Negocio Electrónico

Tema 6. Pagos electrónicos

Profesorado

Antonio Muñoz Gómez

amunoz@lcc.uma.es

Contenido

- **6.1. Introducción**
- 6.2. Tipos de pagos
- 6.3. Dinero electrónico
- 6.4. Pasarelas de pago
- 6.5. Pago electrónico intermediado
- 6.6. Pago móvil
- 6.7. Otros pagos y tendencias futuras

¿Qué es un sistema de pago electrónico?

- **El sistema que realiza la transferencia del dinero entre comprador y vendedor en una compra-venta electrónica.**
- **Ejemplos de sistemas de pago electrónico:**
  - Pasarelas de Pago
  - Pago con tarjeta
  - Monedero electrónico
  - Dinero electrónico…

Contenido

- 6.1. Introducción
- **6.2. Tipos de pagos**
- 6.3. Dinero electrónico
- 6.4. Pasarelas de pago
- 6.5. Pago electrónico intermediado
- 6.6. Pago móvil
- 6.7. Otros pagos y tendencias futuras

Tipos de pagos electrónicos

- **Según la ejecución del pago:**
  - Esquemas de prepago
  - postpago y
  - pago instantáneo
- **Según el mecanismo de pago:**
  - Pagos tradicionales y pasarelas de pago
  - Pagos (puramente) electrónicos
  - Dinero electrónico
  - Monederos electrónicos
- **Según el dispositivo usado**
  - Pago móvil
- **Según la cantidad**
  - Micropagos

Contenido

- 6.1. Introducción
- 6.2. Tipos de pagos
- **6.3. Dinero electrónico**
- 6.4. Pasarelas de pago
- 6.5. Pago electrónico intermediado
- 6.6. Pago móvil
- 6.7. Otros pagos y tendencias futuras

Dinero electrónico

- **Dinero on-line**
  - Exige interactuar con la entidad de pagos para llevar a cabo una transacción con una tercera parte.
- **Dinero off-line**
  - Se dispone del dinero en el dispositivo del comprador y puede gastarse cuando se desee sin necesidad de contactar a la entidad de pagos
- **Cheques electrónicos**

Dinero electrónico

- **Pre y postpagos**
  - Permiten al cliente depositar el dinero en una cuenta y luego usar ese dinero para comprar cosas en internet.
  - Tipos:
    - *Cargo en cuenta*
    - *Tarjetas de crédito*
    - *Moneda electrónica*
    - *Monedero electrónico*
- **Pago instantáneo**
  - Moneda electrónica
  - Fair exchange protocols

PayPal

- **Ventajas para Compradores**
  - Servicio gratuito, sin comisiones ni cuotas.
  - Sólo hay que introducir la dirección de correo electrónico y una contraseña para realizar los pagos.
  - No hay que introducir los datos de la tarjeta en cada compra.
  - Los datos financieros no se comparten con el vendedor.
  - Opción de elegir como pagar: Tarjeta, Cuenta Bancaria o Saldo de Paypal.
  - Compras protegidas hasta 1000 EUR por la Política de Protección.
- **Ventajas para Vendedores**
  - Sin costes de alta, mantenimiento o cancelación.
  - Control de todas sus ventas y acceso a su historial de transacciones desde una sola cuenta.
  - Podrá aceptar pagos con Tarjeta, Transferencia Bancaria y Saldo de Paypal con total seguridad.
  - Amplio mercado internacional con más de 150 millones de usuarios en 190 países.
  - El logotipo de Paypal en los resultados de búsqueda destacan sus artículos sobre los de la competencia.

PayPal

- **Mezcla servicios de monedero y pasarela**
- **Ofrece un servicio de resolución de conflictos**
  - Aparece en pleno apogeo de los fraudes en eBay
- **Impone políticas estrictas pero a cambio todo se hace rápida y fácilmente**
  - La comparativa con una pasarela tradicional es demoledora

DigiCash (E-cash)

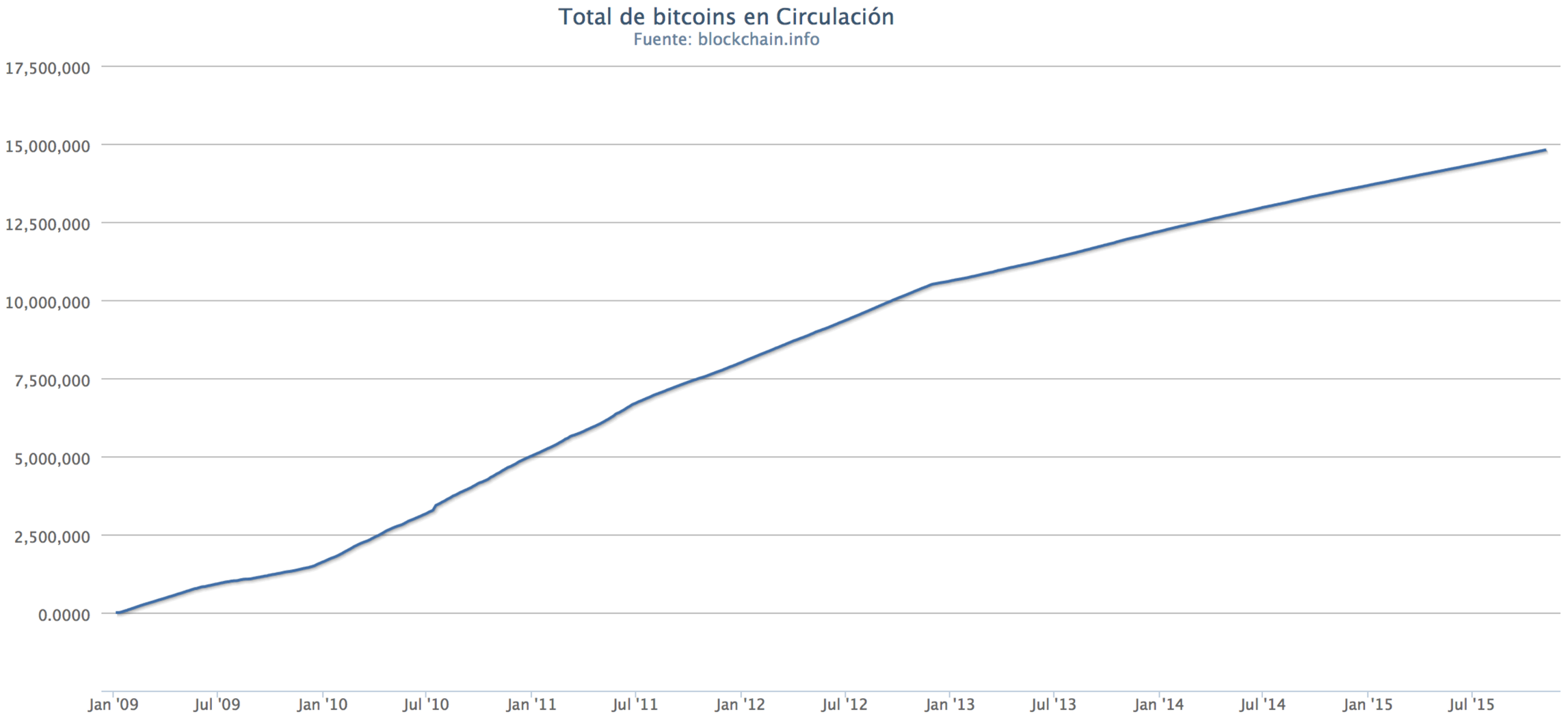
- **Sistema de monedas digitales anónimo**
- **Usa las técnicas de firmas ciegas**
  - Permiten a un actor firmar algo sin saber su contenido
  - Se basan en el algoritmo RSA
- **Se usa un software especial en ambas partes**

