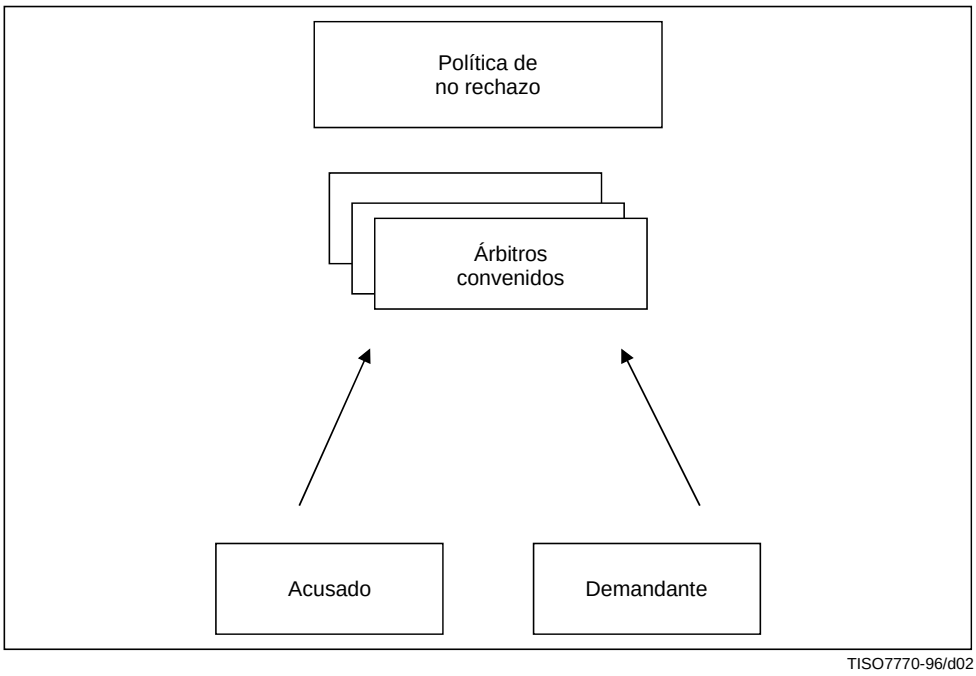
- generación de evidencia;
- transferencia, almacenamiento y recuperación de evidencia;
- verificación de evidencia; y
- resolución de disputas.

La Figura 1 ilustra las tres primeras fases; la Figura 2 ilustra la cuarta fase.



NOTA – Esta figura es a título de ejemplo, no definitiva.

Figura 1 – Entidades que participan en las fases de generación, transferencia, almacenamiento/recuperación y verificación



NOTA – Esta figura es a título de ejemplo, no definitiva.

Figura 2 – Fase de resolución de disputas de un proceso de no rechazo

5.3.1 Generación de evidencia

En esta fase, el peticionario de generación de evidencia pide al generador de evidencia que genere evidencia para un evento o acción. Una entidad cuya participación en el evento o acción queda establecida mediante la evidencia se denomina sujeto de evidencia. Son posibles diferentes agrupaciones de estas entidades: un sujeto de evidencia y un generador de evidencia pueden ser la misma entidad como pueden serlo el sujeto de evidencia, el peticionario de generación de evidencia y el generador de evidencia; el peticionario de generación de evidencia y la tercera parte confiable; y el peticionario de generación de evidencia, el generador de evidencia y la tercera parte confiable. Dependiendo del tipo de servicio de no rechazo, la evidencia puede ser generada por el sujeto de evidencia, quizás en combinación con los servicios de una tercera parte confiable, o por una tercera parte confiable sola.

NOTA – Dependiendo del contexto del servicio de no rechazo, la evidencia correspondiente incluirá normalmente la identidad de las entidades involucradas, los datos y la fecha y la hora. También podría incluirse información adicional, tal como el modo de transferencia (por ejemplo, comunicación OSI; almacenamiento y recuperación en bases de datos), la ubicación de entidades involucradas, el identificador distintivo y el «titular»/creador de los datos.

5.3.2 Transferencia, almacenamiento y recuperación de evidencia

Durante esta fase se transfiere evidencia entre entidades al almacenamiento o desde éste. Esta fase puede no tener lugar en todos los casos de servicio de no rechazo (véase la Figura 1).

5.3.3 Verificación de evidencia

En esta fase, un verificador de evidencia verifica la evidencia a petición de un usuario de la misma. La finalidad de esta fase consiste en que el usuario de la evidencia adquiera la confianza de que la evidencia suministrada será la adecuada en caso de que surja una disputa. Adicionalmente pueden participar servicios de terceros de confianza para proporcionar información de verificación de la evidencia. El usuario y el verificador de la evidencia pueden ser la misma entidad.

5.3.4 Resolución de disputas

En esta fase, un árbitro se encarga de resolver las disputas entre las partes. En ocasiones, las partes en conflicto se conocen como demandante y acusado. En la Figura 2 se representa esta fase de resolución de disputas.

Cuando las disputas son resueltas por un árbitro, éste recoge evidencia de las partes en conflicto y/o de las terceras partes confiables. El proceso utilizado por un árbitro para resolver las disputas queda fuera del alcance de esta Recomendación | Norma Internacional.

Esta fase no siempre es necesaria. Si todas las partes interesadas están de acuerdo en que se ha producido un evento o acción (o que no se ha producido) no hay disputa que resolver. Más aún, incluso si surge una disputa, puede ser resuelta directamente en algunos casos entre las partes sin necesidad de un árbitro. Por ejemplo, si una de las partes en la disputa actúa de buena fe pero está equivocada, puede darse cuenta de su error cuando se le muestre la evidencia de la otra parte.

Aunque esta fase no sea necesaria en cada caso del servicio de no rechazo, todos los mecanismos de no rechazo deben sustentar la fase de resolución de disputas. Es decir, deben facilitar la resolución de las disputas cuando se producen.

5.4 Modalidades del servicio de no rechazo

Hay muchas formas de servicio de no rechazo. De todas ellas, el servicio de no rechazo asociado con la transferencia de datos es una de las consideradas frecuentemente.

La emisión de un mensaje implica al menos a dos entidades, a saber, el originador y el receptor. Las disputas potenciales relativas al evento pueden consistir en lo siguiente:

- disputas en las que se cuestiona la participación del originador en el evento, por ejemplo, cuando el supuesto originador afirma que o bien el receptor o bien un impostor falsificó el mensaje;
- disputas en las que se cuestiona la participación del receptor en el evento, por ejemplo, cuando el supuesto receptor afirma que el mensaje no se envió, se perdió en tránsito o únicamente fue recibido por un impostor.

Para la mensajería, los servicios de no rechazo pueden clasificarse según el tipo de disputa que pueden contribuir a resolver.

La emisión de mensajes de un originador a un receptor puede considerarse como una secuencia de eventos separados:

- la transmisión del mensaje del originador a un agente de transferencia;
- la transmisión del mensaje entre agentes de transferencia (si participa más de uno); y
- la transmisión del mensaje de un agente de transferencia al receptor.

