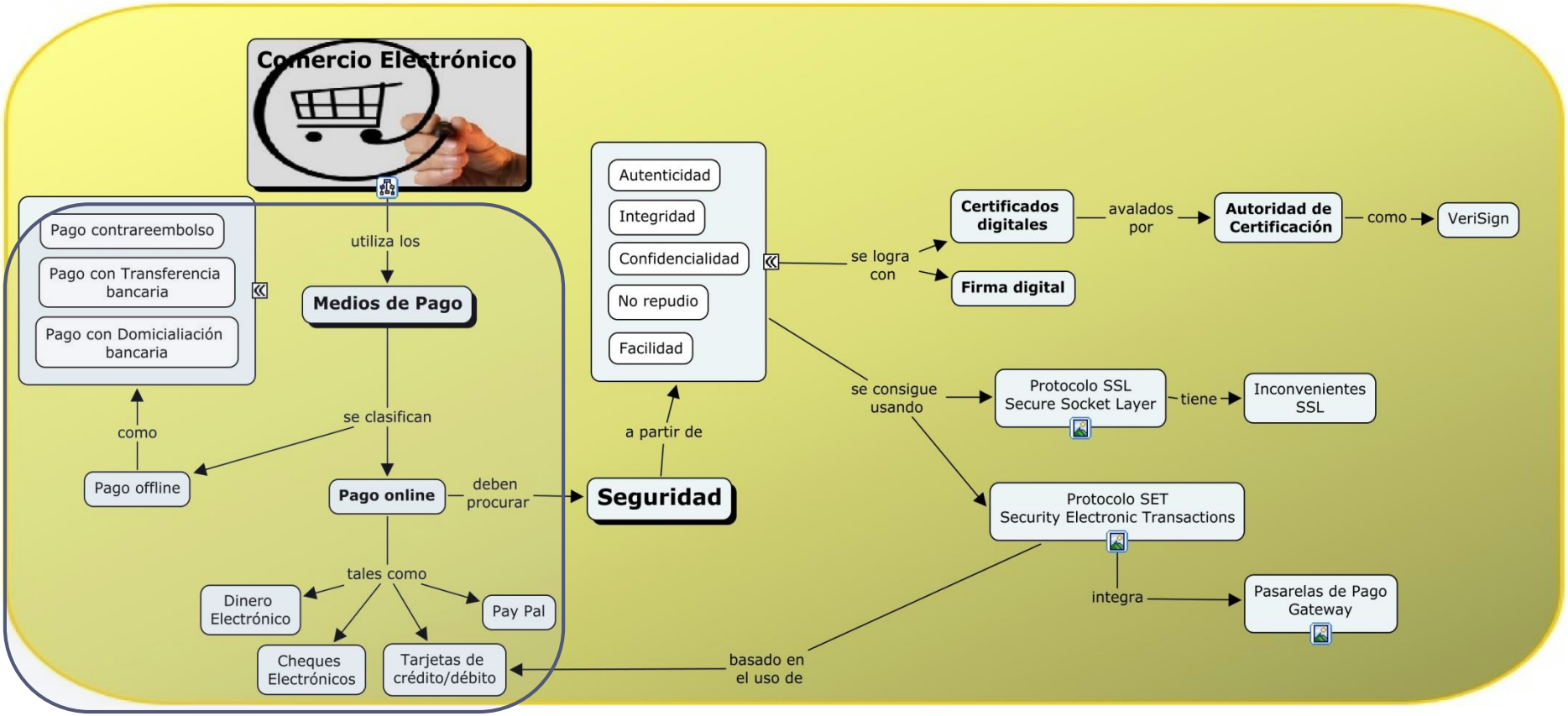
E-COMMERCE

Comercio Electrónico
e-Commerce

Seguridad

Contenido


Comercio Electrónico
utiliza los
Medios de Pago
Pago contrareembolso
Pago con Transferencia bancaria
Pago con Domicialiación bancaria
como
se clasifican
Pago offline
Pago online
deben procurar
Seguridad
a partir de
tales como
Dinero Electrónico
Pay Pal
Cheques Electrónicos
Tarjetas de crédito/débito
Autenticidad
Integridad
Confidencialidad
No repudio
Facilidad
se logra con
Certificados digitales
avalados por
Autoridad de Certificación
como
VeriSign
Firma digital
se consigue usando
Protocolo SSL Secure Socket Layer
tiene
Inconvenientes SSL
Protocolo SET Security Electronic Transactions
integra
Pasarelas de Pago Gateway
basado en el uso de

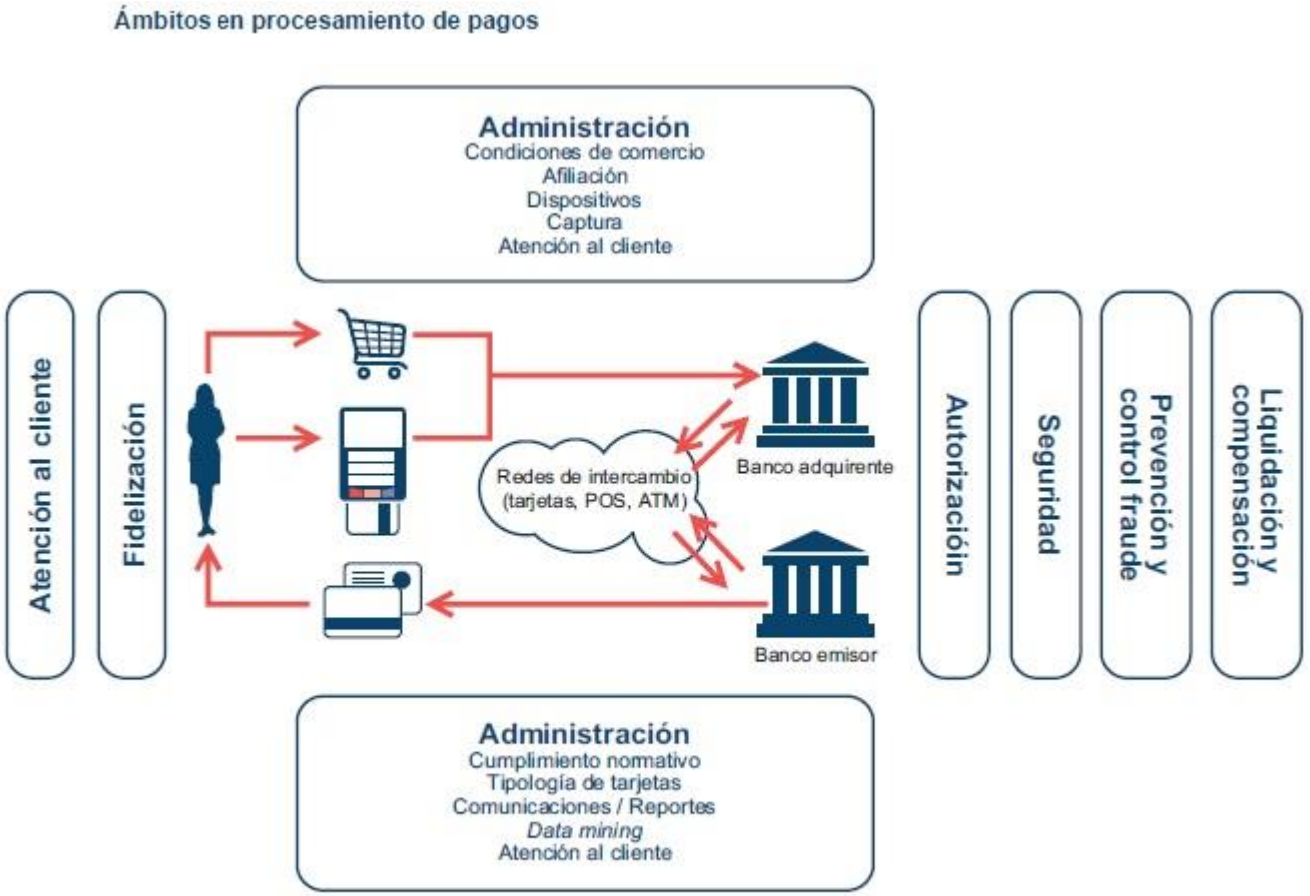
Introducción Medios de Pago

- Los medios de pago en Internet se postulan en este escenario como uno de los **elementos críticos** en la difusión masiva de la venta de productos y servicios a través de la red, siendo la resolución de **problemas** ligados a los medios de pago y a **la gestión de fraude** un área que requiere de notables mejoras por parte de todos los actores intervinientes en el mercado.

- De hecho, la desconfianza sobre la seguridad en los medios de pago sigue siendo el principal factor de preocupación por los usuarios en sus experiencias de compras online.

- La regla básica en el mundo de los medios de pago online es "cuantos más, mejor",

Elementos en el Pago Electrónico



Fuente: Afi y Tecnocom.

POS: Point of Sale
ATM: Automated Teller Machine
Cajeros automáticos

Tipología de medios de pago online

- Los **métodos de pago offline**
  - Pago contra reembolso, transferencia, domiciliación bancaria
  - suelen estar considerados por los compradores más seguros ya que la transmisión de datos bancarios no se realiza a través de la red, lo que disminuye el riesgo de apropiación de estos datos.