BitCoin

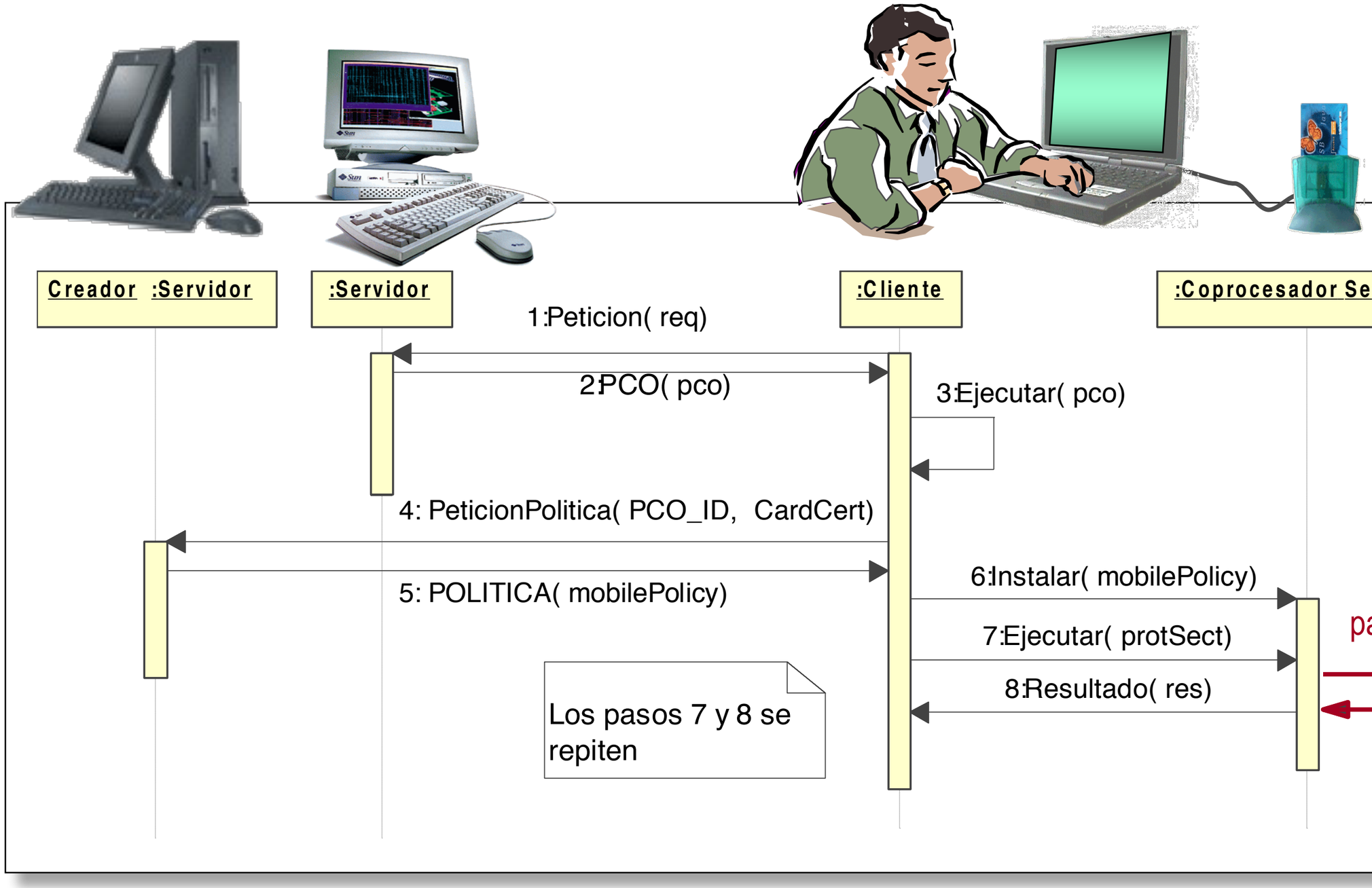
- **Creado en 2009 por “Satoshi Nakamoto”**
  - No se sabe su identidad
- **Se usa en transacciones entre iguales**
- **No hay un banco ni una agencia emisora**
- **Se guardan y envían mediante monederos electronicos**
- **Ha adquirido un gran auge por su simplicidad, seguridad … y por la crisi**
- **Concepto de mining**

BitCoin

- **A mediados de 2015 había algo menos de 15 Millones de BitCoins en circulación**



