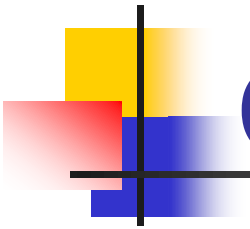
Bloque III
Seguridad en la Internet

Seguridad a nivel de aplicación, transporte y red

Seguridad en Redes de Comunicaciones
María Dolores Cano Baños



Contenidos

1.1 Introducción

1.2 Secure Electronic Transactions (SET)

- 1.2.1 Participantes
- 1.2.2 Servicios
- 1.2.3 Secuencia de acciones
- 1.2.4 Firma Dual
- 1.2.5 Transacciones permitidas

1.3 Secure Socket Layer (SSL)

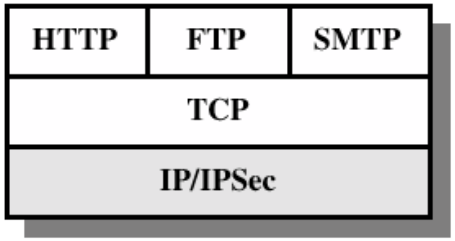
- 1.3.1 Arquitectura
- 1.3.2 Sesiones y conexiones
- 1.3.3 Protocolo Record
- 1.3.4 Protocolo Change Cipher Spec
- 1.3.5 Protocolo Alert
- 1.3.6 Protocolo Handshake
- 1.3.7 Cálculos criptográficos
- 1.3.8 Consideraciones adicionales

1.4 IPSec

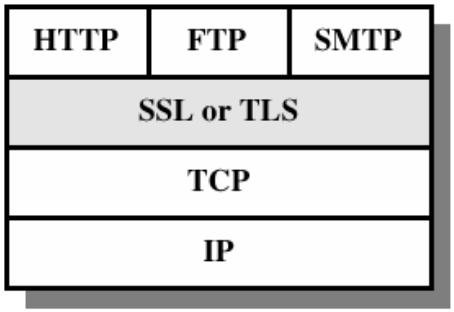
- 1.4.1 Protocolos vinculados a IPSec
- 1.4.2 Asociaciones de seguridad
- 1.4.3 Protocolos IPSec
- 1.4.4 Autenticación entre entidades y formación de asociaciones de seguridad

Introducción

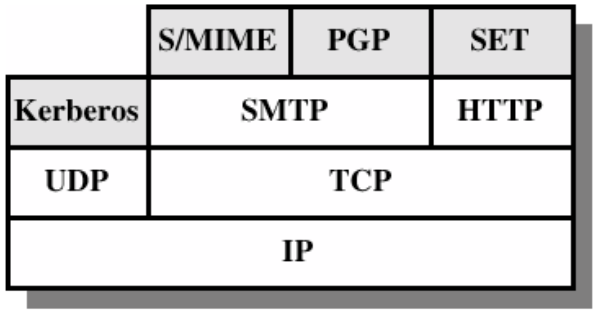
Herramientas de seguridad en la pila de protocolos TCP/IP



(a) Network Level



(b) Transport Level



(c) Application Level

Contenidos

1.1 Introducción ✓

1.2 Secure Electronic Transactions (SET)

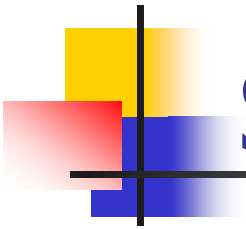
- 1.2.1 Participantes
- 1.2.2 Servicios
- 1.2.3 Secuencia de acciones
- 1.2.4 Firma Dual
- 1.2.5 Transacciones permitidas

1.3 Secure Socket Layer (SSL)

- 1.3.1 Arquitectura
- 1.3.2 Sesiones y conexiones
- 1.3.3 Protocolo Record
- 1.3.4 Protocolo Change Cipher Spec
- 1.3.5 Protocolo Alert
- 1.3.6 Protocolo Handshake
- 1.3.7 Cálculos criptográficos
- 1.3.8 Consideraciones adicionales

1.4 IPSec

- 1.4.1 Protocolos vinculados a IPSec
- 1.4.2 Asociaciones de seguridad
- 1.4.3 Protocolos IPSec
- 1.4.4 Autenticación entre entidades y formación de asociaciones de seguridad



Secure Electronic Transactions

- Es una especificación abierta de cifrado y seguridad (1995).
- Protege transacciones con tarjetas de crédito en Internet.
- Empresas implicadas:
  - MasterCard, Visa, IBM, Microsoft, Netscape, RSA, Terisa y Verisign.
- No es un sistema de pago.
- Es un conjunto de protocolos de seguridad y formatos.