- **Los métodos de pago online**
  - Pago con tarjeta de crédito/débito, PayPal, etc.
  - Si bien no es tan seguro como el anterior sus ventajas lo hacen altamente deseable. De cualquier manera, suponen mayor fiabilidad y seguridad de la que los usuarios suponen

Pago Contra Reembolso

- **Es el sistema más seguro para el comprador,** que no pagará el producto hasta haberlo recibido en su domicilio y haber comprobado que está correcto.
- En este esquema, la empresa de mensajería se encarga de cobrar y después abonar el importe al vendedor restando una comisión.

- La principal **ventaja** es la confianza que infunde este método en el cliente que desconfía de internet y prefiere pagar el producto al recibirlo. Ha sido un método tradicionalmente muy utilizado en comercio electrónico, aunque observamos una acusada tendencia a la baja en los últimos años, según va aumentando la confianza de los usuarios en el medio online.
- El principal **inconveniente** para el vendedor es el aumento de los costes del producto, la demora en el pago y el aumento del porcentaje de devoluciones ligado al cambio de opinión del cliente en el momento de la recepción de la mercancía.

Pago con Transferencia Bancaria

- En este método de pago el comercio notifica al usuario una cuenta bancaria donde el cliente debe realizar una transferencia para que se gestione su pedido.
- Es el caso inverso al anterior, ya que el comprador envía el dinero antes de recibir el pedido, lo que supone una total confianza en el vendedor.
- Su principal **ventaja** es su bajo coste
- Su principal **inconveniente** es el retraso en la ejecución del pedido al estar obligado el vendedor a esperar la recepción del importe antes de proceder al envío del producto.

Pago con Domiciliación bancaria

- Este método se utiliza habitualmente en **compras habituales y repetidas, o servicios de suscripción periódica**, así como en entornos B2B (comercio entre empresas).
- Consiste en que el cliente facilita al comercio un número de cuenta bancaria para que éste le gire un recibo con una periodicidad determinada.
- La principal **ventaja** es la automatización del proceso de cobro periódico para el vendedor
- Esta ventaja es el principal **inconveniente** para el comprador, que en ocasiones pierde el control de sus pagos, al no requerir su intervención.

Pago electrónico
Dinero Electrónico

- **Dinero Electrónico** (Anónimo e Identificado): El concepto de dinero electrónico es amplio, y difícil de definir en un medio tan extenso como el de los medios de pago electrónicos (EPS). A todos los efectos se definirá el dinero electrónico como aquel dinero creado, cambiado y gastado de forma electrónica. Este dinero tiene un equivalente directo en el mundo real: la moneda. El dinero electrónico se usará para pequeños pagos.

Pago electrónico
Cheques Electrónicos

- **Cheques Electrónicos:**
  - Los métodos para transferir cheques electrónicos a través de Internet no están tan desarrollados como otras formas de transferencia de fondos.
  - Los cheques electrónicos podrían consistir algo tan simple como enviar un email a un vendedor autorizándole a sacar dinero de la cuenta, con certificados y firmas digitales asociados. Un sistema de cheques puede ser considerado como un compromiso entre un sistema de tarjetas de crédito y uno de micropagos o dinero electrónico (anónimo).

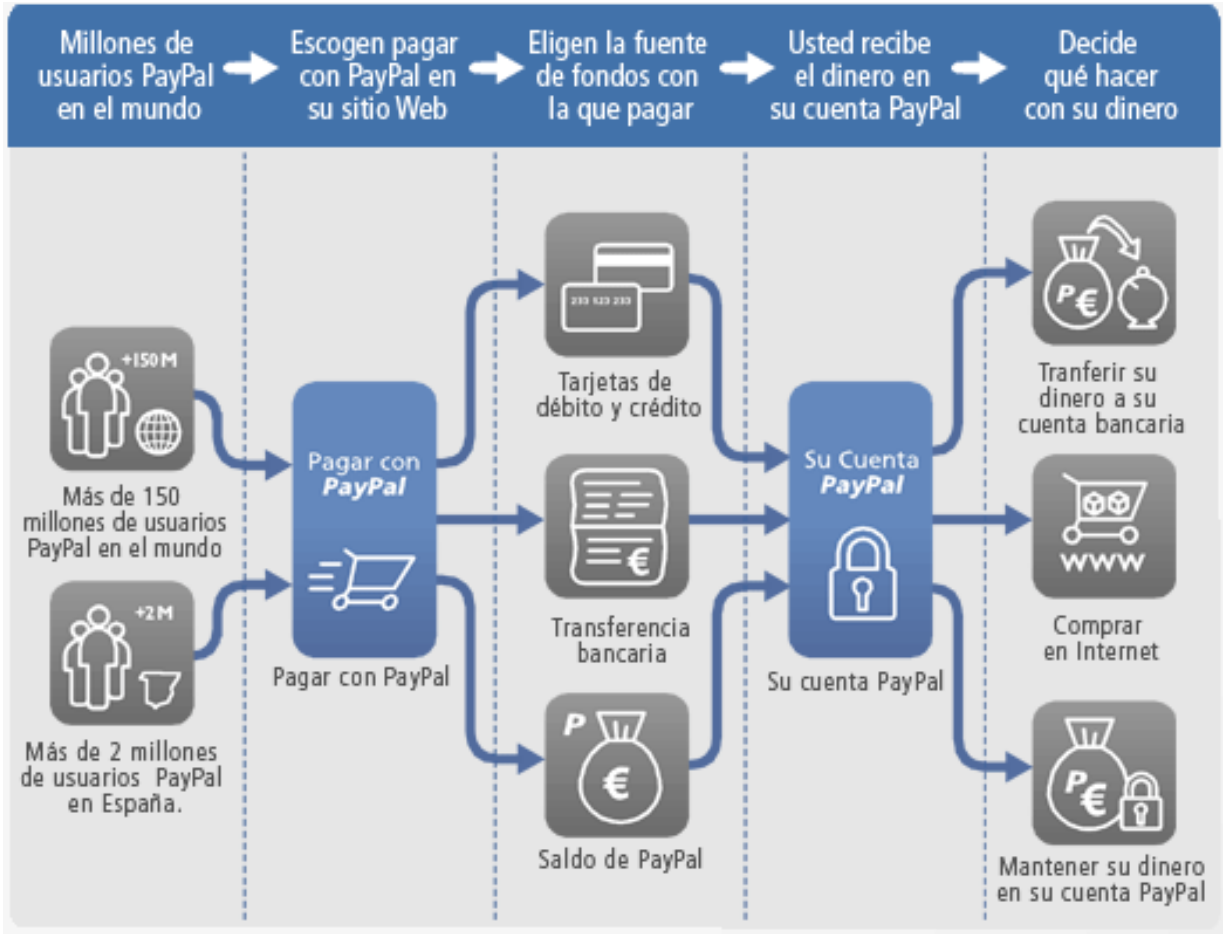
Pago electrónico
Tarjetas de crédito/débito

- Es el sistema de pago electrónico más común y aceptado hoy en día dado el uso generalizado, tanto nacional como internacionalmente, debido a la universalidad de las tarjetas que acepta (Visa, Mastercard, American Express, etc.)
- En el esquema de pago online por tarjeta de débito/crédito, existen dos actores implicados,
  - **banco del vendedor:** entidad financiera responsable del servicio de TPV virtual
  - **banco del comprador:** entidad financiera que ha emitido la tarjeta con la que se realiza la operación de pago.