Monederos Electrónicos: Pagos XSCD



Objetivos XSCD

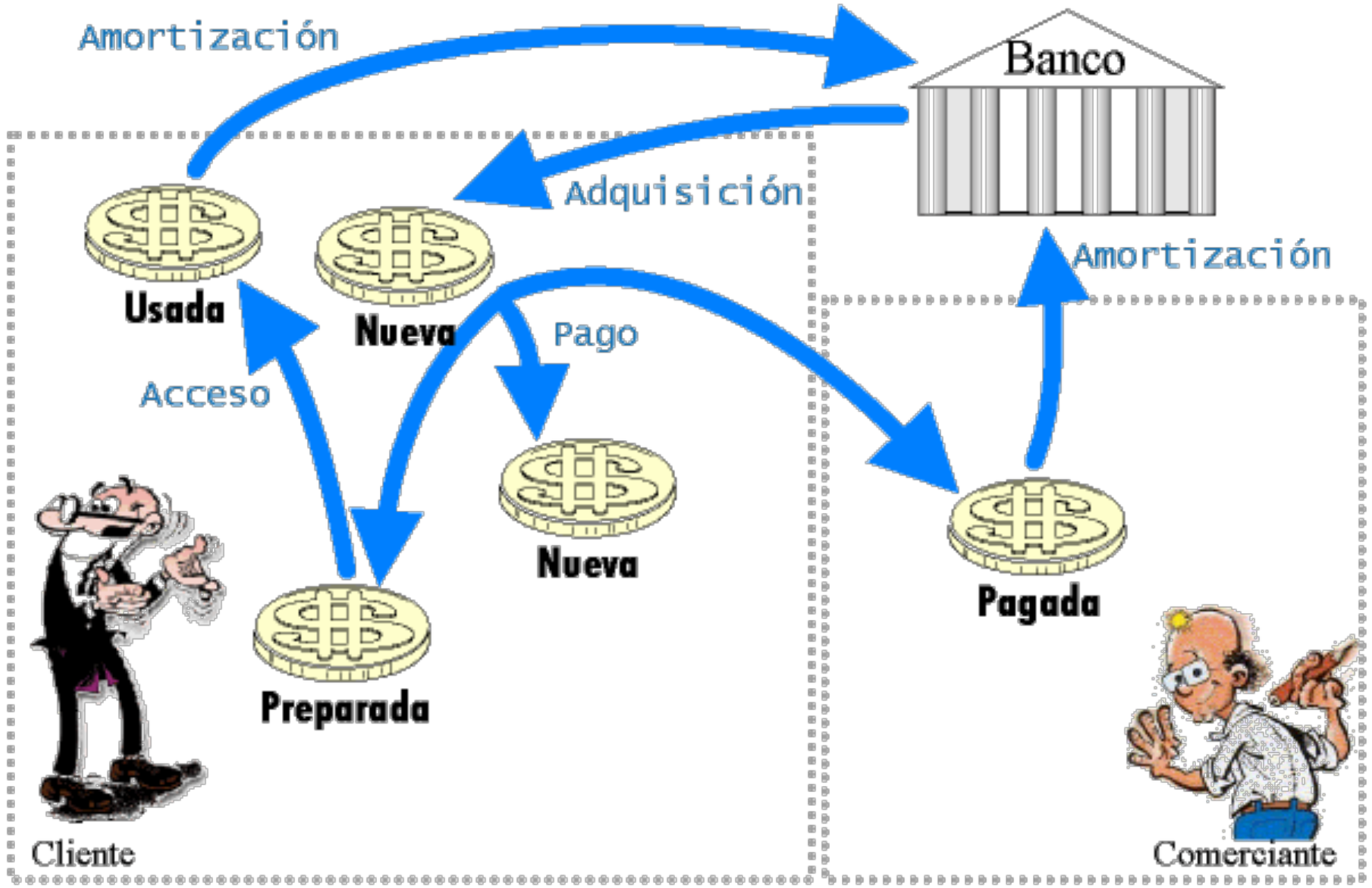
- **Equidad**
- **Atomicidad** (Tygar*)
  - Dinero
  - Bienes
  - Envío certificado
- **Necesidad de un elemento confiable**

*** Atomicity in Electronic Commerce**
J. D. Tygar
January 1996 CMU-CS-96-112

Monedas XSCD

- **Para realizar una compra, una de las monedas "nuevas" se divide en otras tres:**
  - La primera es una moneda "pagada" por el valor de la compra realizada, que se envía cifrada para el comerciante con la petición del objeto a comprar.
  - La segunda es una copia de la primera marcada como "preparada" que permanece en la tarjeta del cliente.
  - La tercera es una moneda "nueva" cuyo valor es el de la moneda original menos la compra.

Protocolo pago XSCD



Protocolo pago XSCD

- **Al recibir la moneda “pagada”, el comerciante produce y envía la licencia (ligada a la correspondiente moneda “preparada”) al cliente.**
- **Si el cliente no recibe la licencia, puede utilizar la moneda “preparada” para evitar el pago.**
- **Si el cliente accede al contenido, el estado de la moneda “preparada” se cambia a “usada”.**
- **Si el cliente decide no acceder al contenido y, por tanto, no ejecuta las secciones protegidas del PCO, la moneda permanece en estado “preparada”, lo cual permite al usuario cancelar el pago.**

Resumen XSCD

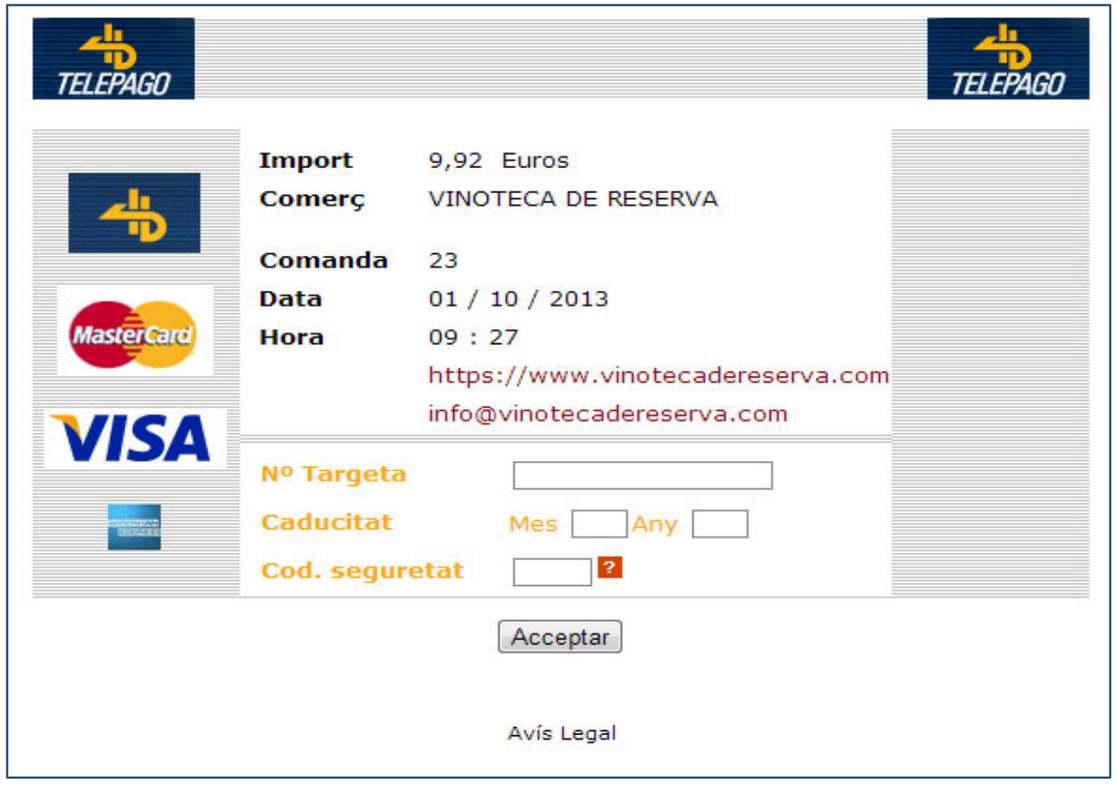
- **Esquema totalmente simétrico**
- **Funcionamiento equitativo**
- **Este mecanismo de pago**
  - garantiza que el comerciante recibe el pago si el usuario accede al contenido (ejecutando las secciones protegidas del PCO),
  - garantiza que el cliente puede anular el pago si no accede al contenido y
  - proporciona pruebas de la transacción (constituidas por la licencia) que pueden ser usadas por el cliente en caso de que el contenido no sea el solicitado.

