LA SEGURIDAD DE LAS TRANSACCIONES BANCARIAS EN INTERNET

Jordi Buch i Tarrats
Director de servicios profesionales de Safelayer

Francisco Jordán
Director de Investigación y Desarrollo de Safelayer

"Las nuevas tecnologías basadas en infraestructuras de clave pública (PKI) y en los protocolos SSL (Secure Sockets Layer) y SET (Secure Electronic Transaction) son las únicas que permiten cubrir las carencias de seguridad de la red Internet."

INTRODUCCIÓN

Las transacciones bancarias se realizan en su mayor parte sobre redes de conmutación de paquetes X.25. Este tipo de redes se consideran suficientemente seguras por estar controladas por operadores autorizados y no por presentar medidas de seguridad basadas en técnicas criptográficas, autentificación segura o integridad de la información. La red Internet es una red pública, por lo que el riesgo de que las amenazas contra la autenticidad, integridad, confidencialidad y el no repudio de las transacciones que sobre ella se realicen será mayor.

Las nuevas tecnologías en el terreno de la seguridad en sistemas de información basadas en infraestructuras de clave pública (PKI) y en los protocolos SSL ("Secure Sockets Layer") y SET ("Secure Electronic Transaction") son las únicas que permiten cubrir las carencias de seguridad de la red Internet que afectan a la protección de la información que fluye a través de la red de redes.

La tecnología PKI también se aplica a los sistemas de banca virtual sobre Internet garantizando la seguridad de las operaciones bancarias tradicionales como órdenes de compra/venda de valores, órdenes de transacciones interbancarias, gestión de cuentas, etc.

DEFINICIONES

Certificado digital: Es la certificación electrónica generada por una autoridad de certificación, que vincula unos datos de verificación de firma a un signatario y confirma su identidad. El certificado tiene una validez determinada y un uso concreto.

Firma electrónica avanzada: Es la firma electrónica que permite la identificación del signatario y ha sido creada por medios que éste mantiene bajo su exclusivo control, de manera que está vinculada únicamente al mismo y a los datos a los que se refiere, lo que permite que la detección de cualquier modificación ulterior de éstos.

Autoridad de Certificación (CA): Un servicio que genera un certificado digital después de verificar la identidad de la persona o entidad que se identificará mediante el uso de éste. La autoridad de certificación también genera las listas de revocación. Aunque existen varios estándares que definen el formato de los certificados digitales y las listas de revocación, el X509v3 para certificados y CRLv2 son los que están reconocidos por la mayoría de proveedores de tecnología.

Lista de revocación (CRL): La lista de revocación está firmada electrónicamente por la autoridad de certificación e indica los certificados que han sido revocados antes de que estos expiren.

Criptografía de clave pública: El conjunto de técnicas y estándares que permiten la identificación electrónica de una entidad, firmar electrónicamente y cifrar datos. Implica el uso de dos claves; una de privada y una de pública. La segunda, se pública en los certificados digitales.

Infraestructura de clave pública (PKI): Los estándares y servicios que facilitan el uso de la criptografía y los certificados en un entorno de red.

"Secure Sockets Layer" (SSL): Es un protocolo que permite la autentificación mutua de un usuario y un servidor con el propósito de establecer una conexión cifrada. "Secure Electronic Transaction" (SET): Protocolo que asegura la confidencialidad y la integridad de los pagos basados en tarjeta hechos por Internet, con independencia de quien sea el comprador y el vendedor del producto. El protocolo garantiza la autenticidad de las partes.

LA SEGURIDAD EN LA RED INTERNET

En el diseño de Internet, parte de la seguridad en Internet fue delegada en el mutuo respeto y honor de los usuarios, así como el conocimiento de un código de conducta considerado "apropiado" en la red. Una mínima seguridad se basa en una protección "blanda", consistente en una identificación del usuario mediante un identificador y una clave secreta que sólo éste conoce (login y password).

La red Internet tiene problemas de autenticidad, integridad, confidencialidad y repudio afectando a los requerimientos de las transacciones electrónicas u operaciones de banca virtual de la siguiente forma:

–Robo de información: El robo de información mediante escuchas de red, permite obtener información del usuario como números de cuentas o de tarjetas de crédito, balances de cuentas o información de facturación. Estos ataques, también

permiten el robo de servicios normalmente limitados a suscriptores. Por el hecho de conocer la realización de una transacción roza la invasión de la privacidad.

–Suplantación de identidad: La suplantación de identidad permite al atacante realizar operaciones en nombre de otro. Una situación de este tipo permitiría a un poseedor de miles de números de tarjetas de crédito la realización de numerosas pequeñas operaciones que representen en su totalidad una cantidad significativa. También puede interesar al atacante la suplantación de identidad del usuario de banca virtual.

–"Sniffers": Los "sniffers" son herramientas informáticas que permiten la obtención la lectura de la información que se transmite por la red (claves de paso o información de operaciones). Los "sniffers" permitirán la consumación de un ataque de suplantación de identidad y/o robo de información.