Contenidos

1.1 Introducción ✓

1.2 Secure Electronic Transactions (SET) ✓

- 1.2.1 Participantes
- 1.2.2 Servicios
- 1.2.3 Secuencia de acciones
- 1.2.4 Firma Dual
- 1.2.5 Transacciones permitidas

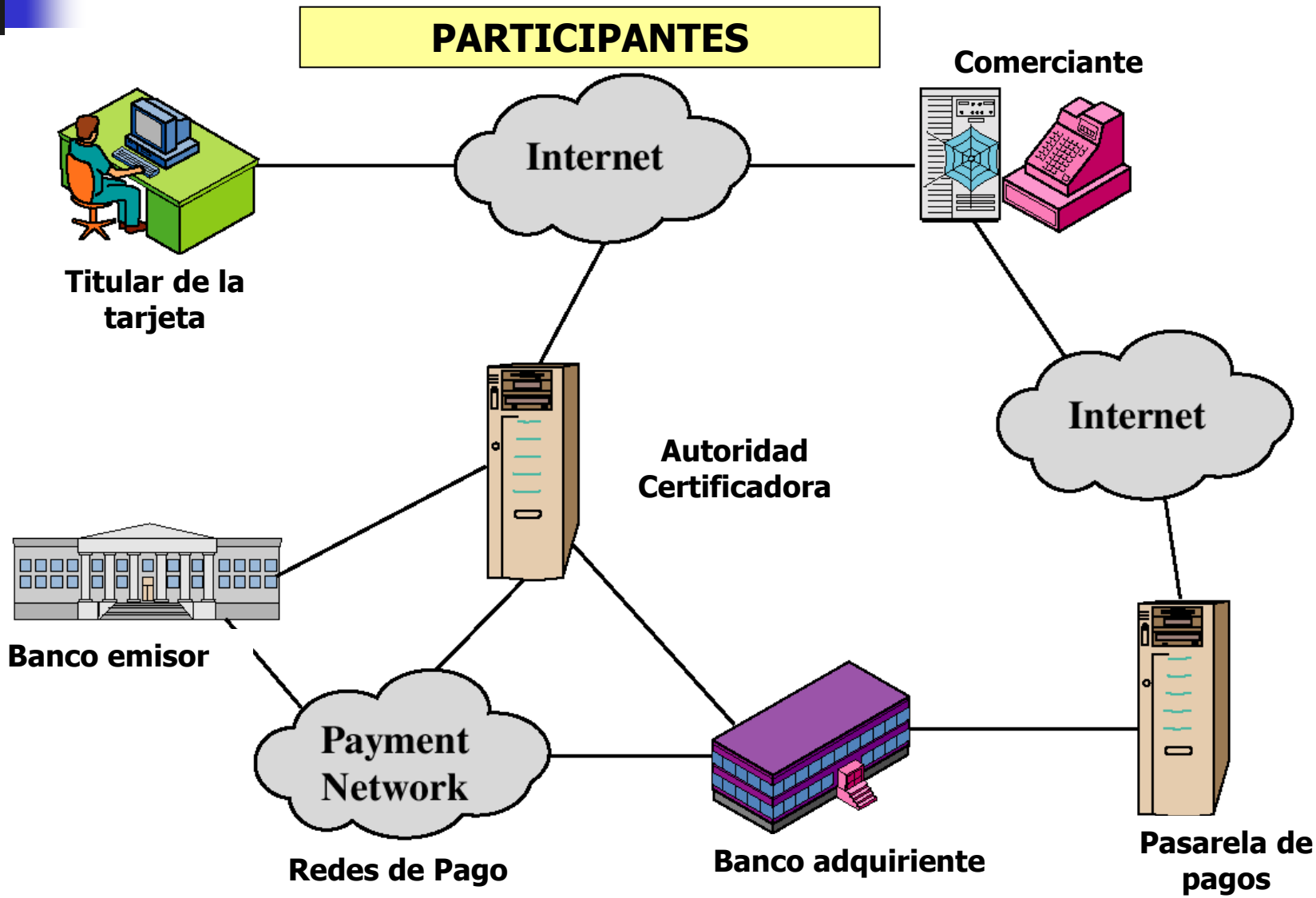
1.3 Secure Socket Layer (SSL)

