UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

UIT-T X.842

(10/2000)

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

SERIE X: REDES DE DATOS Y COMUNICACIÓN ENTRE SISTEMAS ABIERTOS

Seguridad

Tecnología de la información – Técnicas de seguridad – Directrices sobre el uso y gestión de servicios a tercera parte confiable

Recomendación UIT-T X.842

(Anteriormente Recomendación del CCITT)

RECOMENDACIONES UIT-T DE LA SERIE X

REDES DE DATOS Y COMUNICACIÓN ENTRE SISTEMAS ABIERTOS

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 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	
Generalidades	X.300–X.349
Sistemas de transmisión de datos por satélite	X.350–X.369
Redes basadas en el protocolo Internet	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.629
Eficacia	X.630–X.639
Calidad de servicio	X.640–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	
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 y funciones de arquitectura de gestión distribuida abierta	X.730–X.799
SEGURIDAD	**X.800–X.849**
APLICACIONES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	
Compromiso, concurrencia y recuperación	X.850–X.859
Procesamiento 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.

NORMA INTERNACIONAL ISO/CEI TR 14516
RECOMENDACIÓN UIT-T X.842

TECNOLOGÍA DE LA INFORMACIÓN – TÉCNICAS DE SEGURIDAD – DIRECTRICES SOBRE EL USO Y GESTIÓN DE SERVICIOS A TERCERA PARTE CONFIABLE

Resumen

Esta Recomendación | Informe técnico proporciona una orientación para el uso y gestión de los servicios a tercera parte confiable (TTP), una definición clara de las funciones y servicios básicos prestados, sus descripciones y finalidades, y los cometidos y responsabilidades de las TTP y las entidades que utilizan sus servicios.

Esta Recomendación | Informe técnico identifica diferentes categorías principales de servicios TTP que incluyen la identificación de tiempo, el no repudio, la gestión de claves, la gestión de certificados, y la notaría pública electrónica.

Orígenes

La Recomendación UIT-T X.842, preparada por la Comisión de Estudio 7 (1997-2000) del UIT-T, fue aprobada por la Asamblea Mundial de Normalización de las Telecomunicaciones (Montreal, 27 de septiembre-6 de octubre de 2000). Se publica también un texto idéntico como Norma Internacional ISO/CEI TR 14516.

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. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución 1 de la AMNT.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI.

NOTA

En esta Recomendación, la expresión "Administración" se utiliza para designar, en forma abreviada, tanto una administración de telecomunicaciones como una empresa de explotación reconocida de telecomunicaciones.

PROPIEDAD INTELECTUAL

La UIT señala a la atención la posibilidad de que la utilización o aplicación de la presente Recomendación suponga el empleo de un derecho de propiedad intelectual reivindicado. La UIT no adopta ninguna posición en cuanto a la demostración, validez o aplicabilidad de los derechos de propiedad intelectual reivindicados, ya sea por los miembros de la UIT o por terceros ajenos al proceso de elaboración de Recomendaciones.

En la fecha de aprobación de la presente Recomendación, la UIT no ha recibido notificación de propiedad intelectual, protegida por patente, que puede ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los usuarios que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar la base de datos sobre patentes de la TSB.

ÍNDICE

Página

Introducción

La consecución de niveles adecuados de confianza empresarial en la explotación de sistemas IT se soporta en la disposición de controles técnicos y legales apropiados y prácticos. Las empresas deben tener confianza en que los sistemas IT les ofrecerán ventajas positivas y en que podrán contar con que dichos sistemas soportarán compromisos comerciales y crearán oportunidades de negocio.

Un intercambio de información entre dos entidades implica la existencia de un elemento de confianza donde, por ejemplo, el receptor supone que la identidad del emisor es realmente la del emisor, y a su vez, el emisor supone que la identidad del receptor es realmente la del receptor al que está destinada la información. Puede ocurrir que este "elemento de confianza implícito" no sea suficiente y se necesite utilizar una tercera parte confiable (TTP) para facilitar el intercambio fiable de la información.

El cometido de las TTP incluye proporcionar la seguridad de que los mensajes y transacciones comerciales y de otro tipo dignos de confianza (por ejemplo, los referentes a actividades gubernamentales) se transfieren al receptor deseado, en la ubicación correcta, y que estos mensajes se reciben de manera exacta y oportuna en el tiempo, y que para cualquier controversia comercial que pueda surgir existen métodos apropiados que permiten la creación y entrega de la evidencia requerida para probar lo que ha ocurrido. Los servicios prestados por las TTP pueden incluir los necesarios para la gestión de claves, gestión de certificados, soporte de identificación y autenticación, servicio de atributo de privilegio, no repudio, servicios de indicación de tiempo, servicios de notaría publica electrónica y servicios de directorio. Las TTP pueden prestar algunos de estos servicios o todos.

Una TTP ha de ser concebido, implementado y explotado para proporcionar seguridad a los servicios de seguridad que presta, y satisfacer los requisitos legales y reglamentarios aplicables. Los tipos y niveles de protección adoptados o requeridos variarán de acuerdo con el tipo de servicio prestado y con el contexto dentro del que opera la aplicación comercial.

El objetivo de este informe técnico es proporcionar:

a) Directrices destinadas a los gestores, realizadores y personal de explotación de las TTP, así como a la asistencia a los mismos en el uso y gestión de las TTP; y

b) Directrices destinadas a entidades en relación con los servicios prestados por las TTP, y sobre los respectivos cometidos y responsabilidades de las TTP y de las entidades que utilizan sus servicios.

Son aspectos adicionales tratados en esta Recomendación | Informe técnico los de proporcionar:

a) Una visión de conjunto de la descripción de los servicios prestados;

b) Una comprensión del cometido de las TTP y sus características funcionales;

c) Una base para el reconocimiento mutuo de servicios prestados por TTP diferentes; y

d) Una directriz sobre el interfuncionamiento entre entitades y las TTP.

INFORME TÉCNICO ISO/CEI TR 14516
RECOMENDACIÓN UIT-T X.842

TECNOLOGÍA DE LA INFORMACIÓN – TÉCNICAS DE SEGURIDAD – DIRECTRICES SOBRE EL USO Y GESTIÓN DE SERVICIOS A TERCERA PARTE CONFIABLE

1 Alcance

Con la provisión y operación de un servicio de tercera parte confiable (TTP, *trusted third party*) están asociados algunos temas relacionados con la seguridad para lo cuales se necesitan directrices generales destinadas a ayudar a las entidades comerciales, y a los realizadores y proveedores de sistemas y servicios., etc. Incluyen las orientaciones sobre los cometidos, posiciones y relaciones de las TTP y con las entidades que utilizan los servicios TTP, los requisitos de seguridad genéricos, quién debe proporcionar cada tipo de seguridad, cuales son las posibles soluciones de seguridad, y el uso y gestión operacionales de la seguridad de los servicios TTP.

Esta Recomendación | Informe técnico proporciona una directriz sobre el uso y gestión de las TTP, una definición clara de las funciones y servicios básicos prestados, sus descripciones y fines, y los cometidos y responsabilidades civiles de las TTP y de las entidades que utilizan sus servicios. Se destina en primer lugar a los gestores y realizadores de sistemas, a los operadores de las TTP y a los usuarios de las empresas en la selección delos servicios TTP necesarios para exigencias concretas, su gestión, uso y despliegue operacional subsiguientes, así como al establecimiento de una política de seguridad dentro de una TTP. No se pretende que se utilice como base de la evaluación formal de una TTP ni para comparar diversas TTP.

Este documento identifica diferentes categorías principales de los servicios TTP que incluyen: la identificación de tiempo, el no repudio, la gestión de claves, la gestión de certificados y la notaría pública electrónica. Cada una de estas categorías principales comprende varios servicios que están lógicamente agrupados.

2 Referencias normativas

2.1 Recomendaciones | Normas Internacionales idénticas

- Recomendación UIT-T X.509 (2001) | ISO/CEI 9594-8:2001, *Tecnología de la Información – Interconexión de sistemas abiertos – El directorio: Marcos para certificados de claves públicas y de atributos*.
- 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*.
- Recomendación UIT-T X.813 (1996) | ISO/CEI 10181-4:1997, *Tecnología de la Información – Interconexión de sistemas abiertos – Marcos de seguridad en sistemas abiertos: Marco de no rechazo*.

2.2 Pares de Recomendaciones | Normas Internacionales de contenido técnico equivalente

- Recomendación CCITT X.800 (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 9798-1:1997, *Information technology - Security techniques - Entity authentication - Part 1: General*.
- ISO/CEI 11770-1:1996, *Information technology - Security techniques - Key management - Part 1: Framework*.
- ISO/CEI 11770-2:1996, *Information technology - Security techniques - Key management - Part 2: Mechanisms using symmetric techniques*.
- ISO/CEI 11770-3:1999, *Information technology - Security techniques - Key management - Part 3: Mechanisms using asymmetric techniques*.
- ISO/CEI TR 13335-1:1996, *Information technology - Guidelines for the management of IT Security (GMITS): Part 1 - Concepts and models of IT Security*.

- ISO/CEI TR 13335-2:1997, *Information technology - Guidelines for the management of IT Security (GMITS): Part 2 - Managing and planning IT Security*.
- ISO/CEI TR 13335-3":1998, *Information technology - Security techniques - Guidelines for the management of IT Security (GMITS): Part 3 - Techniques for the management of IT Security*.
- ISO/CEI TR 13335-4:2000, *Information technology - Security techniques - Guidelines for the management of IT Security (GMITS): Part 4 - Selection of Safeguards*.
- ISO/CEI 13888-1:1997, *Information technology - Security techniques - Non-repudiation - Part 1: General*.
- ISO/CEI 13888-2:1998, *Information technology - Security techniques - Non-repudiation - Part 2: Mechanisms using symmetric techniques*.
- ISO/CEI 13888-3:1997, *Information technology - Security techniques - Non-repudiation - Part 3: Mechanisms using asymmetric techniques*.
- ISO/CEI WD 15443, *Information technology - Security techniques – A framework for IT security assurance*.

3 Definiciones

NOTA – A lo largo de esta Recommendation | Informe técnico el término entidad se puede referir a un ser humano, una organización, un componente de soporte físico o un elemento de soporte lógico.

A los fines de esta Recommendation | Informe técnico se aplican las definiciones dadas en la Rec. CCITT X.800 e ISO 7498-2: control de acceso, responsabilidad, auditoría, registro de pistas de auditoría, disponibilidad, confidencialidad, integridad de los datos, descifrado, firma digital, cifrado, autenticación de entidad, integridad, clave, gestión de claves, actuación notarial, no repudio, auditoría de seguridad, pista de auditoría de seguridad y firma.

A los fines de esta Recommendation | Informe técnico se aplican las definiciones dadas en ISO 8402: auditoría/evaluación.

A los fines de esta Recommendation | Informe técnico se aplican las definiciones dadas en la Rec. UIT-T X.509 | ISO/CEI 9594-8: certificado de atributos, certificado y autoridad de certificación (CA, *authority certification*).

A los fines de esta Recommendation | Informe técnico se aplican las definiciones dadas en ISO/CEI 9798-1: testigo.

A los fines de esta Recommendation | Informe técnico se aplican las definiciones dadas en ISO/CEI 9798-5: autoridad de acreditación.

A los fines de esta Recommendation | Informe técnico se aplican las definiciones dadas en la Rec. UIT-T X.810 | ISO/CEI 10181-1: clave privada, clave pública, sellado, clave secreta y tercero de confianza.

A los fines de esta Recommendation | Informe técnico se aplican las definiciones dadas en la Rec. UIT-T X.811 | ISO/CEI 10181-2: certificado de autenticación e información de autenticación (AI, *authentication information*).

A los fines de esta Recommendation | Informe técnico se aplican las definiciones dadas en la Rec. UIT-T X.813 | ISO/CEI 10181-4: generador de evidencias y notaría.

A los fines de esta Recommendation | Informe técnico se aplican las definiciones dadas en ISO/CEI 11770-1: técnica criptográfica asimétrica, técnica criptográfica simétrica e indicación de tiempo.

A los fines de esta Recommendation | Informe técnico se aplican las definiciones dadas en el Informe técnico de ISO/CEI 13335-1: activo, autenticidad, impacto, seguridad de la tecnología de la información (IT, *information technology*), política de seguridad IT, fiabilidad, riesgo residual, riesgo, análisis de riegos, gestión de riesgos, salvaguarda, integridad del sistema, peligro y vulnerabilidad.

A los fines de esta Recommendation | Informe técnico se aplican las definiciones dadas en el Informe técnico de ISO/CEI 13888-1: no repudio de aprobación, no repudio de creación, no repudio de entrega, no repudio de acuse de recibo, no repudio de origen, no repudio de recepción, no repudio de emisión, no repudio de presentación y no repudio de transporte.

A los fines de esta Recommendation | Informe técnico se aplican las definiciones adicionales siguientes:

3.1 autoridad de atributos (AA, *attribute authority*): Entidad aceptada como fiduciaria por una o más entidades para crear y firmar certificados de atributos. Se señala que una CA puede ser también una AA.

3.2 autoridad de registro (RA, *registration authority*): Entidad responsable de la identificación y autenticación de sujetos de certificados, pero que no es una CA ni una AA, y por tanto no firma ni expide certificados. Una RA puede ayudar en el proceso de aplicación de certificados, en el proceso de revocación de certificados, o en ambos.

4 Aspectos generales

Una tercera parte confiable (TTP, *trusted third party*) es una organización, o su agente, que proporciona uno o más servicios de seguridad, y es aceptada como fiduciaria por otras entidades con respecto a actividades relacionadas con estos servicios de seguridad.

Una TTP se utiliza para ofrecer servicios de valor añadido a entidades que desean mejorar la confianza y confidencialidad comercial de los servicios que reciben, así como para facilitar comunicaciones seguras entre los partícipes de las transacciones comerciales. Las TTP han de ofrecer valor añadido en cuando a la confidencialidad, integridad y seguridad de los servicios y la información involucrados en las comunicaciones entre aplicaciones comerciales. Las TTP deben poder interoperar entre sí y con las entidades.

Las entidades deben poder elegir la TTP que les prestará los servicios requeridos. A su vez, las TTP deben poder elegir las entidades a las prestarán sus servicios.

Para resultar eficaces, las TTP deben, por lo general:

a) operar dentro de un marco legal que sea coherente entre las entidades participantes;

b) ofrecer una gama de servicios que comprenda unos servicios mínimos claramente definidos;

c) tener políticas definidas, en particular una política de seguridad pública;

d) ser gestionados y explotados de manera segura y fiable, en base a un sistema de gestión de la seguridad de la información y sistemas de tecnología de la información (IT) fiables;

e) cumplir las normas nacionales e internacionales cuando sean aplicables;

f) seguir un código de actuación de elevada aceptación;

g) publicar declaraciones de práctica;

h) registrar y archivar toda forma de evidencia que interese para sus servicios;

i) permitir un arbitraje independiente, sin comprometer la seguridad;

j) ser independientes e imparciales en su funcionamiento (por ejemplo, en cuanto a las reglas de acreditación); y

k) asumir la responsabilidad profesional y civil dentro de los límites definidos en cuanto a la disponibilidad y la calidad del servicio.

4.1 Bases de la garantía de seguridad y de la confianza

El uso de una TTP y sus servicios se basa en la observación fundamental de que en los servicios prestados por la TTP sólo confiarán otras TTP y otras entidades. Esta confianza resulta de la seguridad de que la TTP es gestionada correctamente y de que sus servicios se prestan de manera segura. Por ello, deberá garantizarse que la propia TTP y sus servicios están de acuerdo con las políticas definidas. La política de seguridad especialmente debe abarcar todos los aspectos de la seguridad relacionados con la gestión de la TTP y la prestación de los servicios.

La confianza puede establecerse por la evidencia de los aspectos de la TTP relacionados con la gestión y el funcionamiento. Deberá evidenciarse que los aspectos de la gestión son los adecuados y suficientes para alcanzar plenamente los objetivos, que el sistema de gestión es eficaz y apropiado para reducir al mínimo los riesgos y contrarrestar los peligros, y que las salvaguardas están documentadas y las conoce el personal, no han quedado obsoletas ni invalidada y se implementan correctamente.

Para ganar confianza en los aspectos relativos a la gestión y el funcionamiento de la TTP, deberá sobre todo aportar evidencia en el sentido de que:

a) se ha establecido una política de seguridad adecuada;

b) la solución de los problemas de seguridad se ha acometido mediante una combinación de procedimientos y mecanismos de seguridad implementados correctamente;

c) el funcionamiento se lleva a cabo correctamente y asignando un conjunto claramente definido de cometidos y responsabilidades;

d) las interfaces y procedimientos de comunicación con entidades son adecuados a las funciones que han de realizarse y se utilizan correctamente;

e) la gestión y el personal siguen las reglas y regulaciones con un nivel elevado de responsabilidad establecido o fijado como objetivo;

f) la calidad de los procesos, las operaciones y las practicas de trabajo ha sido acreditada adecuadamente;

g) la TTP cumple sus obligaciones contractuales de acuerdo con un contrato formal acordado con sus usuarios;

h) hay un conocimiento y una aceptación claros de los aspectos relativos a la responsabilidad civil;

i) se mantiene y verifica el cumplimiento de las leyes y regulaciones;

j) están claramente identificados los peligros conocidos y las salvaguardas para mitigar dichos peligros;

k) se realiza inicialmente una evaluación de peligros y riesgos, y se revisa y actualiza periódicamente esta evaluación para garantizar que se cumplen los requisitos de confidencialidad, integridad, disponibilidad y fiabilidad;

l) se cumplen las medidas organizativas y de personal;

m) puede contarse con la confianza de la TTP y dicha confianza se puede comprobar y verificar; y

n) la TTP es supervisada por alguna autoridad administrativa que vigila el que su funcionamiento se mantiene dentro de las reglas de su acreditación.

