



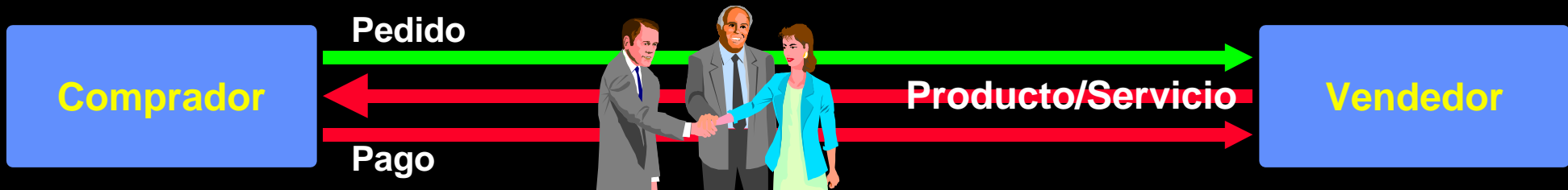
# Ciber comercio

¿seguridad técnica o confianza psicológica?

Julián Marcelo  
UPV-DOE

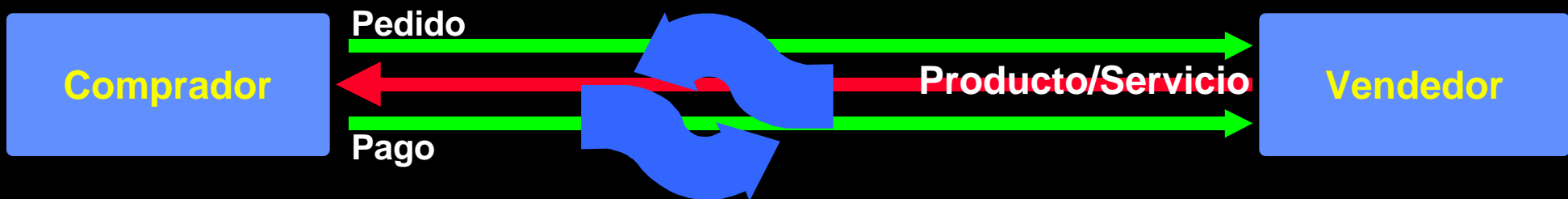
# Qué es el Ciber comercio

- **Comercio:** conjunto de actividades que soportan el intercambio de bienes materiales o inmateriales y servicios



- **Comercio electrónico:** Comercio soportado con tecnologías de la información y comunicaciones (teléfono, télex, fax, tarjetas, EDI)

Al compartir el medio (paso de unos sistemas a otros sin discontinuidad) se evita la reintroducción manual de datos, fuente de errores y 'ruido'; y se mejora la calidad de los datos correctos a lo largo de la cadena de valor.

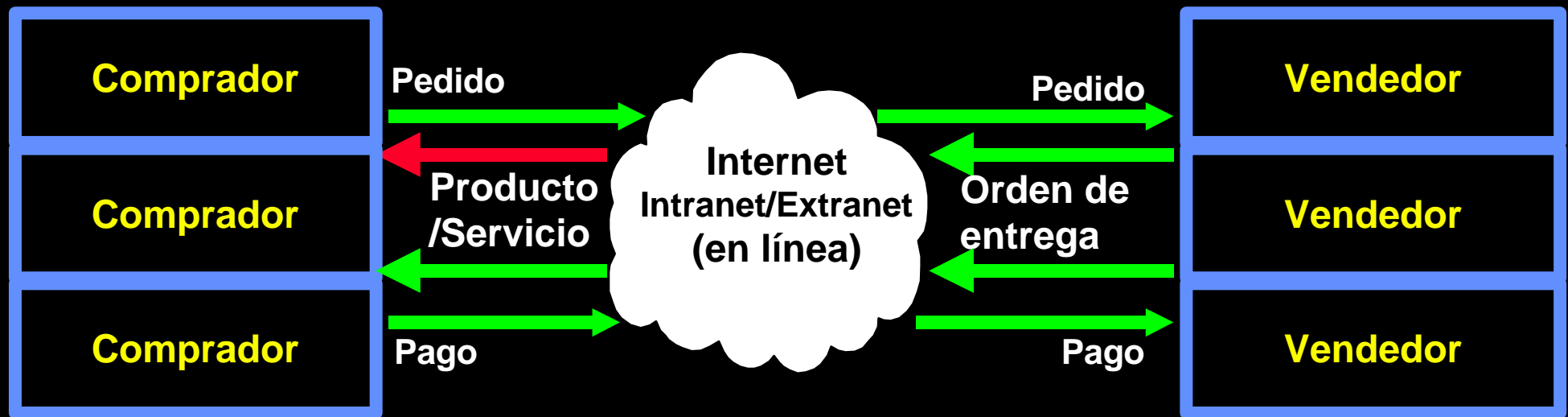


# Qué es el Ciber comercio

- **Ciber comercio: Comercio Electrónico** soportado por redes Internet (o sea, protocolos multimedia mundialmente aceptados)

⇒ **Ciber comercio: cambio radical en la forma de hacer negocios:**

- expansión mundial mercados actuales o creación de nuevos
- nuevos tipos de relación entre los actores de un negocio
- mejor proceso de intercambio de información entre empresas y AAPP



# Qué es el Ciber comercio

---

## Internet: lo 'vendido', lo real y lo futuro

- Accesible desde todo el mundo (pero no tanto)
- Tecnología multimedia barata (en infraestructura, no en servicios)
- Browser Universal (no están universal y a veces ni sirve)
- Tecnología “casi” madura, a adoptar tarde o temprano (pero pocas empresas de servicios la dominan)
- No hay más inseguridad de información (si nuevos problemas)

**Futuro inminente: Internet de alta velocidad (cable, 200 M bps); primera generación masiva de 'internautas'; el cliente ¡pide' Internet**

# Algunas Estimaciones

---

## Ventas por Comercio Electrónico

- 2.700 M \$ en 1996; 24.000 M \$ en 1999 (según Andersen)
- 13.000 M \$ en 1997; 300.000 M \$ en 2000 (según Forrester)