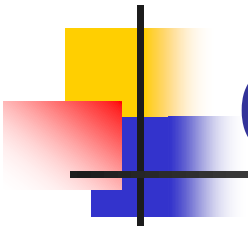
- 1.3.1 Arquitectura
- 1.3.2 Sesiones y conexiones
- 1.3.3 Protocolo Record
- 1.3.4 Protocolo Change Cipher Spec
- 1.3.5 Protocolo Alert
- 1.3.6 Protocolo Handshake
- 1.3.7 Cálculos criptográficos
- 1.3.8 Consideraciones adicionales

1.4 IPSec

- 1.4.1 Protocolos vinculados a IPSec
- 1.4.2 Asociaciones de seguridad
- 1.4.3 Protocolos IPSec
- 1.4.4 Autenticación entre entidades y formación de asociaciones de seguridad

Secure Electronic Transactions





Contenidos

1.1 Introducción ✓

1.2 Secure Electronic Transactions (SET) ✓

- 1.2.1 Participantes ✓
- 1.2.2 Servicios
- 1.2.3 Secuencia de acciones
- 1.2.4 Firma Dual
- 1.2.5 Transacciones permitidas

1.3 Secure Socket Layer (SSL)

- 1.3.1 Arquitectura
- 1.3.2 Sesiones y conexiones
- 1.3.3 Protocolo Record
- 1.3.4 Protocolo Change Cipher Spec
- 1.3.5 Protocolo Alert
- 1.3.6 Protocolo Handshake
- 1.3.7 Cálculos criptográficos
- 1.3.8 Consideraciones adicionales

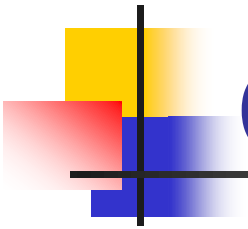
1.4 IPSec

- 1.4.1 Protocolos vinculados a IPSec
- 1.4.2 Asociaciones de seguridad
- 1.4.3 Protocolos IPSec
- 1.4.4 Autenticación entre entidades y formación de asociaciones de seguridad

Secure Electronic Transactions

SERVICIOS

- Autenticación, certificados digitales X.509 v3
- Confidencialidad, información de pago cifrada
- Integridad, uso de firma digital
- Gestión de pago
- Intimidad
- Verificación inmediata



Contenidos

1.1 Introducción ✓

1.2 Secure Electronic Transactions (SET) ✓

- 1.2.1 Participantes ✓
- 1.2.2 Servicios ✓
- 1.2.3 Secuencia de acciones
- 1.2.4 Firma Dual
- 1.2.5 Transacciones permitidas

1.3 Secure Socket Layer (SSL)

- 1.3.1 Arquitectura
- 1.3.2 Sesiones y conexiones
- 1.3.3 Protocolo Record
- 1.3.4 Protocolo Change Cipher Spec
- 1.3.5 Protocolo Alert
- 1.3.6 Protocolo Handshake
- 1.3.7 Cálculos criptográficos
- 1.3.8 Consideraciones adicionales

1.4 IPSec

- 1.4.1 Protocolos vinculados a IPSec
- 1.4.2 Asociaciones de seguridad
- 1.4.3 Protocolos IPSec
- 1.4.4 Autenticación entre entidades y formación de asociaciones de seguridad

Secure Electronic Transactions

SECUENCIA DE ACCIONES CONVENCIONAL

1. Titular presenta tarjeta a comerciante
2. Comerciante para tarjeta por Terminal de Punto de Venta (TPV)
3. Datos de transacción a través de sistema de redes de pago hasta banco emisor
4. Banco emisor comprueba datos y remite aprobación
5. El banco adquiriente recibe información, lo mismo el TPV que emite recibo
6. Comerciante tiene ingresado dinero
7. Al cliente se le descuenta de su cuenta corriente

Secure Electronic Transactions

SECUENCIA DE ACCIONES (I)