–Modificación de información: La modificación de datos permite alterar el contenido de ciertas transacciones como el pago, la cantidad o incluso la propia orden de compra.

–Repudio: El rechazo o negación de una operación por una de las partes puede causar problemas a los sistemas de pago. Si una parte rechaza un previo acuerdo con la respectiva, ésta deberá soportar unos costos adicionales de facturación.

–Denegación del servicio: Un ataque de denegación de servicio inhabilita al sistema para que éste pueda operar en su normalidad, por lo tanto imposibilita a las partes la posibilidad de realización de operaciones transaccionales. Éstos son de extrema sencillez y la identificación del atacante puede llegar a ser imposible. Las soluciones pueden no son únicas y no se tratarán en adelante.

PKI COMO SOLUCIÓN DEFINITIVA

El establecimiento de una infraestructura de clave pública permite garantizar los anteriores requerimientos. La confidencialidad se garantiza cifrando los datos que viajarán por la red. Mediante el uso de firmas digitales, se garantiza la autenticidad, la integridad y el no repudio de los datos. Sin embargo, la estructura no se puede desplegar sin la existencia del servicio de los componentes necesarios que aporten la confianza en el uso de las claves públicas mediante la generación de los certificados, su gestión y revocación cuando sea necesario.

Para el despliegue de la infraestructura se precisan los siguientes componentes:

–Autoridad de Certificación (CA). La CA emite certificados para las partes que intervienen, en definitiva, da fe de quien nos presenta una clave pública es quien

dice ser. La CA también mantiene las listas de revocación de certificados para resolver los casos de robo, pérdida o suspensión de claves privadas. La seguridad de la CA es crítica; un problema de seguridad que afecte a la CA puede afectar a toda la infraestructura existente.

–Directorio. El directorio es la base de datos donde se publican los certificados. De esta forma, los certificados están disponibles todas las entidades. En el directorio, además se guardan otros datos las listas de revocación.

–Sistema de revocación de certificados: Aunque sea un servicio asociado a la autoridad de certificación, éste se puede suministrarse por otra entidad.

–Actualización, históricos y copias de claves: Son los componentes que permiten la renovación del certificado, y el uso de claves antiguas. En los sistemas donde interviene datos cifrados hay que suministrar el servicio de recuperación de claves.

–Soporte para el no repudio: La protección de las claves privadas puede ser crítica para el no repudio de las firmas digitales realizadas. Los sistemas basados en tarjetas criptográficas son los que ofrecen las mayores garantías. Estos componentes deben existir y pueden estar gestionados por la propia entidad bancaria (por ejemplo Banco de Sabadell), un consorcio (por ejemplo, Iberion) o otra entidad externa.

BANCA VIRTUAL

En banca virtual, los clientes realizan las operaciones bancarias de forma remota. El sistema se implanta sobre redes TCP/IP (Internet), WAP (comunicaciones móviles) o propietaria (por ejemplo, cajeros automáticos). En el segundo, también interviene la red Internet.

El sistema de banca virtual distingue entre:

–Autentificación de usuario.

–Autorización de transacciones.

El sistema debe disponer de un servicio de acreditación fuerte para accesos a servicios (los basados en web son especialmente cómodos de implantar, aunque pueden complementarse con soluciones de mensajería segura) y ofrecer la plataforma electrónica para que los usuarios puedan firmar digitalmente datos. Es importante resaltar que los sistemas actuales implantan mejoras en el sistema de autentificación, que aunque es más segura, sigue basándose en identificadores de usuario y contraseñas.

Para la acreditación fuerte se recomienda el protocolo SSL (o TLS) de forma que el usuario que dispone de un certificado digital de operación bancaria puede acreditarse al sistema, mientras que éste se acredita al usuario con su respectivo certificado de servidor. El mismo protocolo garantizará la confidencialidad y integridad de los datos. Si el usuario opera con un teléfono móvil, se usará el protocolo WTLS.

El sistema bancario virtual deberá guardar las órdenes de transacciones generadas por los usuarios, para los que éstos deberán firmarlas digitalmente con su clave de firma digital. Los estándares usados son el PKCS#7 definido por RSA y S/MIME si el sistema de basa en mensajería segura.

Procedimientos

La autentificación consiste en que el usuario entrega al servidor un desafío-respuesta (un paquete de datos aleatorios) firmado digitalmente con su clave privada. El servidor verificará que la el certificado se ha emitido por una Autoridad Reconocida (la propia del Banco u otra que reconozca), que el certificado no haya expirado ni revocado y que se ha usado el apropiado. En este momento, el sistema ya ha asociado el identificador o alias presente en el certificado a un contrato de banca virtual de un cliente.

En el procedimiento de autorización de transacciones, el usuario devuelve la orden firmada digitalmente y el servidor, una vez validada mediante el mismo procedimiento anterior la guardará para asegurarse el no repudio de ésta. La orden de transferencia no se procesará hasta que se hayan realizado los pasos anteriores.