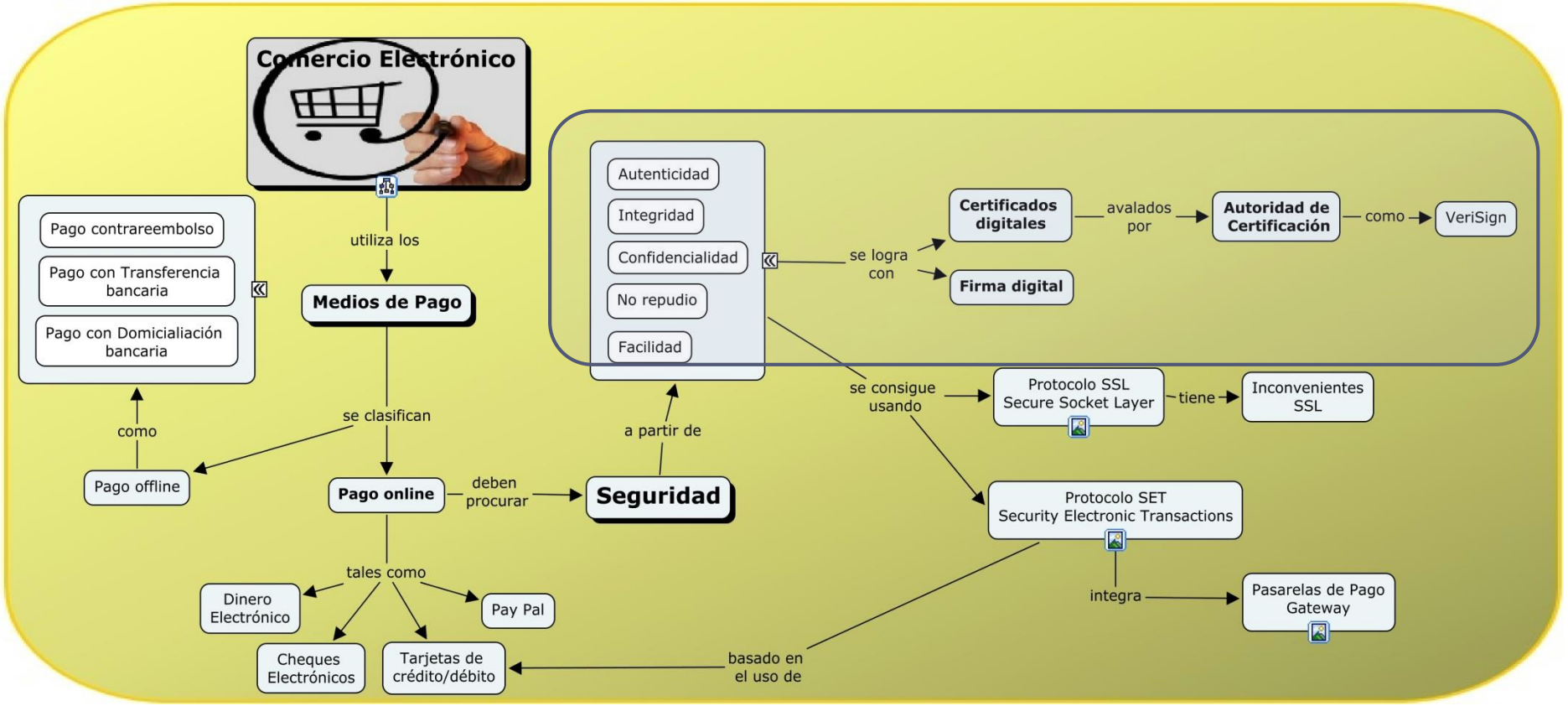
Pago electrónico PayPal.

- Perteneciente al sector del comercio electrónico por Internet que permite la transferencia de dinero entre usuarios que tengan correo electrónico, una alternativa a los medios de pago tradicionales.
- PayPal también procesa peticiones de pago en comercio electrónico y otros servicios webs, por los que cobra un porcentaje.
- PayPal es un sistema que permite enviar y recibir pagos de forma segura por Internet usando su tarjeta de crédito, tarjeta de débito o cuenta bancaria. Es la empresa líder en pagos en Internet.
- PayPal ayuda a proteger la información de las tarjetas de crédito con los mejores sistemas de seguridad y prevención de fraude del sector. Cuando se utiliza PayPal la información financiera nunca se comparte con el vendedor.
- En PayPal se puede almacenar dinero virtual en diferentes monedas, como Euros, Dólares

PayPal.


Millones de usuarios PayPal en el mundo
Escogen pagar con PayPal en su sitio Web
Eligen la fuente de fondos con la que pagar
Usted recibe el dinero en su cuenta PayPal
Decide qué hacer con su dinero
+150M
Más de 150 millones de usuarios PayPal en el mundo
+2M
Más de 2 millones de usuarios PayPal en España.
Pagar con PayPal
Pagar con PayPal
Tarjetas de débito y crédito
Transferencia bancaria
Saldo de PayPal
Su Cuenta PayPal
Su cuenta PayPal
Tranferir su dinero a su cuenta bancaria
Comprar en Internet
Mantener su dinero en su cuenta PayPal

Seguridad en los Pagos online

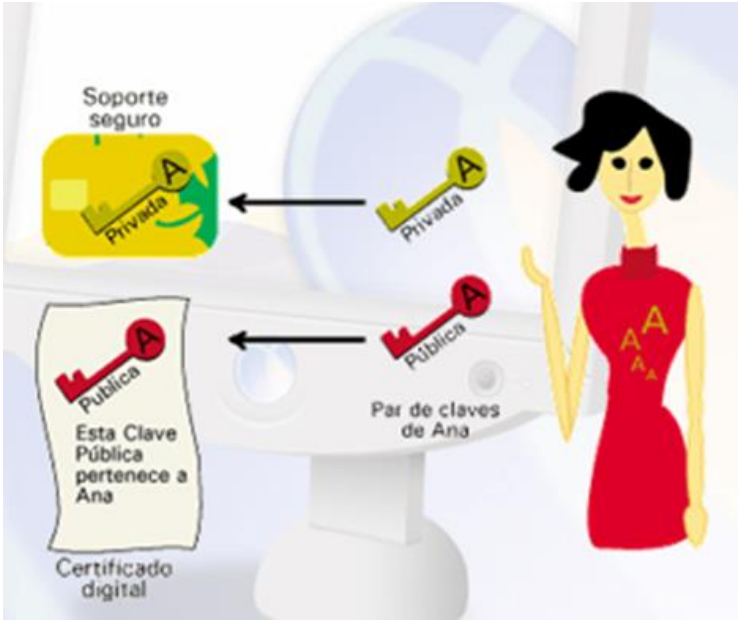


Elementos de la seguridad informática

- Autenticidad:
  - todas las entidades participantes en la transacción deben estar perfecta y debidamente identificadas antes de comenzar la misma. Debemos estar seguros de qué la persona con la que nos comunicamos es realmente quién dice ser, ya que si no podemos estar facilitando datos íntimos y/o sensibles a una persona o entidad no deseada, que puede hacer con ellos luego lo que quiera.
  - La Autenticidad se consigue mediante el uso de los **certificados** y **firmas digitales**.
- Confidencialidad:
  - debemos estar seguros de que los datos que enviamos no pueden ser leídos por otra persona distinta del destinatario final deseado, o que si ocurre esto, el espía no pueda conocer el mensaje enviado. Es decir, debemos estar seguros de que ninguna persona ajena a la transacción puede tener acceso a los datos de la misma.
  - La confidencialidad de consigue en las transacciones electrónicas con el uso de la **Criptografía**.
- Integridad:
  - es necesario estar seguro de que los datos que enviamos llegan íntegros, sin modificaciones, a su destino final.
  - La integridad se consigue combinando **Criptografía**, **funciones hash** y **firmas digitales**.
- No repudio:
  - debemos estar seguros de que una vez enviado un mensaje con datos importantes o sensibles el destinatario de los mismos no pueda negar el haberlos recibido. Y en una compra on-line debe garantizarse que una vez finalizada la misma ninguna de las partes que intervienen pueda negar haber participado en ella.
  - El no repudio se consigue mediante los **certificados y la firma digital**.

Certificados digitales

- Para solucionar el problema de la Autentificación en las transacciones por Internet se buscó algún sistema identificativo único de una entidad o persona.
- El problema era estar seguro de que efectivamente la clave pública que nos envían sea de la persona correcta, y no de un suplantador. Entonces se pensó en implementar una especie de documento de identidad electrónica que identificara sin dudas a su emisor.
- La solución a este problema la trajo la aparición de los **Certificados Digitales** o **Certificados Electrónicos**, documentos electrónicos basados en la criptografía de clave pública y en el sistema de firmas digitales
- Su **objetivo** es garantizar con toda confianza el vínculo existente entre una persona, entidad o servidor web con una pareja de claves correspondientes a un sistema criptográfico de clave pública.



Un Certificado Digital es un documento electrónico que contiene datos identificativos de una persona o entidad (empresa, servidor web, etc.) y la clave pública de la misma, haciéndose responsable de la autenticidad de los datos que figuran en el certificado otra persona o entidad de confianza, denominada **Autoridad Certificadora**.
Las principales Autoridades Certificadoras actuales son Verisign (filial de RSA Data Security Inc.) y Thawte.