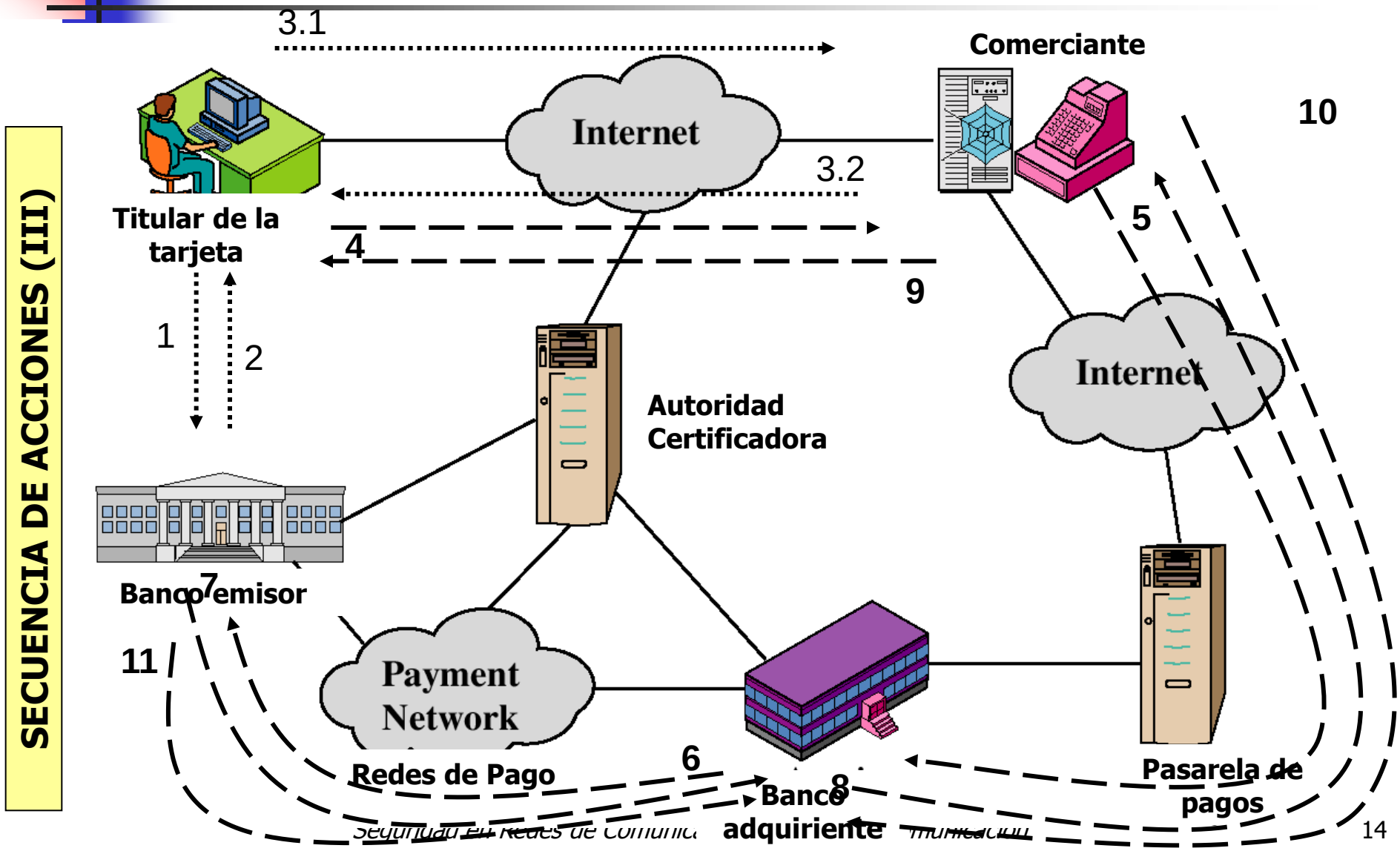
1. Comprador abre una cuenta y obtiene VISA o MasterCard válida para SET
2. Comprador recibe certificado digital X.509 v3 firmado por el banco. Vendedor debe tener dos (firma e intercambio de claves)
3. El cliente decide comprar a través de Internet (recibe identificador de transacción)
4. Cliente comprueba pedido y envía orden de compra, información de pago y certificado -> se inicia SET
5. Comerciante envía petición de pago a su banco

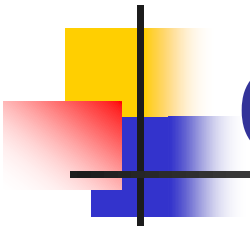
Secure Electronic Transactions

SECUENCIA DE ACCIONES (II)

6. Banco adquiriente valida cliente y comerciante y obtiene autorización de banco emisor.
7. Banco emisor autoriza el pago.
8. Banco adquiriente envía a comerciante testigo de transferencia de fondos.
9. Comerciante envía recibo y mercancía a cliente.
10. Comerciante emplea testigo de transferencia de fondos para cobrar transacción
11. Dinero se descuenta de la cuenta del cliente