## Publicidad en USA:

- 176 M \$ en 1997; 2.577 M \$ en 2000

## Tráfico electrónico

- 20% comercio (80% correo); 16% comercio interempresas

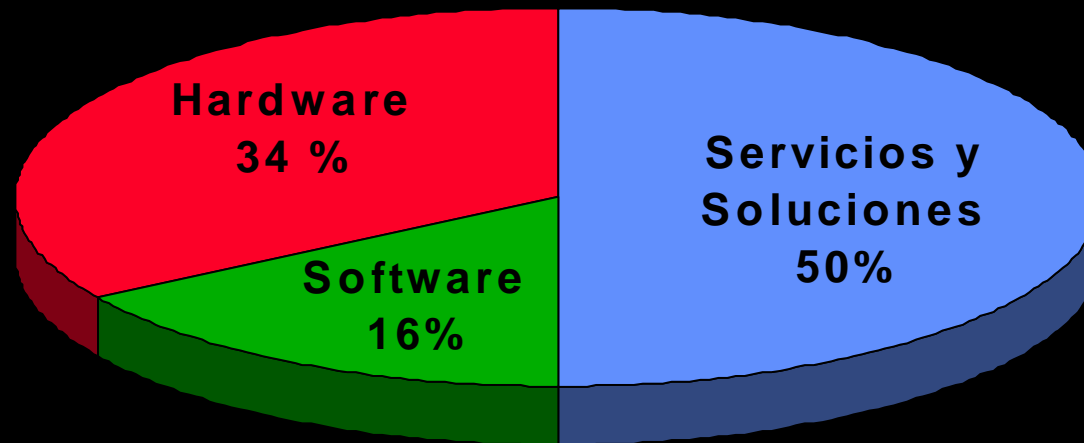
## Clientes potenciales

- Compañías conectadas: 126.000 en 1997; 840.000 en 2000
- Usuarios conectados: 60 Millones en 1996; 200 M en 2000

# Algunas Estimaciones

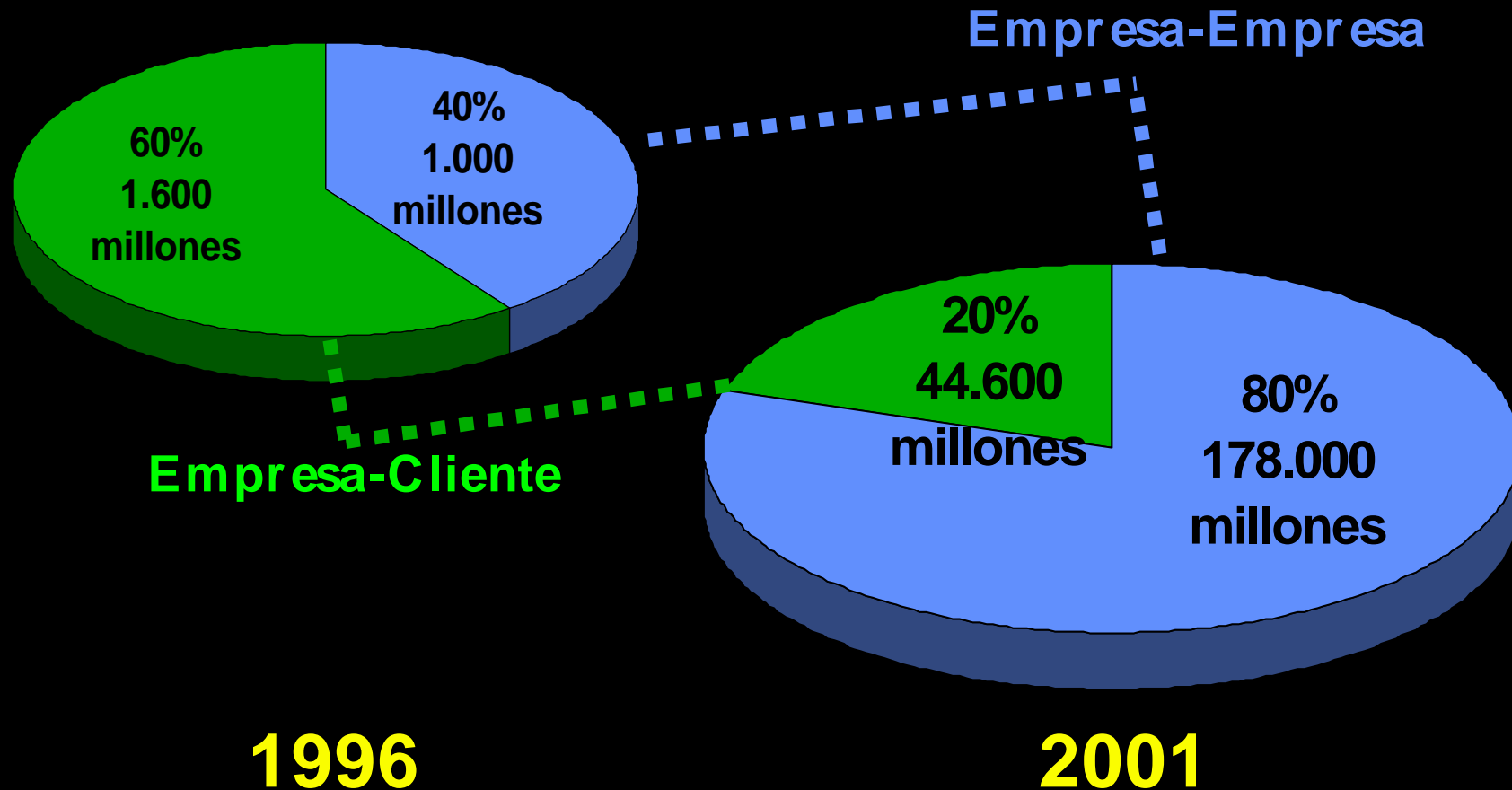
---

***Al negocio Cibercomercio acuden fuertes inyecciones de capital. Para tener rentabilidad rápida y alta ofrecen capital-riesgo para apoyo del nacimiento de nuevas empresas muy agresivas y/o las absorben para tomar posiciones estratégicas.*** En el 2000, de toda la inversión en IT, un 30% (400.000 M \$) va a Internet y Extranet y se reparte así:



# Algunas Estimaciones

## Crecimiento por el tipo de Comercio electrónico



# Tipos de Comercio electrónico

---

## **Cerrado: entre empresas (B2B) AAPP (A2A) mixto (B2A)**

*Diferido, Exclusivo, Formalizado (pre-contrato), muy regulado*

- las PYMEs entran con Internet en comercio electrónico (EDI, TEF)
- PYMEs y PYMAPs facilitan relaciones (SS, tributos, concursos)