Contenido

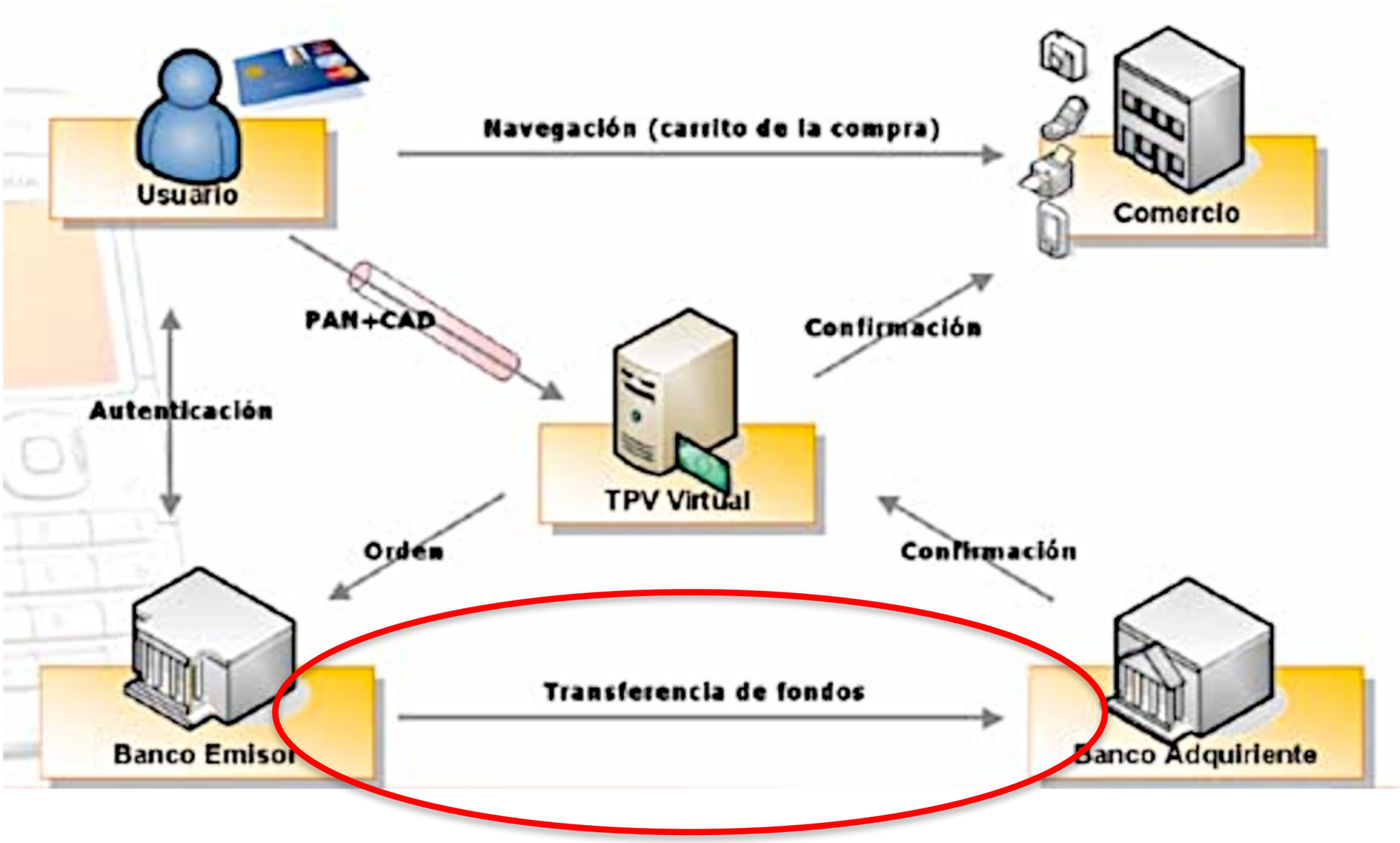
- 6.1. Introducción
- 6.2. Tipos de pagos
- 6.3. Dinero electrónico
- **6.4. Pasarelas de pago**
- 6.5. Pago electrónico intermediado
- 6.6. Pago móvil
- 6.7. Otros pagos y tendencias futuras

Pasarelas de pago

- **Funcionamiento de una pasarela de pago o TPV Virtual**
  - Un cliente compra un producto o servicio mediante alguna aplicación de e-commerce
  - En el momento del pago, la aplicación redirige al cliente al sitio web del banco indicando el importe, comerciante, etc.
  - La conexión se hace por http seguro (https)
  - El número de tarjeta de crédito viaja cifrado al banco
  - El banco comprueba validez de la tarjeta, hace el cargo en la misma y realiza el pago en la cuenta del vendedor
  - El banco devuelve el control a la aplicación de comercio electrónico indicando si se pudo hacer el cobro



Pasarelas de pago



Contenido

- 6.1. Introducción
- 6.2. Tipos de pagos
- 6.3. Dinero electrónico
- 6.4. Pasarelas de pago
- **6.5. Pago electrónico intermediado**
- 6.6. Pago móvil
- 6.7. Otros pagos y tendencias futuras

SET

- **SET (Secure Electronic Transactions) es un protocolo desarrollado por VISA y Mastercard para enviar información de pagos mediante tarjeta a través de Internet.**
- **Objetivos:**
  - Permitir la transmisión **confidencial**.
  - **Autenticar** a las partes involucradas y sus cuentas/tarjetas.
  - Asegurar la **integridad** de las instrucciones de pago por bienes y servicios.