Ejemplo de un certificado digital

Versión: *identifica el formato del certificado*

N° de serie: *cada certificado es único dentro de la Autoridad Certificadora*

Algoritmo: *se pueden utilizar múltiples algoritmos para firmar el certificado*

Autoridad Emisora: *nombre de la Autoridad de Certificación que emite el certificado*

Periodo de validez: *desde / hasta*

Asunto: *Nombre del usuario y NIF o NIE*

Clave Pública del usuario: *incluye además algoritmo usado y longitud clave*

Firma de la Autoridad de Certificación

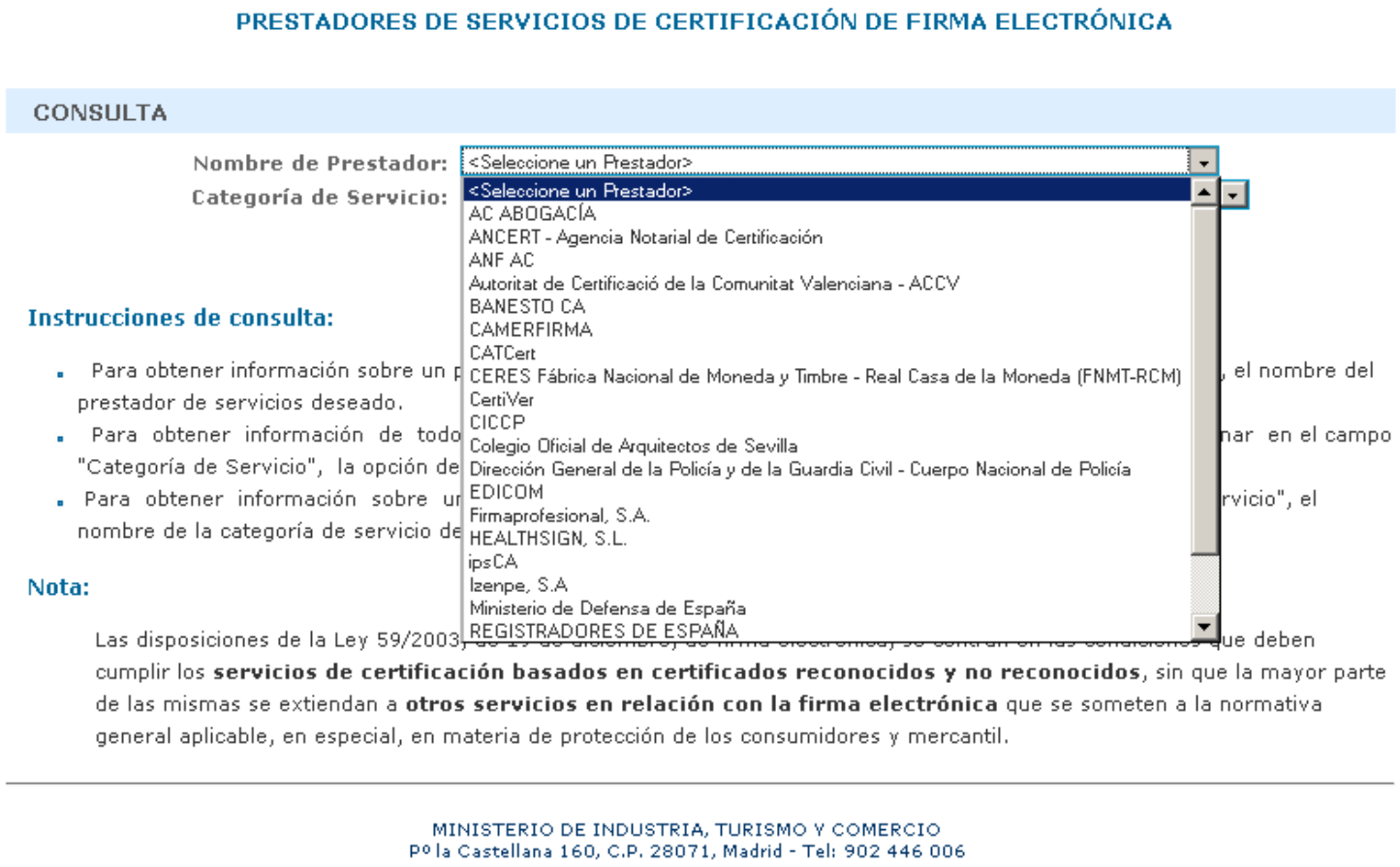
¿Quién avala a la Autoridad Certificadora?

- El problema que se plantea ahora es: si la Autoridad Certificadora avala los datos del certificado ¿Quién avala a la autoridad Certificadora?.

- Para solventar esto se han creado una serie de entidades autorizadas a emitir certificados, de tal forma que éstas a su vez son avaladas por otras entidades de mayor confianza, hasta llegar a la cabeza de la jerarquía, en la que figuran unas pocas entidades de reconocido prestigio y confianza, como Verisign, que se auto-firman su certificado.

- Cada certificado emitido por una AC debe estar firmado por una AC de mayor grado en el esquema **jerárquico de autoridades certificadoras**, formándose así una cadena de certificados, en los que unas AC se avalan a otras hasta llegar a la AC superior, que se avala a sí misma.

Agencias de Certificación Acreditadas



Firma electrónica

- El Certificado Digital vincula indisolublemente a una persona o entidad con una clave pública. Mediante el sistema de firma digital se asegura que el certificado que recibimos es realmente de la persona que consta en el mismo.

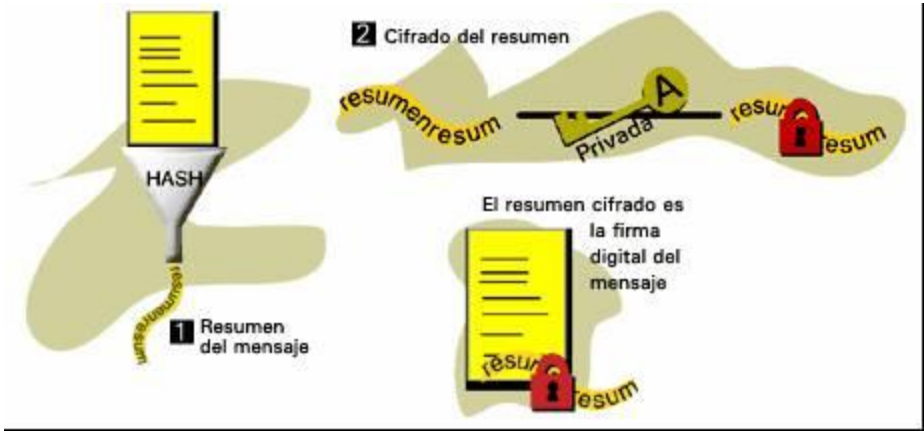
- El sistema de Firma digital liga un documento digital con una clave de cifrado

- ¿Qué es una firma digital?
  - El concepto de firma digital fue introducido en 1976
  - Es un conjunto de datos asociados a un mensaje que permite asegurar la seguridad informática del mensaje
  - Para que pueda equiparse a la firma manuscrita se le exige además:
    - Ser barata y fácil de producir
    - Ser fácil de reconocer tanto por el propietario como por los otros
    - Ser imposible de rechazar por el propietario

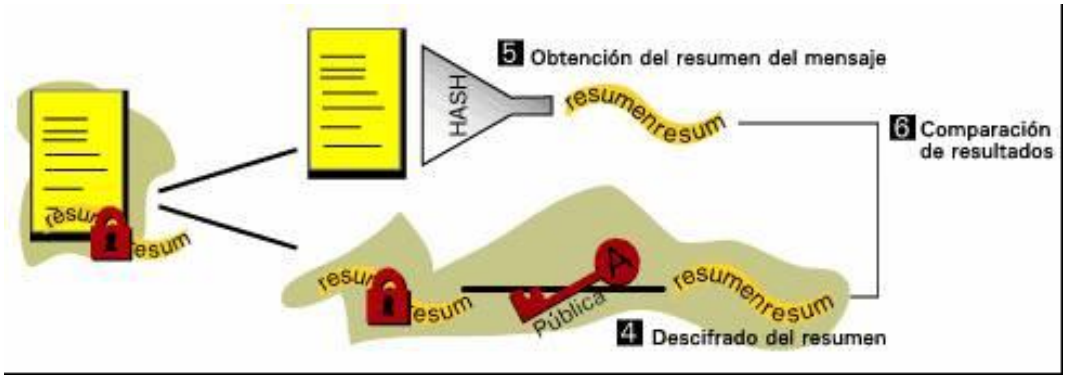
Proceso de la firma digital

- Ana escribe un mensaje a Bernardo.
- Es necesario que Bernardo pueda verificar que realmente es Ana quien ha enviado el mensaje. Por lo tanto Ana debe enviarlo firmado:

1. Resume el mensaje mediante una función hash.
2. Cifra el resultado de la función hash con su clave privada. De esta forma obtiene su firma digital.
3. Envía a Bernardo el mensaje original junto con la firma.



Proceso de la firma digital



Bernardo recibe el mensaje junto a la firma digital. Deberá comprobar la validez de ésta para dar por bueno el mensaje y reconocer al autor del mismo (integridad y autenticación).

1. Descifra el resumen del mensaje mediante la clave pública de Ana.
2. Aplica al mensaje la función hash para obtener el resumen.
3. Compara el resumen recibido con el obtenido a partir de la función hash. Si son iguales, Bernardo puede estar seguro de que quien ha enviado el mensaje es Ana y que éste no ha sido modificado.