Para cada uno de estos eventos hay modalidades del servicio de no rechazo que proporcionan evidencia relativa al evento de que se trate. Se han definido, en consecuencia, los siguientes servicios de no rechazo adicionales:

- el servicio de no rechazo con prueba de depósito, que se utiliza como protección contra la falsa negación de un agente de transferencia de haber aceptado un mensaje para transmitir (bien procedente del originador o de otro agente de transferencia);
- el servicio de no rechazo con prueba de transporte, que se utiliza como protección contra la falsa negación de un agente de transferencia de haber transmitido un mensaje (bien al receptor o bien a otro agente de transferencia).

NOTA – Al contrario que los servicios de no rechazo con prueba de origen y no rechazo con prueba de entrega, los servicios de no rechazo con prueba de depósito y no rechazo con prueba de transporte no proporcionan evidencia de que una entidad sea responsable del mensaje o haya comprendido la información que éste contiene.

5.5 Ejemplo de evidencia de no rechazo en OSI

Dependiendo de cuáles sean los servicios de no rechazo en OSI invocados, se necesitan formas particulares de evidencia para cada tipo de evento o acción, como se muestra a continuación.

5.5.1 Para el no rechazo de origen

La evidencia debe incluir lo siguiente (que puede estar o bien firmado o bien notarizado):

- el identificador distintivo del originador;
- los datos enviados, o una huella digital de los datos.

La evidencia también puede incluir lo siguiente:

- el identificador distintivo del receptor;
- la fecha y hora en que se enviaron los datos.

5.5.2 Para el no rechazo de entrega

La evidencia debe incluir lo siguiente (que puede estar o bien firmado o bien notarizado):

- el identificador distintivo del receptor;
- los datos recibidos, o una huella digital de los datos.

La evidencia puede incluir también lo siguiente:

- el identificador distintivo del originador;
- la fecha y hora en que se recibieron los datos.

Cuando se utiliza una autoridad de entrega, la evidencia también puede incluir lo siguiente (que puede estar o bien firmado o bien notarizado):

- el identificador distintivo de la autoridad de entrega;
- la fecha y hora en que la autoridad de entrega intentó efectuar la entrega por vez primera;
- la fecha y hora en que se obtuvo del receptor un intento de recibir;
- la fecha y hora en que la autoridad de entrega efectuó la entrega;
- la fecha y hora en que la autoridad de entrega no fue capaz de efectuar la entrega;
- la causa probable de las condiciones de no entrega (por ejemplo, la ruptura del canal de comunicación);
- una etiqueta de seguridad que indique los requisitos de manejo que se cumplieron al entregar el mensaje.

6 Políticas de no rechazo

Una política de no rechazo puede incluir lo siguiente:

- Reglas para la generación de evidencia, por ejemplo la especificación de las clases de actividad para las que debe generarse evidencia de no rechazo; las especificaciones de las TTP que se han de utilizar para generar evidencia; los cometidos en que pueden actuar esas TTP; los procedimientos que deben seguir las entidades cuando generan evidencia.
- Reglas para la verificación de evidencia, por ejemplo la especificación de las TTP cuya evidencia es aceptable; para cada TTP, las formas de evidencia que serán aceptadas de esa TTP.

- Reglas para el almacenamiento de evidencia, por ejemplo los medios que se han de utilizar para asegurar la integridad de la evidencia almacenada.
- Reglas para el uso de evidencia, por ejemplo la especificación de las finalidades para las que puede utilizarse la evidencia.

  NOTA – Con algunos mecanismos de no rechazo puede ser difícil evitar el uso no autorizado de evidencia.
- Reglas para el arbitraje, por ejemplo la especificación del(de los) árbitro(s) que puede(n) mediar en una disputa.

Cada uno de estos conjuntos de reglas pueden ser definidos por una autoridad diferente. Por ejemplo, las reglas para la generación de evidencia podrían ser definidas por el titular de un sistema, mientras que las reglas para el arbitraje podrían ser definidas por la legislación del país en el que se encuentra el sistema.

Si diferentes partes de la política son incompatibles, el servicio de no rechazo puede no funcionar correctamente, por ejemplo permitiendo que se consuma la negación de un evento, que en realidad no ocurrió, durante la fase de resolución de la disputa.

El árbitro puede utilizar la propia política de no rechazo cuando resuelve una disputa. Por ejemplo, el árbitro podría hacer referencia a la política de no rechazo para determinar si se han cumplido las reglas de generación de evidencia.

Las políticas de seguridad pueden enunciarse de manera explícita, o bien ser definidas implícitamente por las implementaciones. Un enunciado explícito de la política de no rechazo (por ejemplo, un documento en lenguaje natural) puede ayudar a detectar conflictos entre partes diferentes de la política y puede también ayudar al árbitro.

Las políticas de no rechazo contemplan también los casos en los que se ha comprometido o revocado la evidencia.

Las políticas de no rechazo para la interacción entre ámbitos de seguridad pueden ser el resultado de acuerdos entre dominios de seguridad independientes o bien pueden ser impuestos por un super-dominio.

7 Información y facilidades

7.1 Información

La información que puede utilizarse para resolver una disputa se conoce como evidencia. La evidencia puede ser almacenada localmente por un usuario de evidencia o bien ser almacenada por una tercera parte confiable. Formas particulares de evidencia son firmas digitales, sobres de seguridad y testigos de seguridad. Las firmas digitales se utilizan con técnicas de clave pública mientras que los sobres de seguridad y los testigos de seguridad se utilizan con técnicas de clave secreta. Algunos ejemplos de evidencia son los siguientes:

- un identificador de la política de seguridad de no rechazo;
- el identificador distintivo del originador;
- el identificador distintivo del receptor;
- una firma digital o un sobre de seguridad;
- el identificador distintivo del generador de evidencia;
- el identificador distintivo del peticionario de generación de evidencia;
- el mensaje, o una huella digital del mensaje;

  NOTA – Cuando se utiliza la huella digital en lugar del mensaje, se requiere un indicador para identificar el método utilizado en la derivación.
- el identificador del mensaje;
- una indicación de la clave secreta necesaria para validar el testigo de seguridad;
- una identificación de la clave pública particular necesaria para validar la firma digital (por ejemplo, el identificador distintivo de la autoridad de certificación y el número de serie certificado);
- el identificador distintivo del notario, TTP de indicación de tiempo, TTP dentro de la línea, etc.;
- un identificador único de la evidencia;
- la fecha y hora en que se depositó o registró la evidencia;
- la fecha y hora en que se generó la firma digital o el testigo de seguridad.

7.2 Facilidades de no rechazo

En esta subcláusula se identifican diversas facilidades de no rechazo que pueden utilizarse para generar, enviar y validar evidencia, o depositar evidencia en una TTP.

7.2.1 Facilidades relativas a la gestión

Las actividades de no rechazo relativas a la gestión pueden consistir en la distribución de información, contraseñas o claves (utilizando la gestión de claves) entre las entidades a las que se exige que efectúen el no rechazo. Esto puede suponer el uso de un protocolo entre entidades comunicantes y otras entidades que proporcionan servicios de no rechazo. La gestión del no rechazo también puede consistir en la revocación de la evidencia.

Las facilidades de gestión del no rechazo permiten a un usuario obtener, modificar y suprimir información necesaria para la prestación del servicio de no rechazo. En términos generales, estas facilidades son:

- instalar información de gestión;
- modificar información de gestión;
- suprimir información de gestión;
- listar información de gestión.