## **Abierto: entre empresas y consumidores (B2C)**

*Interactivo, General, Espontáneo, poco regulado*

- Cambia la cadena de valor: distribución, intangibles, servicios
- Implica otros intermediarios: tecnológicos, financieros, consultores
- Escenarios: Escaparate, 'Rastro', Compra

# Tipos de Ciber comercio

---

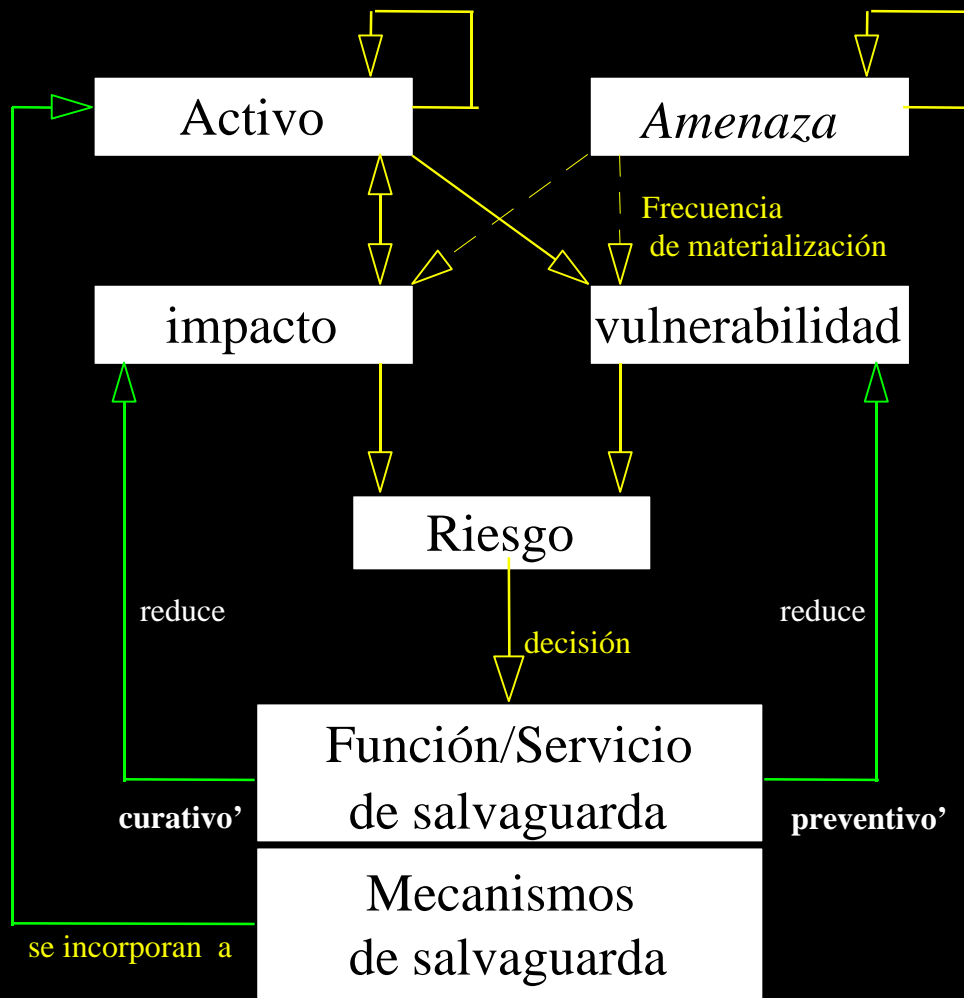
**El Ciber comercio abarca el ciclo completo de ventas**

- **Preventa (marketing):** llega a nuevos clientes
- **Venta:** disminuye el coste de la venta, aumenta el margen
- **Postventa:** Servicio al cliente, aumento de la fidelización

## Tramos de negocio

- **Contenido: 72%** Productos tangibles, Servicios interactivos, Información y Medios
- **Contexto: 10%** Publicidad, cuotas de subscripción
- **Resto: 18%** Acceso, Transporte

# Análisis y Gestión de Seguridad



- **Activo:** Sistema de Información
- **Amenazas:** Intencionales, inteligentes, internas/externas
- **Vulnerabilidad:** posibilidad/ frecuencia de materialización de cada amenaza
- **Impacto:** degradación de la función que cumplimenta el activo
- **Riesgo:** composición del Impacto en el activo y la vulnerabilidad a la amenaza
- **Salvaguardas:** medidas para restablecer el nivel de seguridad:
  - técnicas (cifrado)
  - organizativas (PKI)

# Análisis y Gestión de Seguridad

---

El estado de seguridad de un S.I. tiene varios aspectos y *niveles*:

- **Subestado A de Autenticación de los Actores**, ligado a la formalización, autorización y responsabilidad probatoria en el conocimiento o la comunicación de datos (no repudio de recepción o de envío)
- **Subestado C de Confidencialidad de la Información**, ligado a poder conocer su contenido por terceros no autorizados.
- **Subestado I de Integridad de la Información**, ligado a su reobtención con *calidad* suficiente (completa y no 'corrompida' para el uso deseado)
- **Subestado D de Disponibilidad de la Información**, ligado al *tiempo máximo de carencia* sin graves impactos para la Organización.

Los niveles de riesgo en los distintos subestados, combinados con cada tipo de cibercomercio, conforman las medidas de seguridad (salvaguardas) que éste necesita.

# Seguridad en Comercio electrónico

---

Su carácter diferido, exclusivo, formalizado y muy regulado exige mecanismos que aseguren en prioridad los subestados de:

- Confidencialidad
- Integridad
- Autenticidad

La confidencialidad se asegura con mecanismos técnicos de CIFRADO de CLAVE PRIVADA, sin complicaciones organizativas. La relación bilateral bien regulada permite transmitir la clave secreta sin demasiado peligro.

Se sigue usando el mecanismo DES para TEF en la red bancaria SWIFT. Las aplicaciones WebEDI se apoyan en intercambios MIME sobre plantillas de control XML.

# Seguridad en Comercio electrónico

---

## DES (Data Encryption Standard)

El mecanismo de salvaguarda DES, desarrollado por el National Bureau of Standards NBS -hoy NIST- es norma de hecho pese a las restricciones impuestas a su exportación. El algoritmo de DES, robusto al criptoanálisis aunque es de dominio público, consiste en una compleja combinación de operaciones de *sustitución*, *permutación* y *lógica xor* en función de una clave  $k$  que sólo si se conoce permite descifrar la información cifrada.