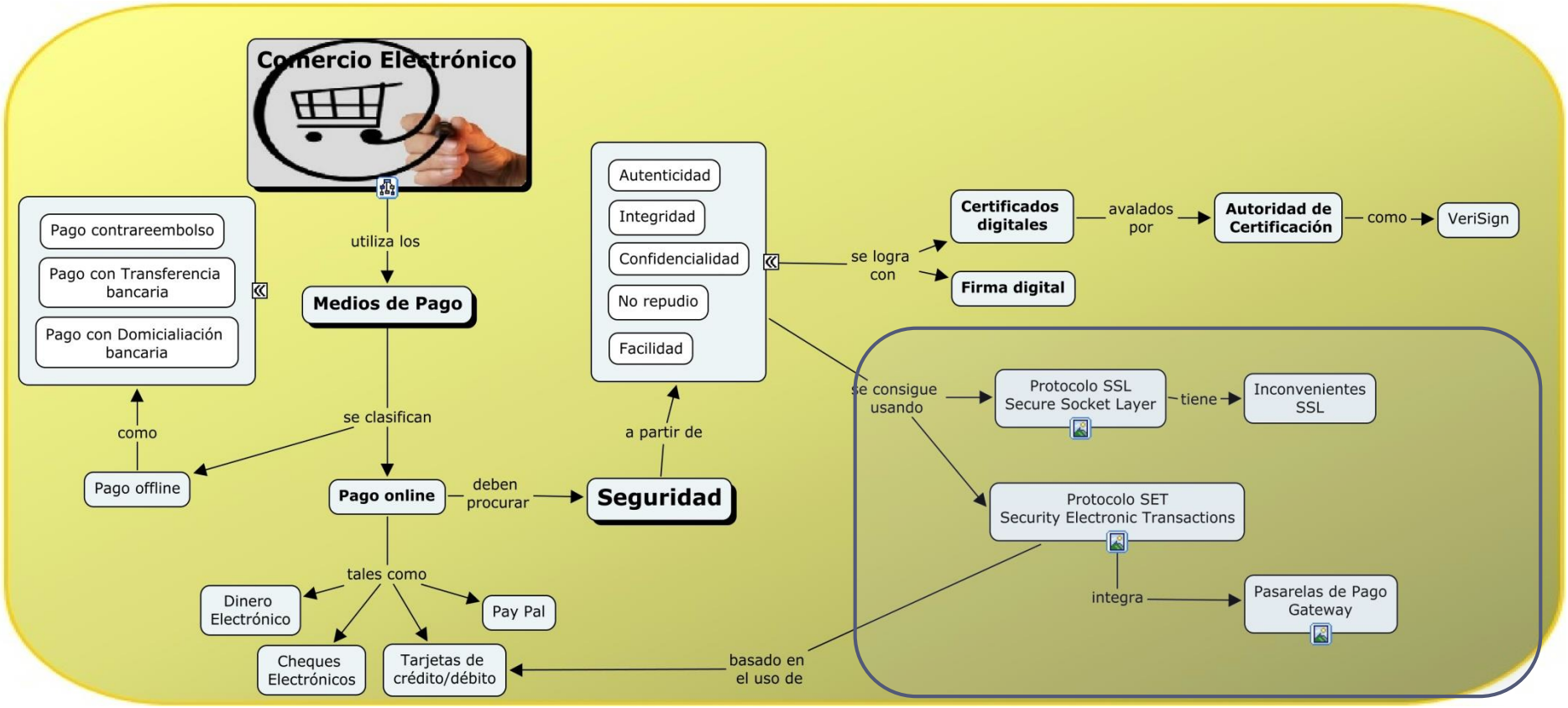
La firma electrónica

- La firma digital es un cifrado del mensaje que se está firmando pero utilizando la clave privada en lugar de la pública.

- Sin embargo ya se ha comentado el principal inconveniente de los algoritmos de clave pública: su lentitud que, además, crece con el tamaño del mensaje a cifrar. Para evitar éste problema, la firma digital hace uso de funciones *hash*.

- Una función hash es una operación que se realiza sobre un conjunto de datos de cualquier tamaño de tal forma que se obtiene como resultado otro conjunto de datos, en ocasiones denominado *resumen* de los datos originales, de tamaño fijo e independiente el tamaño original que, además, tiene la propiedad de estar asociado unívocamente a los datos iniciales, es decir, es prácticamente imposible encontrar dos mensajes distintos que tengan un resumen hash idéntico

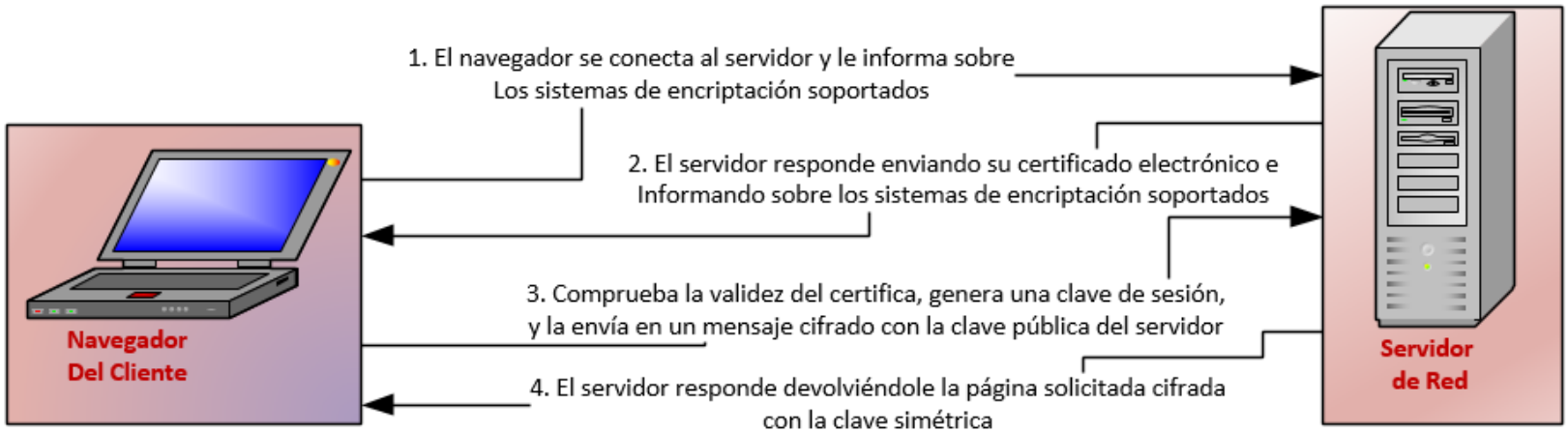
¿Cómo se consigue?



Protocolo SSL/TLS

- SSL (Secure Socket Layer) o su versión actualizada y estandarizada TLS (Transport Layer Security), en esencia, no es en realidad un protocolo de pagos, sino que se trata de un protocolo para proteger la información que se intercambia a nivel de transporte y que es independiente del protocolo de la capa de aplicación. En el intercambio sólo se autentica el servidor por medio de certificados digitales. Opcionalmente, y a petición del servidor, se podría requerir la autenticación del cliente por medio de un certificado digital.
- A día de hoy, este protocolo es el más utilizado para realizar pagos en Internet
- En una transacción de pago con SSL hay dos formas de enviar la información bancaria del cliente a la entidad financiera.
  - Primera: es el vendedor quien envía la información bancaria a la entidad financiera.
  - Segunda: cuando se inicia el pago, el vendedor redirige al cliente a la entidad financiera para realizar el pago, así la información de la tarjeta de crédito sólo la conoce la entidad financiera. Una vez efectuado el pago, la entidad financiera redirige al cliente al vendedor.

Protocolo SSL



Ventajas SSL

- Protocolo sencillo de implementar, puesto que todos los servidores web y todos los navegadores actuales lo soportan.
- Protocolo transparente tanto al software del comercio del vendedor como al cliente. Para los vendedores no hay ningún coste de integración de SSL en sus sistemas, salvo el de instalar un certificado. Para los clientes, el único requisito es el soporte SSL, que ya incluye el navegador.
- Protocolo que garantiza la integridad y la confidencialidad de la información entre cliente y servidor, así como la autenticación del servidor (opcionalmente la del cliente)
- Facilita la movilidad de los clientes, las transacciones se pueden hacer en cualquier ordenador que disponga de navegador web
- Baja complejidad, de forma que el protocolo supone un impacto mínimo en el tiempo de la transacción.

Inconvenientes SSL

- No garantiza el No Repudio, el cliente puede realizar el pago y no recibir el producto solicitado puesto que no cuenta con evidencias para probar que no recibió el producto.

- En la mayoría de los casos, los clientes no tienen certificado puesto que no es obligatorio. En estos casos el vendedor no está seguro de la identidad del cliente y éste no aceptar un pedido realizado, con los costes de devolución a cargo del vendedor.

- En los casos en el que el vendedor conoce la información bancaria del cliente, la privacidad no queda garantizada después de efectuada la operación. El vendedor puede utilizar esos datos para cargar al cliente con nuevos pagos. El almacenamiento también puede constituir un problema si el vendedor es atacado.