Pueden requerirse las siguientes acciones relativas a la gestión en apoyo de los servicios de no rechazo:

- registro del evento en el registro de auditoría;
- registro de los resultados del arbitraje de la disputa;
- notificación local del evento;
- notificación a distancia del evento.

La acción específica que ha de efectuarse para cada evento depende de la política de seguridad vigente.

7.2.2 Facilidades relativas a la explotación

7.2.2.1 Generar evidencia

Esta facilidad se utiliza para generar evidencia. La evidencia puede ser generada directamente por el sujeto de evidencia (sin que participe una TTP), por una o más TTP actuando en nombre del sujeto de evidencia o por el sujeto de evidencia y una o más TTP actuando conjuntamente.

Las entradas posibles son las siguientes:

- la política de no rechazo;
- el identificador distintivo del sujeto de evidencia;
- el identificador distintivo del peticionario del servicio de no rechazo;
- los datos, o la huella digital de los datos;
- el identificador distintivo de la TTP que se utilizará para generar la firma digital, el testigo de seguridad u otra evidencia.

Las salidas posibles son las siguientes:

- evidencia (por ejemplo, una firma digital o un testigo de seguridad);
- el identificador distintivo de la TTP que generó la firma digital, el testigo de seguridad u otra evidencia.

7.2.2.2 Generar indicación de tiempo

Esta facilidad se utiliza para generar indicaciones de tiempo.

Las entradas posibles son las siguientes:

- el identificador distintivo de la entidad peticionaria de indicación de tiempo;
- el identificador distintivo de la TTP en el cometido de indicación de tiempo;
- los datos (por ejemplo, mensaje firmado, acuse de recibo) o una firma digital o una huella digital de los datos.

Las salidas posibles son las siguientes:

- contrafirma computada por la TTP;
- una identificación del método y/o algoritmo criptográfico utilizado para generar la contrafirma (que secundariamente indica si se utilizan los datos o la huella digital de los datos);
- el identificador distintivo del servicio de indicación de tiempo;
- la fecha y hora en que se recibió la petición de indicación de tiempo;
- la fecha y hora en que se generó la contrafirma;
- un mensaje firmado que incluye una indicación de tiempo y una huella digital de los datos de entrada.

7.2.2.3 Generar evidencia notarizada

Esta facilidad se utiliza para depositar evidencia en la TTP.

Las entradas posibles son las siguientes:

- el identificador distintivo del peticionario de generación de evidencia;
- la evidencia (por ejemplo, una firma digital o testigo de seguridad);
- el identificador distintivo del generador de evidencia;
- el identificador distintivo de la política de no rechazo.

Las salidas posibles son las siguientes:

- el número de registro de la evidencia;
- la fecha y hora del registro de evidencia.

7.2.2.4 Validar evidencia

Esta facilidad se utiliza para validar evidencia.

Las entradas posibles son las siguientes:

- evidencia;
- el identificador distintivo del sujeto de evidencia;
- el identificador distintivo del usuario de evidencia;
- el identificador de la clave que se ha de utilizar para la verificación de evidencia;
- una indicación del uso que se pretende hacer de la evidencia (para que pueda efectuarse una valoración a fin de determinar si la evidencia es apropiada para este uso a tenor de la política de no rechazo).

Las salidas posibles son las siguientes:

- el resultado de la verificación (es decir, válida o no válida);
- el identificador distintivo del sujeto de evidencia;
- el identificador distintivo del generador de evidencia;
- el identificador distintivo del peticionario de verificación de evidencia;
- el identificador distintivo de la TTP que verificó la firma digital o el testigo de seguridad;
- los datos o la huella digital de los datos.

7.2.2.5 Generar evidencia para transferencias de datos mediante una TTP dentro de la línea

En vez de enviar directamente datos y/o acuses de recibo entre un originador y un receptor, se pueden transferir los datos mediante una TTP, de forma que la TTP asegure la evidencia de no rechazo. Esta facilidad también puede utilizarse cuando se sospecha que un receptor podría alegar fallo del canal de comunicación para negar la entrega de los datos.

Para utilizar esta facilidad debe presentarse lo siguiente a la tercera parte confiable dentro de la línea:

- los datos;
- el identificador distintivo del receptor.

Además, puede presentarse lo siguiente:

- una huella digital de los datos;
- el identificador distintivo del originador;
- una firma digital;
- el identificador distintivo de la TTP dentro de la línea;
- la política de no rechazo.

Las salidas posibles de la tercera parte confiable dentro de la línea son las siguientes:

- el identificador distintivo de la tercera parte confiable dentro de la línea;
- el identificador distintivo del receptor;
- el número de registro de la evidencia;
- la fecha y hora del registro;
- los datos o la huella digital de los datos.

8 Mecanismos de no rechazo

El servicio de no rechazo puede proporcionarse mediante el uso de mecanismos tales como firmas digitales, cifrado, notarización y mecanismos de integridad de los datos, con soporte de otros servicios, por ejemplo el de indicación de tiempo. Pueden utilizarse algoritmos criptográficos tanto simétricos como asimétricos para el no rechazo. El servicio de no rechazo puede utilizar una combinación de estos mecanismos y servicios como apta para satisfacer los requisitos de seguridad de la aplicación en cuestión.

Esta cláusula describe mecanismos que pueden utilizarse para proporcionar el servicio de no rechazo y describe algunas de las amenazas a esos mecanismos.

8.1 No rechazo utilizando un testigo de seguridad de TTP (sobre de seguridad)

En este esquema, la evidencia de no rechazo consiste en un testigo de seguridad, sellado con una clave secreta conocida únicamente por la TTP. La TTP genera el testigo de seguridad a petición del peticionario de generación de evidencia y puede verificarlo, a continuación, para el usuario de evidencia o el árbitro. En este caso, la TTP es el generador de evidencia y el verificador de evidencia.

Un peticionario de generación de evidencia transmite a la TTP los datos o una huella digital de los datos, junto con una petición que genere un testigo de seguridad. Esta petición debe ser de integridad protegida (por ejemplo, utilizando un sello), y también de confidencialidad protegida (por ejemplo, utilizando cifrado). En ocasiones un método de protección de este tipo se denomina de sobre de seguridad.

Las entradas posibles utilizadas en la generación del testigo de seguridad son las siguientes:

- una identificación del método y/o algoritmo criptográfico utilizado para asegurar la integridad del testigo de seguridad;
- una identificación del método y/o algoritmo criptográfico utilizado para asegurar la confidencialidad del testigo de seguridad;
- el identificador distintivo del sujeto de evidencia;
- el identificador distintivo del peticionario de generación de evidencia;
- la política de no rechazo aplicable;
- la fecha y hora del evento o acción;
- datos que describan el evento o acción.

Las salidas posibles son las siguientes:

- un testigo de seguridad;
- la fecha y hora en que se generó el testigo de seguridad.

8.2 No rechazo utilizando testigos de seguridad y módulos resistentes a la manipulación

En este esquema, la evidencia de no rechazo consiste en un testigo de seguridad, sellado con una clave secreta que se almacena en módulos criptográficos resistentes a la manipulación que poseen el generador de evidencia, el verificador de evidencia y el árbitro. Los módulos resistentes a la manipulación limitan las operaciones que pueden realizarse con la clave secreta e impiden que se revele fuera del módulo el valor de la clave.