TRANSACCIONES BASADAS EN SET

Con la ayuda de los grandes fabricantes de la industria de ordenadores y programas, Visa y MasterCard han desarrollado el que se está erigiendo en el protocolo de pago por excelencia para la práctica del Comercio Electrónico minorista (es decir, venta entre comerciante y usuario final). SET (Secure Electronic Transaction) es un protocolo que emula de forma electrónica, mediante el uso de certificados y firmas digitales, el pago de bienes y/o servicios mediante tarjeta de crédito[1].

1. Inicialmente sólo se pensó en tarjetas de crédito dada la naturaleza de sus patrocinadores, sin embargo posteriormente también se ha introducido el uso de tarjeta de débito con uso de PIN por Internet.

Arquitectura SET

Como método de pago basado en tarjeta, la solución SET (ver figura) conlleva la presencia de 3 nuevas entidades electrónicas a parte de los sistemas tradicionales ya utilizados en la actualidad. Los nuevos componentes son:

–Entidad “Merchant” SET o Comerciante SET es la entidad encargada de gestionar el pago del bien o servicio iniciado por un comprador. El pago siempre lleva asociado una transacción con un aceptador (“acquirer”) para la autorización del importe a pagar por el comprador. Habitualmente a esta entidad se le denomina POS (“Point Of Sale”) o TPV (Terminal Punto de Venta) virtual ya que su comportamiento, entre otras funciones, simula el de los sistema tradicionales.

–Entidad “Cardholder” SET o Titular SET es la encargada de actuar en nombre del titular de la tarjeta virtual para realizar el pago. Habitualmente a esta entidad se le conoce como Wallet o Cartera ya que su funcionalidad es muy similar a una cartera en la cual se almacenan las tarjetas.

–Entidad “Gateway” SET o Pasarela SET cuya función es la de hacer de puente entre el sistema aceptador SET y el sistema financiero propietario ya existente. Esta entidad es muy importante en cuanto supone la conexión de los sistemas y redes de autorización privados existentes con el mundo de Internet.

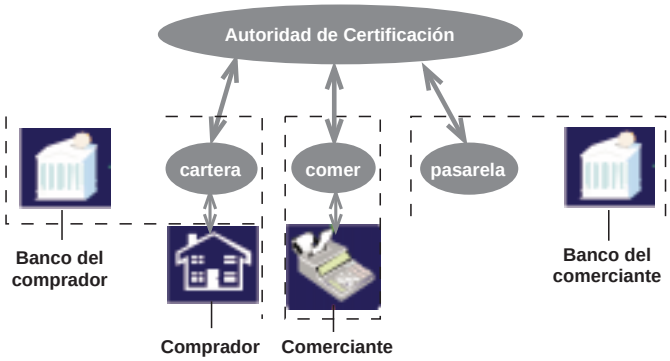

Figura 1. Componentes de SET

En el sistema SET la seguridad en las transacciones se ha cuidado hasta el último detalle. El sistema utiliza las últimas tecnologías de firma digital y certificación para llevar a cabo la protección de los datos a través de Internet.

Todas las entidades implicadas en el SET deben estar en posesión de un certificado válido para poder intervenir en una transacción de pago. Esto quiere decir que

tanto titulares, comerciantes y pasarelas SET deben de ser identificadas previamente y proveerles de un certificado para que puedan funcionar dentro del sistema.

Las entidades que generan los certificados para las entidades SET participantes se denominan CA SET o Autoridades de Certificación SET y generalmente son operadas por instituciones financieras capaces de emitir tarjetas (emisores) o instituciones asociadas, como bancos, que solicitan la emisión de tarjetas.

Las Autoridades de Certificación siempre están asociadas a una Marca de tarjeta particular. Esto quiere decir que los certificados de todas las entidades sólo son válidos para una Marca determinada siendo imposible utilizarlo en otro ámbito (al igual que en los sistemas tradicionales, es imposible utilizar una tarjeta Visa como si se tratase de una MasterCard). De lo que se desprende que una entidad deberá estar en posesión de tantos certificados como Marcas diferentes utilice (de ahí la acepción cartera para referirse a la entidad SET de titulares). Esto por otra parte hace muy flexible el sistema lo que, como se verá a continuación, nos permitirá utilizarlo dentro del ámbito de Marcas privadas.

Por último mencionar que existen varios tipos de Autoridades de Certificación SET dependiendo de su función y a quien certifiquen.

Protocolo de Pago SET

El protocolo de pago SET define los mensajes e interacciones entre las entidades SET (comprador, comerciante y pasarela de pago) para llevar a cabo una transacción de pago desde que el comprador acepta pagar hasta que dicho pago se realiza mediante un abono en la cuenta del comerciante desde la cuenta del comprador. La siguiente figura muestra un esquema en el que aparecen los mensajes e interacciones típicas de un pago (existen varias combinaciones de mensajes y este es el que obedece al esquema implantado en España).