Secure Electronic Transactions





Contenidos

1.1 Introducción ✓

1.2 Secure Electronic Transactions (SET) ✓

- 1.2.1 Participantes ✓
- 1.2.2 Servicios ✓
- 1.2.3 Secuencia de acciones ✓
- 1.2.4 Firma Dual
- 1.2.5 Transacciones permitidas

1.3 Secure Socket Layer (SSL)

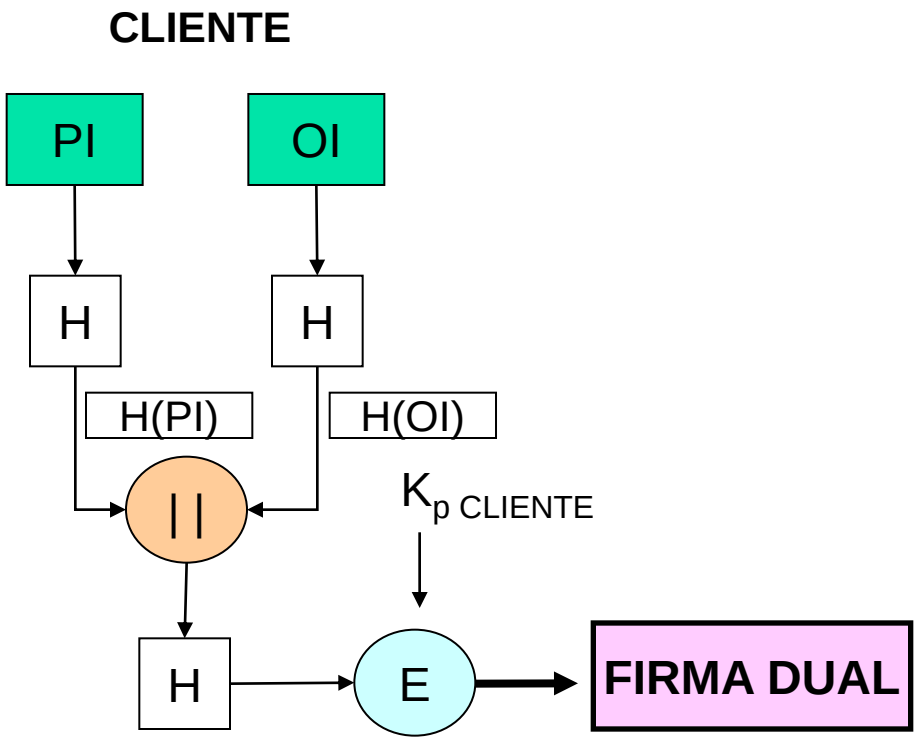
- 1.3.1 Arquitectura
- 1.3.2 Sesiones y conexiones
- 1.3.3 Protocolo Record
- 1.3.4 Protocolo Change Cipher Spec
- 1.3.5 Protocolo Alert
- 1.3.6 Protocolo Handshake
- 1.3.7 Cálculos criptográficos
- 1.3.8 Consideraciones adicionales