El cifrado arranca dividiendo el mensaje en bloques  $B$  de 64 bits. Aplica el mismo proceso de operaciones a cada uno con ayuda de una clave  $k$  de 56 bits (+ 8 de paridad para detectar errores). DES usa sustituciones (con tablas), la operación binaria 'xor' y tres tipos de permutaciones (simples, que expanden bits, que los reducen).

# Seguridad en Comercio electrónico

---

## Variantes y ampliaciones de DES (p.ej. a 112 bits)

- **RSA serie RC1 a RC9: algoritmos secretos de robustez no comprobable**
- **IDEA, *International Data Encryption Algorithm*: sustituye a DES en el freeware PGP (*Pretty Good Privacy*) y usa claves de 128 bits, fuera por ahora de ataque brutal**
- **Skipjack, algoritmo secreto de la NSA, equipa el chip 'espía' Clipper que permite 'pinchar' los mensajes, sólo cifrables legalmente con Skipjack**
- **AES, *Advanced Encryption Standard*, reemplazante de DES, (los expertos aún no han fijado los algoritmos criptográficos que lo soportarán).**

Los fabricantes (Intel, Motorola, etc.) construyen chips VLSI que implementan DES y se conectan al bus del microprocesador como otro dispositivo más. Otros fabrican chips especializados DES de alta velocidad (VLSI Tech. a 200 M bytes/s y DEC a 1.000 M bytes/s por 300 \$).

# Seguridad en Comercio electrónico

---

Su carácter interactivo, general, espontáneo y poco regulado (entre muchas empresas y consumidores) implica amenazas extendidas que afectan en prioridad los subestados de:

- Autenticidad (quién envía y quién recibe), contradictorio a la
- Confidencialidad (quién conoce el mensaje)
- Integridad (qué contiene el mensaje)

El comercio electrónico exige MECANISMOS DE CIFRADO más adecuados que los de clave secreta:

- vulnerables a una amenaza esencial: la débil confidencialidad en su transporte del emisor al receptor.
- Ineficaces por la explosión del número de claves bilaterales necesarias,  $n * (n-1)/2$  para  $n$  comunicantes

# Seguridad en Comercio abierto

---

## Cifrado basado en algoritmo unidireccional con clave pública

Se basa en una función doble  $(C, I)$  de una dirección con 'trampa', o sea una función directa  $C = f(I)$  fácil de calcular (por un algoritmo  $C$ ), con función inversa  $I = f^{-1}(C)$  muy difícil de calcular (por otro algoritmo  $D$ ) aunque se conozca  $C$ , salvo si se conoce  $k$  (la clave secreta de descifrado).

Si además se cumple  $I = f^{-1}(f(I))$ , la función  $(C, I)$  es permutación unidireccional con trampa y permite implementar salvaguardas de autenticidad (firma electrónica).

Entre estas funciones  $(C, I)$ , algunas han mostrado particular sencillez y robustez al criptoanálisis las funciones de cifrado exponencial (base del algoritmo RSA, p.ej.) y las llamadas curvas elípticas.

# Seguridad en Comercio abierto

---

## Los algoritmos basados en funciones C,I dan muchas ventajas

- **Combinan sólo dos claves por comunicante A, la pública A-pub y la privada A-priv; la gestión de claves para n comunicantes se reduce a  $2n$  claves, n públicas y n privadas (frente a las  $n(n-1)/2$  anteriores**
- **Garantizan la confidencialidad (no se transporta la clave entre comunicantes) sin merma de empleabilidad (la difusión de cada clave pública A-pub no permite deducir su clave privada A-priv; pero todo mensaje cifrado con una de las dos claves puede ser descifrado con la otra.**
- **Los comunicantes A B resuelven la autenticación simple empleando sus claves. Sólo A puede usar su clave A-priv y todo B puede comprobar ese origen en A con la clave A-pub, pero no leer el mensaje (ni suplantar al emisor A si además A uso en el mensaje la autenticación fuerte que da su firma digital).**
- **La integridad del mensaje se resuelve con métodos parecidos**

# Seguridad en Comercio abierto

## Funcionamiento del algoritmo RSA (Rivest, Shamir y Adleman)

**RSA, el sistema de clave pública más conocido, se basa en la asimetría de la función de factorización de grandes números. ¿Cómo A debe usar RSA?**

- **A elige dos números primos grandes  $p$ ,  $q$  y los mantiene en secreto (los usa sólo una vez para obtener las claves)**
- **A calcula  $An = p * q$  (lo publicará).**
- **A escoge un  $A\text{-priv} > p$ ,  $> q$ ,  $< An$  y sin divisores comunes con  $r = (p-1) * (q-1)$**
- **A calcula  $A\text{-pub}$  tal que**

$$A_{\text{pub}} * A_{\text{priv}} = 1 \pmod{((p-1) * (q-1))}$$

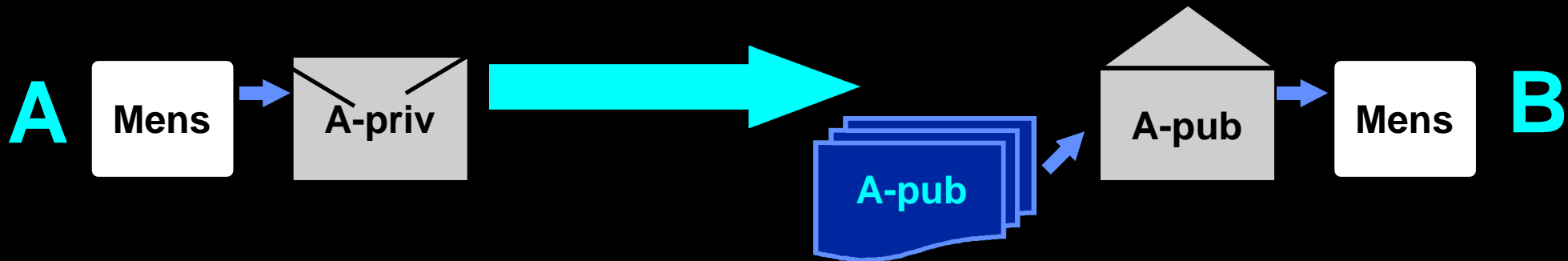
**operador módulo/resto de la división entera**

$$\Rightarrow A_{\text{pub}} * A_{\text{priv}} \pmod{((p-1) * (q-1))} = 1$$

$$\Rightarrow A_{\text{pub}} = \text{inv} \{A_{\text{priv}}, \pmod{((p-1) * (q-1))}\} \text{ función inversa.}$$