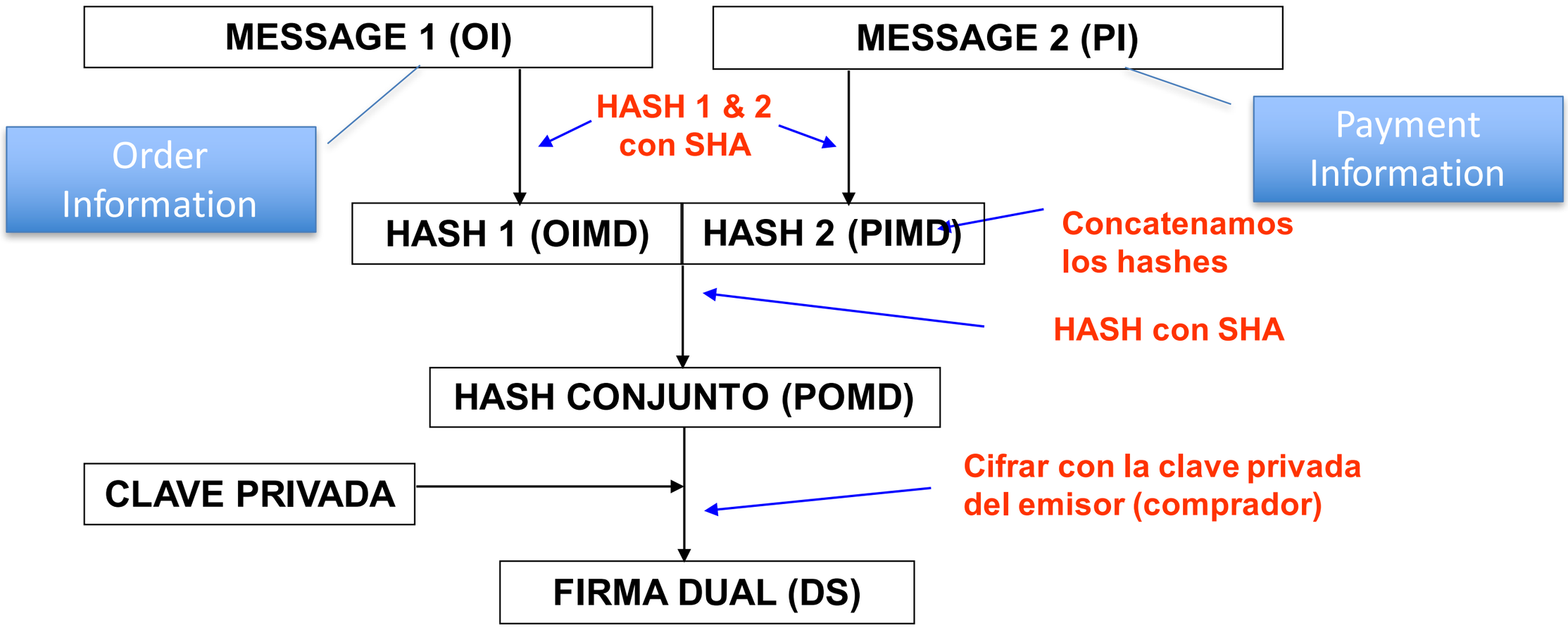
SET

- **Seguridad SET**
  - cifrado para garantizar la confidencialidad de la comunicación,
  - y firmas digitales para autenticación.
- **Los bancos tienen certificados digitales emitidos por SET**
- **Los comerciantes tienen certificados digitales emitidos por sus bancos**
  - para los consumidores es opcional.

SET

- **SET permite incluir información privada para el consumidor y el comerciante y para el consumidor y el banco en una sola transacción firmada mediante una estructura criptográfica llamada firma dual.**
  - El campo del comerciante se cifra con la clave pública del comerciante
  - El campo del banco se cifra con la clave pública del banco
- **La firma dual permite tanto al comerciante como al banco leer y validar su firma en la mitad de la solicitud de compra sin necesidad (ni posibilidad) de descifrar el campo de la otra parte.**

Firma dual



- **El comerciante recibe DS y PIMD**
- **El banco recibe DS y OIMD**
- **Cada uno puede verificar la firma sin conocer lo que no necesita**
  - El comerciante puede reconstruir OIMD
  - El banco puede reconstruir PIMD