1.4 IPSec

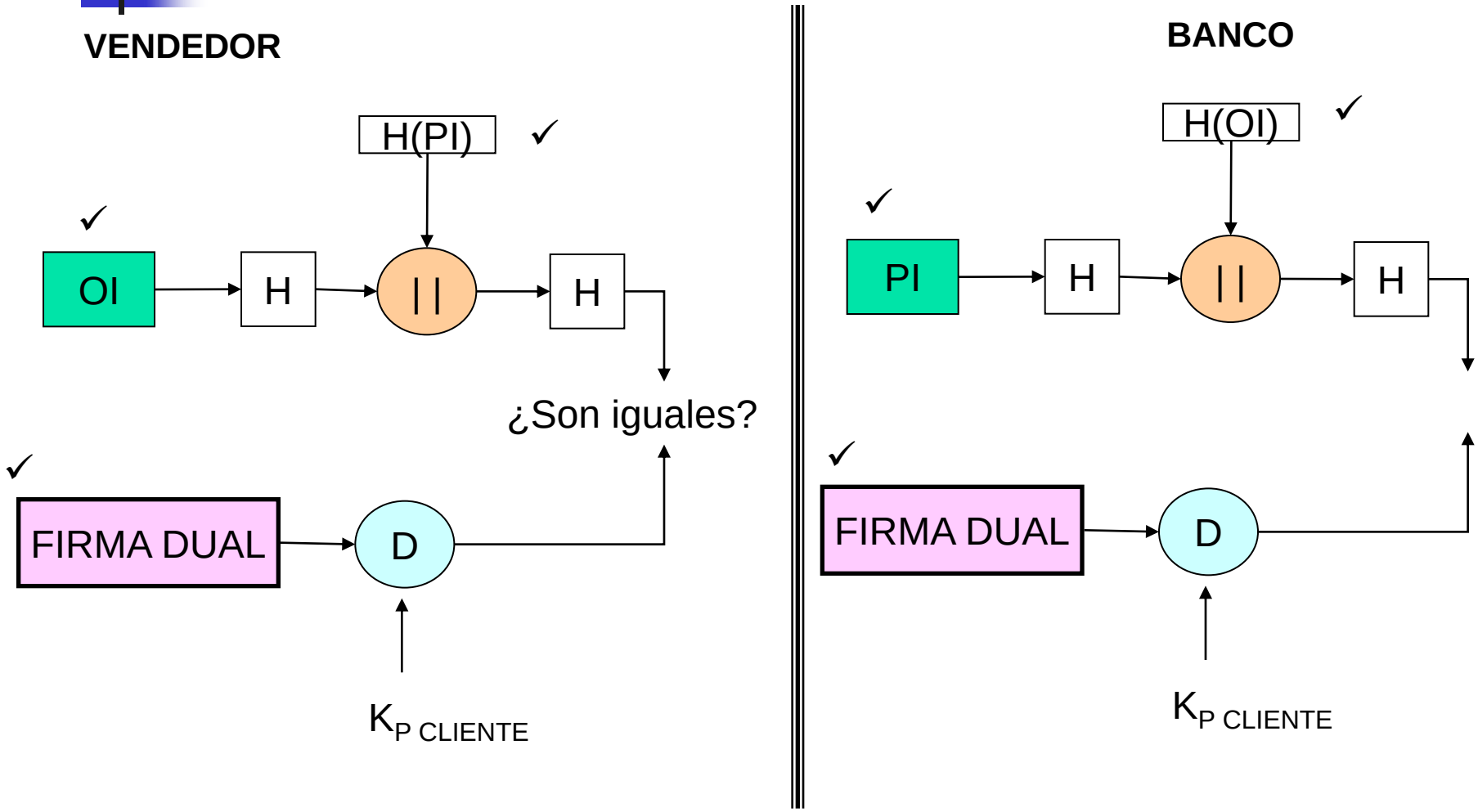
- 1.4.1 Protocolos vinculados a IPSec
- 1.4.2 Asociaciones de seguridad
- 1.4.3 Protocolos IPSec
- 1.4.4 Autenticación entre entidades y formación de asociaciones de seguridad

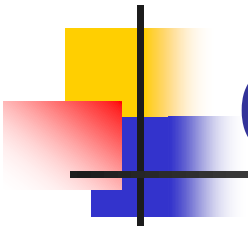
Secure Electronic Transactions

- **Firma Dual**, Orden de compra (OI) e información de pago (PI) en un único mensaje
- Funcionamiento:



Secure Electronic Transactions





Contenidos

1.1 Introducción ✓

1.2 Secure Electronic Transactions (SET) ✓

- 1.2.1 Participantes ✓
- 1.2.2 Servicios ✓
- 1.2.3 Secuencia de acciones ✓
- 1.2.4 Firma Dual ✓
- 1.2.5 Transacciones permitidas

1.3 Secure Socket Layer (SSL)

- 1.3.1 Arquitectura
- 1.3.2 Sesiones y conexiones
- 1.3.3 Protocolo Record
- 1.3.4 Protocolo Change Cipher Spec
- 1.3.5 Protocolo Alert
- 1.3.6 Protocolo Handshake
- 1.3.7 Cálculos criptográficos
- 1.3.8 Consideraciones adicionales

1.4 IPSec

- 1.4.1 Protocolos vinculados a IPSec
- 1.4.2 Asociaciones de seguridad
- 1.4.3 Protocolos IPSec
- 1.4.4 Autenticación entre entidades y formación de asociaciones de seguridad