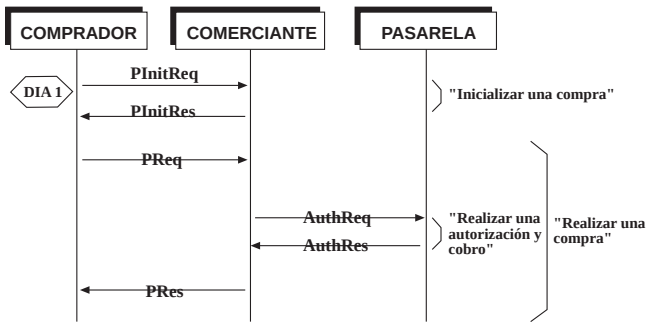

Figura 2. Protocolo de pago SET

Como se observa existen 3 fases:

1.–Fase de Inicialización: que corresponde al mensaje *PInit* y en la que el comprador contacta con el comerciante. El comprador informa de la marca de tarjeta que va a utilizar en el pago y el comerciante responde con un mensaje firmado que contiene el certificado de cifrado de la pasarela de pago asociada.

2.–Fase de Pago: que corresponde al mensaje *P* y en la que el comprador, si acepta el pago después de verificar la identidad del comerciante y las condiciones, realizara la orden de pago. La respuesta de este mensaje contiene información sobre la aceptación o denegación del pago proveniente de la autorización.

3.–Fase de Autorización: que corresponde al mensaje *Auth* y en el que el comerciante solicita a la pasarela de pago (que a su vez solicitará al sistema financiero tradicional) si el comprador puede hacerse cargo de dicho pago (tiene crédito o saldo, la tarjeta no está revocada, etc.). La respuesta de este mensaje contiene información sobre la aceptación o denegación del pago. En este esquema se ha optado realizar la captura o cobro del pago en la misma fase de autorización.

Mencionar que SET implementa el sistema de *firma dual* en el que el comprador en el mensaje *PReq* incluye datos protegidos para el comerciante y para la pasarela de forma que, el comerciante sólo puede ver los datos de la compra (pedido, modo de pago, cantidad, etc.) y la pasarela sólo puede ver los datos de pago (número de tarjeta, modo de pago, cantidad, etc.) que se enviarán en el mensaje *AuthReq*. De esta forma el comerciante nunca tendrá el número de tarjeta del comprador y la entidad financiera (a través de la pasarela) nunca tendrá los datos de la compra.

Como se puede observar del esquema presentado la fase de autorización ocurre durante la fase de pago. A esta modalidad se le conoce como pago en línea inmediato y es la más utilizada, aunque SET admite diferentes modalidades siendo un sistema que se adapta a los sistemas existentes en diferentes países.

Además de las fases y mensajes vistos, SET proporciona también servicios para retrocesos o cambios de autorizaciones realizadas y administración de “batchs”.

Problemas de implantación

En la actualidad existen varias implantaciones SET en el mercado (ver la lista de fabricantes en la web de SETCo-www.setco.org) pero hasta llegar a este punto se han encontrado con diferentes problemas. En el presente todavía persisten ciertos problemas que hacen que SET no se esté utilizando de forma masiva sin embar-

go dichos problemas se están paliando con la modificación de ciertos aspectos del sistema. A continuación se enumeran algunas de las barreras que se han encontrado en el desarrollo de SET:

–Debido a su gran contenido de funcionalidad y sus altos grados de seguridad, SET es un sistema complejo y ha hecho que los fabricantes tardaran mucho en tener un sistema completo y estable en el mercado. La misma causa ha hecho que los distintos desarrollos comerciales se encontraran ciertos aspectos de incompatibilidad a nivel de protocolo y funcionalidad.

–Las grandes inversiones de los fabricantes de sistemas SET en el desarrollo han hecho que los precios de los productos sean elevados frenando de este modo su adquisición masiva. Además, coyunturalmente tampoco parece que el comercio electrónico (minorista en este caso) haya despegado masivamente así que las inversiones en infraestructura no suponen una de las prioridades inmediatas y se hacen a un ritmo lento.

–Existe algún problema de aceptación en el usuario final (sobre todo del comprador). Debido también a la complejidad del sistema, en la mayoría de los casos el producto final resulta complejo de instalar y administrar.

TRANSACCIONES BASADAS EN SSL

Quizás por las dificultades de implantación del protocolo SET, la mayor parte de los sistemas transaccionales se basan en la actualidad en soluciones basadas en SSL y no en el protocolo SET, relajando las medidas de seguridad. A estos sistemas se les conoce de forma genérica como punto de venta virtual (TPV virtual).

La principal carencia de los pagos SSL es la imposibilidad de firmar digitalmente la orden de transacción que emite el comprador eliminando de esta forma el requisito que éste posea un certificado digital. Finalmente, se soluciona la problemática que supone el hecho de que el comerciante tenga acceso al número de tarjeta de crédito del comprador situando el TPV virtual en la pasarela de pagos (que se encuentra en la entidad financiera), y solicitando éste la autentificación al comerciante (en contra a la solución SET que es el comerciante quien traslada la orden que de compra a la pasarela).