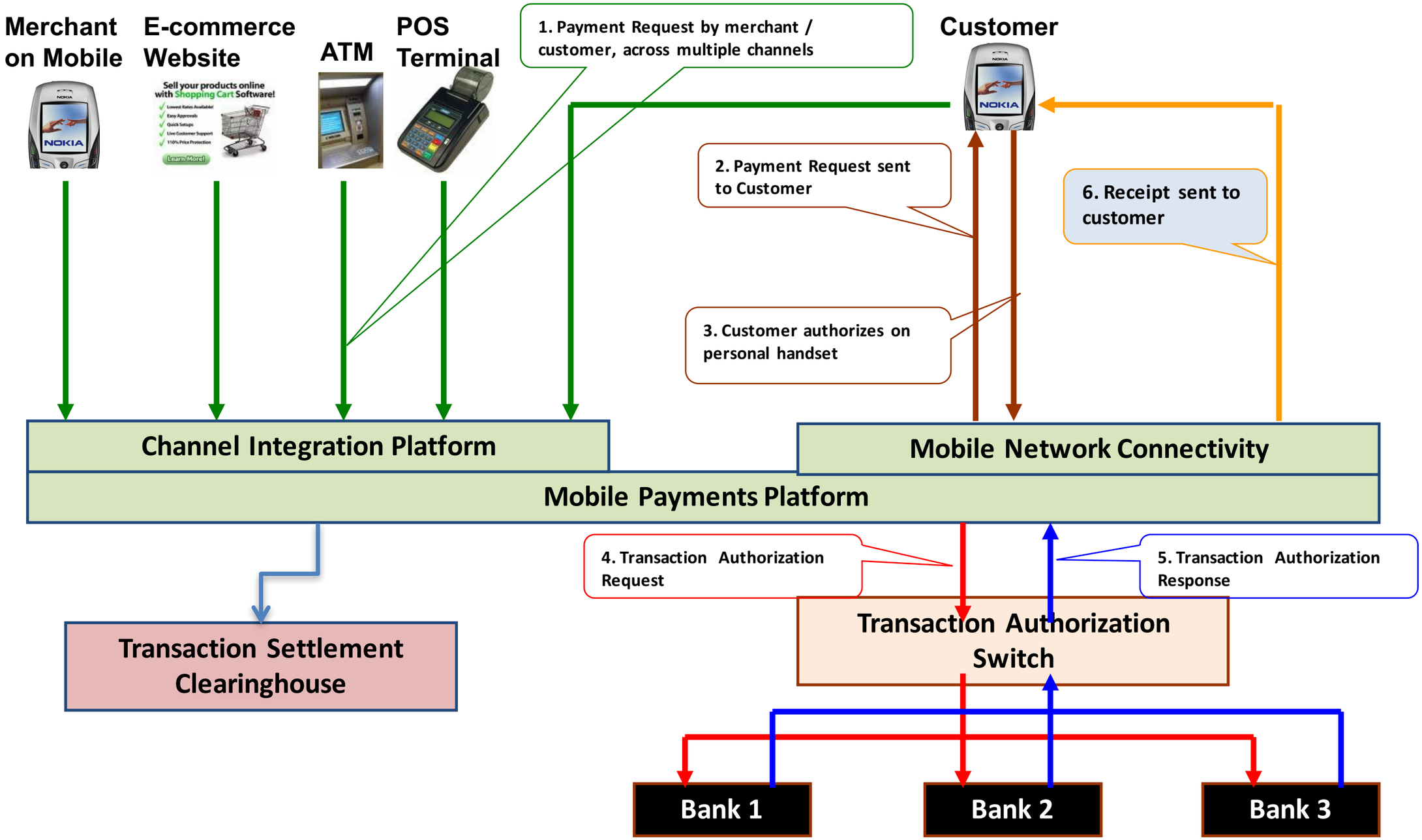
Contenido

- 6.1. Introducción
- 6.2. Tipos de pagos
- 6.3. Dinero electrónico
- 6.4. Pasarelas de pago
- 6.5. Pago electrónico intermediado
- **6.6. Pago móvil**
- 6.7. Otros pagos y tendencias futuras

Pagos móviles

- **Numerosas iniciativas que no cuajaron**
  - Móvilpago (BBVA y de Telefónica);
  - Pagomóvil (Bsantander y Airtel/Vodafone);
  - Caixamóvil (La Caixa y VISA); y
  - Paybox (Deutsche Bank).
- **Destinado a cubrir mercados que no estaban cubiertos todavía por otros medios electrónicos de pago como es el de las pequeñas compras (micropagos), como revistas, cine, pan, etc.**
- **Todos ellos operaban sobre una tarjeta (de crédito o de débito).**

Una transacción móvil tipo



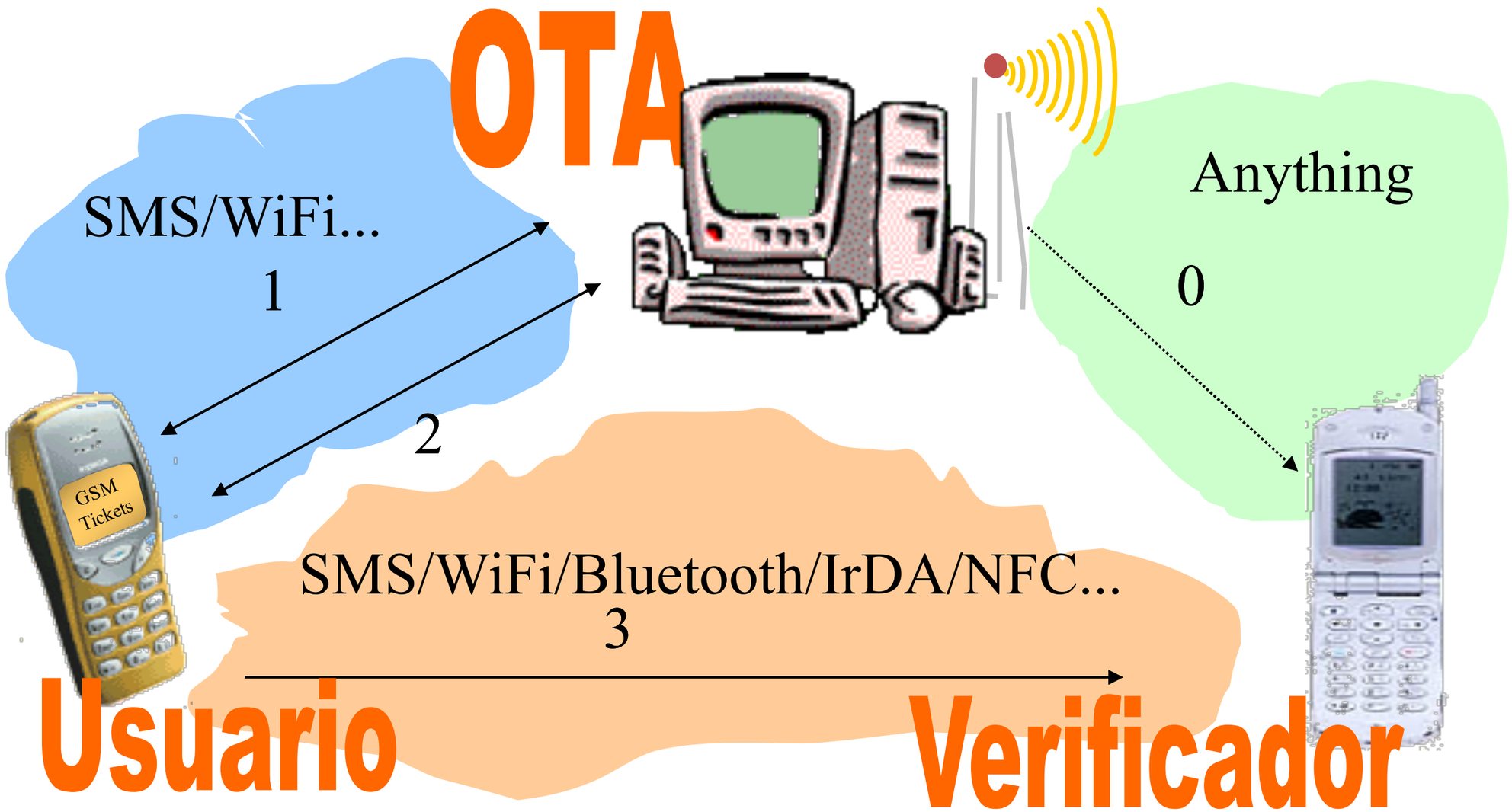
Contenido

- 6.1. Introducción
- 6.2. Tipos de pagos
- 6.3. Dinero electrónico
- 6.4. Pasarelas de pago
- 6.5. Pago electrónico intermediado
- 6.6. Pago móvil
- **6.7. Otros pagos y tendencias futuras**