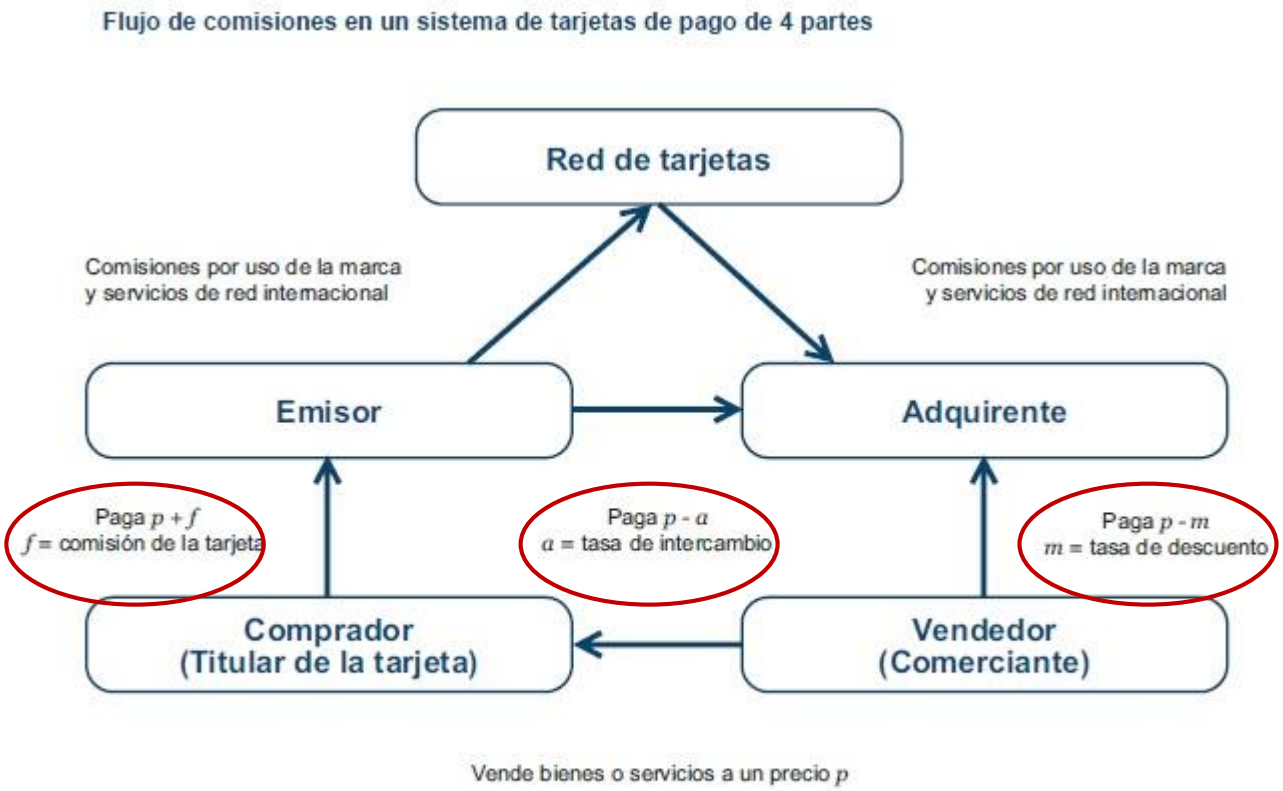
Protocolo SET

- El protocolo SET (Secure Electronic Transaction) tiene como objetivo proteger la privacidad de la información de pago y asegurar su autenticidad, para evitar los problemas que presentaba SSL.

- A diferencia de SSL, SET es un protocolo de pagos basado en tarjetas de crédito/débito.

- SET se basa en el uso de certificados digitales para asegurar la perfecta identificación de todas aquellas partes que intervienen en una transacción on-line basada en el uso de tarjetas de pago, y en el uso de sistemas criptográficos de clave pública para proteger el envío de los datos sensibles en su viaje entre los diferentes servidores que participan en el proceso

Modelo genérico en las transacciones



Nota: f generalmente presenta el formato de cuota fija anual, a menudo condicionado su importe a la intensidad de uso de la tarjeta de pago, pudiendo ser cero en función de la política comercial del emisor. Su uso en cajeros automáticos sí puede contemplar comisiones, especialmente cuando las transacciones se realizan en cajeros ajenos a la red del emisor.

Fuente: Afi.

Entidades

- Red (o esquema) de tarjetas:
  - entidad propietaria de la marca de la tarjeta y responsable de establecer los estándares y las reglas del negocio para las partes.
- Titular de la tarjeta:
  - tenedor, persona física o jurídica a cuyo nombre se encuentra emitida la tarjeta de pago, quien la utiliza para hacer las compras de bienes y servicios.
  - Asume **el pago de una comisión** compuesta por **una parte fija** (comisión anual), y una **variable** (a menudo negativa por la aplicación de programas de fidelidad y puntos ofrecidos por el banco emisor). La comisión anual suele ser menor cuando existe un alto grado de competencia entre los emisores y una mayor elasticidad-precio de la demanda de servicios de pago con tarjeta.
- Comerciante:
  - proveedor de bienes y servicios que acepta la tarjeta como forma de pago por la compra al ser depositario del dispositivo TPV instalado por el adquirente para la recepción de la operativa de tarjeta.
  - Asume dos tipos de costes:
    - **Tasa de Descuento:** variable, basado en el valor de las transacciones y
    - **Uso de Plataforma:** fijo, que suele incluir el alquiler de equipos (TPV) y el mantenimiento de software.

Entidades

- Entidad emisora:

  - entidad financiera responsable de poner en circulación las tarjetas, establecer y mantener la relación con el titular de la tarjeta, incluyendo la verificación de requisitos de acceso, identificación, autorización, establecimiento de límites de crédito, recaudo de pagos, comisiones y otros cargos, y programas de fidelidad, fundamentalmente.

  - Realiza el pago al banco adquirente, a cambio de una comisión (**tasa de intercambio)** que remunera el servicio de conectar "los dos lados" del mercado de tarjetas de pago. Las tasas de intercambio pueden acordarse a nivel bilateral (banco emisor- banco adquirente) o multilateral (miembros de una asociación de bancos).

Entidades

- Entidad adquirente:

  - Recibe la operativa de las tarjetas realizada por los titulares, por medio de los dispositivos que habrá instalado previamente, ya sean los TPV (Terminal Punto de Venta) o POS (*Point of Sale) para compras* en comercios, o los cajeros automáticos (ATM - *Automated Teller Machine) para las retiradas de efectivo.*

  - Es responsable de la administración del contrato con el comerciante, que establece las reglas de participación de éste en el esquema de pagos con tarjeta, proporciona el TPV al comerciante y deposita los fondos en su cuenta. Si éste acepta tarjetas de crédito, el banco adquirente habilita una línea de crédito al comerciante.

  - Recibe el pago de la transacción realizada por el titular de la tarjeta y hecha efectiva por el banco emisor (descontando el importe de la tasa de intercambio), para trasladarlo a la cuenta del comerciante.

Protocolo SET

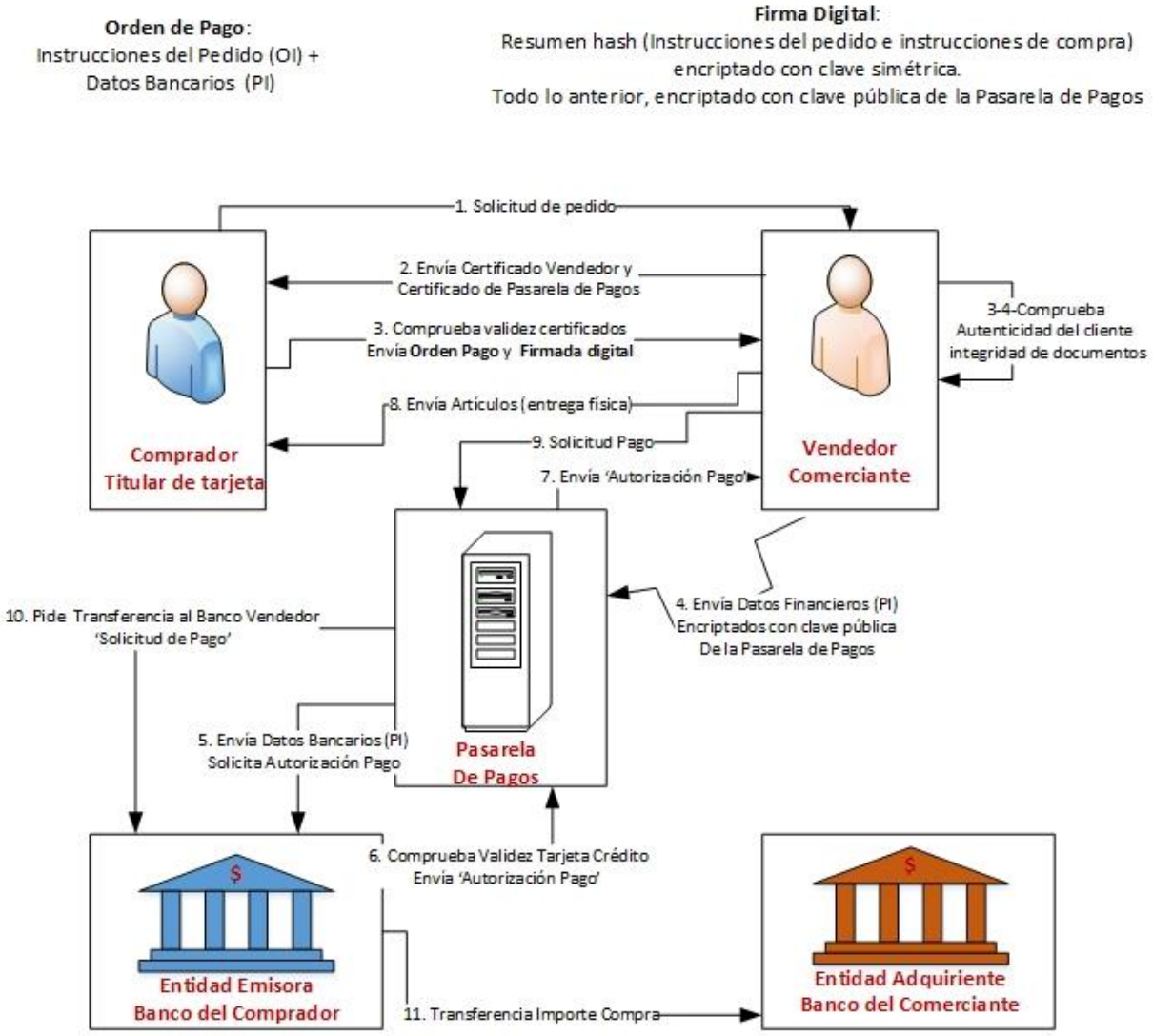
Inicialización: el cliente obtiene los certificados del vendedor y de la pasarela de pagos