- **A guarda  $A\text{-priv}$  como clave privada**
- **A difunde  $(A\text{-pub}, An)$  como clave pública**

# Seguridad en Comercio electrónico

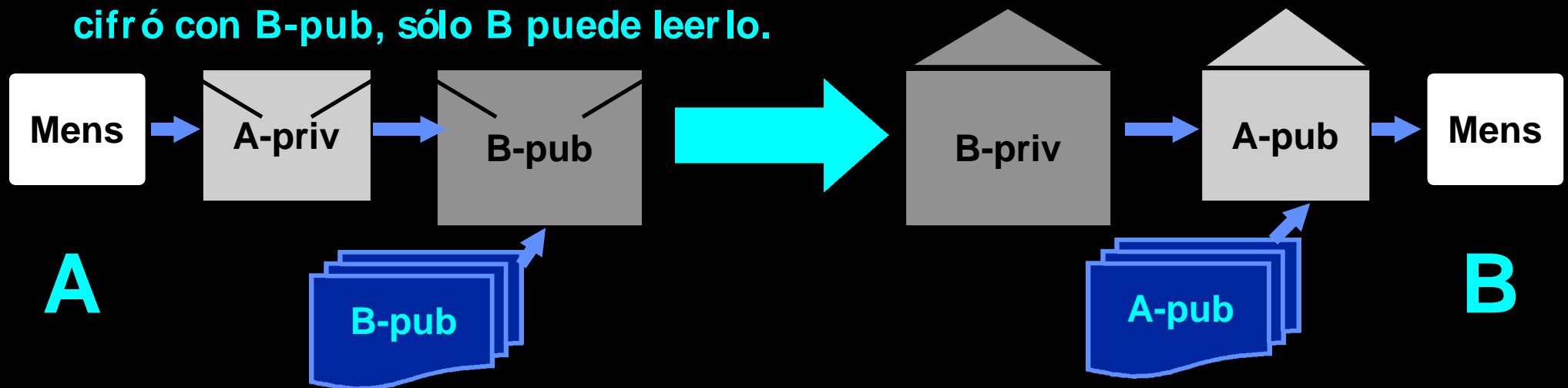


- La función de autenticación simple **protege a las dos partes A, B que intercambian mensajes frente a terceras partes C; pero no protege a una de la otra frente a disputas entre ambas (B puede falsificar un mensaje y afirmar que lo recibió de A; A puede negar que lo envió).**
- La función de firma digital **permite resolver las disputas entre A y B.**
- La función de autenticación simple está incluida, es más simple y se usa más que la función de firma digital, pues ésta
  - no se necesita si sólo se requiere la autenticación simple
  - es más compleja, lenta, costosa
  - requiere mecanismos de control administrativo adicionales (lo que hace a la firma más vulnerable en cierta forma).

# Seguridad en Comercio electrónico

## Firma digital

- A puede usar RSA para implantar su firma digital como salvaguarda de autenticidad y garantizar la integridad del mensaje (no alteración durante la transmisión).
- La firma puede aplicarse al mensaje completo o ser algo añadido a éste.
- Se precisa un mecanismo de 'doble cifrado' para impedir impostores (cualquiera puede enviar un mensaje a B utilizando su clave B-pub).  
Como el mensaje M se cifró con A-priv, sólo pudo venir de A; y como se cifró con B-pub, sólo B puede leerlo.



# Seguridad en Comercio electrónico

---

## Problemas de identidad/autenticación de cliente/vendedor

- La presencia en red de un vendedor no prueba que sea quien dice (puede estar pinchada). Ha de asegurar su identidad a sus clientes
- El uso de la tarjeta del cliente no prueba su propiedad
- El vendedor puede engordar la compra (tras saber el PIN)

## La compra segura para ambos está ligada al medio de pago

- Contrareembolso: *óptimo para cliente; complejo para vendedor*
- Cargo en cuenta: *Inseguro para cliente; óptimo para vendedor*
- Tarjeta crédito (débito): *inseguro para ambos; fácil pago-cobro*
- Tarjeta prepago (chip): *seguro para cliente; complejo para vendedor (terminales especiales)*
- Diner electrónico: *compra anónima (alta seguridad para cliente)*

# Seguridad en Comercio electrónico

---

## Tipos de firma digital: firma con respaldo

- **Autenticación directa**- A cifra el mensaje con su clave privada A-priv. B descifra el mensaje con la clave pública A-pub de A
- **Firma Digital (con Autenticación y Secreto)**. A cifra el mensaje con A-priv y el resultado con la B-pub de B. B lo descifra con su B-priv y vuelve a descifrar el resultado con la A-pub de A (ojo a la seguridad de A-priv).
- **Firma Digital Arbitrada**. A podría negar el envío del mensaje - repudio-, aduciendo pérdida de su A-priv o falsificación de su 'firma'. Se evita usando un *árbitro*: cada mensaje firmado de A a B va primero al árbitro C, que somete el mensaje y su firma a pruebas (para verificar su origen, contenido y fecha) y lo envía a B con una indicación sobre la validez de lo verificado. La presencia de C implica que A no puede repudiar el mensaje, siempre que A y B reconozcan la autoridad de C. C desempeña un papel notarial donde es crucial la noción de CONFIANZA.