El módulo del generador de evidencia permite el uso de la clave secreta para crear un testigo sellado, mientras que los módulos que poseen el verificador de evidencia y el árbitro únicamente permiten la verificación del testigo. Todas las partes involucradas deben confiar en que se han instalado correctamente las claves secretas en módulos criptográficos resistentes a la manipulación, de forma que la misma clave secreta pueda ser utilizada únicamente por una entidad para la generación de evidencia y por las otras entidades sólo para la verificación de evidencia.

Si surge una disputa, el usuario de evidencia presenta el testigo sellado al árbitro, y arguye que debe de haber sido creado utilizando el módulo del generador de evidencia, ya que los otros módulos que contienen la misma clave no son capaces de generar un testigo de seguridad.

8.3 No rechazo utilizando una firma digital

En este esquema, la evidencia de no rechazo consiste en una estructura de datos firmada digitalmente. La generación de firma utiliza una clave de firma y la verificación de firma utiliza una clave de verificación.

Dependiendo de cual sea la política de seguridad, puede exigirse información de tiempo. Ésta se puede incluir en la firma digital proporcionada por una entidad y/o una TTP actuando como autoridad de indicación de tiempo. Cuando la información no la proporciona una TTP es posible que otras entidades no confíen en ella. Si el árbitro necesita una indicación de tiempo y/u otra información contextual para resolver las disputas, esa información ha de obtenerse de fuentes de confianza (por ejemplo, las TTP).

El verificador de evidencia y el árbitro deben ser capaces de obtener la clave de verificación para verificar la evidencia. Si no puede garantizarse que el árbitro conozca la clave pública del generador de evidencia por otros medios, la evidencia debe incluir también un certificado de seguridad para esta clave.

La firma digital puede ser creada por el sujeto de evidencia o generada por una TTP en un cometido de generación de firma.

Una firma digital generada por el sujeto de evidencia se denomina firma digital directa. Un mecanismo de firma digital generado por una TTP en nombre del sujeto de evidencia se denomina firma digital negociada

Las firmas digitales no bastan por sí solas para resolver disputas cuando el certificado utilizado para verificar la firma ha sido revocado. Para resolver esas disputas es necesario, además, proporcionar al árbitro evidencia sobre la revocación de los certificados [por ejemplo, listas de revocación de certificados (CRL, *certificate revocation lists*)] que muestre que el certificado todavía era válido en el momento en que se generó la firma digital. Sin embargo, este esquema no permite el arreglo de disputas cuando el propietario de la clave privada la utiliza de manera voluntaria en momento inadecuado, o cuando un agresor viola la clave privada utilizada para generar la firma. Para solucionar esas disputas es necesario, además, una referencia de tiempo confiable o una contrafirma de una TTP en su cometido de indicación de tiempo (véase el Anexo E).

Un verificador de evidencia puede utilizar un servicio de Directorio para obtener la información (tal como los certificados de seguridad) necesaria para el proceso de verificación. El verificador de la evidencia ha de obtener la clave pública del generador de evidencia. La clave puede estar incorporada en un certificado de seguridad almacenado en el Directorio. Quizás se necesite más de un certificado. Para asegurar que un certificado es válido, hace falta además solicitar los certificados de revocación que correspondan. Esto es necesario para toda autoridad de certificación que aparezca en una trayectoria de certificación (véase Rec. UIT-T X.509 | ISO/CEI 9594-8).

Un usuario de evidencia puede recabar la asistencia de una TTP que actúa en un cometido de verificación de firma para validar una firma digital. La TTP verifica la relación existente entre el mensaje original (o, si se utiliza, una huella digital del mensaje) y la firma digital.

En este caso, la TTP tiene como cometido ahorrar al usuario de evidencia la complejidad del proceso de verificación de firma y mantener los resultados de las peticiones de verificación anteriores a fin de optimizar las respuestas a futuras peticiones de verificación. Para ello, la TTP puede requerir alguna interacción con un Directorio. Se prevé que la TTP que actúe en un cometido de verificación de firma tenga la clave pública de al menos una autoridad de certificación. La TTP también tiene en cuenta las relaciones de confianza existentes entre diferentes autoridades de certificación.

8.4 No rechazo utilizando indicación de tiempo

Cuando se necesita una referencia de tiempo de confianza y cuando no se puede confiar en el reloj que proporciona la entidad que produce la firma digital o el testigo de seguridad, es necesario confiar en una tercera parte confiable para proporcionar la indicación de tiempo. La indicación de tiempo puede utilizarse para probar que se firmó un mensaje antes de que se violara la clave de firma, y por tanto que el mensaje no es falso. En un cometido de indicación de tiempo, la tercera parte confiable proporcionará una firma digital o testigo de seguridad para probar cuándo se recibió la petición. La indicación de tiempo puede ser solicitada por el peticionario del servicio de no rechazo.

La indicación de tiempo añade a los datos la hora y fecha y un sello o firma digital y no requiere la autenticación del peticionario del servicio de no rechazo. El verificador de evidencia debe determinar si las indicaciones de tiempo están dentro de una gama aceptable según las directrices de la política de seguridad.

La indicación de tiempo puede combinarse con la generación de firma o la generación de testigo. Si la entidad que genera la firma digital incluye un reloj fiable, en el que se ha depositado confianza, quizás no se necesite una contrafirma.

8.5 No rechazo utilizando una tercera parte confiable dentro de la línea

Las facilidades de la tercera parte confiable dentro de la línea pueden ser solicitadas explícitamente por un peticionario del servicio de no rechazo o bien proporcionadas de manera implícita. La TTP dentro de la línea actúa entonces como intermediario en todas las interacciones en las que se solicita el servicio de no rechazo y puede proporcionar evidencia a un usuario de evidencia (tal como un árbitro). En todos los casos, la TTP dentro de la línea retransmitirá los datos y podrá supervisar el evento o la acción.

Se confía en que la TTP mantenga los registros para la solución de futuras disputas. Los datos, o la huella digital de éstos, pueden ser evidencia si los mantiene la TTP.

8.6 No rechazo utilizando un notario

En el modelo de OSI, un mecanismo de notarización proporciona seguridad sobre las propiedades de los datos comunicados entre dos o más entidades, tales como su integridad, origen, hora y destino. Las entidades involucradas confían en que el notario mantenga la información necesaria para proporcionar seguridad de carácter verificable y para mantener registros con miras a la resolución de futuras disputas. Pueden utilizarse mecanismos de firma digital, cifrado e integridad, según convenga, en apoyo del servicio prestado por el notario.

En un cometido de generación de evidencia, el notario registrará la evidencia para asegurar las propiedades de los datos. Además, puede utilizarse un número de registro para identificar esta evidencia.

En un cometido de verificación de evidencia, el notario confirmará la validez de la evidencia.