Para reducir el riesgo que supone la imposibilidad de realizar una autentificación fuerte al comprador (basta conque el número de tarjeta tenga saldo para poder realizar una transacción), se han creado las denominadas tarjetas virtuales caracterizadas por disponer de un saldo fijo que se agota, siendo necesaria su recarga posterior.

Pagos SSL

Las pasarelas de pago SSL se activan en el momento que un comprador desea realizar el pago después de haber seleccionado los artículos deseados.

1.–El comercio informa a la pasarela que desea cargar un importe a un número de tarjeta de crédito o débito de un comprador. Para esto envía el importe a cargar, una referencia al TPV virtual. La operación implica un proceso de autentificación fuerte del comercio al TPV virtual (mediante un canal SSL y con un certificado generado por la CA de la pasarela).

2.–El comprador es redireccionado al TPV virtual, quien informa al comprador del importe, los datos del comercio y la referencia de la compra. La conexión entre el comprador y TPV virtual se realiza con el protocolo SSL, pero solo autenticando al servidor, garantizando al comprador que va a enviar datos al servidor correcto.

3.–El comprador introduce el número de tarjeta.

4.–El TPV virtual obtiene de la pasarela de pagos el resultado de la transacción presentándose ésta al cliente y informando al comerciante.

5.–El TPV virtual redirecciona el comprador al comercio.

Finalmente, el comercio puede gestionar el TPV virtual de forma remota mediante la correspondiente acreditación. Las operaciones que podrá realizar son las de operaciones “batch”, descarga de operaciones y consultas en general. Una operación adicional que permiten algunos TPV virtuales es la realización de operaciones manuales, actuando como un terminal punto de venda clásico.

Migración a SET

La mayor parte de las soluciones de TPV virtual permiten también la operación en SET y se deja en manos del comprador la posibilidad de realizar el pago SET o SSL. Se trata de una solución SET en donde el componente POS reside en el TPV virtual (confundiéndose con el componente pasarela) y no en el sitio del comerciante.

Actualmente la cartera SET del comprador sigue esta misma tendencia, situándose ésta en la propia entidad emisora de tarjetas. La solución se conoce como “server wallet” y esta apoyada por VISA y MASTERCARD.

CONCLUSIONES

La implantación de seguridad en las transacciones realizadas sobre la red Internet implica la disponibilidad de una infraestructura de clave pública (PKI) y el uso de protocolos seguros como SET o SSL. El componente CA de dicha infraestructura es crítico y debe gozar del suficiente grado de confianza por todas las partes. La CA puede gestionaste por un banco, un consorcio de bancos o alguna otra entidad externa.

SET es el protocolo que aporta el mayor grado de seguridad a al vez que es extremadamente complejo. Esta circunstancia ha imposibilitado el despliegue definitivo de los sistemas de pago basados en el protocolo definido por VISA y MasterCard. Se espera que el nuevo concepto de "server wallet", que se fundamenta en que los certificados digitales SET no residen en el cliente, sino en un servidor gestionado por las entidades de pago, suponga el despliegue definitivo. El "server wallet" supone una mayor facilidad de uso para el usuario aportando además un alto grado de movilidad a la vez que provoca una disminución del nivel de seguridad.

Las soluciones de pago basadas en SSL ofrecen una solución alternativa, mucho menos segura pero gozan de fuerte implantación. Se prevé que dichas soluciones migren a una solución final de SET basada en "server wallet" y pasando por una solución mixta en donde el TPV virtual se ofrezcan como servicio del banco.

La firma digital aplicada a los sistemas de banca virtual aporta la propiedad del no repudio a las órdenes de transacción emitidas por los clientes. Aunque en la actualidad el sistema no esta implantado en la mayoría de las soluciones de banca electrónica, la rápida consolidación de la tecnología PKI y el reconocimiento legal del sistema fuerce la implantación masiva a corto plazo.

REFERENCIAS

1. Sistema de Certificación Global <http://www.verisign.com>
2. Criptografía <http://www.rsa.com>
3. Protocolo SET <http://www.setco.org>
4. SSL, Firma de formularios, firma de código <http://www.netscape.com>
5. Microsoft Windows 2000 PKI <http://www.microsoft.com>
6. Demos de SET y SSL <http://www.safelayer.com>

PKI CASO PRÁCTICO: BANCO SABADELL

"Banco Sabadell, PRIMER banco en España que ofrece a sus clientes la tecnología PKI en tarjeta-chip para asegurar las operaciones de Banca Internet"

RESUMEN

Tras una introducción de las características de la PKI y diferentes aspectos a considerar, se explica como se implantó la solución de banca electrónica en el Banco de Sabadell. El modelo se fundamenta en una Autoridad de Certificación que emite lotes de certificados de autentificación y firma digital en tarjetas con sistema operativo TIBC.