En la cláusula 5, Aspectos relativos a la gestión y el funcionamiento de una TTP, se examinan estos temas con detalles.

Los distintos tipos de negocios y las diferentes aplicaciones precisarán distintos niveles de confianza y pueden requerir distintos niveles de robustez en los mecanismos y procedimientos de protección aplicados. Por ejemplo, el nivel de confianza requerido para la autenticación de las transacciones administrativas puede ser diferente del que se necesita para las transacciones financieras, el cual puede a su vez ser distinto del requerido en algunas aplicaciones militares. Los diferentes niveles de confianza se derivan de normas y políticas de seguridad distintas, y de la medida en que estas se implementan correctamente.

4.2 Interacción entre una TTP y las entidades que utilizan sus servicios

Desde el punto de vista de la comunicación, la disposición del emplazamiento de las TTP y de las entidades puede adoptar diferentes configuraciones: dentro de línea, en línea y fuera de línea. En 4.2.1 a 4.2.3 se da un ejemplo de cada configuración.

Algunos servicios TTP pueden estar basados en diferentes configuraciones, por lo que la configuración que se adopte repercutirá en los servicios que la TTP sea capaz de prestar, por ejemplo, la oportunidad del intercambio, la denegación del servicio, el registro de prueba, y sus características, tales como el retardo en la revocación de un certificado.

4.2.1 Servicios de TTP dentro de línea

Se necesita una TTP dentro de línea cuando dos o más entidades pertenecen a diferentes dominios de seguridad y no utilizan el mismo mecanismo de seguridad. En este caso las entidades no pueden realizar intercambios directos y seguros. Sin embargo, una TTP ubicado justamente en el trayecto de comunicación entre las entidades puede facilitar intercambios seguros entre estas entidades, tal como se ilustra en la figura 1.

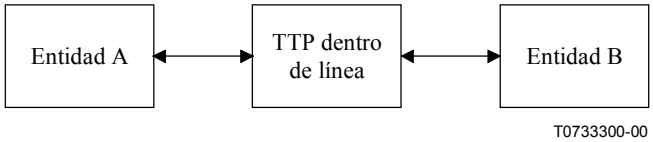


Figura 1 – Servicios de TTP dentro de línea entre entidades

Los servicios de TTP dentro de línea pueden incluir los servicios de autenticación, traslación y atributo de privilegio, y la TTP puede desempeñar un cometido en el aprovisionamiento de los servicios de no repudio, control de acceso, recuperación de claves, confidencialidad e integridad de los datos transmitidos.

4.2.2 Servicios de TTP en línea

Cuando una o ambas entidades solicitan a una TTP en línea o registro de información relativa a la seguridad, la TTP interviene en todos los primeros intercambios de seguridad entre las entidades. Sin embargo, la TTP no es requerida para los intercambios siguientes y no está posicionada en el trayecto de comunicación entre las entidades, tal como se ilustra en la figura 2.

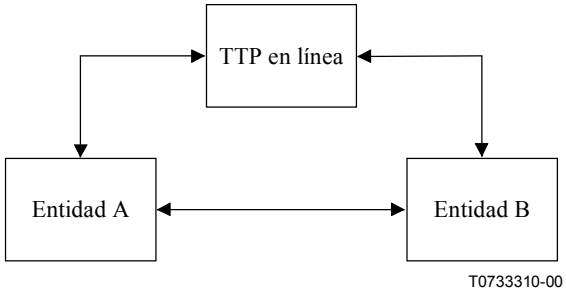


Figura 2 – Servicios de TTP en línea entre entidades

Los servicios de TTP en línea pueden incluir los servicios de autenticación, certificación y atributo de privilegio, y la TTP puede desempeñar un cometido en el aprovisionamiento de los servicios de no repudio, control de acceso, gestión de claves, entrega de mensajes, indicación de tiempo, confidencialidad e integridad.

4.2.3 Servicios de TTP fuera de línea

Un tercer tipo de disposición para el aprovisionamiento de servicios TTP es la configuración fuera de línea. La TTP no interactúa directamente con las entidades durante el proceso de intercambios seguros entre las entidades. En su lugar, las entidades utilizan los datos generados previamente por la TTP, tal como se ilustra en la figura 3 con línea de puntos.

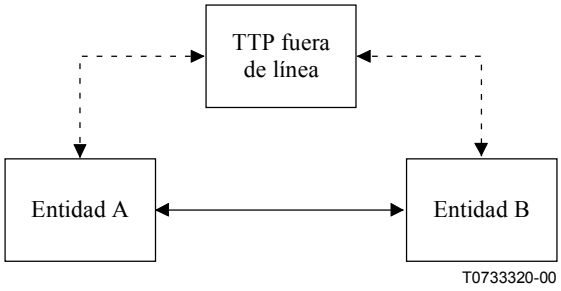


Figura 3 – Servicios de TTP fuera de línea entre entidades

Los servicios de TTP fuera de línea pueden incluir los servicios de autenticación, certificación, atributo de privilegio, no repudio, distribución de claves y recuperación de claves.

4.3 Interfuncionamiento de los servicios TTP

Una TTP puede ofrecer los diversos servicios que se describen en la cláusula 7. Todos los servicios pueden ser prestados por una sola TTP o prestados por más de una TTP. También pueden prestarse desde uno o más lugares. En este último caso, las obligaciones y los deberes deberán definirse y establecerse en un contrato formal, y deberán tenerse en cuenta las repercusiones de tipo técnico y organizativo. Dependiendo de la arquitectura de la TTP (responsabilidad y ubicación), puede haber requisitos adicionales, relacionados sobre todo con la seguridad, que habrán de ser considerados por la gestión de la TTP.

NOTA – Cada servicio puede tener requisitos de seguridad específicos que deberán cumplirse. Por lo general se recomienda que, si es posible, se dividan los aspectos de gestión y operativos de una TTP en aspectos generales y específicos relacionados con cada servicio. Un sistema de gestión con estructura modular se maneja mucho más fácilmente cuando se producen cambios, sobre todo la identificación de las muy importantes consecuencias que tiene, en materia de seguridad, la introducción de modificaciones.

5 Aspectos relativos a la gestión y la explotación de una TTP

Para la gestión y explotación de una TTP debe disponerse de una estrategia de paraguas que tenga en cuenta los aspectos que se examinan en las subcláusulas a continuación. El compromiso de una TTP de prestar servicios relativos a la seguridad debe tomar la forma de una política documentada formalmente. Se recomienda que una TTP opere según unas directrices en la protección de sus servicios. En el Informe Técnico de ISO/CEI 13335-1, 13335-2, 13335-3 y anexos A-H de 13335-4. Se pueden encontrar directrices generales para la gestión de la seguridad de la tecnología de la información (GMITS).

Se han tomado numerosas decisiones, que dependen de los servicios prestados por una TTP. Es preciso definir políticas no solamente para los servicios, sino también políticas más específicas, tales como las de creación y de validación de firmas. Unas y otras tendrán implicaciones y consecuencias de tipo técnico que deberán ser consideradas previamente. Además, existen interdependencias entre equipos técnicos y no técnicos, por ejemplo, la prestación de servicios de directorio mediante el protocolo de estado de certificado en línea o la lista de revocación de certificados. Todos esos factores llevarán a implementaciones técnicas y tendrán consecuencias que deberán quedar reflejadas por adelantado. En "Internet X.509 Public Key Infrastructure, RFC 2527: Certificate Policy and Certification Practice Framework" figura un ejemplo de política de seguridad referida a los certificados de claves públicas.

5.1 Aspectos legales

Además de la exactitud básica de los servicios concretos proporcionados, por ejemplo, el tiempo exacto para una autoridad de indicación de tiempo, una TTP heredará amplias responsabilidades derivadas de las expectativas de sus usuarios. Estas responsabilidad incluirán disposiciones sin fisuras con relación a la confidencialidad, integridad, disponibilidad, control de acceso, rendición de cuentas; autenticidad, fiabilidad, privacidad, aspectos éticos (como el uso legítimo), aspectos legales (esto es, leyes y reglamentos), técnicas y mecanismos, y aspectos financieros. La dejación accidental o deliberada de estas responsabilidades por parte de una TTP puede ocasionar pérdidas substanciales a sus usuarios, los cuales tratarán de recuperarlas de la TTP. Para gestionar las expectativas de sus usuarios y limitar su responsabilidad civil, debe establecerse un contrato claramente definido y legalmente vinculante entre la TTP y sus usuarios. Este contrato debe recoger como mínimo los aspectos legales relativos a los siguientes temas:

a) responsabilidad civil;

b) privacidad, sobre todo en relación con la ley de protección de datos;

c) marcas registradas y propiedad intelectual;

d) uso de la criptografía;

e) interceptación legal y acceso legal;

f) legalidad de un servicio vinculante, tal como las firmas digitales;

g) anonimato de las entidades;

h) derecho de investigar, por ejemplo, las credenciales;

i) requisitos legislativos y reglamentarios aplicables a la jurisdicción y la industria;

j) los tipos de servicio que han de prestarse;

k) disposiciones de acceso, incluidos los métodos de acceso permitidos y los procedimientos de autorización de usuarios (y de cambio de usuarios autorizados);

l) procedimientos de resolución de problemas (incluidos los puntos de contacto autorizados);

m) responsabilidades concernientes a los requisitos de soporte físico y soporte lógico, la gestión y el control de los cambios; y

n) disposiciones sobre la ejecución de informes, la notificación y la investigación de los incidentes relacionados con la seguridad.

Los compromisos y la responsabilidad civil de la TTP deben ser coherentes con su capacidad financiera y con las garantías y promesas que ha recibido de otras entidades. Las entidades deben tener el compromiso de que la información que proporcionan a una TTP está protegida contra su revelación, salvo que se especifique otra cosa en sus contratos con la TTP. La TTP ha de atender las demandas legales de protección de la información personal, especialmente las referentes a la adecuada protección técnica y organizativa de las bases de datos que contienen datos personales.

El comercio electrónico es internacional por naturaleza, y las TTP deben cumplir con todas las obligaciones legales con respecto a la legislación, reglamentos y acuerdos nacionales e internacionales. El cumplimiento de algunas de estas obligaciones puede tener una repercusión importante en el diseño o la implementación de una TTP.

Los conceptos de responsabilidad civil, y el marco legal básico pueden diferir de una nación a otra. Por consiguiente, habrán de adoptarse unas directrices generales para cumplir las exigencias de los sistemas legales individuales. Si la legislación nacional relativa a las TTP no es coherente cuando se atraviesan fronteras nacionales, las TTP que deseen autorizar a sus usuarios comunicar a través de estas fronteras deben poseer un acuerdo contractual especial vigente para resolver las diferencias jurisdiccionales.

En caso de interfuncionamiento a través de fronteras nacionales, las TTP deben ser conscientes de las consecuencias legales de tal situación en relación con las posibles diferencias o incompatibilidades entre sus políticas de seguridad y declaraciones de explotación real.

5.2 Obligaciones contractuales

Los contratos formales entre una TTP y entidades que utilizan sus servicios deben establecer claramente las responsabilidades de la TTP y la calidad del servicio que éste ha de prestar, así como las responsabilidades de las entidades que utilizan servicios de la TTP.

El contrato debe explicar la política de gestión y organización de la TTP, así como los procedimientos operacionales. La TTP debe también expedir una Declaración Práctica que describa qué entidades se pueden esperar de los servicios de la TTP con el fin de definir claramente de forma pública los aspectos y requisitos de explotación, la calidad de servicio, los aspectos éticos y las tasas de los abonados.

El contrato debe especificar las disposiciones que describan con claridad cómo la TTP cumple con la legislación y reglamentación pertinentes. El contrato debe especificar la jurisdicción de operación y la jurisdicción bajo la cual deben resolverse las controversias**.**

Los errores accidentales o deliberados de una TTP pueden ocasionar daños importantes a las empresas. Para gozar de confianza suficiente en el uso de los servicios TTP, el contrato debe definir los límites de la responsabilidad civil de la TTP con sus usuarios. Cuando resulte aplicable, la responsabilidad civil debe estar cubierta por un contrato de seguro apropiado en caso de litigio. La cobertura requerida debe definirse en el contrato de la TTP con sus usuarios.

El contrato debe incluir una lista de todas las materias amparadas por las responsabilidades civiles entre la TTP y sus usuarios, de modo que éstos últimos tengan posibilidad de acceder a un asesoramiento profesional adecuado con el fin de obtener la asistencia legal conveniente sobre cualquier tema que surja de la provisión y uso de los servicios de la TTP.

El contrato debe describir los usos a que se destina el servicio y sus parámetros de servicio, y se debe poder retirar el servicio en caso de que se esté utilizando de manera inadecuada o ilegal por parte de alguna de las partes contratantes.

El contrato puede tener disposiciones que establezcan claramente la posibilidad de pedir a un tercero independiente e imparcial (árbitro) que preste su asistencia en la resolución de los litigios entre la TTP y sus usuarios.

El contrato debe especificar cómo se protegerá la privacidad de las personas u otra información sensible, así como las circunstancias bajo las cuales se puede producir su revelación.

5.3 Responsabilidades

Una TTP debe definir la extensión de la responsabilidad que adquiere en cuanto al funcionamiento seguro de su servicio. Además, la TTP debe delinear la extensión de las responsabilidades civiles que pueden aceptarse en relación con los incumplimientos en materia de seguridad.

Las responsabilidades de la TTP, así como las del usuario, deben establecerse de manera clara en un contrato formal entre el usuario y la TTP. La mayor parte de las responsabilidades deben recogerse en un contrato, y algunas al menos deben definirse como materia comercial, mientras que otras se referirán a las calidades de servicio estándar.

Otros documentos, como los que contienen la definición de los servicios que han de prestarse, el arreglo de servicio y los anexos técnicos incluidos como adjuntos al contrato, determinan también las responsabilidades respectivas de las distintas entidades involucradas. Estos documentos forman parte del arreglo contractual global.

5.4 Política de seguridad

Una TTP acepta ciertas obligaciones basadas en la confianza y la fiabilidad de los servicios ofrecidos al ofrecer y prestar servicios relativos a la seguridad de funcionamiento, así como la política de seguridad formalmente documentada de la organización que ofrece el servicio.

La política de seguridad de una TTP es un instrumento fundamental para describir las importantes actividades de las que se deriva el establecimiento de la relación fiduciaria, y ganar confianza en la gestión de la TTP y el funcionamiento de sus servicios. Por ello, la política de seguridad de una TTP no sólo deberá abarcar asuntos específicos de la seguridad sino también contener todos los aspectos relacionados con el servicio de la TTP. El desarrollo y el mantenimiento de la política de seguridad de una TTP deberán llevarse a cabo de manera simétrica y lógica.

Como se expone en ISO/CEI TR 13335-3, anexo A, una política de seguridad de la TTP debe estar compuesta de dos partes:

a) una política de seguridad general que exprese de forma breve los aspectos no técnicos relativos a la seguridad y la fiabilidad de los servicios TTP; y

b) una política de seguridad técnica que exprese con concisión todos los aspectos técnicos de la funcionalidad y la relación de confianza (fiducia) relativos a la seguridad, junto con las descripciones de las rutinas, procedimientos, etc, relacionados con los aspectos técnicos.

Una evaluación rigurosa de la seguridad de los servicios TTP vigentes verifica la confianza en los sistemas técnicos de acuerdo con la medida de la confianza en la política de seguridad de la TTP.

Una política de seguridad de la TTP es de vital importancia en el mantenimiento de la confianza entre sistemas, especificando las bases para una revisión continua (interna) y una auditoría periódica (interna y externa) de la seguridad, así como la confianza en los sistemas y la organización que explota el servicio.

El compromiso adquirido por una TTP de prestar un servicio de seguridad debe adoptar la forma de una política de seguridad formal y documentada. La política de seguridad debe identificar todas las metas, objetos y peligros potenciales pertinentes relativos a los servicios prestados así como las salvaguardas requeridas para evitar o limitar los efectos de tales peligros. Debe describir las reglas, directivas y procedimientos referentes al modo de concesión de los servicios especificados y la garantía de seguridad asociada.