Secure Electronic Transactions

- Tipos de Transacciones
  - Registro del titular
  - Registro del vendedor
  - **Solicitud de compra**
  - **Autorización de pago**
  - Captura de pago
  - Informe y estado de certificado
  - Informe de compra
  - Deshacer autorización
  - Deshacer captura
  - Crédito
  - Deshacer crédito
  - Solicitud de certificado de pasarela de pago
  - Admimistración por lotes
  - Mensaje de error

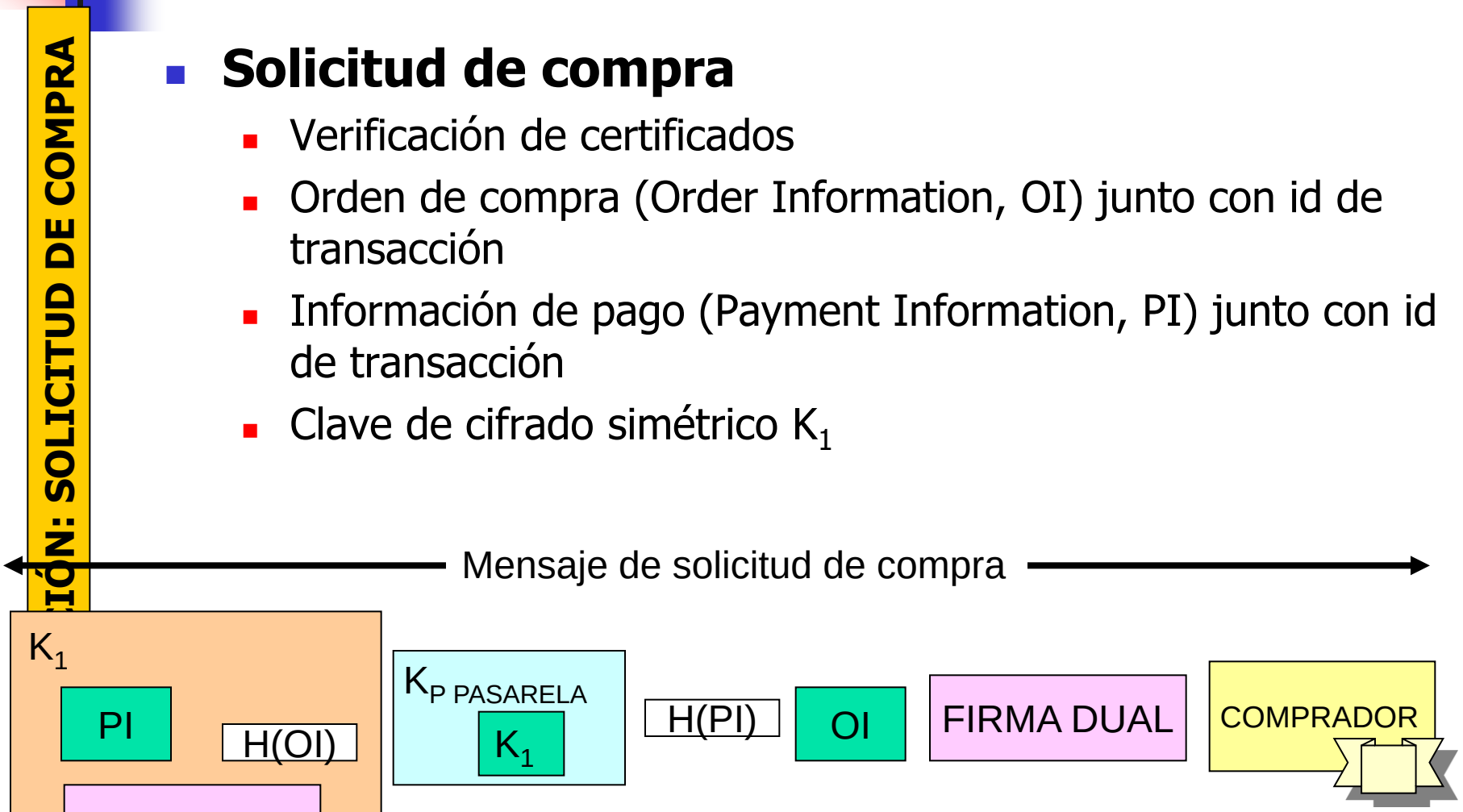
Secure Electronic Transactions

TRANSACCIÓN: SOLICITUD DE COMPRA

- Solicitud de inicio, respuesta de inicio, solicitud de compra y respuesta de compra
- **Solicitud de inicio**
  - Solicita certificados (vendedor y pasarela de pago)
  - Incluye tipo de tarjeta, nº de secuencia y *nonce*
- **Respuesta de inicio**
  - *Nonce* del comprador, *nonce* del próximo mensaje e identificador de transacción
  - Certificado digital de vendedor y de pasarela de pago
  - Mensaje firmado por el vendedor