Los certificados emitidos no están asociados a ningún cliente en particular, dicha asociación se realiza a posteriori. Esta característica permite que los clientes obtengan todo lo necesario para "Home Banking" de una sola vez y no deban volver a completar el procedimiento tal y como es habitual en otros sistemas PKI.

La emisión de este tipo de certificados se basa en el suministro de una clave privada y un certificado de firma digital y autentificación. Su fortaleza y viabilidad presenta tres pilares tecnológicos:

–Tamaño de llaves de 1024 bits

–Soporte de tarjetas inteligentes TIBC

–Integración con la tecnología existente usando un plug-in de acceso a la tarjeta inteligente para Netscape Communicator y Microsoft Internet Explorer

PKI COMO SOLUCIÓN DEFINITIVA

La implantación de una solución de infraestructura de clave pública –en adelante PKI– en una corporación tiene como finalidad la securización total de las comunicaciones, dando la mejor solución a los problemas de integridad, confidencialidad y acreditación. En una estructura PKI, los clientes –en adelante usuarios– y servidores disponen de un par de claves asimétricas, guardando la privada preferiblemente en una tarjeta inteligente y distribuyendo la pública en un certificado

emitido por un centro certificador –en adelante CA–. La CA garantiza la autenticidad de los datos que figuran en el certificado (nombre, clave pública, etc.) durante un período de validez también indicado en el propio certificado, definido por la CA. El certificado también indica los usos de su clave privada (ejemplo: firma digital, acreditación en servidores, sellos de tiempo, cifrado, etc.).

Los problemas más inmediatos que soluciona una estructura PKI son:

–Control de acceso: Acreditación de usuarios en servidores.

–No repudio: La firma digital, que tiene asociadas las propiedades de autentificación y integridad, posibilita que el firmante no pueda repudiar su acción.

–Confidencialidad: Cifrado de datos usando la clave pública de los destinatarios.

Aunque a también se extiende a soluciones de "single sign-on", VPNs, firma de código, firma de datos, "secure desktop", etc.

Problemas a resolver

El sistema de acreditación tradicional o basado en identificador de usuario y contraseña tiene tres importantes carencias:

–Copia/interceptación fácil y de difícil detección: La acreditación del usuario se basa en una/unas contraseña/s ("password") que se puede/n copiar sin que el propietario disponga de los mecanismos necesarios para la detección de copia y por lo tanto pueda iniciar un proceso de revocación.

–En ocasiones, el usuario dispone de diferentes contraseñas o incluso diferentes identificadores de usuario, lo que provoca que éstas acaben apuntadas en un papel.

–No se guarda constancia firmada por el usuario de las transacciones autorizadas.

Los dos primeros problemas no se dan con la PKI, y si se usan tarjetas inteligentes, son prácticamente inexistentes. Por otra parte, la PKI afronta directamente el tercer problema.

Características de la PKI

La solución PKI es el único esquema que no presenta las anteriores carencias. En definitiva, el sistema permite:

–Establecer un servicio de acreditación fuerte para accesos a servicios. Los basados en web son especialmente cómodos de implantar, pero la solución se extiende a sistemas de "single sign on".

–Ofrecer la plataforma electrónica para que los usuarios puedan firmar digitalmente datos.

–Ofrecer la plataforma tecnológica para que los usuarios puedan ejecutar programas en su navegador de forma segura (firma de código).

–Ofrecer la tecnología para que los usuarios dispongan de correo seguro (S/MIME) y puedan securizar sus archivos (PKCS#7) de la forma más estándar.

–Ofrecer la plataforma para que los servidores puedan ser certificados y garantizar de esta forma su autenticidad.

–Total integración en cualquier solución futura basada el PKI (redes privadas virtuales, accesos a servidores, etc.).

Características de los certificados emitidos

Los certificados emitidos se deben ajustar a las especificaciones X509v3 y soportar las extensiones de Netscape. Esta característica permite la generación de certificados sin tener que conocer qué software va a usar el cliente, requisito importante en entornos donde no existe una política clara de soporte a un único proveedor.

Se generan diferentes tipos de certificados:

–Certificados de cliente para acreditarse en servidores seguros y firmar datos.

–Certificados para servidores.

–Certificados para programadores. Permiten firmar código ejecutable para garantizar a los usuarios la autenticidad del programa. Es la forma más segura de acabar con los virus y caballos de troya.

Es importante destacar que no se precisa de modo alguno de la clave de cifrado ya que las comunicaciones entre el cliente y la entidad se realiza sobre una conexión cifrada mediante el uso del protocolo SSL.

ESCENARIOS DE USO

En PKI existen diferentes escenarios para la implantación del modelo de certificación. La solución adoptada es un compromiso entre los procedimientos de registro, la facilidad de uso del cliente u la seguridad del sistema.