5.4.1 Elementos de la política de seguridad

El contenido de la política de seguridad de una TTP dependerá de los servicios prestados por la TTP. La política de seguridad debe ser un marco que trate los temas de seguridad en relación con varios elementos. Los elementos técnicos de la política de seguridad de una TTP constituyen la base para una evaluación de la seguridad técnica. Como se examina en ISO/CEI TR 13335-2, la política de seguridad de una TTP debe incluir al menos los siguientes elementos:

a) requisitos de seguridad IT, por ejemplo en términos de confidencialidad, integridad, disponibilidad, autenticidad, responsabilidad y fiabilidad, en particular desde el punto de vista de los propietarios de la información;

b) infraestructura organizativa y asignación de responsabilidades;

c) integración de la seguridad en el desarrollo y adquisición de los sistemas;

d) formación teórica ay práctica

e) directivas y procedimientos;

f) definición de clases para la clasificación de la información;

g) estrategias de gestión del riesgo;

h) planificación de contingencias;

i) asuntos de personal, con especial atención al personal en posiciones que requieren confianza, tales como el personal de mantenimiento y los administradores de sistemas;

j) obligaciones legales y reglamentarias;

k) gestión externa; y

l) tratamiento de incidentes.

La implementación de una política de seguridad de TTP que cubra los requisitos técnicos, administrativos y de organización para la seguridad, debe prestar especial atención a los siguientes requisitos:

a) asegurar que la TTP realiza sus funciones de modo que la integridad del sistema no pueda ser degradada o dañada;

b) la integridad de los datos de la entidad, que debe ser completa, no debe verse modificada y su fuente y origen podrán ser verificados;

c) las entidades autorizadas tendrán asegurada la disponibilidad de, y el acceso a, los servicios y la información de los que son titulares;

d) garantizar la confidencialidad de la información sensible y privada para la cual la entidad ha otorgado su confianza a la TTP; y

e) los procedimientos de auditoría de la seguridad del sistema de la TTP.

5.4.2 Normas

Las TTP deben utilizar normas cuando sea pertinente y aplicable. La normativa puede incluir normas y reglas de ámbito internacional, nacional, regional, del sector industrial y corporativas, seleccionadas y aplicadas de acuerdo con los requisitos de seguridad de sus organizaciones. Los beneficios derivados de esta normalización incluyen la interoperabilidad, la seguridad integrada, la coherencia, portabilidad e interfuncionamiento entre organizaciones. Si las distintas organizaciones desarrollan y usan sus propios sistemas o productos basados en normas propietario, pueden aparecer problemas de interoperabilidad entre los distintos sistemas. La normativa ha de examinarse a dos niveles: normas detalladas para tecnologías específicas y su uso, y normas para la interoperabilidad entre las diferentes tecnologías.

5.4.3 Directivas y procedimientos

Las directivas y los procedimientos son elementos necesarios de una política de seguridad de TTP. Incluyen las reglas y regulaciones requeridas establecidas por la organización, así como los procedimientos de orientación que son necesarios para que la organización provea los servicios a sus usuarios.

5.4.4 Gestión del riesgo

Para alcanzar un nivel aceptable de seguridad del sistema de tecnología de la información (IT), una TTP debe implementar métodos de gestión del riesgo. El proceso de gestión del riesgo para la seguridad de un sistema IT de TTP debe basarse en un análisis de riesgos detallado o en un enfoque combinado. Debe efectuarse una evaluación de toda la información para determinar la sensibilidad de la misma y los niveles de protección apropiados para mantener la confidencialidad, integridad y disponibilidad. Debe realizarse una evaluación periódica de los peligros, riesgos y salvaguardas. Las directrices para la selección de una estrategia adecuada de análisis de riesgos y una descripción detallada del proceso de análisis de riesgo se recogen en el Informe técnico de ISO/CEI 13335-3. Con base en los resultados del análisis de riesgos se elegirán, probarán e implementarán las salvaguardas adecuadas.

5.4.5 Selección de salvaguardas

La TTP está sujeta a muchos peligros accidentales o deliberados de origen natural o humano. La TTP debe estar protegida contra tales peligros con salvaguardas destinadas a reducir sus vulnerabilidades mediante la mitigación del impacto de los incidentes no deseados y/o la mejora de la facilidad de recuperación.

Las medidas, prácticas y procedimientos de seguridad deben tener en cuenta todos los aspectos técnicos, organizativos, administrativos, comerciales, humanos y legales pertinentes e integrarlos en, o coordinarlos con, las medidas, practicas y procedimientos de la organización.

Los niveles, costos, medidas, prácticas y procedimientos de seguridad deben se apropiados y proporcionados a la gravedad de los peligros, los impactos de los riesgos potenciales y el nivel de seguridad otorgado.

En el Informe Técnico de ISO/CEI TR 13335-4, cláusulas 8 a 11, se pueden ver las directrices detalladas para la selección de las salvaguardas.

5.4.5.1 Medidas físicas y ambientales

Deben implantarse controles de seguridad físicos y ambientales para proteger las instalaciones que albergan los recursos del sistema, los recursos del sistema propiamente dichos y las instalaciones utilizadas para soportar su funcionamiento. Un programa de seguridad física y ambiental de la organización debe llevar a cabo el control del acceso físico, la protección contra el fuego, la protección de las instalaciones soporte (eléctricas, de agua y de aire acondicionado), la protección contra el robo, la protección del cableado, etc.

Una organización de efectuar periódicamente una planificación de continuidad comercial que contemple estos aspectos, con el fin de mantener operativas sus funciones comerciales críticas en caso de interrupciones, tanto de larga como de corta duración, o en caso de desastres. La planificación de la continuidad comercial debe incluir capacidades de tratamiento de incidentes que permitan reaccionar de manera rápida y eficaz en caso de que se produzcan interrupciones en un modo normal (véase también 5.4.7.3, Planificación de contingencias).

5.4.5.2 Medidas organizativas y de personal

Una organización debe tener políticas de seguridad que contengan reglas, directivas y prácticas describiendo el modo en que los activos son gestionados, protegidos y distribuidos dentro de la organización. Todas las funciones críticas que soportan los procesos comerciales deben ser identificadas y documentadas, con personal asignado y responsable para estas funciones.

Una organización debe tener del compromiso de todos los niveles de gestión para soportar los requisitos de seguridad de la tecnología de la información (IT). Debe existir una buena disposición para satisfacer estos requisitos de seguridad IT y asignar los recursos de modo que se cumplan dichos requisitos.

Una organización debe disponer de descripciones puestos de trabajo definidas desde el punto de vista de la separación de funciones y menores privilegios, que determinen la sensibilidad de la posición basada en las tareas y los niveles de acceso, la valoración de la experiencia y la formación teórica y práctica de los empleados. La asignación y separación apropiadas de las responsabilidades debe garantizar que se lleven a cabo todas las tareas importantes, y que esto se haga de un modo eficaz.

Una organización debe asegurar la administración eficaz del acceso al computador de la entidad para mantener la seguridad del sistema, incluida la gestión de las cuentas de usuario, la auditoría y la modificación o supresión oportuna del acceso.

5.4.5.3 Medidas específicas de la IT

Una TTP que presta servicios relacionados con la seguridad depende mucho de los sistemas de tecnología de la información (IT). Por ello se necesitan salvaguardas IT específicas que los hagan seguros y adecuados. Las salvaguardas específicas pueden dividirse en categorías técnicas, de comunicaciones y de interfuncionamiento de redes. Las salvaguardas se pueden elegir de acuerdo con una evaluación detallada de los riesgos y peligros de la seguridad, o de acuerdo con el tipo de sistemas IT.

a) Las medidas de acuerdo con los riesgos y los peligros de la seguridad consisten en salvaguardas para la confidencialidad, la integridad, la disponibilidad y la responsabilidad civil.

   - Confidencialidad – La seguridad de un servicio TTP puede estar basada en un sistema de claves ampliamente utilizadas, por ejemplo, las claves de certificación. La protección de estas claves puede realizarse físicamente mediante el uso de un soporte físico fiable, y lógicamente mediante esquemas secretos compartidos.
   - Integridad – La información sensible intercambiada en la interfaz usuario-TTP, para los modos de comunicación en línea, fuera de línea y fuera de banda debe protegerse contra su alteración, interrupción y bloqueo.
   - Disponibilidad – Las TTP deben implementar mecanismos que garanticen a sus usuarios el acceso a los servicios TTP cuando los necesiten. La no disponibilidad, es decir la denegación del servicio, puede tener una importante repercusión en la actividad de la TTP. Deberán considerarse los mecanismos apropiados que eviten las "inundaciones" de telecomunicaciones, los problemas de encaminamiento y la interrupción del servicio.
   - Responsabilidad civil – Deben definirse la incumbencia y la responsabilidad de todas las actividades para las TTP y los usuarios de los servicios TTP. Las TTP deben implementar mecanismos apropiados, de modo que cada evento y cada acción puedan ser señalados a la entidad responsable. La responsabilidad puede ser asumida mediante el uso de la supervisión de pistas de auditoría de seguridad y a través de auditorías periódicas. Deberán mantenerse los correspondientes ficheros cronológicos de auditoría para poder disponer de una pista de auditoría de cada acción, transacción, proceso, etc. La propiedad de información sensible y las responsabilidades de seguridad asociadas con la auditoría son importantes con miras a la prestación de unos servicios TTP eficaces.

b) Las medidas de acuerdo con el tipo de sistema IT consisten en salvaguardas para el control de acceso.

   - Control de acceso – La protección frente al uso no autorizado de servicios TTP puede ser proporcionada por medio de salvaguardas de control de acceso. Debe considerarse la implementación de mecanismos apropiados en las siguientes áreas:
     - identificación y autentificación;
     - control de acceso físico;
     - control de acceso lógico;
     - criptografía; y
     - gestión de privilegios.

En ISO/CEI TR 13335-4 y en la Rec. UIT-T X.812 | ISO/CEI 10181-3 se dan detalles sobre el control de acceso.

5.4.6 Aspectos de la implementación de la seguridad IT

5.4.6.1 Formación teórica y práctica

Todo el personal de la organización TTP debe tener una formación teórica y práctica eficaces en materia de seguridad de computador que les capacite para la adquisición de conocimientos adecuados y de información acerca de la existencia y amplitud general de las medidas, prácticas y procedimientos aplicados a la seguridad de los sistemas de información. Si no hay una aceptación e implicación del personal a todos los niveles, un programa de formación en seguridad no puede tener éxito. Es de importancia especialmente crítica para la gestión que la organización sea consciente de la necesidad de

la seguridad y de promover la adquisición de conocimientos sobre seguridad por parte de su plantilla de personal. El objetivo de un programa de formación es convencer al personal de la existencia de importantes riesgos para los sistemas IT y de que la pérdida de información, o su modificación no autorizada o su revelación, pueden tener consecuencias graves para la organización y su personal. En el Informe Técnico de ISO/CEI 13335-2 puede encontrarse información detallada sobre la formación teórica y práctica al respecto.

5.4.6.2 Fiabilidad y garantía

La garantía de seguridad otorgada por las TTP debe derivarse de:

a) la selección de los mecanismos apropiados en relación con los servicios prestados y la política de seguridad;

b) La implementación adecuada de estos mecanismos, en particular con relación a los aspectos físicos de la seguridad, el entorno, la continuidad comercial, etc; y

c) el funcionamiento de estos mecanismos, dependiendo de la definición y de los procedimientos apropiados, en particular con relación a la gestión de personal, la clasificación de la información, la autorización, el tratamiento de incidentes, etc.

Los servicios TTP solamente deben utilizar sistemas fiables cuando pongan en marcha sus servicios. Una evaluación formal de los sistemas puede comprobar su fiabilidad. En ISO/CEI 15408 (*Common Criteria* - Criterios comunes) se recoge información detallada sobre los criterios de evaluación que sirven de ayuda al decidir el nivel mínimo de seguridad que debe implementarse en las TTP.

Para que una TTP sea fiable debe ser operada de conformidad con sus especificaciones. La certificación es el procedimiento mediante el cual un entidad independiente garantiza que un producto, proceso o servicio se adecua a los requisitos especificados. El proceso de certificación consiste principalmente en un análisis del documento y una evaluación técnica por parte de un organismo de certificación imparcial.

Tal certificación de conformidad de una TTP garantizará que la seguridad pretendida por una TTP es realmente proporcionada. Las entidades que utilizan servicios TTP pueden por tanto emplear tales certificaciones de conformidad de la TTP sobre seguridad como base para la determinación del nivel de confianza que ellas pueden depositar en la TTP.

Dependiendo de los servicios TTP que han de soportarse, el proceso de certificación de conformidad debe incluir un análisis de:

a) la conformidad con la legislación y regulación nacionales e internacionales pertinentes que gobiernan su estatus, actividades y comportamiento;

b) la conformidad con las normas técnicas;

c) la conformidad con la política de seguridad;

d) la conformidad con las reglas específicas sectoriales y profesionales; y que estas reglas han sido perfectamente definidas, implementadas y cumplidas en el sentido administrativo y técnico

e) la conformidad con los códigos de ejecución práctica más convenientes; y

f) la adecuación de las medidas de seguridad con respecto a los peligros, riesgos y política de seguridad.

La decisión por parte de la gestión de una organización de obtener una certificación de conformidad de la TTP puede tener repercusiones muy importantes en la concepción e implementación de la TTP. En la German Digital Signature Act y en las regulaciones que la acompañan puede verse un ejemplo de requisitos de seguridad para las TTP. Las autoridades de certificación que expiden certificados a las TTP deben también obtener una certificación de conformidad. En B.2, puede verse un ejemplo de los requisitos para la certificación de conformidad de las autoridades de certificación.

5.4.6.3 Acreditación de los organismos de certificación TTP

El nivel de confianza que los usuarios pueden depositar en una TTP es susceptible de aumentar si el organismo de certificación de la TTP es acreditado bajo un esquema de pertinencia con la aplicación La acreditación asegura que los procedimientos de organismos de certificación TTP diferentes son similares y que las certificaciones resultantes de diferentes organismos de certificación son comparables. La acreditación se define en ISO/CEI Guide 2. La acreditación de un organismo de certificación TTP significa que el organismo de certificación TTP es ampliamente reconocido como competente y fiable en la provisión de servicios de certificación TTP. Por consiguiente, la acreditación de los cuerpos de certificación TTP es un medio adicional de proporcionar una garantía de calidad de servicio de la TTP ya que las organizaciones acreditadoras son independientes y operan de conformidad con reglas ampliamente aceptadas.

El acreditador evalúa los aspectos técnicos y de procedimiento del sistema de gestión de los organismos de certificación TTP de conformidad con ISO/CEI Guide 61 u otros esquemas similares como la serie de normas European 450xx.

La acreditación de un organismo de certificación TTP es un medio de garantizar la calidad del trabajo del organismo de certificación TTP, pero no dice nada acerca de los servicios proporcionados por una TTP concreta. La TTP define los servicios prestados y el organismo de certificación TTP certifica la calidad de la prestación.

5.4.7 Aspectos operacionales de la seguridad de IT

5.4.7.1 Auditoría

Si bien la evaluación es un medio de probar la confiabilidad de los sistemas IT, la auditoría y valoración son los medios de lograr confianza y fiabilidad en la política de seguridad documentada y en el sistema de gestión de seguridad realizado que ofrece los servicios TTP. La evaluación se utiliza en el contexto de las inspecciones de seguridad de sistemas IT y de los medios de examen frente a los criterios de evaluación (en ISO/CEI 15408 se dan detalles). La auditoría se utiliza en el contexto de revisiones de gestión o comprobaciones básicas así como en los métodos para examinar que los elementos son conocidos y que han sido documentados y ejecutados realmente. La valoración se aplica en la mejora de productos/procesos y se destina a examinar sus puntos fuertes y puntos débiles. Todos los exámenes se efectúan periódicamente o a petición.

El objetivo de una auditoría de seguridad es determinar si las políticas de seguridad se están aplicando de manera eficaz y se consiguen con ellas los objetivos pretendidos. La auditoría de seguridad se basa en el análisis de los documentos existentes y en la inspección de los mecanismos implementados y de los controles de seguridad, por lo que una TTP deberá tener la documentación apropiada y conveniente puesta al día.

Las entidades que utilizan servicios TTP pueden requerir que se realicen inspecciones y auditorías para comprobar y validar el nivel de seguridad realmente prestado por la TTP. Las entidades pueden requerir que las auditorías sean llevadas a cabo por sus propios equipos internos de auditoría, o por auditores externos independientes. Las auditorías pueden también ser iniciadas por la TTP con el objetivo de revisar su propia seguridad, sus propios riegos o para proporcionar a las entidades la evidencia de su buen hacer. También los organismos de acreditación pueden pedir que se lleven a cabo auditorías. Las auditorías se pueden iniciar como resultado de diversas circunstancias, pudiendo ser: periódicas (por ejemplo, anualmente), a petición, iniciadas después de un cambio importante o iniciadas después de un incidente. Las auditorías pueden considerar los aspectos operacionales de una TTP, tales como:

a) política de seguridad;
b) selección de los mecanismos de seguridad;
c) implementación de los mecanismos de seguridad;
d) organización;
e) procedimientos;
f) gestión de los cambios;
g) personal (especialización, adiestramiento, etc.);
h) seguridad física;
i) aspectos financieros;
j) seguro de responsabilidad civil, cuando sea aplicable; y
k) documentación.