Inicio pago: cliente envía al vendedor información de la compra y información para el pago (para la pasarela de pagos).

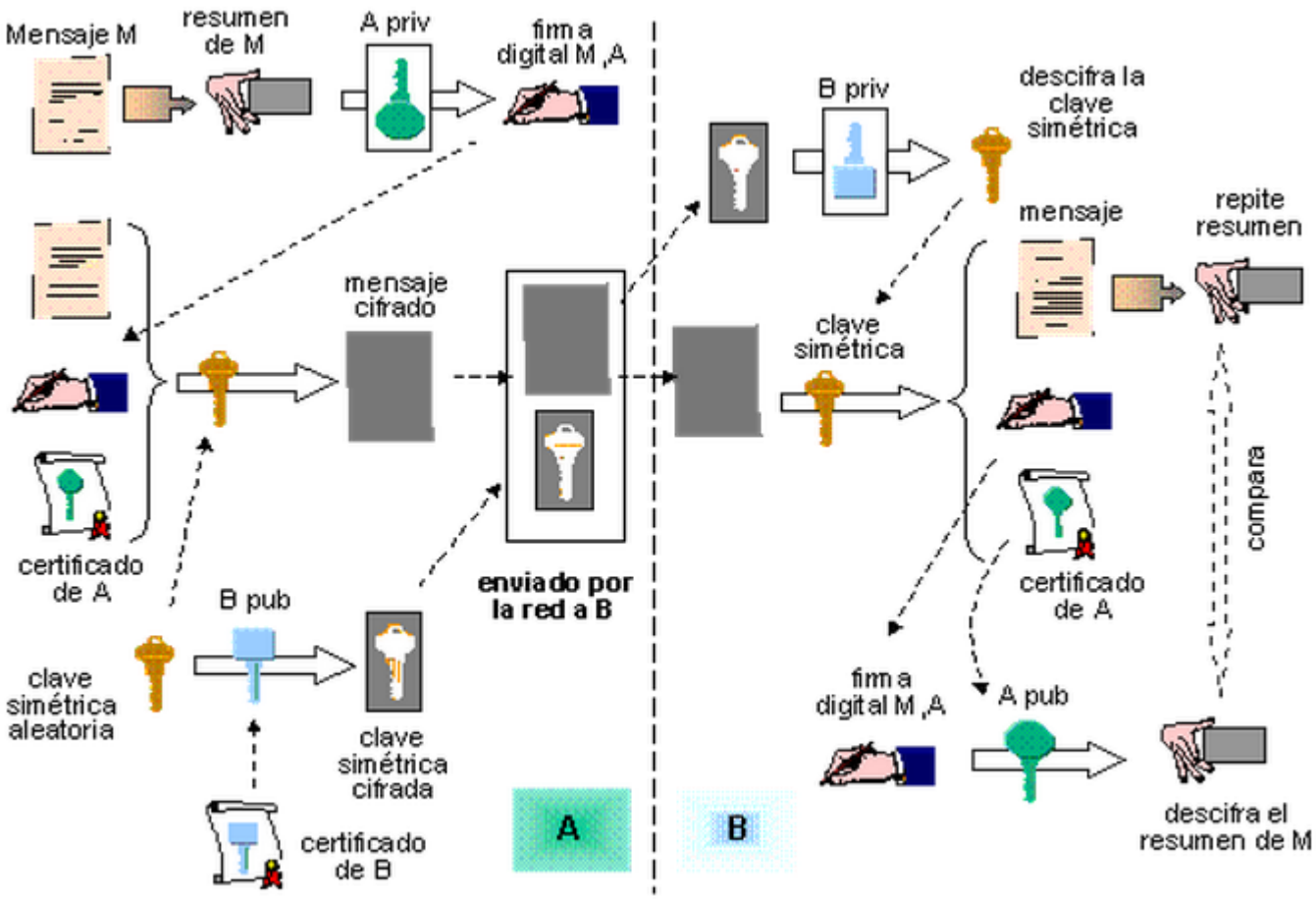
Autorización: el vendedor conecta con la pasarela de pagos para saber si autoriza el pago para la entrega del producto solicitado

Confirmación del pago: recibo para el cliente

Liquidación de pago: el vendedor hace efectivo el cobro y suministra el producto al cliente



Esquema de Cifrado en SET



Apub, Apriv: claves pública y privada de A; Bpub, Bpriv: claves pública y privada de B

http://www.internautas.org/documentos/pista.htm

Ventajas SET

- Satisface los requisitos de seguridad: confidencialidad, autenticación, integridad y resistencia a ataques de reenvío
- Garantiza que cada parte sólo tenga visible la información que realmente necesita conocer
  - El vendedor no conoce la información bancaria del cliente y la pasarela de pagos no conoce el pedido solicitado.
- Disminuyen las posibilidades de anulación de las transacciones realizadas por el cliente.

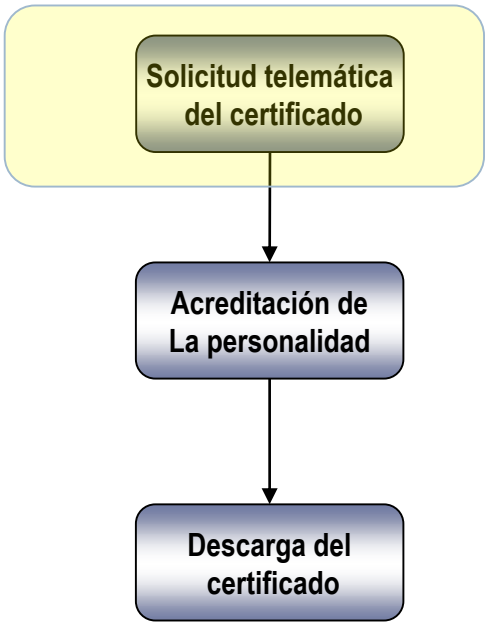
Inconvenientes SET

- El más complejo que SSL puesto que necesita que el cliente tenga un certificado digital
- El cliente sólo puede realizar compras en el ordenador en el que tenga instalado el certificado o tiene que exportarlo e instalarlo en un nuevo ordenador.
- El vendedor debe tener cuenta bancaria con las entidades financieras que son capaces de operar con SET
- Las entidades bancarias deben desarrollar las pasarelas de pago
- No garantiza el no repudio puesto que el cliente en una transacción en SET no obtiene un recibo seguro de pago.

Fuentes de información

- 'Sistemas y Entornos de pago para la adquisición de contenidos y servicios electrónicos en Red', de Antonio Ruiz Martínez
- 'Estudio de situación del comercio electrónico en España'. PISTA. Promoción e Identificación de Servicios Emergentes de Telecomunicaciones Avanzadas
  - http://www.internautas.org/documentos/pista.htm
- 'Libro blanco del comercio electrónico'. Editado por adigital
- 'Sistemas de Pago Electrónico' de Marlon Altamirano Di Luca
- Informe Tecnocom sobre Tendencias en Medios de Pago 2013.
- 'Transacciones seguras' de Luciano Moreno, del departamento de diseño web de BJS Software
- Ministerio de Industria, Turismo y Comercio, sección de Firma Electrónica
  - http://www.mityc.es/dgdsi/es-ES/Servicios/FirmaElectronica/Paginas/FirmaElectronica.aspx
- Autoridad Pública de certificación española: CERES. Fábrica nacional de moneda y timbre
  - http://www.cert.fnmt.es/
- Delitos informáticos
  - http://www.delitosinformaticos.com/firmaelectronica/

-ANEXO-
Procedimiento para solicitar el certificado de la Fábrica Nacional de Moneda y Timbre