Modelos de Certificación: El problema del registro de los usuarios

Se contemplaron dos modelos de certificación de usuarios:

–Modelo tradicional: Los clientes generan su par de claves para solicitar la certificación a la CA, a partir de un formulario dispuesto para tal fin. Este es el esquema usado, por ejemplo por Verisign < hyperlink “http://www.verisign.com” http://www.verisign.com>.

–Un modelo donde la CA genera los pares de claves y los certificados por lotes, a partir de los datos suministrados por la entidad de registro (lista de clientes, personal en plantilla, etc.). Los certificados junto con las claves privadas se entregan en soporte de tarjeta inteligente (“smartcard”) o bien en fichero (PKCS#12).

El segundo modelo presenta importantes ventajas diferenciales sobre el primero, para el entorno objetivo del proyecto:

–En el primer modelo, el proceso de aprobación de peticiones se debe realizar una a una. Este proceso se caracteriza por ser necesaria la comprobación de los datos del solicitante mediante la solicitud del DNI, o cualquier documento acreditativo. Es el modelo válido en centros certificadores globales, pero puede llegar a ser redundante en corporaciones, empresas, etc. que ya disponen de los datos de los posibles solicitantes a priori, y que ya cuentan con medios seguros de comunicación con éstos. El segundo modelo, en cambio, admite como entrada peticiones ya validadas, para generar directamente los certificados y claves privadas en lotes, y reduciendo de forma considerable la carga administrativa.

–En el primer modelo, el usuario debe contactar con el centro certificador primero y esperar a que se le apruebe su solicitud, mientras que en el segundo, el usuario o cliente obtiene directamente el certificado. Para el usuario es más simple el segundo.

–El primer modelo precisa la necesaria formación del personal de las oficinas bancarias para que actúen de aprobadores de solicitudes de certificación.

–El servicio de certificación del segundo modelo no tiene que estar conectado en red, permitiendo de esta forma un mayor nivel de seguridad de forma inmediata.

–Finalmente, en el segundo modelo, no necesariamente se deben conocer los datos de los clientes, siendo posible el uso de “alias” que posteriormente se asociarán a éstos.

Modelos de firma y navegación

En los modelos de seguridad de PKI se distinguen tres modelos:

–"Modelo de seguridad web": Usa los mecanismos de seguridad de que disponen los navegadores más populares (Netscape y Internet Explorer). Tiene carencias de seguridad posiblemente no asumibles por la política de certificación corporativa (por ejemplo, en esta solución de "Home Banking").

–"Modelo de seguridad PROXY", donde se desconfía de la seguridad de los navegadores y se controla ésta mediante programas independientes (que interpretan la política de seguridad corporativa) y

–"Modelo de seguridad mixto" que pretende suplir las carencias de seguridad de los navegadores añadiéndoles módulos o "plug-ins". Este modelo soluciona las carencias de los anteriores garantizando que la ni la clave privada ni el PIN de la tarjeta del usuario van a estar en el ordenador del cliente[1] simplemente facilitando la interfaz PKCS#11/CSP con una tarjeta chip para integrarse de forma cómoda y eficiente en el programa.

Los tres basan su solución en el modelo PKI. La solución mixta es la que permite garantizar el nivel máximo posible de seguridad en un entorno como el requerido, solucionando las carencias del "modelo de seguridad web", manteniendo el nivel óptimo de libertad de los usuarios en la elección de su plataforma de trabajo y evitando en la medida de lo posible los posteriores problemas de dimensionado de carga de una "hot line"

SOLUCIÓN IMPLANTADA

El Banco de Sabadell se planteó el problema de cómo suministrar 10.000 certificados (en una primera fase) sin que tuviesen que pasar todos los clientes dos veces "por ventanilla".

La Autoridad de Certificación se creó con el propósito de que generase todos los certificados a partir de una lista de identificadores únicos que entrega la propia entidad –que por lo tanto, actúa de Autoridad de Registro–. Los identificadores únicos se incluyen en el atributo nombre ("CN") del campo sujeto del certificado X509. Dicho atributo se considera como un alias para asignarlo posteriormente a un contrato de "Home Banking" de un cliente de la entidad.

1. Usando un lector de tarjetas con teclado numérico y procesador o una tarjeta con procesador.

Este modelo además presenta otras importantes ventajas:

–La seguridad de la Autoridad de Certificación es extremadamente alta: Se trata de una autoridad que está desconectada de la red. Sólo se pone en marcha cuando es necesaria la generación de un lote de certificados.

–Calidad en la generación de las claves privadas: Es la CA quien genera las claves privadas de los usuarios, con lo que se garantiza una calidad óptima de éstas.

–Facilidad de administración: El número de personal de administración se reduce a dos operadores de un grupo superior a dos que tienen autorización para procesar un lote. No se precisan de administradores de registro.

Procedimiento de entrega de claves

Las tarjetas inteligentes generadas se distribuyen de forma estratégica en las oficinas de la entidad, junto con los PINs de acceso a éstas.