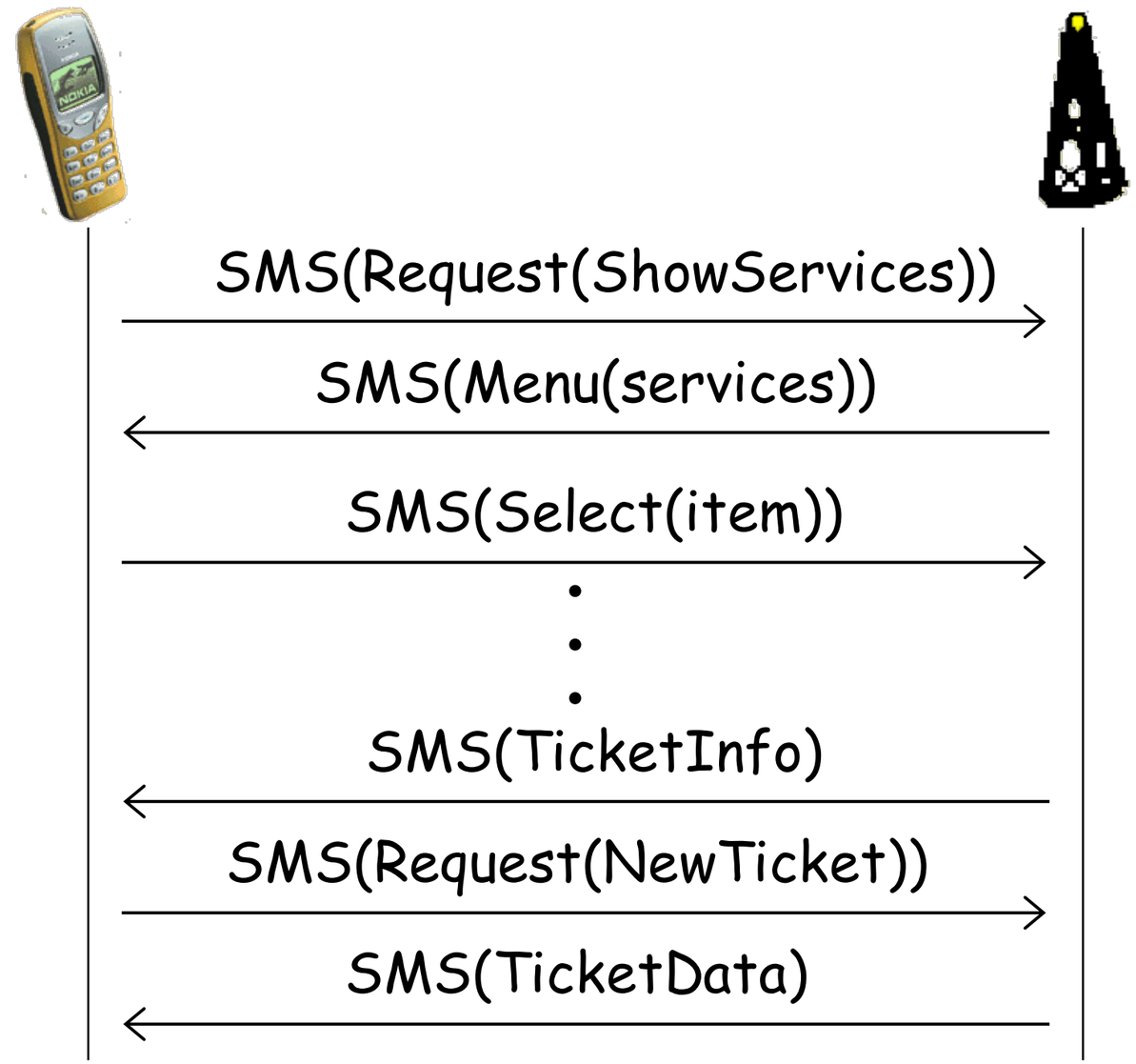
Otros pagos y tendencias futuras

- Tickets
- Pagos NFC y tarjetas contactless
- Conclusiones

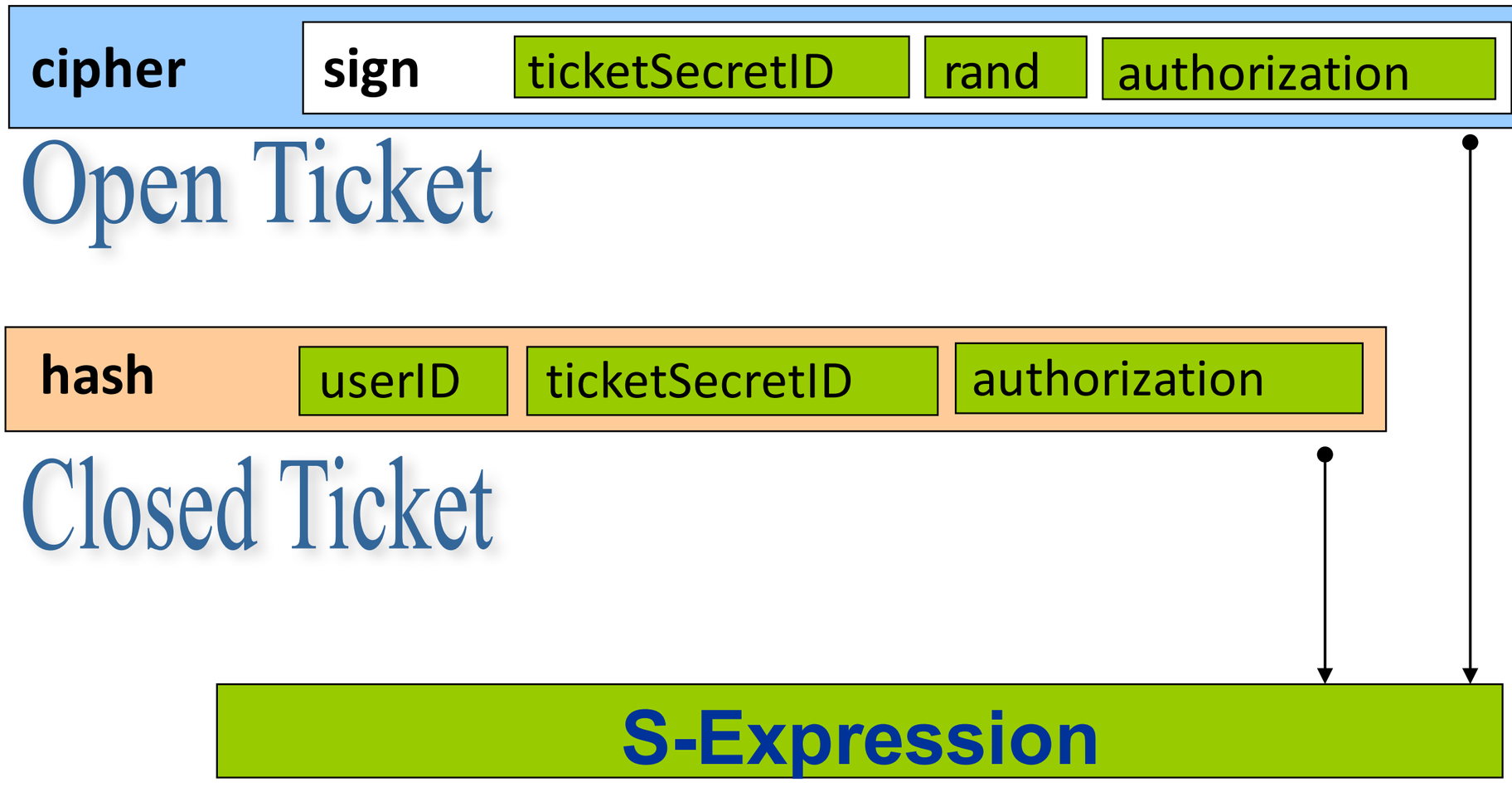
GSM-Ticket: Visión global



GSM-Ticket: Compra



Representación GSM-Tickets



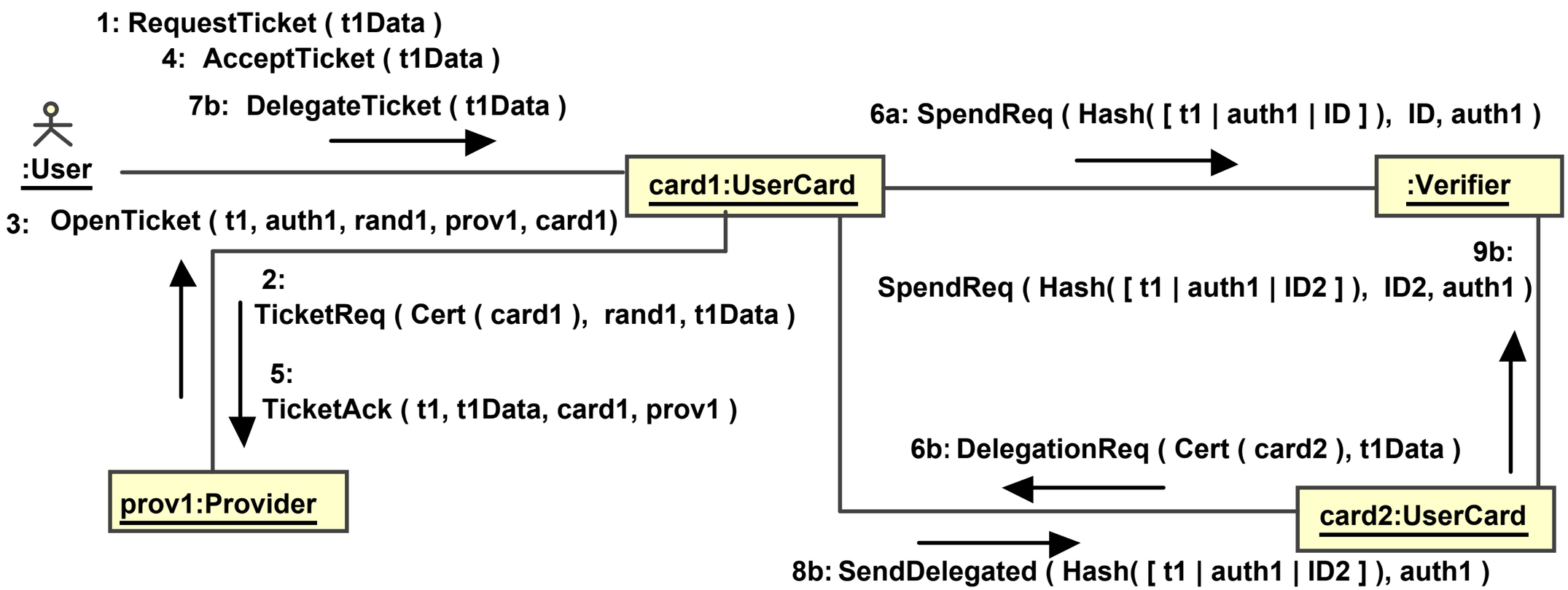
S-Expressions

```
(certificate
   (issuer
    (name
       (public-key rsa-with-md5
          (e |NFGq/E3wh9f4rJIQVXhS|)
          (n |d738/4ghP9rFZ0gAIYZ5q9y6iskDJ
          wASi5rEQpEQq8ZyMZeIZzIAR2I5iGE=|)
       )
       ticket-merchant1
    )
   )
...
```

S-Expressions

```
(subject
 (ref
    (DNI “12344321e")
 )
)
(not-before "2013-07-18_19:00:00")
(not-after "2013-07-18_19:30:00")
(tag
 (cinema
    (session "Matrix")
    (site "Victoria.Malaga.Spain")
 )
)
)
```

Escenarios de uso GSM-Tickets



Cert(entity) ::= Sign([PubKey(entity) | entityID], PrivKey(GSMoperator))

BCert (data, signer, recipient) ::= Encipher (Sign (data, PrivKey(signer)), PubKey(recipient))

OpenTicket (ticketSecretID, auth, rand, Provider, UserCard) ::= BCert ([ticketSecretID | auth | rand], Provider, UserCard)

TicketAck (ticketSecretID, ticketData, UserCard, Provider) ::= BCert ([ticketSecretID | ticketData], UserCard, Provider)

auth includes t1Data and Cert (Provider) t1Data includes t1Price, t1Conditions, t1PublicID,...

Pagos NFC y otros

- **Actualmente se está popularizando la idea de realizar pagos mediante chips específicos con comunicación mediante tecnología NFC (Near Field Communication)**
  - Google, Apple y otras están interesadas
  - Se transforma el móvil en "tarjeta"
  - Se transforma el operador o el fabricante en banco
- **Otras alternativas low-tech se está extendiendo**

Conclusiones

- **Existen numerosos sistemas de pago posibles**
  - Cada uno aporta ventajas y tiene escenarios de uso
  - Los consumidores deben poder elegir
- **La seguridad debe garantizarse más allá de la simple confidencialidad**
- **Pueden desarrollarse sistemas de pago específicos**
  - Mejor adaptados a un escenario
  - Problemas de aceptación
- **Tendencias**
  - Multiplicidad de medios
  - Convergencia móvil-tarjeta