Las auditorías se deben realizar de conformidad con las normas y prácticas profesionales aplicables normalmente. En particular, los auditores, tanto internos como externos, deben respetar estrictamente las normas de confidencialidad. Los organismos de acreditación deben dictar directivas sobre el modo de llevar a cabo las auditorías. Cuando los informes de auditoría se hacen llegar al público en general o a las entidades que utilizan los servicios TTP, estos informes deben ser comprobados cuidadosamente para asegurarse de que no contienen ninguna información susceptible de ser utilizada para debilitar la seguridad de la TTP.

NOTA – En ISO 8402 figuran la descripción y los detalles de los procedimientos de auditoría y evaluación de la calidad.

5.4.7.2 Tratamiento de los incidentes

Una TTP debe actuar de una manera coordinada y oportuna en el tiempo, de modo que responda rápidamente a los incidentes y limite la aparición de brechas en la seguridad. Todos los incidentes deben ser comunicados lo antes posible después de su detección. Deberá disponerse de procedimientos para hacer frente a los eventos de seguridad específicos detectados por la TTP, o puestos en su conocimiento, por ejemplo el compromiso de una clave secreta o par de claves pública/privada , o la pérdida de un testigo de seguridad personal. Los procedimientos deben formar parte del esquema de análisis de incidentes (IAS, *incident analysis scheme*).

Las brechas de la seguridad producidas por las entidades, tanto de modo accidental como intencionado, deben ser difíciles y, cuando puedan ocurrir, las tentativas de abuso de los derechos de acceso por parte de una entidad deben ser detectables por la TTP.

5.4.7.3 Planificación de contingencias

La continuidad de los servicios TTP se debe proteger contra los efectos de fallos o desastres. Debe disponerse de un proceso de gestión para el desarrollo y mantenimiento de procedimientos sobre contingencias. La planificación de contingencias debe cubrir:

a) la identificación de funciones comerciales críticas;

b) la identificación de los recursos internos y externos que soportan funciones y servicios críticos;

c) la elección de una estrategia de continuidad;

d) el establecimiento de planes y procedimientos;

e) la implementación de planes y procedimientos; y

f) la prueba y actualización de planes y procedimientos.

En ISO/CEI TR 13335-3 y en varios documentos normativos de ámbito nacional se recogen directrices detalladas sobre la planificación de contingencias.

5.5 Calidad de servicio

Los requisitos generales relativos a la calidad de servicio son: fiabilidad, disponibilidad, facilidad de utilización por el usuario, eficacia, implementación correcta, documentación y control de acceso.

5.6 Aspectos éticos

Los servicios TTP deben prestarse y utilizarse respetando los derechos e intereses legítimos de todas las entidades involucradas.

5.7 Tasas

Las TTP pueden facturar las tasas del abonado por el uso de sus servicios. Si es solicitado por las entidades que utilizan estos servicios, las TTP deben poner a su disposición una lista con todas las tasas correspondientes, indicándose bajo que circunstancias estas tasas pueden modificarse.

6 Interfuncionamiento

El interfuncionamiento requiere varias TTP y entidades que hayan de conectarse juntos como una red con interfaces, protocolos y formatos de datos claramente definidos de modo que se posibilite el interfuncionamiento entre ellos. Cada TTP proporciona servicios a entidades dentro de su propio dominio de acuerdo con su propia política de seguridad. Existen varios métodos de interacción que incluyen: TTP-usuarios; usuario-usuario; TTP-TTP; y, cuando sea aplicable, TTP- agencia de ejecución legal.

Una TTP puede tener arreglos de confianza con otras TTP para formar una red, permitiendo de este modo que una entidad de una TTP comunique de manera segura con las entidades de otros TTP. Cuando una TTP no pueda proporcionar todos los servicios requeridos, los arreglos de fiducia permiten a otros TTP subcontratar y proporcionar aquellos servicios adicionales. Cuando se analizan los requisitos de interfuncionamiento debe señalarse que la relación legal entre una TTP y sus abonados es diferentes de la relación entre la TTP y los no abonados (por ejemplo, usuarios que verifican firmas digitales basadas en certificados procedentes de la CA). Véanse los ejemplos de estructuras de interfuncionamiento de TTPs (CAs) de la Rec. UIT-T X.509 | ISO/CEI 9594-8.

6.1 TTP-Usuarios

Los medios por los cuales un usuario interactúa con una TTP para solicitar y recibir un servicio TTP se conocen como interfaz de usuario. Cada usuario puede interactuar con la TTP de modos diferentes según sea el tipo de servicio que se ofrece.

6.2 Usuario-usuario

Después de que la TTP ha completado sus tareas, toda comunicación posterior entre entidades puede efectuarse sin asistencia de la TTP. La relación entre entidades así como la formalización contractual de esta relación depende grandemente de su confianza en la TTP y los mecanismos de interfuncionamiento de las TTP.

6.3 TTP-TTP

La interfaz TTP a TTP soporta comunicaciones seguras entre usuarios a través del intercambio de información concerniente a los servicios de seguridad prestados. En muchos dominios de la seguridad, se supone que las TTP disponen de certificación cruzada. Por ejemplo, en la figura 4 más adelante se ilustran las interfaces utilizadas cuando la entidad A pide a la TTP A una clave secreta para comunicar con la entidad B (1), la TTP A transfiere la clave secreta apropiada a la entidad A (3) y a TTP B (2), el cual pasa la clave a la entidad B (3). Con esta clave común las entidades A y B pueden cursar comunicaciones seguras (4). Como alternativa, utilizando la tecnología de claves públicas, la entidad A pediría comunicaciones seguras con la entidad B desde la TTP A (1). La TTP A pasaría el certificado de la entidad A a la TTP B y pediría el certificado de la entidad de la TTP B (2). La TTP B pasaría el certificado de la entidad A a la entidad B (3) y transferiría el certificado de la entidad B a la TTP A (2), el cual lo pasaría a la entidad A (3). Con el certificado de la entidad B en posesión de la entidad A, y viceversa, se pueden establecer comunicaciones seguras entre las entidades A y B (4).

Se pueden utilizar una gran variedad de mecanismos para estos intercambios de comunicaciones seguras.

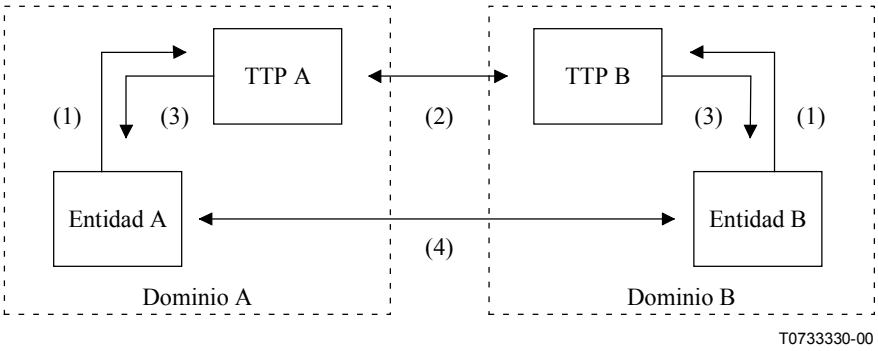


Figura 4 – Interfuncionamiento de TTP situados en dominios diferentes

NOTA – Los mecanismos utilizados caen fuera del alcance de esta Recomendación │ Informe técnico.

Ha de considerarse que un servicio de seguridad dado puede resultar de la combinación de diferentes TTP que ofrecen servicios complementarios, los cuales pueden tener diferentes niveles de seguridad. Por consiguiente, han de establecerse reglas encaminadas a la evaluación y clasificación del nivel de seguridad ofrecido por las TTP y deben proponerse métodos para la evaluación del nivel de seguridad de un servicio de múltiples TTP.

El examen a continuación resulta pertinente en los casos en que la TTP es una autoridad de certificación (CA).

Las CA se pueden organizar en arquitecturas jerárquicas o no jerárquicas.

En una arquitectura jerárquica, los trayectos de certificación tienen una jerarquía que va desde la CA raíz a su CA subordinada siguiendo su arquitectura jerárquica.

En una arquitectura no jerárquica, las CA han de cruzarse certificaciones recíprocas para permitir un uso flexible y el intercambio de certificados. Esta certificación cruzada ha de realizarse utilizando niveles de seguridad elevados y un código cuidadoso de ejecución práctica. Una vez que existe certificación recíproca entre CAs, se pueden construir trayectos de validación de los certificados de claves públicas. Una entidad solamente ha de tener confianza en la clave de verificación de una CA. Esta confianza se extiende entonces vía el trayecto de certificación a las otras claves públicas de la entidad emitidas por la otra CA.

6.4 TTP-Agencia de ejecución legal

La preocupación principal planteada por las autoridades de ejecución legal y las agencias de seguridad nacionales es que el uso extensivo de comunicaciones criptadas reducirá su capacidad para luchar contra el crimen y para impedir actividades criminales y terroristas.

Siempre que se aplicable, en las naciones con este tipo de interacción, esta interfaz suministra los medios en virtud de los cuales la agencia de ejecución legal puede pedir y recibir de una TTP información archivada confidencial. Esta información permitirá descriptar las comunicaciones criptadas interceptadas legalmente.

7 Principales categorías de servicios TTP

7.1 Servicio de indicación de tiempo

Un servicio de indicación de tiempo sella un documento digital vinculando criptográficamente a éste (típicamente a la representación de troceo del mismo denominada "resumen de mensaje" o "marca de mensaje" un tiempo de confianza, con lo cual proporcionan un medio de detectar cualquier modificación, como el antefechado, y de evitar la reanudación de agresiones u otras falsificaciones.

El servicio de indicación de tiempo depende de la autenticidad del reloj que se está utilizando, por lo que la TTP necesita un servicio de indicación de tiempo que utilice un reloj de fiabilidad, disponibilidad y exactitud muy elevadas.

Un resumen de mensaje puede crearse utilizando las técnicas descritas en ISO/CEI 10118-1, 10118-2, y 10118-3. Los testigos de indicación de tiempo se describen en ISO/CEI 13888-1.

Opcionalmente, la TTP que proporciona los servicios de indicación de tiempo debe registrar todos los sellos electrónicos por orden cronológico en un archivo permanente. Asimismo, se puede proveer un servicio de verificación de indicaciones de tiempo.

7.1.1 Autoridad de indicación de tiempo

Una autoridad de indicación de tiempo (TSA, *time stamp authority*) es una TTP que crea testigos de indicación de tiempo para señalar que un mensaje ha existido en un instante de tiempo concreto.

La TSA proporciona una "prueba de existencia" de este mensaje concreto en un instante dado. Una TSA puede también utilizarse cuando se necesita una referencia de tiempo de confianza y cuando el reloj local disponible no puede ser considerado fiable por todas las entidades. El cometido de la TSA es indicar la hora de la marca de un mensaje para establecer pruebas fehacientes que indiquen la hora antes de la cual el mensaje ha sido generado. Por ejemplo, la indicación de tiempo se puede utilizar para:

a) verificar que una firma digital se ha aplicado antes de que el certificado haya sido revocado permitiendo así que un certificado de claves públicas revocado pueda ser utilizado para la verificación de firmas creadas antes del tiempo de revocación, o

b) indicar el tiempo de presentación cuando un plazo límite es crítico, o

c) indicar momento de la transacción.

La TSA debe:

a) garantizar solamente la fuente fiable de tiempo;

b) incluir un valor de la hora del día que se incremente monotónicamente (nunca creciente o nunca decreciente) dentro de su testigo de indicación de tiempo (el tiempo elegido que se utilizará puede ser el tiempo universal [GMT]o el tiempo local);

c) producir un testigo de indicación de tiempo tras recibir una petición válida del peticionario;

d) incluir dentro de cada testigo de indicación de tiempo un identificador para indicar inequívocamente la política de confianza y validación bajo la cual fue creado el testigo;

e) tratar con la indicación de tiempo solamente a una representación de troceo del mensaje;

f) firmar cada testigo de indicación de tiempo mediante una clave generada exclusivamente para esta finalidad, y haber indicado esta propiedad de la clave en el certificado correspondiente (se pueden emplear otros métodos criptográficos distintos del de la firma);

g) incluir información temporal suplementaria (por ejemplo, los resultados de los deportes o de la lotería) en el testigo de indicación de tiempo si lo solicita el peticionario; y

h) proporcionar al peticionario, cuando resulte adecuado, un recibo firmado en la forma de un testigo de indicación de tiempo definido apropiadamente, según venga definido por la política aplicada.

En PKIX Part V, y en ISO/CEI WD 18014, se puede encontrar información detallada y un ejemplo de protocolo de indicación de tiempo.

7.2 Servicios de no repudio

Las TTP pueden estar involucrados en el aprovisionamiento de servicios de no repudio, que dependen de los mecanismos utilizados y de la política de no repudio vigente. De conformidad con ISO/CEI 13888-1, 13888-2 y 13888-3, la finalidad del no repudio es proporcionar una prueba verificable o una evidencia del registro de datos, en base a valores de prueba criptográficos generados utilizando técnicas criptográficas simétricas o asimétricas, así como de la aprobación, envío, origen, presentación, transporte, recibo, acuse de recibo y entrega de los mismos. Un componente importante del no repudio para proporcionar la prueba verificable es la indicación de tiempo.

Se pueden aplicar dos enfoques básicos para decidir si una TTP es o no esencialmente necesario dentro del servicio de no repudio.

1) De conformidad con ISO/CEI 13888-2, los servicios de no repudio basados en técnicas simétricas necesitan:

   a) un servicio en línea para la generación de evidencias, verificación de evidencias y generación de sobres seguros; y

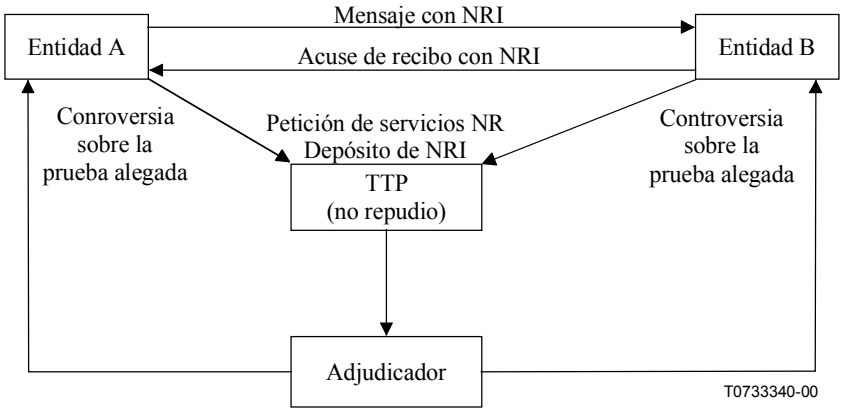
   b) un servicio fuera de línea para la personalización de claves adecuadas en un dispositivo criptográfico de confianza, por ejemplo, una tarjeta inteligente o un módulo de seguridad.

Es importante señalar que el no repudio basado en técnicas simétricas depende de una sola clave, la cual puede ser utilizada por una TTP cuando ofrece un servicio de notaría. El uso de esta clave es restrictivo, y debe controlarse su distribución a las entidades.

2) De conformidad con ISO/CEI 13888-3, se pueden especificar técnicas asimétricas para establecer mecanismos destinados a los servicios de no repudio de origen, entrega, presentación y transporte.

Si una TTP no está implicada directamente en el servicio de no repudio, se pueden utilizar otros servicios TTP, tales como el de asignación de claves certificadas, con o sin generación de claves, o los servicios de gestión de certificados, para establecer la infraestructura necesaria.

En la figura 5 se muestra un ejemplo de una TTP que proporciona servicios de no repudio a las entidades A y B.



(NRI: Non-repudiation Information - información de no repudio)

Figura 5 – Ejemplo de arquitectura de no repudio

En ISO/CEI 13888-1 se dan más detalles sobre la implicación de la TTP en el aprovisionamiento de servicios de no repudio.

7.3 Servicios de gestión de claves

De conformidad con la norma de control de claves ISO/CEI 11770-1, la gestión de claves depende de los servicios básicos de generación, registro, certificación, distribución, instalación, almacenamiento, derivación, archivo, revocación, desregistro y destrucción. Otros servicios relativos a la seguridad que pueden utilizarse son los servicios de control de acceso, auditoría, autenticación, criptográficos y de indicación de tiempo.

Una TTP en línea actúa como un servidor de gestión de claves en apoyo de servicios que utilizan técnicas criptográficas. Dependiendo del modo de generar el material de claves, el servicio puede ser un servicio de distribución de claves (cuando la clave es generada por la TTP) o un servicio de traslación de claves (cuando la clave es generada por una de las entidades y transmitida a la otra por la TTP).

7.3.1 Servicio de generación de claves

Este servicio es invocado para generar claves de un modo seguro para un algoritmo criptográfico determinado. La generación de números secretos e imprevisibles con ciertas propiedades es de importancia fundamental para la generación de claves. Por ejemplo, los números aleatorios pueden ser generados por un generador de números seudoaleatorios asegurados criptográficamente o por una fuente aleatoria tal como una desintegración radioactiva. Los diferentes elementos relativos a los números aleatorios incluyen la generación de números aleatorios, la validación de la generación de números aleatorios, la generación de parámetros de dominio, la validación de parámetros de dominio, la generación de pares de claves y la validación de claves públicas. Una introducción útil a los números aleatorios que incluye los métodos de generación se encuentra disponible en RFC 1750.