# Origen de la confianza

---

- **En una autoridad universalmente reconocida**

Árbol jerárquico estricto

- SET, PEM Servicio de Privacidad en Mensajería electrónica

- **En alguna autoridad reconocida por el usuario**

Árboles jerárquicos-islas, o certificación cruzada

- SSL, S/MIME

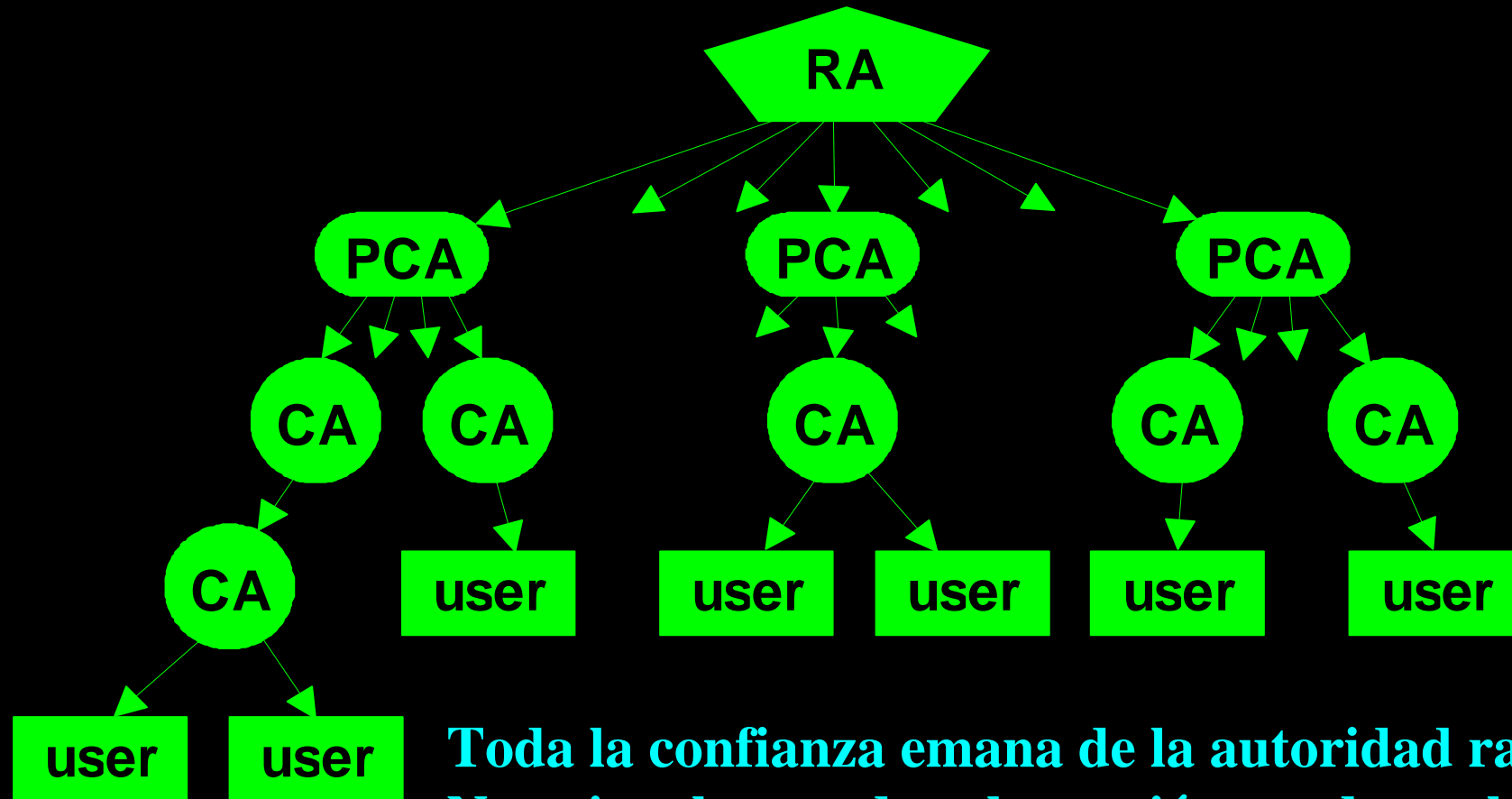
- **En uno mismo**

Grafos y cadenas centrados en el usuario

- PGP, SDSI / SPKI

# Origen de confianza: árbol

---



**Toda la confianza emana de la autoridad raíz RA.  
Necesita el acuerdo sobre quién puede ser la RA.**

# Origen de confianza: Cadena

---



# Gestión de Certificados: antecedentes

---

- 1976: Diffie y Hellman piensan que el problema organizativo de la distribución de claves se resolvería con un simple directorio público
- 1978: L. Kohnfelder propone el uso de certificados



**La confianza en el signatario AC se transmite al ente certificado A**

# Gestión de Certificados: desarrollo

---

- 1988: las PTT reinventan el directorio electrónico universal (X.500), lo distribuyen y reducen el acceso a escritura: KP identifica editores (X.509)
- 1989: el Servicio PEM Privacidad en Mensajería electrónica usa certificados para validar direcciones de correo electrónico ... pero no materializa el directorio universal (X.509)
- 1991: PGP usa certificados para asociar claves a direcciones e-mail; pero sin directorio universal: cada uno decide de quién fiarse y a quien incorporar en el círculo de confianza
- 199x: los mecanismos usan el actual X.509v3 (certificado muy flexible)
  - S/MIME, SSL, TLS, IPsec, ...
  - PKI reemplaza el no nato directorio o listín universal
- 1996: MIT lanza SDSI/SPKI para evitar la complejidad, enemiga de la seguridad

# Gestión de Certificados: tipos

---



# Certificado X.509 v3

---

Versión
Número de serie
Algoritmo de firma
Nombre x.500 del proveedor
validez
Nombre x.500 del sujeto
Datos de clave pública del sujeto
Identificación única del proveedor
Identificación única del sujeto
Extensión {tipo, criticidad, valor}
Extensión {tipo, criticidad, valor}
Extensión {tipo, criticidad, valor}
Firma digital de la CA

version 3

la autoridad de certificación

start= 01/01/1998, end= 31/12/2002

la identidad del sujeto

la clave pública del sujeto

Key usage: cifrado + firmado

rfc822: jmardelo@ati.es

CRL distribution: <http://www.ati.es>

# PGP, Pretty Good Privacy

---

- **PGP se limita a certificar identidades de correo electrónico.**
- **En PGP, cada sujeto cree en sí mismo, establece la red en torno a sí y decide en quién confía (los amigos de mis amigos, son mis amigos, pero hay amigos y amigos :-)** => **4 niveles de confianza.**
  - 0. Confianza completa:** Toda clave avalada por esta clave amiga se incorpora al anillo de claves local. El nuevo usuario puede 'presentar' a otros
  - 1. Confianza marginal:** Una clave firmada por esta clave sólo se incorpora al anillo si viene avalada por otra. Este usuario no puede 'presentar' a otros
  - 2. Ninguna confianza:** La clave así marcada no se incluye en el anillo de claves. No se acepta lo que afirme su usuario sobre fiabilidad de otros
  - 3. Fiabilidad desconocida:** En la práctica se trata igual que la anterior ya que se duda sobre la fiabilidad de otro usuario, pero sin desconfianza motivada.