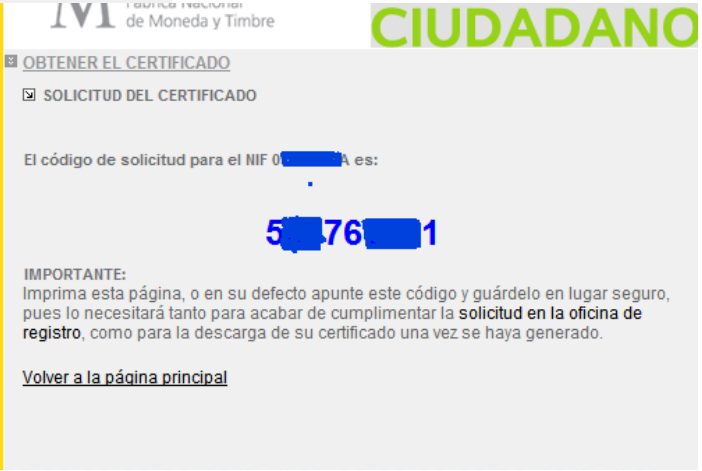
http://www.cert.fnmt.es/index.php?cha=cit&sec=4&lang=es

Procedimiento para solicitar el certificado de la Fábrica Nacional de Moneda y Timbre

Solicitud telemática del certificado

Acreditación de La personalidad

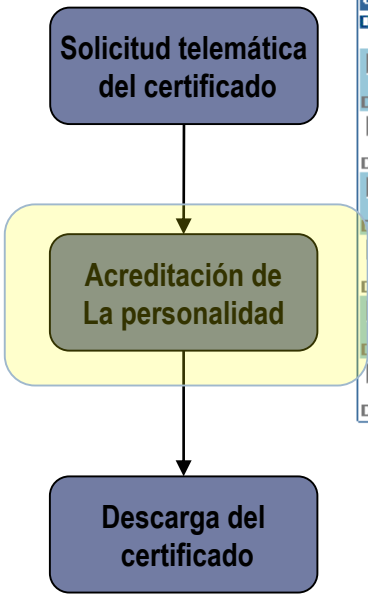
Descarga del certificado

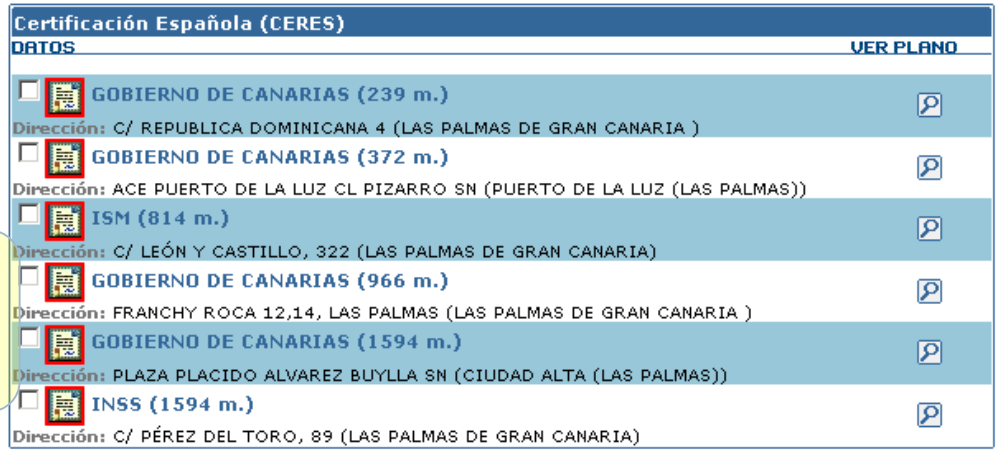


Acepta las pantallas de seguridad que se suceden y la aplicación generará una referencia. **Anótala o imprime la pantalla** porque la necesitarás para acreditarte e instalar el certificado.

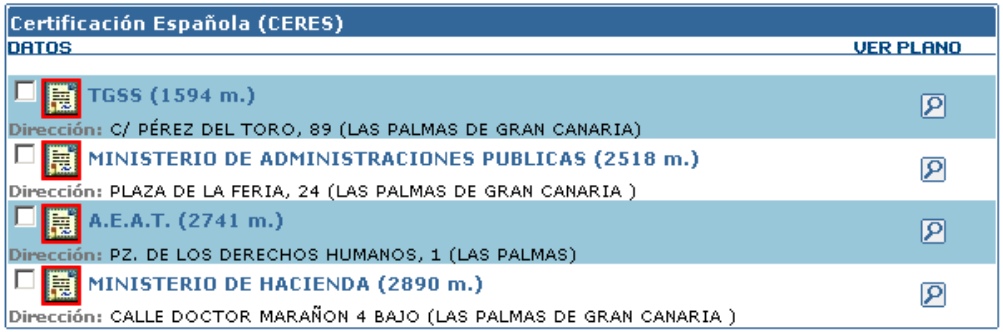
Se introduce el NIF (formato nueve dígitos sin puntos) y se pulsa "Enviar petición".

Procedimiento para solicitar el certificado de la Fábrica Nacional de Moneda y Timbre





Con el código de solicitud del paso anterior, deberás personarte en una Oficina de Registro para acreditar tu identidad. Debes llevar el código de solicitud y el DNI (original y una copia).



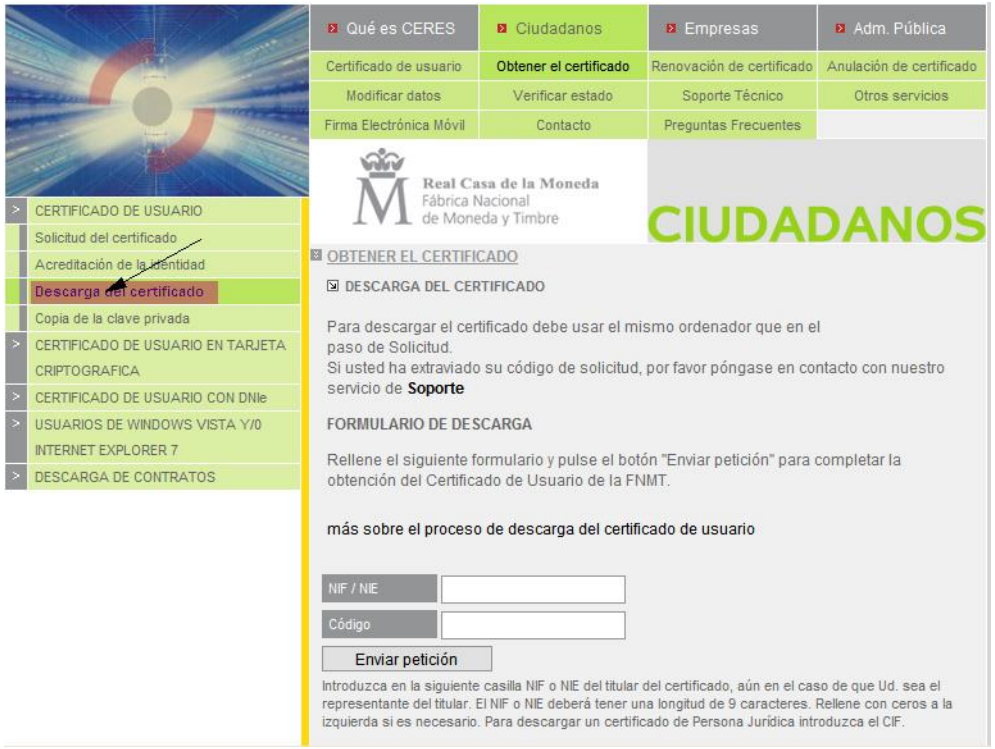
Procedimiento para solicitar el certificado de la Fábrica Nacional de Moneda y Timbre

Una vez acreditado, debes descargar el certificado desde el mismo ordenador en el que hiciste la solicitud. Para ello vuelva a entrar en la dirección: http://www.cert.fnmt.es/index.php?cha=cit&sec=4&lang=es

Solicitud telemática del certificado

Acreditación de La personalidad

Descarga del certificado



Pulsa en descarga del certificado y rellena los campos de NIF y código y envía la petición.
Sigue las instrucciones que de tu ordenador e instala el certificado.
Es conveniente hacer una copia de seguridad del certificado (claves pública y privada) a un soporte extraíble.

Servicios con Certificado de Usuario

AGENCIA ESTATAL DE ADMINISTRACIÓN TRIBUTARIA

http://www.aeat.es

DIRECCIÓN GENERAL DE LA GUARDIA CIVIL

http://www.guardiacivil.org/index.jsp

INSTITUTO NACIONAL DE ESTADÍSTICA

http://www.ine.es

OFICINA ESPAÑOLA DE PATENTES Y MARCAS

Oficina Española de Patentes y Marcas

http://www.oepm.es/

LOTERÍAS Y APUESTAS DEL ESTADO

http://www.onlae.com

MINISTERIO DE ADMINISTRACIONES PÚBLICAS

MINISTERIO DE ADMINISTRACIONES PÚBLICAS

http://www.map.es/servicios.html

Fuente: http://www.cert.fnmt.es/index.php?o=cert