Es importante considerar los siguientes puntos, tanto para las técnicas simétricas como las asimétricas:

a) claves débiles posibles para el algoritmo; y

b) uso del espacio de claves completo.

7.3.2 Servicio de registro de claves

En este ejemplar la TTP es una autoridad de registro acreditada para proveer el registro de claves para entidades, donde cada clave registrada está asociada con una entidad específica. Este servicio comprende el mantenimiento de un registro de claves y de la información relacionada de una manera convenientemente segura, por ejemplo, un registro de claves públicas para una clave pública de entidad. Las claves públicas deben ser certificadas por una o más autoridades de certificación. Para incrementar la disponibilidad y fiabilidad de este servicio deben distribuirse claves certificadas a múltiples directorios públicos accesibles y fiables, en cuyo caso es preciso efectuar una actualización periódica de todos los directorios para mantener la coherencia entre los mismos. Una autoridad de registro de claves proporciona los servicios de registro y desregistro. Los detalles sobre el contenidos de una registro de claves pueden verse en ISO/CEI 11770-1, anexo B.

7.3.3 Servicio de certificación de claves

En este ejemplar la TTP es una autoridad de certificación acreditada que crea un certificado de claves. La autoridad de certificación indica el tiempo y firma las claves públicas o atributos para hacerlos válidos y auténticos en una infraestructura de claves de confianza. Las entidades que utilizan certificados han de aceptar como fiduciaria a la misma autoridad de certificación o al menos a una autoridad común dentro de una jerarquía de certificación. Las claves certificadas pueden ser generadas por un servicio de generación de la TTP o por el propietario de las claves. El servicio también incluye la nueva certificación de los certificados caducados. Los certificados para claves públicas se examinan en detalle en ISO/CEI 11770-1, anexo D.

Es importante señalar que los servicios de:

1) aprovisionamiento de seguro de prueba de posesión de la clave privada por el propietario pretendido; y

2) aprovisionamiento de seguro de validez del valor de la clave pública candidato (y validez de los valores de un conjunto candidato de parámetros de dominio, cuando resulte apropiado),

pueden ser invocados fuera del servicio de certificación, y como parte de un servicio de certificación.

7.3.4 Servicio de distribución de claves

La finalidad de un servicio de distribución de claves es distribuir claves de modo seguro a entidades autorizadas. Dependiendo de cuál sea la política de seguridad de la TTP, las claves pueden ser reenviadas a otros servicios de la TTP, por ejemplo, un servicio de directorio. Estos servicios pueden ser prestados por la misma TTP o por otra. La distribución de claves entre las TTP y también entre las TTP y entidades, especialmente si la distribución se efectúa a través de canales no seguros, debe estar protegida mediante protocolos y mecanismos criptográficos. Detalles sobre diferentes mecanismos para distribuir claves entre entidades se pueden ver en ISO/CEI 11770-2. Detalles sobre diferentes mecanismos relativos al arreglo sobre claves secretas y mecanismos de transporte para claves secretas y públicas se pueden ver en ISO/CEI 11770-3. Los detalles sobre diferentes mecanismos no recogidos en ISO/CEI 11770-3 se pueden hallar en ISO/CEI 15946-3.

De conformidad con ISO/CEI 11770-1, un caso especial de la distribución de claves es la traslación de claves. El cometido de un servicio de traslación de claves consiste en trasladar claves para su distribución entre entidades de modo que cada entidad comparta un clave exclusiva con un centro de conversión de claves.

7.3.5 Servicio de instalación de claves

Este servicio se necesita siempre antes que una clave pueda ser utilizada, ya que establece la clave dentro de una facilidad de gestión de claves de modo la protege del compromiso.

7.3.6 Servicio de almacenamiento de claves

Este servicio proporciona un almacenamiento seguro de las claves destinadas al uso actual o a corto plazo, o destinadas a copias de seguridad, normalmente en una ubicación separada físicamente para garantizar la confidencialidad e integridad de las claves. Es esencial que se pueda detectar cualquier tentativa de compromiso.

7.3.7 Servicio de derivación de claves

Este servicio crea un número potencialmente elevado de claves utilizando una clave original secreta denominada clave de derivación, datos variables no secretos y un proceso de transformación. Esta clave de derivación necesita una protección especial, y el proceso de transformación no debe ser reversible ni previsible para asegurar que el compromiso de una clave derivada no revela la clave de derivación o cualquier otra clave derivada. Un número potencialmente elevado de claves se crea mediante el proceso de transformación utilizando una clave original, denominada clave de derivación, y datos variables no secretos.

7.3.8 Servicio de archivo de claves

Aunque este servicio es similar al servicio de almacenamiento de claves, su finalidad es sin embargo mantener un almacenamiento seguro a largo plazo de las claves después de suspendido su uso normal. El servicio se destina a claves que puede haber necesidad de recuperar en fecha muy posterior para justificar, o rechazar, determinadas reclamaciones.

7.3.9 Servicio de revocación de claves

La finalidad de este servicio es garantizar la desactivación segura de una clave cuando esta clave es conocida o sospechosa de estar comprometida. Debe distribuirse regularmente una lista de claves revocadas. La revocación puede ser solicitada por el propietario de la clave, por otra persona autorizada o por una entidad de confianza si existe la sospecha de que la clave ha sido comprometida. De conformidad con ISO/CEI 11770-1, Anexo D, cada inserción en lista de suspensión debe incluir el tiempo de revocación, el tiempo de la petición y el tiempo del compromiso conocido o sospechado. En algunos casos la revocación puede tener que cumplir las restricciones del tiempo de la firma, y debe transcurrir un intervalo de tiempo corto entre el tiempo de la petición y la distribución de la notificación de revocación. La TTP solamente puede ocuparse de la revocación de las claves de sus clientes, por lo general informando a cada cliente sobre cuales son las claves del mismo que han sido revocadas.

7.3.10 Servicio de destrucción de claves

En este ejemplar la TTP es una autoridad de registro acreditada para proporcionar la destrucción de claves que ya no se necesitan. La TTP debe proporcionar en primer lugar el servicio de desregistro para eliminar la asociación de una clave con su entidad. Después seguirá la destrucción de la clave, la cual se efectúa mediante la destrucción de toda la información relacionada con la clave, de modo que no haya modo alguno de recuperar la clave destruida. Esto incluye la destrucción de todas las copias de claves archivadas después de una investigación que asegure que jamás en adelante se necesitará ningún material archivado protegido por estas claves.

7.4 Servicios de gestión de certificados

El formato de un certificado de claves públicas y de un certificado de atributos se define en la Rec. UIT-T X.509 | ISO/CEI 9594-8. El formato del certificado de atributos es compatible con el certificado X.509, y su uso no está restringido a un área específica. Esto es importante porque permite tratar el mismo "sujeto" (por ejemplo, una entidad) con los atributos (por ejemplo, nombre de entidad) utilizados en un certificado (de clave pública) X.509. En el anexo D de ISO/CEI 11770-1 se recogen más detalles sobre la gestión de certificados.

En la subcláusulas a continuación se describen algunos servicios de gestión de certificados.

7.4.1 Servicio de certificados de claves públicas

Una autoridad de certificación (CA) es una tercera parte confiable (TTP) que proporciona certificados de claves públicas y se cuida de la información necesaria para la revocación de tales certificados expedidos. Esto se lleva a cabo verificando la identidad del peticionario antes de expedir un certificado de claves públicas, que incluye un periodo de validez limitado. La CA debe asegurar que el peticionario tenga conocimiento de la clave privada. La CA puede asegurar que la clave pública del peticionario completa una prueba de validación y, si es aplicable, las pruebas de validación de parámetros de dominio.

El ciclo de vida de los certificados de claves públicas es gestionado por una TTP mediante el aprovisionamiento de los servicios de una CA. La CA ejerce de agente fiduciario de sus usuarios mediante el uso adecuado de mecanismos y equipos criptográficos y mediante la práctica de una gestión y control profesionales. Esta relación de confianza es confirmada por una función de auditoría independiente que pone sus resultados a disposición de las entidades. Las responsabilidades de la CA comprenden:

a) la identificación de las entidades cuya información de claves públicas es presentada para certificación; los procedimientos para describir esta materia se recogen con más detalle en B.1, Procedimientos del proceso de registro;

b) el aseguramiento de la calidad del par de claves asimétricas utilizado para producir certificados de claves públicas;

c) el aseguramiento del proceso de certificación y la clave privada utilizada para firmar la información de claves públicas;

d) la gestión de los datos específicos del sistema que han de incluirse en la información de claves públicas, tales como el número de serie del certificado de claves públicas, la identificación de la autoridad de certificación, etc.;

e) la asignación y comprobación de los periodos de validez;

f) el aviso a la entidad identificada en la información de claves públicas de que se ha expedido un certificado de claves públicas; los medios utilizados para cursar este aviso deben ser independientes del método empleado para cursar la información de claves públicas a la CA;

g) el aseguramiento de que toda la información incluida en un certificado cumple los requisitos de la política de certificados aplicable, por ejemplo, garantizando que no se asigna la misma identidad a dos entidades diferentes, de modo que ellas pueden distinguirse adecuadamente;

h) el mantenimiento y emisión de listas de revocación; e

i) el registro cronológico de todos los pasos involucrados en el proceso de generación de los certificados de claves públicas.

Una CA puede certificar información de claves públicas de otra CA para proporcionar un certificado de claves públicas. En consecuencia, la autenticación puede estar formada por una cadena de certificados de claves públicas. El primer certificado de claves públicas en tal cadena debe obtenerse y autenticarse por métodos diferentes de los que se emplean con los certificados de claves públicas.

NOTA – Puesto que el receptor de una firma digital puede no haber tenido ningún contacto anterior con la CA expedidora del certificado que acompaña a esa firma digital, se necesita un mecanismo por medio del cual el receptor pueda establecer un nivel de confianza en la CA. Esta confianza se establece a través del proceso de certificación cruzada (recíproca). Se puede disponer de la certificación cruzada mediante un arreglo bilateral entre las dos CA, expidiendo una de ellas, o ambas, a la otra un certificado.

Durante la certificación cruzada se consideran varios aspectos, que incluyen:

a) procesos de identificación;

b) procesos de generación y de almacenamiento de claves;

c) responsabilidad civil;

d) procesos de revocación;

e) procesos de seguridad; y

f) diferencias en las políticas y en las declaraciones de ejecución práctica.

7.4.2 Servicio de atributos de privilegio

Algunos atributos de privilegio pueden cambiar más a menudo que otros atributos. Por tanto, se espera que solamente los atributos que se utilizan con frecuencia, y que son modificados pocas veces, deben incluirse en un certificado de claves públicas. Asimismo, debe utilizarse una estructura de datos independiente (por ejemplo, certificados de claves públicas, tickets, etc.) para "asegurar" aquellos atributos que han cambiado a menudo (por ejemplo, límite de crédito, privilegios de acceso, poder de representación dado por una compañía, etc.).

Para "asegurar" los atributos se pueden aplicar dos enfoques básicos:

1) Tickets – un ticket es una estructura de datos que contiene varios atributos y que es criptado por una TTP. Tales tickets se utilizan, por ejemplo, dentro de Kerberos (RFC 1510), y pueden contener una identidad de la entidad, dirección de red, etc.; y

2) Certificados de atributos – un certificado de atributos puede o no existir en combinación con un certificado de claves públicas. Ambos certificados pueden existir en combinación porque la clave pública asociada con el certificado de claves públicas debe utilizarse para probar que una entidad es el sujeto auténtico del certificado de atributos.

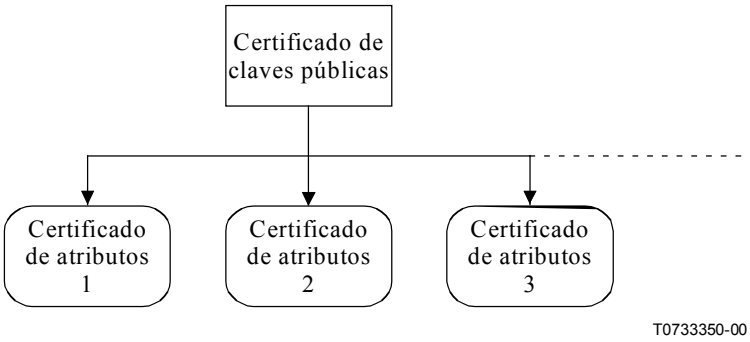


Figura 6 – Enlaces entre un certificado de atributos y un certificado de claves públicas

En la figura 6 se ilustra el segundo enfoque, en el cual un certificado de atributos se refiere inequívocamente a un certificado de claves públicas. Con un certificado de claves públicas se pueden enlazar más de un certificado de atributos. Diferentes certificados de atributos pueden soportar diferentes áreas de aplicación, por ejemplo, temas relacionados con las personas (crédito límite para el comercio electrónico), o autoridad dentro de una organización.

Cuando asigna solamente certificados de atributos, una TTP actúa como una autoridad de atributos (AA). En este caso los enlaces funcionales entre certificados de claves públicas y certificados de atributos, que se describen en la figura 6, implicarán la existencia de acuerdos apropiados entre las CA y las AA.

7.4.3 Servicio de autenticación en línea

Un proceso de autenticación en línea de una TTP se comporta como un servicio de certificación para certificados; de autenticación; la recuperabilidad de los certificados de autenticación puede hacerse en el siguiente intercambio de autenticación. Dicha TTP se conoce comúnmente como un servidor de autenticación.

7.4.4 Servicio de revocación de certificados

Una entidad autorizada para revocar un certificado, y quien desee revocar su certificado, deben ponerse en contacto con la CA que ha expedido el certificado para notificarla que éste no será válido en adelante. Después de que la CA haya comprobado el estado del certificado, la CA genera una CRL utilizando la firma de la clave privada de CA.

Una CRL es una lista firmada digitalmente que contiene la información de certificados revocados generada por la CA que ha expedido los certificados.

Cada CA debe gestionar la CRL que contiene todos los certificados revocados, y la información de la CRL debe contener un número de serie exclusivo y una fecha de revocación del certificado.

En otro enfoque puede utilizarse una TTP en línea como servidor de validación de certificados que proporcionan información sobre el estado (incluida la revocación) de un certificado identificado.

7.5 Servicios públicos de notaría electrónica

Los servicios públicos de notaría son servicios de alto nivel que utilizan varios servicios básicos, como la indicación de tiempo, la certificación, el servicio de directorio, el archivo digital y el no repudio. En principio, un documento será entregado a la TTP, y la TTP atestigua o certifica este documento mediante firmas digitales o por algún otro medio. Parte de este servicio puede ser un servicio de directorio, donde la información, tal como los documentos certificados anteriormente, puede recuperarse de una base de datos o directorio.

Un servicio público de notaría puede dar testimonio y certificar ciertas clases de documentos, por ejemplo que un documento ha existido en un momento determinado, a fin de darle credibilidad y autenticidad. Este servicio puede utilizarse por mediación de una controversia entre entidades y puede ser autorizado por alguna autoridad.

El servicio de certificación notarial opera como una notaría pública electrónica. Está capacitado para almacenar documentos firmados digitalmente y con indicación de tiempo. (Obsérvese que todos estos documentos han de estar registrados.)

Existen muchos temas complejos en las áreas de evidencia, autoridad notarial y responsabilidad civil. Los temas varían según las diferentes jurisdicciones, por lo que se sugiere una revisión y asesoramiento legal formal en estas áreas.

7.5.1 Servicio de generación de evidencias

La generación de evidencias (pruebas fehacientes) consiste en la recopilación de información TTP relativa a un documento, mensaje o evento relacionados con la seguridad, en una red o sistema. Puede incluir:

a) las identidades de las entidades involucradas;

b) la ubicación de las entidades;

c) los datos transferidos;

d) el método de transferencia; y

e) la indicación de tiempo.

Gran parte de esta información es la información típica requerida para proporcionar un seguimiento de auditoría.

Cuando una TTP recopila datos sobre eventos relativos a la seguridad en nombre de entidades, se puede necesitar para el análisis y estudio disponer de una lista similar de información y, sin que haya que identificar a los originadores de los datos, compartir los resultados con todas las entidades. Los detalles referentes a la recogida de estos datos deben describirse en acuerdos de nivel de servicio entre las entidades participantes y la TTP.

7.5.2 Servicio de almacenamiento de evidencias

De conformidad con ISO/CEI 13888-1, el servicio de almacenamiento de evidencias (pruebas fehacientes) se presta en combinación con los servicios de transferencia y recuperación de evidencias.

7.5.3 Servicio de arbitraje

Si se produce una controversia, y fallan los mecanismos y procedimientos de resolución de controversias de la TTP, puede ser necesario que un adjudicador proporcione servicios de arbitraje. El adjudicador es responsable de la recogida de evidencias de las partes en litigio y de la adopción posterior de una decisión que resuelva la controversia.