**Las últimas versiones de PGP incluyen una foto**

# SSL , Secure Sockets Layer

---

Plataforma diseñada por Netscape, sencilla y muy usada

- **Afecta sólo a la relación cliente-vendedor**  
(la relación vendedor-banco tiene protocolos privados)
- **Sólo el vendedor se certifica**  
(identidad segura para el cliente)
- **El cliente puede comprar con cualquier identificador personal PIN válido**  
(autenticación insegura para el vendedor)
- **El mensaje se cifra y el vendedor recibe los datos del cliente, no el banco.**
  - El vendedor podría alterar datos  
(integridad insegura para el cliente)
  - El vendedor accede a los datos de la tarjeta  
(confidencialidad insegura para el cliente)
- **No está garantizado el repudio de la transacción**  
(ambas partes inseguras)

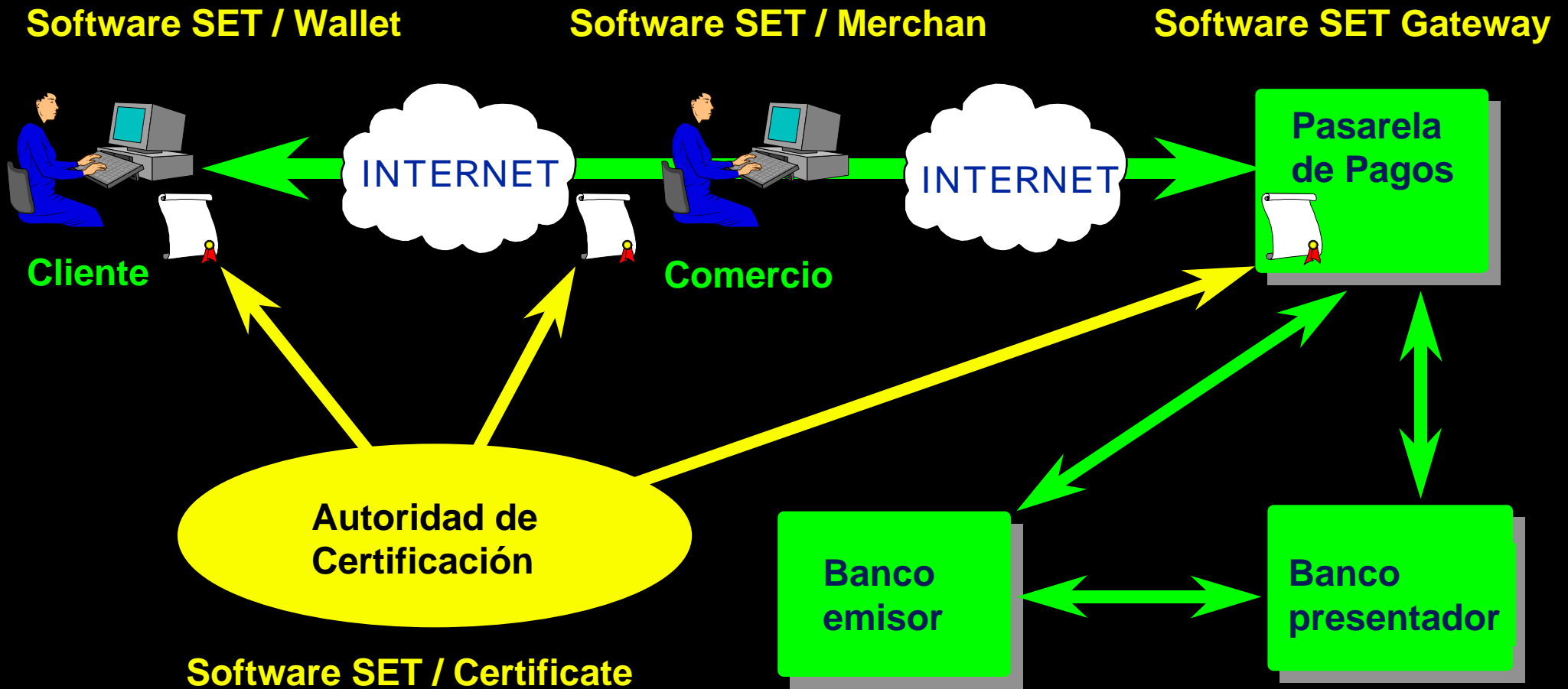
# SET, Secure Electronic Transaction

---

## Plataforma diseñada por Visa y Mastercard

- **Afecta a 3 relaciones: cliente-vendedor, vendedor-banco, entre bancos**
- **Se han de certificar los 3 (incluido el cliente)**  
(identidad segura para todos sobre todos)
- **Todos han de instalar software específico SET**  
(complejo, compra no espontánea => SET poco usado)
- **El vendedor no accede a los datos bancarios del cliente y el banco no accede a los datos de la compra**  
(confidencialidad segura para todos)
- **El mensaje se cifra y se firma**  
(integridad segura para todos)
- **No repudio de la transacción técnicamente garantizado**  
(seguro para todos)

# SET, Secure Electronic Transaction



# PKI, Public Key Infrastructure

---

## Definición de IETF - PKIX (grupo de trabajo de Internet)

- El conjunto de dispositivos, programas, personas, política y procedimientos necesarios para crear, gestionar, almacenar, distribuir y revocar certificados basados en criptografía de clave pública.