8.7 Amenazas al no rechazo

Ningún mecanismo de no rechazo es completamente inmune a todas las amenazas. Un mecanismo en el que interviene una TTP puede no ser seguro si la TTP se comporta de manera indebida. Algo que puede ocurrir como resultado de un fallo accidental o de un ataque efectuado por un intruso. Las consecuencias de esta amenaza pueden ser importantes pero no son objeto de análisis en la presente Recomendación | Norma Internacional. Los mecanismos de no rechazo varían con respecto a las consecuencias del comportamiento incorrecto de la TTP, y con respecto a la mayor o menor facilidad que pueda tener una TTP para causar fallos de protocolo. Se debe efectuar una estimación de cuáles son las amenazas probables y cuáles tienen consecuencias importantes en un determinado entorno, para elegir un conjunto de mecanismos que mantenga el riesgo total dentro de límites aceptables. A continuación se analizan algunos ejemplos de estas amenazas, junto con las posibles contramedidas.

8.7.1 Violación de claves

8.7.1.1 Violación de clave de generación de entidad

En el periodo comprendido entre la violación de una clave y la detección de la violación por el propietario legítimo de la clave, existe el riesgo de que un agresor pueda utilizar la clave violada para generar evidencia que aceptará como válida un usuario de evidencia. El mecanismo de no rechazo no puede recuperarse de cualquier daño causado por esa utilización incorrecta de la clave de generación de evidencia. Sin embargo, es posible determinar la magnitud del daño mediante una autoridad de generación de evidencia (por ejemplo, una autoridad de generación de firmas) que mantenga

un registro de auditoría de la evidencia generada y posibilite, de ese modo, descubrir qué evidencia se ha generado y cuándo ha sido generada. Conviene también divulgar tanto como se pueda el hecho de que la clave ha sido utilizada incorrectamente, si bien no siempre se podrá llegar a todos los receptores que hubieran recibido evidencia basada en la utilización de la clave de generación violada.

Tan pronto como la violación de la clave sea detectada por el propietario legítimo de la misma, deberá revocarse la clave de generación. Si dicha clave es una clave privada, se ha de revocar el certificado de clave pública correspondiente, lo que puede hacerse utilizando listas de revocación de certificados definidas en la Rec. UIT-T X.509 | ISO/CEI 9594-8. Pero no basta con esto, ya que no se impide alguna utilización incorrecta de la clave. Una posible manera de contrarrestar esta amenaza consiste en utilizar un mecanismo de no rechazo en el que la generación de evidencia requiera la cooperación de una TTP así como la del sujeto de evidencia. Por ejemplo, la utilización de firmas digitales negociadas o contrafirmas de una autoridad de indicación de tiempo puede proteger contra esta forma de amenaza. En el segundo caso, la política de no rechazo específica que la evidencia sólo es válida si está contrafirmada por una autoridad de indicación de tiempo (véase el Anexo E).

La violación de una clave puede ser también deliberada. Si la política de no rechazo especifica que un sujeto de evidencia no sea considerado responsable de la utilización incorrecta de su clave entre el momento en que la clave es violada y el momento en que se detecta esa violación, el sujeto de evidencia puede aprovecharse de ello para alegar que su clave ha sido violada y, de este modo, rechazar una acción o evento que ha tenido lugar realmente. Esta amenaza se puede contrarrestar definiendo el periodo de tiempo máximo que puede transcurrir antes de notificar la violación de una clave. Según esta política, si un usuario de evidencia no declara la violación de su clave dentro de ese límite, se considera al sujeto de evidencia responsable de cualesquiera consecuencias de la utilización incorrecta de su clave. Los verificadores de evidencia pueden comprobar entonces que el plazo de tiempo permitido para la declaración de violación de clave ha concluido antes de aceptar cualquier evidencia.

8.7.1.2 Violación de clave de generación de TTP

Cuando se detecte la violación de una clave de TTP, debe procederse a la revocación de la misma. Si la clave de generación es una clave privada, se ha de revocar el certificado de clave pública correspondiente, lo que puede hacerse utilizando las listas de revocación de certificados definidas en la Rec. UIT-T X.509 | ISO/CEI 9594-8. Para el tratamiento de la evidencia generada anteriormente con la clave (posiblemente) violada, es preciso que la TTP mantenga un registro de auditoría de cada una de las utilizaciones de su clave. Si la clave de la TTP es violada, se pueden utilizar los registros de auditoría para solucionar disputas.

8.7.1.3 Sustitución de clave de verificación de entidad

Esta es una amenaza que acecha al usuario/verificador de evidencia que cree equivocadamente que tiene evidencia válida. Cuando se plantea una disputa precisa de arbitraje se descubre, sin embargo, que la evidencia no es válida. Es decir, el usuario de evidencia pierde porque actuó de buena fe en base a una evidencia aparentemente válida pero el árbitro dictamina en contra de él. Una posible manera de contrarrestar esta amenaza consiste en utilizar procedimientos fuertes para tener la seguridad de que la entidad correcta está asociada con la clave de verificación correcta. Si se produjera una sustitución, la clave de verificación errónea deberá ser eliminada tan pronto como la sustitución sea detectada.

8.7.1.4 Sustitución de clave de verificación de TTP

Si la clave de verificación es una clave pública utilizada por una TTP para verificar evidencia directamente, la TTP puede ser inducida engañosamente a aceptar evidencia falsificada falsificando lo que quiera que lleve la clave de verificación al árbitro (por ejemplo, un documento sobre papel, una cadena de certificados, etc.). Un ejemplo concreto de esto es el caso en el que la copia del árbitro de una clave pública es sustituida por un agresor.

Cuando se detecte un ataque de este tipo, deberá divulgarse la sustitución tanto como sea posible pero teniendo en cuenta que no siempre se podrá llegar a todos los usuarios de evidencia que utilizaron evidencia que podría haber sido verificada empleando la clave sustituida. Es posible determinar qué evidencia se verificó antes del aviso de la sustitución utilizando una autoridad de verificación de evidencia (por ejemplo, una autoridad de verificación de firmas) que mantenga un registro de auditoría de evidencia verificada. De este modo se puede saber qué evidencia se verificó antes y qué evidencia se verificó después del aviso.

Si la clave de verificación es una clave pública utilizada por usuarios de evidencia para verificar directamente certificados, deberá cambiarse tan pronto como se detecte la sustitución.

8.7.2 Compromiso de evidencia

Información que en su momento se aceptó como evidencia puede dejar de ser aceptable. A esa información se la denomina evidencia comprometida.

8.7.2.1 Modificación no autorizada o destrucción de evidencia

En este caso, ocurrió la acción o el evento, pero la parte a la que interesa rechazar el evento interviene para modificar o destruir la evidencia almacenada. A continuación puede lograr el rechazo de un evento que, de hecho, sí ocurrió. Frente a esta amenaza cabe protegerse empleando mecanismos de seguridad apropiados con los que se evite la modificación o destrucción de la evidencia (por ejemplo, el almacenamiento redundante). La utilización de una TTP para almacenar evidencia puede aportar una mejor protección contra esta amenaza ya que los medios de almacenamiento que tiene una TTP se pueden proteger mejor que los medios de almacenamiento del usuario de evidencia.

8.7.2.3 Destrucción o invalidación de evidencia

Se trata de la amenaza de que sea destruida la evidencia almacenada por la TTP. Esta amenaza puede surgir si la TTP no es suficientemente cuidadosa y no ha tomado medidas de salvaguardia adecuadas. Es posible protegerse contra esta amenaza utilizando mecanismos de no rechazo en los que toda la evidencia necesaria para resolver disputas sea almacenada por el usuario de evidencia. El usuario de evidencia puede garantizar entonces la no destrucción de la misma incluso si una TTP es mal intencionada o descuidada.