7.5.4 Autoridad notarial

Una autoridad notarial (NA, *rotary authority*) es una tercera parte confiable (TTP) que registra datos en un instante dado y puede también verificar la corrección de los datos específicos que han sido registrados de acuerdo con alguna política de seguridad. En su cometido principal, la NA actúa como un servicio de registro, mientras que en su función más amplia actúa como un servicio de validación. El servicio notarial puede de este modo contribuir a la prestación de un servicio de no repudio. Cuando realiza la verificación, la notaría añadirá información a los datos originalmente registrados. Esto puede permitir que las entidades que otorgan crédito a la notaria se aseguren de que los datos han sido verificados de conformidad con la política de seguridad en un momento dado.

A título de ejemplo, una notaría puede dar fe de una firma digital de acuerdo con una política de seguridad. En este caso, la NA verifica que el certificado incluido en la petición es un certificado válido, conforme a la política de seguridad, y determina su estado de revocación en un momento especificado. A continuación, supervisa el trayecto de certificación completo desde la entidad de firma del certificado a un punto de confianza . La NA puede ser capaz de confiar en todas las listas de revocación de certificados (CRL, *certificate revocation lists*) y listas de revocación de atributos (ARL, *attribute revocation lists*) pertinentes, o la NA puede tener necesidad de suplementar estas listas con el acceso a información de estado más actual para la CA. Incluye esta información, junto con un tiempo de confianza, para crear un testigo notarial.

Como segundo ejemplo, una notaría puede dar fe de una firma digital de acuerdo con una política de seguridad. La NA verifica que la firma digital y el trayecto de certificación son conformes con la política de seguridad. En este caso, se comprobará que la validez y el estado de revocación de un certificado de claves públicas de entidad y/o la validez y el trayecto de certificación completo desde la entidad de firma al punto de confianza (por ejemplo, la CA de NA, o la CA raíz en una jerarquía) son conformes con la política de seguridad. La NA puede ser capaz de confiar en todas las CRL y ARL pertinentes, o puede tener necesidad de suplementar estas listas con el acceso a información de estado más actual procedente de la CA. Incluye un tiempo de confianza y crea un testigo notarial.

Como ejemplo último, una notaría puede dar fe de datos formatados. La NA verifica la corrección de los datos y crea un testigo notarial. En este caso, sin embargo, la "corrección" de los datos no se centra solamente en la corrección de la firma; la definición concreta que ha de aplicarse depende por tanto necesariamente de la política de seguridad – y del tipo de datos –. Por ejemplo, los propios datos pueden contener una o más firmas (donde "corrección" se refiere a la validez de estas firmas), o puede contener aserciones (donde "corrección" se refiere al valor verdadero de estas declaraciones), o puede contener un contrato (donde "corrección" se refiere a la validez del documento).

La autoridad notarial puede:

a) verificar la corrección de la firma digital incluida utilizando toda la información de estado y certificados de claves públicas apropiados y, si lo solicita el peticionario, producir un testigo notarial firmado que atestigüe la validez de la firma;

b) verificar la validez del certificado incluido y su estado de revocación en el momento especificado utilizando toda la información de estado y certificados de claves públicas apropiados, y producir un testigo notarial firmado que atestigüe la validez y estado de revocación del certificado, si lo solicita el peticionario;

c) incluir un valor de la hora del día creciente monotónicamente o un testigo de indicación de tiempo en su testigo notarial;

d) incluir dentro de cada testigo notarial firmado un identificador que determine inequívocamente la política de confianza y validación de esta firma;

e) firmar cada testigo notarial con una clave generada exclusivamente para esta finalidad y tener esta propiedad de la clave indicada en el certificado correspondiente;

f) indicar en el testigo si la firma o certificado han sido verificados o no, y en caso negativo el motivo del fallo en la verificación; y

g) proporcionar un recibo firmado (esto es, en forma de un testigo notarial definido adecuadamente) al peticionario, cuando sea apropiado, como se define en la política.

En los Protocolos notariales IETF se pueden ver más detalles y un ejemplo de protocolo notarial.

7.6 Servicio de archivo digital electrónico

Un servicio de archivo digital electrónico es un servicio prestado por un registrador de documentos en el cual los documentos electrónicos son almacenados y mantenidos retenidos y seguros como registro permanente. El archivo de documentos electrónicos en forma criptada puede ser necesario en algunas instancias, en especial cuando los datos son altamente sensibles y requieren una protección adicional.

Las operaciones básicas de un servicio de archivo son:

a) almacenamiento de documentos – la TTP guarda una versión fechada de los documentos en una ubicación de almacenamiento segura durante un periodo fijo de tiempo; y

b) expedición de copias de documentos – el servicio de archivo expedirá, a petición de una entidad autorizada, una copia firmada de documentos registrados incluida la fecha de registro.

La autenticidad de los documentos registrados depende en primer término de técnicas criptográficas como las firmas digitales.

El archivo electrónico de documentos de larga duración, por ejemplo por motivos legislativos o legales, debe tener en cuenta cuatro aspectos básicos:

a) el medio de archivo puede tener necesidad de una regeneración periódica, por ejemplo, cinta magnética, CD-ROMs, etc.;

b) puede ocurrir que el equipo técnico de acceso a los datos archivados no tenga una duración de vida suficientemente larga para continuar proporcionando acceso a los datos archivados después del periodo de tiempo completo para el cual el acceso debe ser posible. El cambio de equipo exigirá la realización de una copia de seguridad y la transferencia de la información archivada a los nuevos equipos;

c) para interpretar un documento recuperado correctamente, puede también ser preciso proporcionar información adicional, tal como el formato de datos del documento (por ejemplo, ASCII, Postscript y HTML), el nombre del fichero y la fecha de creación. Además, se necesita el soporte lógico que trabajará con estos formatos de datos; y

d) puede suceder que los algoritmos criptográficos no tengan suficiente fortaleza para resistir los ataques durante el periodo de archivo; en estos casos se han utilizar técnicas de seguridad alternativas (por ejemplo, la seguridad física).

El servicio de archivo puede ser también utilizado (desde la perspectiva de los requisitos de funcionamiento) por una organización para la recuperación de documentos.

Un aspecto del servicio de archivo es el servicio de custodia o depósito que mantiene de forma segura los documentos electrónicos durante un periodo de tiempo definido. No debe entregarse un documento a otras entidades hasta que no se cumplan ciertas condiciones. La política de seguridad debe establecer las circunstancias bajo las cuales una entidad puede tener acceso a estos documentos, incluida la interceptación legislativa y legal (cuando sea aplicable), y el acceso de usuarios/empresas. Una TTP debe conservar una lista de todos los documentos custodiados ordenados cronológicamente.

Por ejemplo, si las entidades A y B tienen un acuerdo contractual que establece que la entidad A entregue a la TTP el código fuente del programa para mantenerlo de manera fiable en el caso de que la entidad A no pueda soportar o mantener más el programa. En una fecha posterior la entidad B puede obtener el código fuente del programa a partir de la TTP para soportar las funciones comerciales si se ven afectadas.

7.7 Otros servicios

Una TTP puede proporcionar varios servicios adicionales.

7.7.1 Servicio de directorio

En muchos casos los servicios de seguridad dependen de la información real y fidedigna, por ejemplo, los certificados de claves públicas, las listas de revocación de certificación, los certificados de atributos o un extracto de un registro comercial electrónico proporcionado por un directorio.

Antes de que pueda establecerse un servicio de directorio han de identificarse mediante un nombre los objetos en consideración. Para identificar un objeto de manera inequívoca, el nombre, o por lo menos el conjunto de objetos que ha de tratarse, debe ser exclusivo.

Una opción es aplicar la norma OSI de asignación de nombres y direcciones de la Rec. UIT-T X.650 | ISO/CEI 7498-3. Un ejemplo de servicio de directorio y sus correspondientes protocolos de acceso se ilustra en las Recomendaciones de la serie UIT-T X.500 | ISO/CEI 9594. Después de un acceso apropiado, un servicio de directorio permite a las entidades pedir información de la base de datos (colección de datos almacenados de modo permanente en alguna forma de almacenamiento).

En la figura 7 se ilustra una visión global de una arquitectura de servicio de directorio. Después del registro de entrada y la autenticación efectiva, cada consulta para solicitar datos del directorio se realiza a través del sistema de autorización. Si los derechos de acceso de la entidad concuerdan con las reglas de autorización, se concederá el acceso. En caso contrario, se puede enviar un mensaje de error a la entidad. Las tentativas de acceso fracasadas, por ejemplo, el fallo de la autenticación, deben producir una inserción en el registro de trabajo.

El gestor de peticiones tramita las peticiones autorizadas. Su tarea es compilar las consultas, acceder a la base de datos y entregar la respuesta a la entidad. No es necesario que toda la información esté localizada en una base de datos local.

La gestión de la seguridad de un servicio de directorio comprende los siguientes cometidos:

a) el administrador de la seguridad se ocupara de la definición de las reglas de autorización de conformidad con la política de seguridad; la gama de las reglas de autorización es amplia, por ejemplo, el servicio de directorio puede estar a disposición pública, o quedar restringido a un grupo cerrado de usuarios que está dispuesto a pagar el servicio;

b) el auditor revisa el fichero de trabajo periódicamente con el fin de detectar violaciones de la seguridad o la presencia de intrusos; y

c) el administrador de la base de datos se ocupa del mantenimiento la parte del directorio que contiene información relativa a la seguridad. Este agente tiene derechos de acceso y puede leer, escribir y suprimir información de la base de datos.

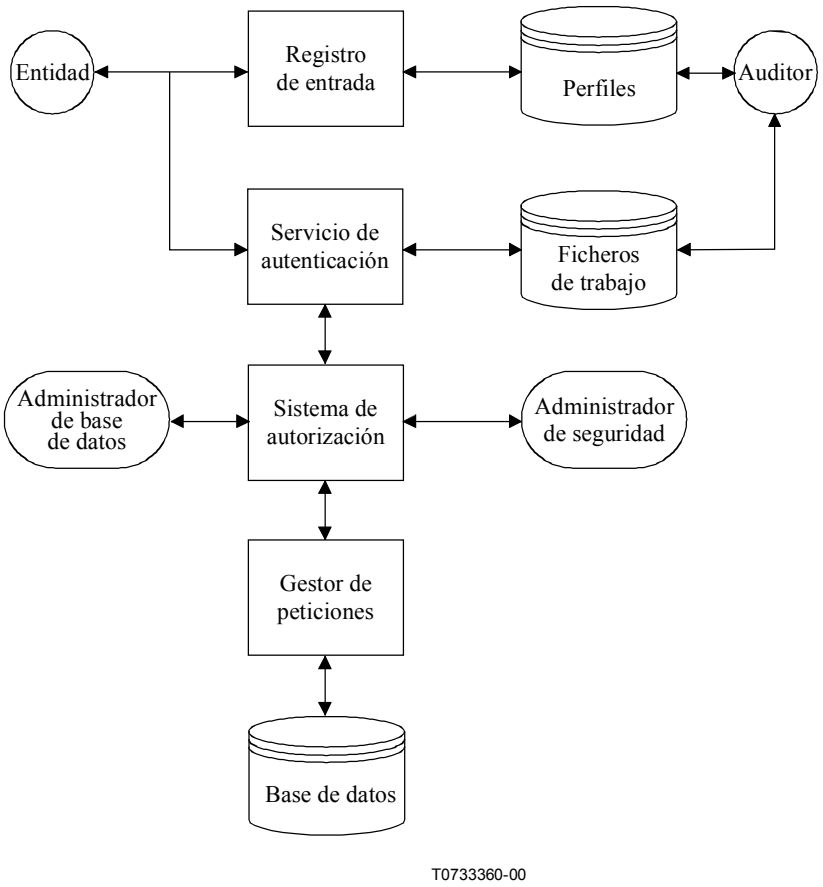


Figura 7 – Arquitectura del servicio de directorio

La información del directorio se puede recuperar por diferentes medios:

a) acceso fuera de línea: este método proporciona la distribución automática a los abonados de vez en cuando; el esquema temporal debe definir cuándo se espera la siguiente actualización; y

b) acceso en línea: este método proporciona la distribución a petición de las entidades; un directorio X.500 es un ejemplo típico.

7.7.2 Servicio de identificación y autenticación

En un escenario típico, donde una arquitectura distribuida está constituida por clientes y servidores distribuidos o centralizados, una entidad logra acceder a un servidor desde una estación de trabajo local (cliente). En este entorno, la seguridad puede ser facilitada por un servicio de autenticación soportado por una TTP.

Este servicio puede incluir la inicialización y el mantenimiento de un servicio de autenticación, así como el funcionamiento del equipo necesario, como un servidor de autenticación. Este servicio puede prestarse en línea o fuera de línea. Véase ISO/CEI 9798 para más detalles sobre las técnicas de autenticación. Han de considerarse requisitos adicionales de seguridad, por ejemplo, la protección de entidades contra la impostura, la integridad de los datos, la autenticidad del origen de los datos y la autenticación mutua entre entidades.

El servicio de autenticación puede incluir la autenticación de entidades (usuarios) o la autenticación de datos. En la mayor parte de los casos se necesita disponer de este servicio en línea. El servicio puede proporcionar la verificación de certificados o firmas y puede utilizar un protocolo de autenticación criptográfica o un código de autenticación de mensajes (MAC) para proporcionar una prueba de origen o una prueba de entrega de datos.

La implementación más común de un servicio de autenticación es el servicio de concesión de tickets del sistema Kerberos. (Para más información, véase Steiner y otros: Kerberos: an authentication service for open network systems in the proceeding winter 1988 USENIX Conference, págs. 191-202.)

7.7.2.1 Servicio de autenticación en línea

Cuando un número elevado de entidades necesitan comunicarse, una TTP puede utilizar un servicio de autenticación entre pares para evitar que cada entidad tenga que disponer de información de autenticación de todas las entidades. La TTP en línea interviene en cada operación de autenticación. La TTP puede autenticar la entidad A y dotarla de un certificado para presentarlo a la entidad B, o puede verificar la información de autenticación de la entidad A recibida por la entidad B en su nombre.

Los esquemas de autenticación simétricos requieren que cada entidad que desee ser autenticada deba compartir una clave secreta con cada una de las otras entidades. En lugar de generar y distribuir una número elevado de claves [n(n-1)/2 claves para un grupo de n entidades], puede utilizarse un autenticación en línea para reducir el número de claves. El resultado es el siguiente:

a) solamente la TTP que proporciona el servicio de autenticación compartiría una clave secreta con cada entidad; y

b) cada entidad compartiría una clave secreta con la TTP.

Se pueden aplicar dos métodos generales:

a) un método basado en testigos. Antes de que la entidad sea capaz de autenticar ella misma, la entidad puede pedir un testigo a la TTP. Este testigo se utiliza en el procedimiento de autenticación descrito con detalle más adelante; y

b) la entidad que desee ser autenticada envía un mensaje sellado, directamente, como el verificador no dispone de medios (no hay clave común) para validar este mensaje, la TTP lo procesa en nombre del verificador y le notifica el resultado.

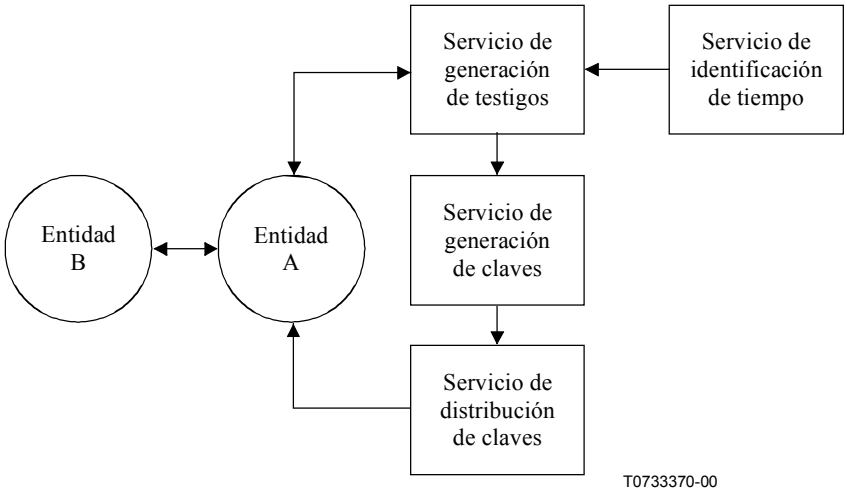


Figura 8 – Ejemplo de servicio de autenticación en línea

En la figura 8 se ilustra un modelo general para un servicio de autenticación en línea. Este servicio puede dividirse en dos fases:

a) fase de inicialización: Durante esta fase las tareas principales pueden ser la identificación adecuada de las entidades y el aprovisionamiento de material de claves; y

b) fase de funcionamiento: Se supone que el usuario, entidad A, tiene que autenticar por sí mismo a una TTP local que proporciona servicios de autenticación. Este servicio provee a la entidad A con las credenciales necesarias para que pueda acceder al usuario distante, entidad B.

En principio, este servicio se lleva a cabo en varios pasos, y cada paso puede estar constituido por más de un intercambio de mensajes. Si la entidad A desea acceder a una aplicación o servicio proporcionado por la entidad B, la entidad A puede efectuar los pasos 1 y 2:

1) La entidad A envía un petición al proveedor del servicio de autenticación junto con sus medios de autenticación (por ejemplo, contraseña, o testigo de autenticación generado mediante una tarjeta inteligente), solicitando credenciales.