## Legislación reciente -1999- sobre firma electrónica

- La Directiva europea y el RD español sobre firma electrónica establecen de facto las condiciones organizativas y legales de las Infraestructuras de Clave Pública PKI

## Legislación en curso sobre Comercio electrónico

# Partes de una PKI

---

- **Perfiles**
- **Protocolos operativos**
- **Protocolos de gestión**
- **Política**
- **Fecha (TSA, Time Stamping)**

TSA: fundamental saber en qué momento se realizan actividades y/o se está en posesión de ciertos datos

El fechado digital aparece como un servicio necesario, esté empotrado o lo proporcione una autoridad específica

# Funciones de una PKI

---

- **Registro**
- **Inicialización**
- **Certificación**
- **Generación de claves**
- **Recuperación de claves**
- **Renovación de claves**
- **Certificación cruzada**
- **Revocación**

# Infraestructuras simples SDSI / SPKI

---

- **Se centran en la clave pública, elemento central para verificar firmas; la identidad es secundaria**

El propietario de la clave puede hacer afirmaciones verificables, en particular gestionar el control de acceso (ACL) que es la base de un sistema distribuido de confianza

- **Espacio local de nombres:**

- alice's bob's mother's doctor's address

(cada sujeto de la línea de nombres opera su propio servidor)

+ algunos nombres globales que todos reconocen

(p.ej. DNS, el sistema mundial de BD)

# CRL, Lista de revocaciones de certificados

---

versión

version 2

Algoritmo de firma

Nombre x.500 del proveedor

la autoridad de certificación

Actualización actual

Actualización siguiente (opcional)

Certificado {usuario, fecha, extensiones}

123.456.789.0, 28/12/1999, comprometida

Certificado {usuario, fecha, extensiones}

Certificado {usuario, fecha, extensiones}

Extensión {tipo, criticidad, valor}

CRL number: 313

Extensión {tipo, criticidad, valor}

Extensión {tipo, criticidad, valor}

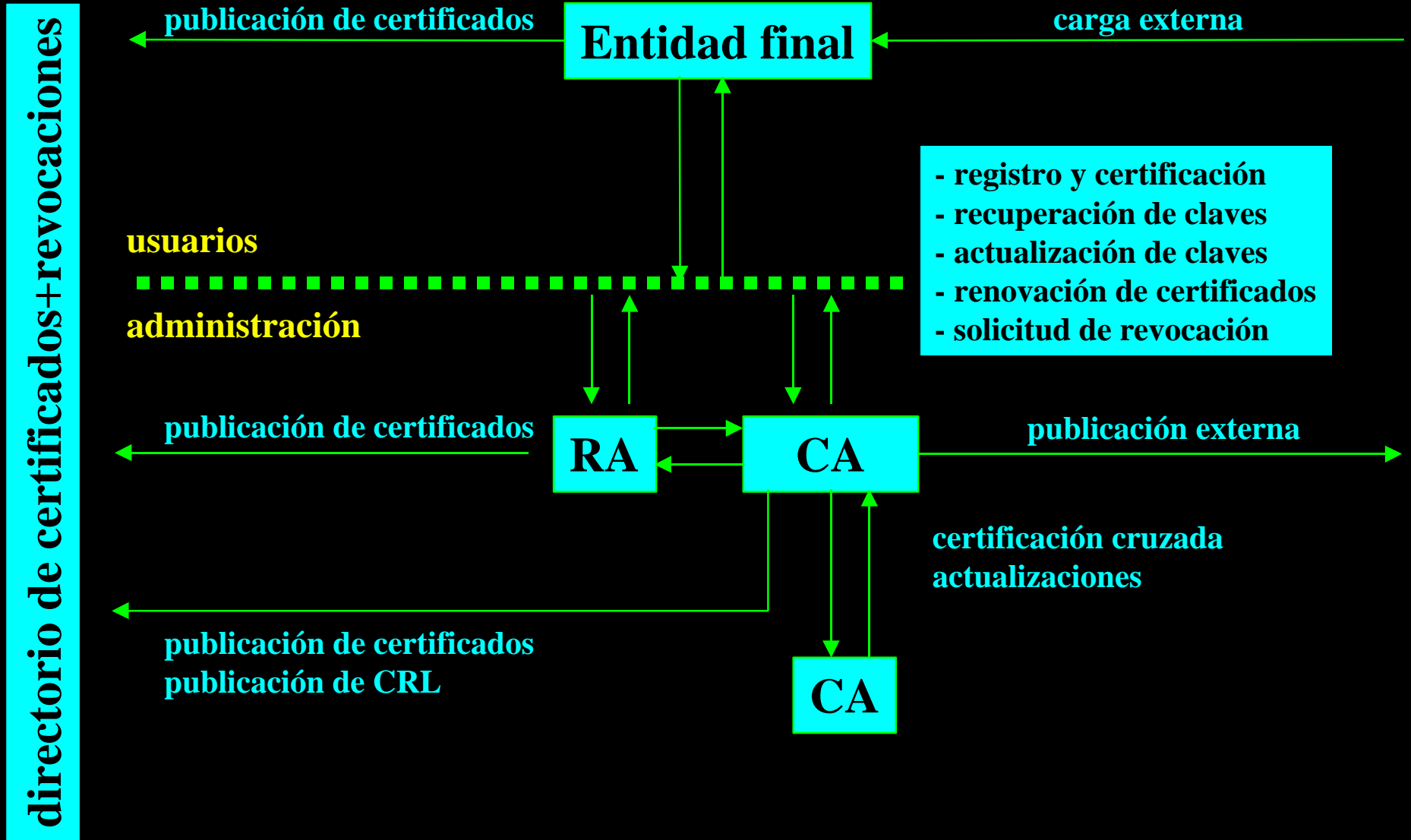
Firma digital de la CA

# CA y/o RAs

---

- **Una CA responde al modelo de una oficina central, con un nivel elevado de seguridad**
  - varias empresas (extranet) implican varias CA, que se reconocen mutuamente
- **Una RA responde al modelo de una delegación, con responsabilidades administrativas y seguridad relativa**
  - varias delegaciones implican varias RA, agentes de la CA central
- **Es posible un modelo de externalización (*outsourcing*) donde la empresa opera una RA y subcontrata la CA**
  - la CA da solvencia; la RA gestiona los datos confidenciales

# Gestión de directorios y revocaciones



# Repositorios y protocolos de acceso

---

## X.500 & DAP (Directory Access Protocol)

- iba a ser el directorio universal y ha resultado excesivo e inviable

## LDAP (Lightweight DAP)

- nace como una forma económica para que clientes ligeros (PC) accedan a directorios x.500
- modelo de información jerarquizada, asocia atributos a los nodos
- servicio de directorio distribuible y coordinable
- por tanto se presta de forma natural a almacenar certificados y CRL

# Repositorios y protocolos de acceso

---

## HTTP & FTP

- soluciones ad-hoc
- puede existir un LDAP detrás, ofreciendo una interfaz amigable

## DNS (sistema mundial de BD)

- asocia nombres de dominio con direcciones IP
- muy adecuado para automatizar la propia seguridad del DNS y de los dispositivos registrados en él
- estructura muy especial de nombres
- soporte local inmediato; pero no hay aún un despliegue masivo