8.7.3 Falsificación de evidencia

8.7.3.1 Falsificación de evidencia por un intruso

En este caso, no ha ocurrido un evento disputado pero un intruso se introduce en el sistema y crea falsa evidencia de que sí ocurrió. Esta situación se puede plantear cuando interviene un notario. Pueden utilizarse mecanismos criptográficos para proteger evidencia almacenada contra su falsificación o modificación por un intruso.

8.7.3.2 Falsa verificación de evidencia

En los mecanismos en los que se utiliza una TTP para verificar evidencia, existe la amenaza de que la TTP diga al usuario de evidencia que ha validado la evidencia, cuando de hecho la evidencia no es válida. Si surge una disputa, el usuario de evidencia será incapaz de convencer al árbitro de que el evento disputado ha ocurrido. Es posible protegerse contra esta amenaza utilizando un mecanismo de no rechazo en el que el verificador de evidencia pueda verificar la evidencia directamente sin utilizar una TTP.

8.7.3.3 Falsificación de evidencia por tercera parte confiable

Esta amenaza consiste en que una tercera parte confiable podría falsificar evidencia para un evento que nunca ocurrió. Si el árbitro confiara en la TTP aceptaría la evidencia falsificada y, por tanto, sería inducido engañosamente a tomar una decisión incorrecta. Es posible protegerse contra esta amenaza utilizando un mecanismo de no rechazo con el que resulte difícil a las TTP falsificar evidencia, o asegurándose de que las TTP utilizadas son dignas de crédito y merecen confianza. En general, es difícil aportar evidencia irrefutable respecto a la fiabilidad de una entidad.

9 Interacción con otros servicios y mecanismos de seguridad

En esta cláusula se describe cómo pueden utilizarse otros servicios de seguridad en apoyo del no rechazo. No se examina aquí el uso del no rechazo como soporte de otros servicios de seguridad.

9.1 Autenticación

Cuando interactúen con una tercera parte confiable, las entidades quizás tengan que probar su identidad utilizando un servicio de autenticación. Los intercambios ulteriores necesitarán asegurarse empleando un servicio de autenticación del origen de los datos. Por ejemplo, cuando se utiliza una TTP para la generación de firma, cabe exigirle que autentique el sujeto de evidencia antes de generar la firma.

9.2 Control de acceso

Puede utilizarse un servicio de control de acceso para asegurar que la información almacenada por una TTP, o un servicio ofrecido por una TTP, únicamente se pone a disposición de las entidades autorizadas.

9.3 Confidencialidad

Pueden requerirse servicios de confidencialidad para proteger los datos contra su revelación no autorizada (incluyendo, en algunos casos, la revelación no autorizada por una TTP o a una TTP) y como protección también contra la revelación no autorizada de evidencia.

9.4 Integridad

Pueden requerirse servicios de integridad para asegurar la integridad de la evidencia.

Con el no rechazo con prueba de origen o el no rechazo con prueba de entrega también debe asegurarse la integridad de los datos para que no puedan modificarse, sin que se detecte, los datos transferidos entre un originador y un receptor.

9.5 Auditoría

Un usuario de evidencia puede utilizar la función de registro de auditoría para almacenar la evidencia y utilizarla posteriormente en caso de disputa.

Un notario o una TTP dentro de la línea puede utilizar la función de registro de auditoría para registrar el contenido, el origen, el destino y la hora de los mensajes.

9.6 Gestión de claves

Puede utilizarse un servicio de gestión de claves para proporcionar las claves que se utilizan en la generación de evidencia y la verificación de evidencia. Quizás se requiera que el servicio de gestión de claves proporcione claves para verificación de evidencia aun cuando haya dejado de estar disponible o de ser válida la clave correspondiente utilizada para la generación de evidencia.

Anexo A

No rechazo en el modelo de referencia básico de OSI

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

A.1 No rechazo con prueba de origen

El servicio de no rechazo con prueba de origen tiene por finalidad proteger al receptor de datos contra la falsa negación de originar datos o contra la falsa afirmación de que los datos habían sido modificados, por parte del originador. Esto puede conseguirse cuando el generador de evidencia (normalmente el originador de los datos, pero quizás una TTP) entrega al verificador de evidencia (normalmente el receptor de los datos, pero quizás una parte que representa al receptor) la evidencia de que los datos fueron enviados por el originador.

Cuando se utiliza un mecanismo de firma, la evidencia es una firma digital de los datos o una huella digital de los datos. El no rechazo con prueba de origen depende de un esquema para la provisión de evidencia validada convenida previamente. Consta de las siguientes etapas:

1) El peticionario del servicio de no rechazo genera evidencia u obtiene evidencia de una TTP y adjunta la firma a los datos.

2) La evidencia se pone a disposición del usuario de evidencia.

3) En caso de disputa, el usuario de evidencia aporta los datos y la evidencia; el árbitro confronta los datos con la evidencia.

A.2 No rechazo con prueba de entrega

El servicio de no rechazo con prueba de entrega tiene por finalidad proteger al originador de datos contra la falsa negación de haber recibido los datos o contra la falsa afirmación de que los datos recibidos no son como se enviaron, es decir, que han sido modificados, por parte del receptor. Esto puede conseguirse cuando el generador de evidencia (normalmente el receptor de los datos, pero quizás también una TTP) entrega al verificador de evidencia (normalmente el originador de los datos, pero quizás también una parte que representa al originador, o una TTP) la evidencia de que los datos fueron entregados.

Este servicio depende de la devolución, por el receptor de los datos, de un acuse de recibo que contenga evidencia. El acuse de recibo contendrá la confirmación de la recepción en forma de firma digital en el mensaje original (o una huella digital del mensaje original) en el momento de la recepción.

Cuando se utiliza un mecanismo de firma, se exige como evidencia un acuse de recibo firmado.

Pueden considerarse dos modalidades de este servicio, dependiendo de si una tercera parte confiable (TTP), que actúa en el cometido de autoridad de entrega, participa en apoyo del servicio.