2) El proveedor del servicio de autenticación verifica los derechos de acceso de la entidad A, y si se cumplen las condiciones responderá con un testigo que permite a la entidad autenticar ella misma y acceder al servidor o aplicación requerido en el sitio de la entidad B. El testigo puede contener una indicación de tiempo, clave de sesión, material criptográfico para la autenticación y, facultativamente, otro material.

Los pasos 3 y 4 no implican al servidor del servicio de autenticación directamente. Pero el testigo que autorice el acceso de la entidad A a servicios de la entidad B ha de seleccionarse de acuerdo con el material de claves compartido por el proveedor del servicio de autenticación y la entidad B.

3) El testigo se envía desde la entidad A a una entidad B distante, la cual verifica el testigo recibido. Este testigo debe seleccionarse de acuerdo con el material de claves que comparten la entidad B y el proveedor del servicio de autenticación . Si hay concordancia, la entidad B concederá el acceso al servicio requerido.

4) Opcionalmente, si se necesita una autenticación mutua, la entidad B debe autenticar ella misma a la entidad A del mismo modo seguro en que la entidad A lo ha realizado anteriormente.

En RFC 1510 proporciona un ejemplo de tal servicio de autenticación.

7.7.2.2 Servicio de autenticación fuera de línea

Los servicios de autenticación fuera de línea dependen en primer término de técnicas simétricas en combinación con servicios de gestión de certificados.

La TTP fuera de línea genera y distribuye con antelación certificados de autenticación fuera de línea que la entidad B puede más tarde utilizar para validar un intercambio de autenticación. Este certificado de autenticación puede ser almacenado por anticipado por la entidad B, o enviado junto con información de autenticación por la entidad A en el momento en que se efectúa la autenticación. Puede también almacenarse en un depósito del que la entidad B puede recuperarlo en caso necesario.

La autenticación fuera de línea que utiliza una TTP está asociada generalmente con el concepto de autoridades de certificación. En ISO/CEI 9798-1 e ISO/CEI 11770-1 se pueden encontrar detalles adicionales.

7.7.2.3 Servicio de autenticación dentro de línea

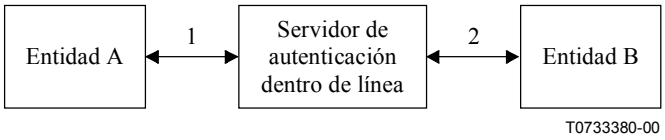


Figura 9 – Ejemplo de servicio de autenticación de TTP dentro de línea

En este ejemplo el servidor de autenticación TTP está situado en el trayecto de comunicación entre ambas entidades, tal como se representa en la figura 9. El proceso de autenticación se divide en dos pasos, y cada paso puede estas constituido por más de un intercambio de mensajes.

Primero, la entidad A intenta autenticar ella misma a una TTP. En segundo lugar, si la autenticación de la entidad A tiene éxito, la TTP autentica el mismo a la entidad B y confirma la identidad de la entidad A incluyendo una autenticación entre la TTP y la entidad B.

7.7.3 Servicio de conversión dentro de línea

Cuando dos entidades pertenecen a dominios de política de seguridad diferentes, la TTP ha de convertir la política de autenticación del dominio objetivo a la del dominio originador, por ejemplo, en términos de fortaleza de los mecanismos de autenticación empleados. Este esquema puede también consistir en una cadena de los TTP enlazando las dos entidades.

7.7.4 Servicios de recuperación

Estos servicios son facultativos y no se ofrecen generalmente como servicios separados, sino en combinación con otros servicios que pueden ser ofrecidos como parte del quehacer comercial diario.

7.7.4.1 Servicios de recuperación de claves

La recuperación de claves, la custodia de claves y el encapsulado de claves son funciones de un sistema criptográfico que proporcionan una capacidad de descriptación de reserva, permitiendo a entidades autorizadas, bajo determinadas condiciones, descriptar datos utilizando información suministrada por uno o más TTP. ("Trusted" (de confianza) en este contexto se utiliza para significar que existe confianza en ambos, el usuario y la entidad autorizada.)

El término recuperación de claves se utiliza de modos diferentes según el contexto en el que se aplica. Por ejemplo, en algunos contextos se utiliza como un término genérico que abarca ambos sistemas, de custodia y/o encapsulado. En otro contexto se aplica como un término de sustitución de custodia y/o encapsulado.

- Custodia de claves: En un sistema criptográfico que utiliza la custodia de claves, una copia de una clave secreta, o los medios para generarla, bien es mantenida por una TTP autorizada o bien puede ser dividida en dos o más partes que son mantenidas por TTP autorizadas. De conformidad con la legislación nacional, las TTP pondrían dichas claves o partes de claves a disposición de las entidades autorizadas.

- Encapsulado de claves: En un sistema criptográfico que utiliza el encapsulado de claves, los parámetros para reconstruir la clave son (a) bien añadidos a los datos criptados, o (b) bien asociados lógicamente con los datos criptados pero transportados o almacenados en una ubicación física independiente. De acuerdo con la legislación nacional, el sistema criptográfico permitiría a una tercera parte reconstruir una clave a petición con ayuda de información suministrada por uno o más TTP autorizadas. Con la encapsulación de claves, las TTP no retienen la clave o claves directamente, sino la información esencial necesaria para el proceso de reconstrucción.

NOTA – Las diferencias entre los distintos esquemas dependen esencialmente de los detalles de la implementación, de la infraestructura (es decir, las funciones y responsabilidades civiles asignadas a las TTP) y de los arreglos institucionales establecidos por la legislación nacional. En cualquier esquema, una vez que una copia de una clave secreta es reconstruida o entregada a una tercera parte, esta clave no se puede considerar en adelante como secreta. Por ejemplo, todas las comunicaciones y datos almacenados criptados con esta clave pueden eventualmente ser descriptados. La recuperación, la custodia y el encapsulado de claves debe utilizarse solamente con claves de confidencialidad.

Los servicios de recuperación de claves permiten que sean descriptados los datos que están siendo comunicados o que se encuentran almacenados. Son campos típicos de aplicación los de interceptación legal (cuando es aplicable) y el acceso usuario/empresa. La principal diferencia entre estos campos se aplicación son las condiciones prescritas bajo las cuales puede tener lugar la descriptación del texto cifrado.

Por ejemplo, una organización puede decidir operar un servicio de recuperación para facilitar claves que permitan recuperar ficheros e información comercial de una compañía que han sido criptados por empleados. Las claves son aplicadas para la descriptación de emergencia en la recuperación de datos criptados mediante claves que se han perdido o han resultado dañadas.

Se necesitan mecanismos de control de acceso fuertes donde solamente las personas autorizadas, identificadas y autenticadas de una lista selectiva puedan acceder a las claves. Para aumentar la confianza y fiabilidad de las claves, pueden almacenarse éstas de forma criptada o ser distribuidas a más de una ubicación.

Cuando una TTP presta servicios de recuperación de claves, puede combinar los cometidos de un agente de generación y/o distribución de claves para sus usuarios con el de suministrador de claves de usuario. Una TTP que explota tales servicios se deberá ocupar también de temas como la revocación, almacenamiento, recuperación y reconstrucción de claves.

7.7.4.2 Servicios de recuperación de datos

Este servicio puede ser cumplimentado mediante uno de los dos esquemas básicos siguientes:

El primer tipo de esquema está caracterizado por claves privadas o secretas asociadas con entidades que se depositan con una o más TTP antes de que sean criptados los datos para su comunicación o almacenamiento. Esta información de claves se puede utilizar de conformidad con los requisitos legales y contractuales en un momento posterior a la recuperación de los datos.

El segundo tipo de esquema se caracteriza porque un particular utiliza material de claves públicas relativo a una o más TTP para la criptación de datos destinados a comunicación o almacenamiento. El procedimiento de criptación permite la descriptación por parte del receptor deseado. Permite también la recuperación de los datos de conformidad con los requisitos legales y contractuales utilizando material de claves privadas, mantenidos por una o más TTP, y de la información asociada con los datos criptados.

7.7.5 Servicio de personalización

El servicio de personalización incluye la criptación de material criptográfico seguro en testigos de seguridad, por ejemplo, tarjetas inteligentes. El material criptográfico comprende entre otros elementos las claves secretas, las claves públicas, los certificados y los números aleatorios. Éstos elementos pueden escribirse en una entorno resistente a la alteración, legibles solamente por entidades deseadas, identificadas y autenticadas. Este servicio debe proveer un registro del testigo personalizado y de los propietarios autorizados.

7.7.6 Servicio de control de acceso

Una TTP en línea puede proporcionar información de control de acceso del mismo modo que suministra información de autenticación cuando la solicita una entidad autorizada. Actúa como un servicio de certificación de privilegios de control de acceso de una entidad, con la finalidad de garantizar que los recursos de un sistema de gestión de claves solamente puede ser accedido por entidades autorizadas y de un modo autorizado. En ISO/CEI 11770-1 se recogen detalles al respecto. Una TTP de control se acceso en línea se conoce como servidor de control de acceso.

7.7.7 Servicio de informe de incidentes y gestión de alertas

De conformidad con ISO/CEI TR 13335 una política de seguridad IT debe revisarse periódicamente y mantenerse actualizada para hacer frente a los cambios rápidos del entorno. Deberá disponerse de procedimientos para tratar los eventos de seguridad específicos detectados por la TTP (o señalados a su atención) que proporciona los servicios de informe de incidentes y gestión de alarmas. Este servicio puede ser procesado manual o automáticamente.

Si se produce un incidente, como el fraude, bien la información detallada sobre el mismo se comunica a la entidad responsable de incidentes notificados, o bien dicha entidad detecta por sí misma el incidente:

a) cualquiera de las entidades puede enviar un mensaje de alerta a una TTP; o

b) una TTP puede recibir automáticamente información sobre el evento, por ejemplo por seguimiento de la comunicación; o mediante petición de información a otras entidades, por ejemplo detección como resultado de la pérdida de disponibilidad.

Tal incidente tiene consecuencias en la organización pertinente y requiere que se efectúen análisis y estudios, adoptándose resoluciones que evitarán o reducirán el impacto de una repetición del incidente.

Cuando una entidad comunica un incidente a su TTP, la TTP debe proporcionar los servicios de gestión de alertas a otras entidades, tal como esté estipulado en sus acuerdos en el nivel de servicio.

Adicionalmente, la información del evento pertinente (ocurrencia, repercusión y actuaciones) debe ponerse a disposición para ulteriores análisis y estudios. Como consecuencia de la información de alerta, las actuaciones de gestión pueden ser, por ejemplo, la transmisión de mensajes de alerta a otras entidades, y posiblemente a otras TTP. Un motivo puede ser que una clave privada de autoridad de certificación o una clave privada (o secreta) de entidad está comprometida.

Hay ejemplares donde las entidades desearían compartir y tener acceso a información reunida acerca de peligros, vulnerabilidades, incidentes y eventos relativos a la seguridad en sus sectores de negocio. Sin embargo, estas entidades son renuentes a compartir información cuando ello puede significar una exposición de su sistema de seguridad o un reducción del grado de confianza de sus clientes. Una TTP puede proporcionar un servicio entre entidades en el que la información es reunida, analizada y compartida con otras entidades de acuerdo con el nivel de los acuerdos de servicio existentes. En la figura 10 se ilustra el ejemplo de una TTP que puede recopilar información sobre incidentes relativos a la seguridad procedente de una entidad y luego, sin identificar la entidad, compartir esta información con las demás entidades. La TTP puede también recoger información de todas las entidades para su análisis y compartir entonces los resultados con todas las entidades.

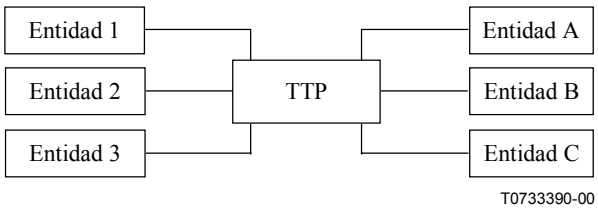


Figura 10 – Ejemplo de servicio de gestión de alertas

Anexo A

Requisitos de seguridad para la gestión de las TTP

(Este anexo no es parte integrante de esta Recomendación | Informe técnico)

En la práctica, debe llevarse a cabo una evaluación para identificar el nivel de riesgo asociado con los servicios TTP que se vayan a implementar. La robustez de los requisitos de seguridad que ha de seleccionarse depende de los servicios específicos proporcionados por la TTP y de los riesgos involucrados en el caso de que deban comprometerse los servicios TTP. Los requisitos de seguridad asociados con estos riesgos identificados deben ser especificados en la política de seguridad de las TTP. Esta evaluación y el desarrollo de la política deben incluir lo siguiente:

a) los usuarios, administradores y personal de explotación de las TTP solamente deben tener acceso a la información y los recursos de los que son titulares;

b) los procedimientos administrativos deben asegurar la identificación única y segura y el registro de los usuarios y operadores de los servicios TTP;

c) la información altamente sensible, que es de importancia fundamental para mantener la confianza en la TTP, tal como la clave privada de una autoridad de certificación (CA) o la clave de nivel superior de un centro de distribución de claves, debe ser generada, instalada y gestionada por procedimientos fiables y perfectamente documentados;

d) para asegurar el rastreo de las operaciones y transacciones y rendición de cuentas de las entidades, deben adoptarse las siguientes medidas con la determinación requerida las siguientes medidas:

   1) autenticación de las entidades;

   2) firma electrónica de todas las peticiones, transacciones y operaciones sensibles a la seguridad; y

   3) restricción de la auditoría de datos a las autoridades apropiadas (por ejemplo, auditores de seguridad).

e) para proteger la privacidad y los intereses comerciales de todas las entidades involucradas, la información en las interfaces, transportada por los protocolos y ubicada en dispositivos de almacenamiento, debe tener el nivel requerido de protección con respecto a su integridad y confidencialidad;

f) el sistema de seguridad, incluido el funcionamiento de dicho sistema de seguridad, de todos los componentes gobernados por la política de seguridad de la TTP, debe proporcionar la protección necesaria en el entorno de funcionamiento real;

g) una gestión adecuada de la seguridad debe abarcar la iniciación, supervisión y control de los servicios de seguridad que protegen a los servicios proporcionados por la TTP;

h) debe disponerse de procedimientos para regresar a un estado seguro en caso de quiebra de la seguridad. Esto implica también la recuperación o reemplazamiento de las claves secretas de alto nivel de la TTP;

i) debe disponerse de mecanismos de salvaguarda frente a cualquier punto aislado de vulnerabilidad que pueda existir en los sistemas; en los cuales una TTP sea capaz de recuperar los datos criptados mediante el uso de la recuperación de claves;

j) si la política de seguridad de las entidades involucradas lo exige, la TTP debe proporcionar los medios de garantizar que solamente las claves requeridas por una entidad autorizada pueden ser recuperadas por la TTP; y

k) deben incluirse procedimientos de recuperación que hagan mínimo el impacto en la entidad, a través de procedimientos de notificación apropiados.

Anexo B

Aspectos relativos a la gestión de la CA

(Este anexo no es parte integrante de esta esta Recommendation | Informe técnico)

B.1 Ejemplo de procedimientos del proceso de registro

La CA se encarga de emprender la realización de los procedimientos fijados para establecer que el solicitante de un certificado es la persona que dice ser. Bajo determinadas circunstancias, la CA puede autorizar a otra entidad, llamada autoridad de registro (RA, *registration authority*) a efectuar el proceso de registro del abonado en nombre de la CA.

El proceso de inscripción del abonado puede ser iniciado por el solicitante (la persona que pretende abonarse), la CA, una RA o un funcionario de la organización que está coordinando el establecimiento de una red de la organización.

La CA (RA) debe verificar que el solicitante de un certificado tiene derecho a obtener ese certificado, y si el certificado determina que el abonado tiene atributos o privilegios particulares, entonces el solicitante tendrá los correspondientes atributos y privilegios.

La relación de un abonado con un empleador y la aprobación por parte del empleador de la expedición de un certificado para el abonado han de estar certificadas por un representante legítimo de la organización empleadora.

En su acuerdo con el empleador, la CA deberá garantizar que la organización empleadora asume la responsabilidad de informar a la CA sobre cambios pertinentes en la situación de empleo durante el periodo de validez de los certificados expedidos.

El (o la) solicitante debe presentarse personalmente a una CA, RA o representante designado de la CA, a fin de ser autenticado antes de la expedición del certificado. Esta gestión es independiente de que el abonado sea autónomo o que esté asociado con un empleador. Es algo que sólo puede ser tratado directamente por el empleador en el caso de que el propio empleador sea una CA o una RA designada por la CA.

El solicitante debe presentar documentos de identificación válidos. En el formulario de solicitud deben recogerse los medios de identificación, y el encargado en la CA, o su RA representante, han de firmar personalmente que la verificación se ha efectuado realmente.

Cuando se realiza la autenticación de un solicitante, el abonado debe presentar a la CA o a la RA una tarjeta de identificación con fotografía certificada y comúnmente reconocida, tal como un carné de identidad nacional.