Cuando el cliente desea darse de alta al servicio de "Home Banking", éste deberá firmar el contrato de Banca Virtual en el que se le asocia un identificador único a su cuenta corriente (dicho identificador incluido en el certificado, también figura en la tarjeta para su comprobación visual). La aceptación de dicho contrato implica una alta en el sistema entregándosele un PIN, un lector y un plug-in de acceso al lector no siendo necesario ningún paso adicional por parte del cliente.

Sistema de "Home Banking"

El sistema se apoya en un servidor web seguro que garantiza la confidencialidad de la comunicación mediante el protocolo SSL usando claves de cifrado de 128 bits.

El sistema de "Home Banking" distingue entre autentificación de usuario y autorización de transacciones.

La autentificación consiste en que en usuario entrega al servidor un desafio-respuesta firmado digitalmente con su clave privada. El servidor verificará que la el certificado se ha emitido por una Autoridad Reconocida (actualmente la propia del Banco de Sabadell), que el certificado no haya expirado ni revocado y que se ha usado el apropiado. En momento, el sistema ya ha asociado el identificador o alias presente en el certificado a un contrato de "Home Banking" de un cliente.

En el procedimiento de autorización de transacciones, el usuario devuelve la orden firmada digitalmente y el servidor una vez validada mediante el mismo procedimiento anterior la guardará para asegurarse el no repudio de ésta. La orden de transferencia no se procesará hasta que se hayan realizado los pasos anteriores.

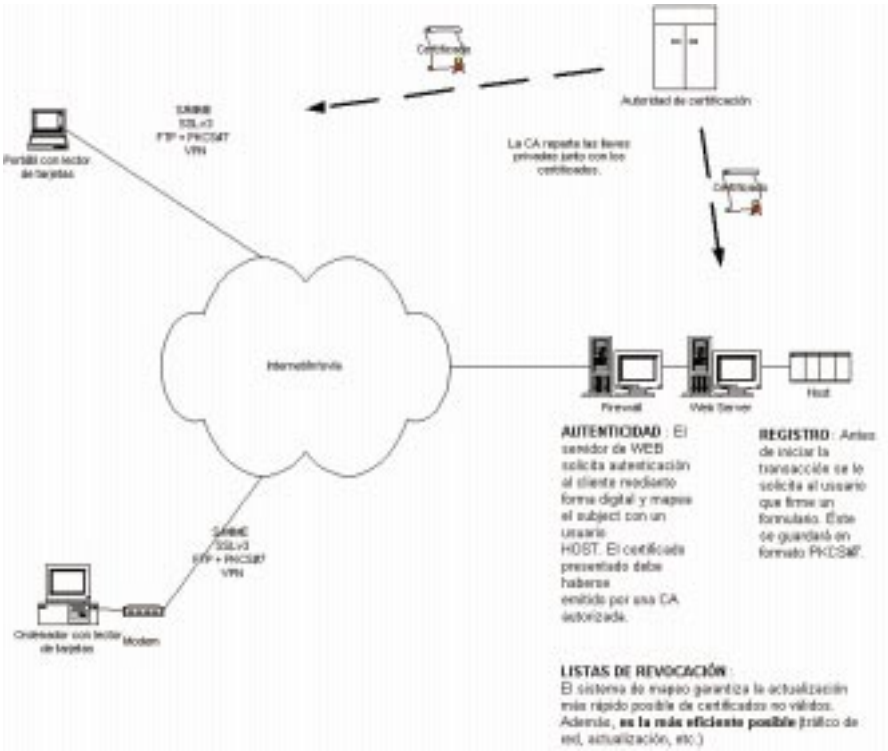

Figura 1. Sistema de “Home Banking”

Extensión del sistema y CRLs

En las operaciones de autentificación y autorización de transacción, debe existir un contrato de “Home Banking” asociado a los datos que presenta el cliente. Cuando el cliente solicita una revocación, se procede a una cancelación de contrato, existiendo un método de consulta de revocación análogo al que se usa en el protocolo SET y manteniendo a la vez, la posibilidad de que la entidad disponga de mecanismos de consulta de certificados revocados según el estándar CRL, OCSP o el mecanismo netscape-url-revocation. Dicha posibilidad permite posibles cambios en la política de certificación orientados a la ampliación de uso de los certificados en el contexto del Banco y para otras aplicaciones diferentes a la de “Home Banking”

Especificaciones funcionales

El modelo permite dar los servicios de correo electrónico seguro (S/MIME), control de acceso en entornos web (acreditación de clientes mediante presentación de certificado en protocolo SSLv3), firma/cifrado de ficheros en formato PKCS#7 y firma de código.

Integración en tarjeta monedero TIBC (Tarjeta Inteligente para Bancos y Cajas) utilizada en España. Soporte para los proveedores de lectores de tarjetas inteligentes que cumplen la norma PC/SC.

Módulo PKCS#11 y CSP (Crypto Service Provider) que permite el uso de cualquier lector en plataformas Windows 95, 98 y NT para aplicaciones Netscape Communicator y Microsoft Internet Explorer.