Anexo B

Resumen de facilidades de no rechazo

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

<table>
<tr><td colspan="2" rowspan="2">Resumen de facilidades de seguridad</td><td>Elemento</td><td colspan="4">Entidad: Sujeto de evidencia, generador de evidencia, verificador de evidencia, usuario de evidencia, TTP de no rechazo, árbitro</td></tr>
<tr><td colspan="4">Objeto de información: Evidencia</td></tr>
<tr><td colspan="2"></td><td colspan="4">Objetivo de la entidad: Obtener, mantener, poner a disposición y validar evidencia irrefutable</td></tr>
<tr><td rowspan="8">ACTIVIDAD</td><td>Entidad</td><td colspan="4">TTP, autoridad de seguridad</td></tr>
<tr><td>Función</td><td colspan="4">(No definida)</td></tr>
<tr><td>Actividad relativa a la gestión</td><td colspan="4">– Instalar
– Modificar
– Suprimir
– Listar</td></tr>
<tr><td>Entidad</td><td>Generador de evidencia</td><td>Verificador de evidencia</td><td>TTP de no rechazo</td><td>Árbitro</td></tr>
<tr><td>Función</td><td>(No definida)</td><td>(No definida)</td><td>(No definida)</td><td>(No definida)</td></tr>
<tr><td>Actividad relativa a las operaciones</td><td>– Generar evidencia
– Generar evidencia notarizada</td><td>– Validar evidencia
– Generar evidencia notarizada</td><td>– Generar indicación de tiempo
– Transferir por medio de TTP</td><td>(No definida)</td></tr>
<tr><td rowspan="3">INFORMACIÓN</td><td>Elemento de datos de entrada/salida gestionado por SDA</td><td colspan="4">– Información de gestión (por ejemplo contraseñas o claves)
– Tipo de información
– Política de no rechazo</td></tr>
<tr><td>Tipo de información utilizada en la operación</td><td colspan="4">– Evidencia
– Firma digital
– Testigo de seguridad
– Certificado de seguridad
– Indicación de tiempo</td></tr>
<tr><td>Información de control</td><td colspan="4">Registro del evento en el registro de auditoría y los resultados del arbitraje en caso de disputa; informe de la relación entre entidades</td></tr>
</table>

Anexo C

No rechazo en los sistemas de almacenamiento y retransmisión

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

En los sistemas de almacenamiento y retransmisión, un mensaje es transferido entre su originador y su receptor por uno o más intermediarios, conocidos como *agentes de transferencia*. En estos sistemas, la transmisión de un mensaje consiste no sólo en la comunicación entre el originador y el receptor sino también en la comunicación entre el originador y un agente de transferencia, la comunicación entre el receptor y un agente de transferencia y la comunicación entre agentes de transferencia. El servicio de no rechazo puede aplicarse por separado en cada uno de los pasos que se llevan a cabo en el transporte del mensaje a su destino final.

El servicio de *no rechazo con prueba de origen* protege contra la falsa negación de un emisor de haber enviado el mensaje o su contenido. Bien el receptor o bien los agentes de transferencia pueden utilizar la evidencia obtenida por este servicio.

El servicio de *no rechazo con prueba de recepción* protege contra la falsa negación de un receptor de haber recibido un mensaje o su contenido. Bien el originador o bien los agentes de referencia pueden utilizar la evidencia obtenida por este servicio.

El servicio de *no rechazo con prueba de depósito* se utiliza para proteger contra la falsa negación de un agente de transferencia de haber aceptado un mensaje (del originador o de otro agente de transferencia) para su transmisión. El originador u otros agentes de transferencia son los usuarios de la evidencia obtenida por este servicio.

El servicio de *no rechazo con prueba de entrega* se utiliza para proteger contra la falsa negación de un agente de transferencia de haber afirmado que ha entregado un mensaje (al receptor o a otro agente de transferencia). El originador es el usuario de la evidencia obtenida por este servicio.

El servicio de *no rechazo con prueba de transferencia* se utiliza para proteger contra la falsa negación de un agente de transferencia de haber aceptado la responsabilidad de la entrega de un mensaje. Este servicio se utiliza cuando participa más de un agente de transferencia en la entrega de un mensaje. Cuando el agente de transferencia que aceptó el mensaje en un primer momento se lo pasa a un segundo agente de transferencia, éste puede proporcionar al primero evidencia de que ha aceptado la responsabilidad del mensaje. Cuando participan más de dos agentes de transferencia, este servicio también puede utilizarse entre el segundo y el tercer agente, y así sucesivamente.

El uso de estas diferentes formas de servicio de no rechazo se resume en el cuadro siguiente:

Nombre del servicio	Protege frente al	Utilizado por el
Prueba de origen	originador	receptor, agente de transferencia
Prueba de depósito	agente de transferencia	originador
Prueba de entrega	agente de transferencia	originador
Prueba de transferencia	agente de transferencia	agente de transferencia
Prueba de recepción	receptor	originador, agente de transferencia

Estas modalidades adicionales del servicio de no rechazo (prueba de depósito, transferencia y entrega) pueden proporcionarse contemplando el sistema a un nivel de granularidad diferente, y utilizando entonces mecanismos que proporcionan formas más fundamentales del servicio de no rechazo (prueba de origen y prueba de recepción). Por ejemplo, la prueba de entrega puede realizarse mejorando la transmisión de un mensaje de un originador a un receptor en una secuencia de intercambios de mensajes, uno de los cuales es un reconocimiento de entrega de un agente de transferencia al originador, y utilizando a continuación el servicio de prueba de origen para proteger este reconocimiento.

Anexo D

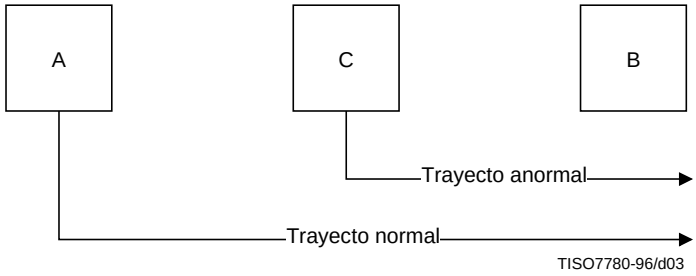
Recuperación en un servicio de no rechazo

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

La recuperación de seguridad se refiere a las situaciones que no deberían ocurrir en circunstancias normales. La realidad de la seguridad informática es, sin embargo, que se producen circunstancias anormales y es mejor prepararse para esa eventualidad.

En concreto, muchos mecanismos de no rechazo dependen de claves criptográficas y de la discreción necesaria para protegerlas. La pérdida o revelación de una clave criptográfica debe preverse con un plan de recuperación para su aplicación inmediata.

Podría darse la siguiente situación cuando se utilizan claves criptográficas privadas para un servicio de no rechazo:



Los datos firmados por una participante fraudulenta (C), que utiliza la clave privada violada de A, pueden comunicarse a un participante honrado (B). Puede suponerse que en algún momento B tendrá motivo para llegar hasta A a consecuencia de una acción (u omisión) relacionada con un mensaje no autorizado, presentando el mensaje firmado como justificación de la acción. A afirmará haber perdido la clave privada en cuestión y emitirá una declaración pública al respecto.

Si se pone en conocimiento de un juez o árbitro, se determinará la responsabilidad de A, comparando la diferencia temporal entre la declaración pública de pérdida de la clave y el mensaje firmado no autorizado. Lo más probable es que se considere responsable a A si el mensaje es anterior a la declaración de pérdida de la clave. Por ello, si C ha fechado el mensaje con anterioridad, se considerará responsable a A, a menos que se hayan tomado medidas para afrontar la situación.

Para recuperarse de esta situación es necesario estar en condiciones de conocer cuándo se firmó exactamente el mensaje. Como no puede confiarse en la referencia temporal del mensaje de C, es necesario invocar a una tercera parte confiable y registrar formalmente el mensaje por uno de estos dos medios:

- copiando el mensaje y la firma en un registro de auditoría de seguridad adecuado (es decir, utilizando un notario); y/o
- aplicando una contrafirma al mensaje que incluya la fecha y hora del registro, obtenida de una tercera parte confiable (TTP) independiente (es decir, un servicio de indicación de tiempo).