Si el solicitante no posee una identificación con fotografía como la señalada anteriormente, esta identificación puede ser sustituida por un documento del gobierno que certifique la existencia de la identidad pretendida asociada a una persona independiente mayor de edad, que es autenticada como se ha descrito anteriormente y que certifica que el solicitante posee la identidad pretendida.

Los detalles presentados sobre dicha persona, tales como los identificadores, el nombre y la dirección registrada exclusivos, deben compararse con la información que reside en un registro oficial, o en otro registro de la organización o de un tercero que ha recibido para esta finalidad la confianza de la CA.

B.2 Ejemplo de requisitos para las autoridades de certificación

Una autoridad de certificación (CA) que expide certificados debe operar de conformidad con una política de certificados apropiada. La política de certificados debe encargarse al menos de:

a) proveer servicios de certificación y custodia que sean coherentes unos con otros;

b) proporcionar controles relativos a los requisitos de funcionamiento;

c) llevar a cabo los procedimientos de autenticación relativos al registro inicial y a las peticiones de revocación;

d) expedir certificados de acuerdo con la definición de la política de certificados y aceptar las distintas representaciones del abonado y partes confiantes presentadas en una declaración de ejecución práctica de la certificación (CPS) (declaración de las prácticas que emplea una autoridad de certificación cuando expide los certificados);

e) reconocer los derechos de los abonados y las partes confiantes que utilizan certificados de conformidad con la legislación y regulación aplicables;

f) revocar certificados y expedir listas CRL de la definición de la política de certificados (el aprovisionamiento de la suspensión de certificados es una facultad de la autoridad de certificación); y

g) acatar todas las disposiciones de su definición de política de certificados y cualquier disposición legal de una CPS publicada.

La CA es responsable de todos los cometidos enumerados anteriormente, con independencia de si son cumplimentados por la CA o por una autoridad de registro (RA) designada por la CA. Los compromisos de la CA frente a todas las entidades externas incluyen por tanto todos los compromisos de la RA.

Las CA deben proporcionar las tareas adicionales concernientes a:

a) *La protección de la clave privada de la CA expedidora*

   Una CA debe proteger su clave privada de conformidad con ciertas disposiciones descritas en la definición de la política de certificados.

b) *Las restricciones en la utilización de la clave privada de la CA expedidora*

   Una clave privada de CA utilizada para la expedición de certificados conformes a esta política de certificados debe utilizarse solamente para los certificados de firma y, opcionalmente, para las CRL y otras informaciones adecuadas coherentes con la expedición de certificados.

   Si una CA determina actuar de acuerdo con otras políticas, utilizando la misma clave privada o identidad expedidora, estas políticas deben estar identificadas en la CPS.

Una RA es una entidad encargada de la identificación y autenticación de entidades de certificados de claves públicas, pero no es una CA o una AA, y en consecuencia no firma o expide certificados. Una RA puede prestar asistencia en el proceso de aplicación de los certificados o en el proceso de revocación de los mismos, o en ambos. No es preciso que la RA sea un cuerpo independiente, sino que puede formar parte de la CA.

A una RA se la pueden asignar las siguientes responsabilidades:

a) validar la identidad de la entidad solicitante de un certificado de claves públicas, de conformidad con la declaración de ejecución práctica de la certificación de CA (CPS, *certification practice statement*);

b) validar que la identidad de la entidad solicitante del certificado es la entidad certificada en el certificado. Esto puede ser cumplimentado habiendo firmado la entidad la petición del certificado y habiendo la RA validado la firma mediante la clave pública presentada para certificación;

c) registrar las entidades autenticadas de modo seguro;

d) notificar a la entidad identificada en el certificado el éxito del registro y comunicarle que el certificado ha sido expedido;

e) mantener los registros de auditoría que soportan los certificados que expide durante el periodo de tiempo determinado por los requisitos de retención de los registros;

f) proporcionar directrices a los abonados acerca de la gestión segura de la clave privada de abonado;

g) utilizar cualquier medio apropiado para comprobar que la entidad identificada en el certificado asume sus responsabilidades y está capacitada para cumplirlas;

h) informar a las entidades del dominio cuándo se ha comprometido la clave privada de CA;

i) tratar las peticiones de revocación de certificados procedentes de entidades;

j) informar a las entidades identificadas en el certificado de que la integridad de sus operaciones se considerarán comprometidas si su clave privada es alguna vez revelada a, o utilizada por, una entidad no autorizada; y

k) mantener una la gestión y unas actuaciones prácticas de control seguras que serán confirmadas por procedimientos y procesos de aseguramiento de la calidad de la seguridad, y por auditorías de conformidad independientes.

Una RA que interviene en actuaciones prácticas relacionadas con la expedición de certificados debe encargarse como mínimo de las siguientes tareas:

a) suministrar los controles referentes a los requisitos operacionales de la definición de la política de certificados;

b) ejecutar los procedimientos de autenticación de conformidad con las reglas expuestas en la definición de la política de certificados;

c) acometer las tareas contratadas y soportar los derechos de los abonados y las partes confiantes que utilizan certificados, de conformidad con la legislación y regulación aplicables de ámbito federal, estatal y provincial; y

d) cumplir las disposiciones relativas a la responsabilidad civil, responsabilidad financiera, tasas, publicaciones y depósito, auditoría de conformidad, confidencialidad, derechos de propiedad intelectual, acuerdos contractuales estipulados en la definición de la política de certificados y en cualquier disposición legal de una CPS publicada.

Además, las RA pueden ser requeridas legalmente para cumplir con otras garantías.

Las RA deben suministrar las tareas adicionales siguientes:

a) protección de su clave privada de conformidad con las disposiciones de la política de certificados;

b) las claves privadas utilizadas en fines asociados con su función de RA no deben emplearse para cualquier otro fin sin la autorización expresa de la CA; y

c) el uso de las claves privadas de la RA debe restringirse de conformidad con las estipulaciones de utilización de claves recogidas en sus certificados asociados.

El abonado tiene también algunas obligaciones que deben estar registradas en el acuerdo entre la CA y el abonado conforme con las disposiciones contractuales, las cuales incluyen:

a) el abonado debe tratar de seguir los procedimientos establecidos cuando solicita un certificado;

b) el abonado debe retener el control de su clave privada, protegerla de acuerdo con partes aplicables de la definición de la política de certificados y adoptar precauciones razonables para evitar su pérdida, revelación a terceros, modificación o uso no autorizado;

c) el abonado debe informar a la CA acerca de cualquier sospecha de que la clave pueda haber sido comprometida ;

d) el testigo criptográfico, en el cual están almacenadas las claves privadas, debe protegerse en una medida comparable a la de documentos personales valiosos, como las tarjetas de crédito o el carnet de conducir. El PIN o contraseña utilizado para desbloquear el testigo no debe guardarse nunca en el mismo sitio que el testigo mismo; y

e) los abonados no deben dejar olvidado su testigo criptográfico en estado de desbloqueado (es decir, olvidado en una estación de trabajo cuando ya se ha introducido el PIN o contraseña).

B.3 Política de certificación y declaración de ejecución práctica de la certificación (CPS)

Cuando una autoridad de certificación expide un certificado, proporciona una declaración a un usuario de certificado (es decir, a una parte que confía) de que una clave pública concreta esta destinada a una entidad determinada (el sujeto de certificado). Sin embargo, la medida en que el usuario de certificado debe confiar en la declaración de CA ha de ser evaluada por el propio usuario. Los diferentes certificados son emitidos siguiendo diferentes prácticas y procedimientos, y pueden ser adecuados para diferentes aplicaciones y/o finalidades.

UIT-T X.509 | ISO/CEI 9594-8 define una política de certificado como un "conjunto denominado de reglas que indica la aplicabilidad de un certificado a una determinada comunidad y/o clase de aplicación con requisitos de seguridad comunes". Un certificado de X.509 Versión 3 puede contener una indicación de política de certificados, la cual puede ser utilizada por un usuario de certificado para decidir si confiar o no un certificado para un objetivo particular.

Una política de certificados, que necesita ser reconocida tanto por el expedidor como por el usuario del certificado, está representada en un certificado por un identificador de objeto registrado exclusivo. El proceso de registro sigue los procedimientos especificados en Recomendación UIT-T | Normas Internacionales. La parte que registra el identificador de objeto también publica una especificación literal de la política de certificados para su examen por los usuarios de certificados. Un certificado normalmente declarará una sola política de certificados o, posiblemente, se emitirán siendo coherente con un número pequeño de políticas diferentes.

Las políticas de certificados constituyen también un base para la certificación cruzada de autoridades CA junto con una Declaración de ejecución práctica de la certificación (CPS). Cada CA es certificada frente a una o más políticas de seguridad que se sabe que están implementadas. Cuando una CA expide un certificado CA para otra CA, la CA expedidora debe evaluar el conjunto de políticas de certificados para las cuales otorga su confianza la CA sujeto (esta evaluación puede estar basada en la certificación con respecto la política de certificados involucrada). El conjunto de políticas de certificados evaluado es entonces indicado por la CA expedidora en el certificado CA. La lógica del procesamiento del trayecto de certificación UIT-T X.509 emplea estas indicaciones de políticas de certificados en su modelo de confianza perfectamente definido. Los conceptos de política de certificados y CPS proceden de diferentes fuentes y han sido desarrollados por diferentes motivos. Sin embargo, su interrelación es importante.

Una CPS es una declaración detallada de una CA en cuanto a sus actuaciones prácticas, cuyo conocimiento y consulta por parte de los abonados y los usuarios de certificados (partes que confían) pueden resultar necesarios. Aunque el nivel de detalle puede variar de una CPS a otra, por lo general serán más detalladas que las definiciones de políticas de certificados. En efecto, las CPS pueden ser documentos robustos muy completos que proporcionan una descripción de los servicios precisos ofrecidos, los procedimientos detallados de la gestión del ciclo de vida de los certificados y, además – un nivel de detalle que asocia la CPS con una implementación determinada (propietario) de un servicio ofrecido.

El detalle de una CPS es necesario para efectuar una evaluación completa de la fiabilidad en ausencia de acreditación o de otra medida reconocida de la calidad. Una CPS detallada no constituye sin embargo por sí sola una base adecuada para la interoperabilidad entre CA explotadas por diferentes organizaciones. Por el contrario, las políticas de certificados sirven mejor como vehículo de las partes confiantes para determinar si un certificado particular es adecuado para su aplicación/finalidad. Una CA con una sola CPS puede soportar múltiples políticas de certificados (utilizadas para diferentes aplicaciones y fines y/o por diferentes comunidades de usuarios de certificados). También, múltiples CA diferentes, con CPS que no son idénticas, pueden soportar la misma política de certificados.

Refiérase también a RFC 2527, Certificate Policy and Certification Practices Framework, S. Chokhani, W.Ford, marzo de 1999.

Anexo C

Bibliografía

(Este anexo no es parte integrante de esta Recomendación | Informe técnico)

Referencias informativas

- AS/NZS 4444, Australian / New Zealand Standard Code of Practice.
- BS 7799, British Standard Code of Practice – Revisión 1, 1999.
- ETSI EG/SEC-003000, *Requirements for Trusted Third Party Services* (Edition 1), Version 7.0, julio 1997.
- FIPS PUB 140-1, Federal Information Processing Standard Publication 140-1, Security Requirements for Cryptographic Modules, *U.S. Department of commerce, National Institute of Standards and Technology, enero 1994*.
- ISO/CEI Guide 61:1996, *General requirements for assessment and accreditation of certification / registration bodies.*
- ISO/CEI Guide 65:1996, *General requirements for bodies operating product certification systems.*
- ISO/CEI 9798-2:1999, *Information technology – Security techniques – Entity authentication – Part 2: Mechanisms using symmetric encipherment algorithms.*
- ISO/CEI 9798-3:1998, *Information technology – Security techniques – Entity authentication – Part 3: Mechanisms using digital signature techniques.*
- ISO/CEI 9798-4:1999, *Information technology – Security techniques – Entity authentication – Part 4: Mechanisms using a cryptographic check function.*
- ISO/CEI 10118-1:2000, *Information technology – Security techniques – Hash-functions – Part 1: General.*
- ISO/CEI 10118-2:2000, *Information technology – Security techniques – Hash-functions – Part 2: Hash-functions using an n-bit block cipher.*
- ISO/CEI 10118-3:1998, *Information technology – Security techniques – Hash-functions – Part 3: Dedicated hash-functions.*
- ISO/CEI 13888-1:1997, *Information technology – Security techniques – Non-repudiation – Part 1: General.*
- ISO/CEI 13888-3:1997, *Information technology – Security techniques – Non-repudiation – Part 3: Mechanisms using asymmetric techniques.*
- ISO/CEI 15408-1:1999, *Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model.*
- ISO/CEI 15408-2:1999, *Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional requirements.*
- ISO/CEI 15408-3:1999, *Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance requirements.*
- ISO TC68 SC2 15782-1, *Banking – Certificate Management Part 1: Public Key Certificates.*
- ISO/CEI 15945, *Information technology – Security techniques – Specification of TTP services to support the application of digital signatures.*
- ISO/CEI 15946-3, *Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 3: Key establishment.*
- Recomendación UIT-T X.520 (2001) | ISO/CEI 9594-6:2001, *Information technology – Open Systems Interconnection – The Directory: Selected attribute types.*
- Recomendación UIT-T X.650 (1996) | ISO/IEC 7498-3:1997, *Information technology – Basic Reference Model: Naming and addressing.*
- Recomendación UIT-T X.680 (1997) | ISO/CEI 8824-1:1998, *Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation.*

– Recomendación UIT-T X.681 (1997) | ISO/CEI 8824-2:1998, *Information technology – Abstract Syntax Notation One (ASN.1): Information object specification.*

– Recomendación UIT-T X.682 (1997) | ISO/CEI 8824-3:1998, *Information technology – Abstract Syntax Notation One (ASN.1): Constraint specification.*

– Recomendación UIT-T X.683 (1997) | ISO/CEI 8824-4:1998, *Information technology – Abstract Syntax Notation One (ASN.1): Parameterization of ASN.1 specifications.*

– Recomendación UIT-T X.811 (1995) | ISO/CEI 10181-2: 1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Authentication framework.*

– Recomendación UIT-T X.812 (1995) | ISO/CEI 10181-3: 1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Access control framework.*

– Recomendación UIT-T X.814 (1995) | ISO/CEI 10181-5: 1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Confidentiality framework.*

– Recomendación UIT-T X.815 (1995) | ISO/CEI 10181-6: 1996, *Information Technology – Open Systems Interconnection – Security frameworks for open systems: Integrity framework.*

– ITSEC, *Information Technology Security Evaluation Criteria (ITSEC)*, Harmonised Criteria of France, Germany, the Netherlands, the United Kingdom, Version 1.2, junio de 1992.

– NIST, *Computer Security Handbook.*

– NIST, *Minimum Interoperability Specification for PKI Components (MISPC)*, 1997.

– PKIX Part V, Internet X.509 Public Key Infrastructure, Internet Draft, Time Stamp Protocols, C. Adams, P. Cain, D. Pinkas, R. Zuccherato, marzo de 2000 (work in progress).

– PKIX Part VI, Internet X.509 Public Key Infrastructure, Internet Draft, Data Certification Server Protocols, C. Adams, Sylvester, Zolotarev, R. Zuccherato, marzo de 2000 (work in progress).

– RFC 1421, *Privacy Enhancement for Internet Electronic Mail: Part 1: Message Encryption and Authentication Procedures*, febrero de 1993.

– RFC 1422, *Privacy Enhancement for Internet Electronic Mail: Part 2: Certificate-Based Key Management*, febrero de 1993.

– RFC 1423, *Privacy Enhancement for Internet Electronic Mail: Part 3: Algorithms, Modes, and Identifiers*, febrero de 1993.

– RFC 1424, *Privacy Enhancement for Internet Electronic Mail: Part 4: Key Certification and Related Services*, febrero de 1993.

– RFC 1510, *The Kerberos Network Authentication Service*, septiembre de 1993.

– RFC 1750, *Randomness Recommendations for Security*, diciembre de 1994.

– RFC 2459, *Internet X.509 Public Key Infrastructure Certificate and CRL Profile*, enero de 1999.

– RFC 2510, *Internet X.509 Public Key Infrastructure Certificate Management Protocols*, marzo de 1999.

– RFC 2527, *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*, marzo de 1999.

– RFC 2559, *Internet X.509 Public Key Infrastructure Operational Protocols – LDAPv2*, abril de 1999.

– S2101/02, *Report to the Commission of the European Communities for the "Code of Practice and Management Guidelines for Trusted Third Party Services"*, Version 1.0, 1993.

– SAA MP75-1996, *Strategies for the Implementation of a Public Key Authentication Framework (PKAF) in Australia.*

– STEINER *et al.:* Kerberos: an authentication service for open network systems in the proceeding winter, *USENIX Conference,* pp. 191-202, 1988.

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	Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedios
Serie K	Protección contra las interferencias
Serie L	Construcción, instalación y protección de los cables y otros elementos de planta exterior
Serie M	RGT y mantenimiento de redes: 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 Y	Infraestructura mundial de la información y aspectos del protocolo Internet
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Ginebra, 2001