Si se sigue este procedimiento, un participante fraudulento documentará sin darse cuenta la fecha y hora real de la firma. Un árbitro podría emitir entonces una opinión de responsabilidad a la parte lesionada (A) en función de lo siguiente:

en primer lugar, una comparación entre la fecha/hora del mensaje y la fecha/hora de la contrafirma que deben situarse en un margen de tiempo bastante estrecho (por ejemplo 24 horas);

en segundo lugar, una comparación entre la fecha/hora del mensaje y la notificación de la clave perdida o violada.

De este modo, el uso indebido de una clave criptográfica perdida o violada se reducirá al margen de tiempo concedido para el registro de los datos por el servicio de indicación de tiempo.

La responsabilidad de A en caso de violación de una clave depende de la política de seguridad en vigor. Las rupturas de la seguridad no siempre se detectan inmediatamente. Por ello, incluso si la parte A informa a la TTP de una violación en cuanto se percata de ella, es posible que la parte C falsee mensajes tras violar la clave privada de A y antes de que A lo detecte.

Al resolver disputas, los dos momentos que se indican a continuación son importantes:

- El momento en que A informó de la violación – A rechazará todos los mensajes de los que pueda demostrarse que fueron firmados después de ese momento. (A deberá dejar de utilizar la clave privada tan pronto como se entere de que ha sido violada).
- El momento que, según A, es anterior a la violación de la clave – A no rechazará los mensajes de los que pueda demostrarse que fueron firmados antes de ese momento. Quizás ese momento no exista. A puede haber descubierto la violación, pero no estar segura de cuando se produjo efectivamente.

Anexo E

Interacción con el directorio

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

Una firma digital puede ser verificada utilizando una clave pública apropiada. Cuando la clave pública está incluida en un certificado de usuario ubicado en el directorio, puede verificarse la corrección de la clave siempre que se conozca la clave pública de la autoridad de certificación.

Como la autoridad de certificación que emitió un certificado puede haber cambiado su clave pública desde que se preparó el certificado, es necesario contar con un medio de verificar la corrección de una clave pública «vencida». Puesto que la única clave conocida normalmente es la clave pública vigente de una autoridad de certificación (CA, *certification authority*) tiene que haber un enlace entre la clave pública vigente y las claves públicas vencidas. Un receptor no está al corriente de los cambios de claves de una CA, por lo que corresponde a las diferentes autoridades de certificación proporcionar una manera de verificar sus certificados «antiguos». Esto puede hacerse de dos maneras:

- certificando toda clave pública de la CA vencida mediante la clave pública de la CA vigente; o bien
- certificando toda clave pública de la CA vencida mediante la clave pública de la CA siguiente.

En el primer caso, es posible verificar directamente la validez de la clave pública antigua de la CA correspondiente a la clave privada utilizada por la autoridad de certificación para emitir el certificado original.

En el segundo caso, es necesario estar en condiciones de recopilar una cadena de certificados, para verificar paso a paso la validez de la clave pública antigua de la CA. Esto se llevará a cabo buscando en primer lugar el certificado con un periodo de validez correspondiente a la fecha/hora del mensaje firmado y buscando a continuación, de manera recursiva, un certificado con un periodo de validez coincidente pero más reciente para encontrar el valor de la clave pública anterior de la CA.

NOTA – En el caso de que exista la posibilidad de violación de una clave pública antigua de la CA, es preferible el primer método porque, con el segundo, se rompería la cadena de certificados hacia la clave pública más antigua de la CA, con lo que se invalidarían implícitamente claves públicas más antiguas de la CA.

No es tarea de la autoridad de certificación mantener un registro de las listas de revocación de las demás autoridades de certificación o de sus usuarios o certificados cuando expira su validez. Por el contrario, un usuario de evidencia tiene que recopilar toda la información necesaria (esto es, incluidas las listas de revocación, incluso si están vacías) cuando aún está disponible, para probar que una determinada clave pública era válida en alguna fecha.

Un certificado de revocación contiene la fecha en que ha sido emitido por la autoridad. También contiene otra fecha que puede ayudar a resolver las disputas en algunos casos: la fecha en que el usuario aún tenía la seguridad de que no se había violado su clave. A este respecto, todas las firmas emitidas por el usuario antes de esta fecha serán reconocidas como válidas por el usuario. En el peor de los casos, sin esta fecha, todas las firmas emitidas durante el periodo de validez de la firma se considerarían no válidas. En un entorno comercial puede ser muy importante para un usuario que aún se reconozca como válido un documento firmado incluso en el caso en que se haya perdido la clave utilizada para firmar el mensaje. La presencia de esta fecha opcional en un certificado de revocación, pero es obligatoria cuando la clave del certificado correspondiente puede utilizarse para un servicio de no rechazo.

Las relaciones de confianza pueden variar con el tiempo. Por ejemplo, un árbitro puede confiar hoy en una CA pero no necesariamente mañana. Tiene que existir este tipo de confianza para que un receptor pueda conocer si una disputa potencial puede resolverse o no en beneficio propio. Debe expresarse qué tipo de relaciones de confianza reconoce un determinado árbitro. Estas condiciones de confianza pueden modelarse utilizando las siguientes expresiones:

- autoridades de certificación de confianza plena y cuya clave pública vigente se conoce;
- autoridades de certificación de confianza para emitir tanto certificados de CA como certificados de usuario;
- autoridades de certificación de confianza únicamente para emitir certificados de usuario (pero no certificados de CA).

Esta información tiene que estar a libre disposición del usuario de evidencia. Puede adoptar la forma de un certificado de seguridad que incluya un periodo de validez. Se definen dos formas de certificados de confianza: certificados de confianza en los que es responsabilidad del árbitro mantener su registro y certificados de confianza en los que dicha responsabilidad corresponde receptor.

Anexo F

Bibliografía

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

– Recomendación UIT-T X.402 (1995) | ISO/CEI 10021-2:1996, *Tecnología de la información – Sistemas de tratamiento de mensajes: Arquitectura global*.

– Recomendación X.435 del CCITT (1991), *Sistemas de tratamiento de mensajes: Sistemas de mensajería con intercambio electrónico de datos*.

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

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie B	Medios de expresión: definiciones, símbolos, clasificación
Serie C	Estadísticas generales de telecomunicaciones
Serie D	Principios generales de tarificación
Serie E	Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos
Serie F	Servicios de telecomunicación no telefónicos
Serie G	Sistemas y medios de transmisión, sistemas y redes digitales
Serie H	Sistemas audiovisuales y multimedios
Serie I	Red digital de servicios integrados
Serie J	Transmisiones de señales radiofónicas, de televisión y de otras senales multimedios
Serie K	Protección contra las interferencias
Serie L	Construcción, instalación y protección de los cables y otros elementos de planta exterior
Serie M	Mantenimiento: sistemas de transmisión, circuitos telefónicos, telegrafía, facsímil y circuitos arrendados internacionales
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Calidad de transmisión telefónica, instalaciones telefónicas y redes locales
Serie Q	Conmutación y señalización
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios de telegrafía
Serie T	Terminales para servicios de telemática
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
Serie X	**Redes de datos y comunicación entre sistemas abiertos**
Serie Z	Lenguajes de programación