Secure Electronic Transactions

- **Solicitud de compra**
  - Verificación de certificados
  - Orden de compra (Order Information, OI) junto con id de transacción
  - Información de pago (Payment Information, PI) junto con id de transacción
  - Clave de cifrado simétrico K_1



Secure Electronic Transactions

TRANSACCIÓN: SOLICITUD DE COMPRA

- **Respuesta de compra**
  - Tras verificar certificado comprador y firma dual se procesa pedido y se envía información de pago a la pasarela
  - Incluye reconocimiento de pedido y número de transacción correspondiente
  - Firmado con firma digital de vendedor

Secure Electronic Transactions

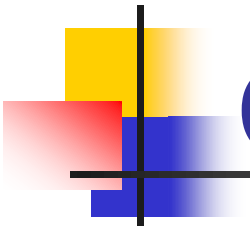
TRANSACCIÓN: AUTORIZACIÓN DE PAGO

- **Autorización de pago**: Solicitud de autorización y respuesta de autorización
- Solicitud de autorización
  - Información relativa a la adquisición (PI, firma dual , H(OI), clave K_1) obtenida del mensaje solicitud de compra
  - Información relativa a la autorización (identificador de la transacción firmado con clave privada de vendedor y cifrado con clave simétrica K_2, y clave K_2 cifrada con clave pública de pasarela de pago)
  - Certificado de comprador y certificado de vendedor

Secure Electronic Transactions

TRANSACCIÓN: AUTORIZACIÓN DE PAGO

- Respuesta de autorización
  - Tras verificar certificados
    - Obtiene K_2 y descifra información relativa a autorización
    - Verifica firma de vendedor
    - Obtiene K_1 y descifra información de adquisición
    - Verifica firma dual
    - Verifica identificador de transacción del vendedor con el recibido del comprador (contenido en PI)
    - Solicita y recibe autorización del banco emisor de tarjeta
  - Contiene información de autorización, información de bono de captura, certificado de pasarela



Contenidos

1.1 Introducción ✓

1.2 Secure Electronic Transactions (SET) ✓

- 1.2.1 Participantes ✓
- 1.2.2 Servicios ✓
- 1.2.3 Secuencia de acciones ✓
- 1.2.4 Firma Dual ✓
- 1.2.5 Transacciones permitidas ✓

1.3 Secure Socket Layer (SSL)

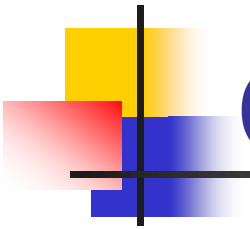
- 1.3.1 Arquitectura
- 1.3.2 Sesiones y conexiones
- 1.3.3 Protocolo Record
- 1.3.4 Protocolo Change Cipher Spec
- 1.3.5 Protocolo Alert
- 1.3.6 Protocolo Handshake
- 1.3.7 Cálculos criptográficos
- 1.3.8 Consideraciones adicionales

1.4 IPSec

- 1.4.1 Protocolos vinculados a IPSec
- 1.4.2 Asociaciones de seguridad
- 1.4.3 Protocolos IPSec
- 1.4.4 Autenticación entre entidades y formación de asociaciones de seguridad

Secure Socket Layer

- SSL ≡ Capa de socket segura (Secure Socket Layer)
  - Confidencialidad, integridad, autenticación y no repudio
  - Aplicaciones cliente/servidor sobre transporte fiable (TCP)
- Netscape creó SSL (1996 v.3)
- El grupo de trabajo TLS se formó dentro de la IETF
  - La primera versión de TLS puede verse como SSLv3.1
- Características:
  - Autenticación servidor SSL
  - Autenticación cliente SSL
  - Sesiones SSL cifradas



Contenidos

1.1 Introducción ✓

1.2 Secure Electronic Transactions (SET) ✓

- 1.2.1 Participantes ✓
- 1.2.2 Servicios ✓
- 1.2.3 Secuencia de acciones ✓
- 1.2.4 Firma Dual ✓
- 1.2.5 Transacciones permitidas ✓

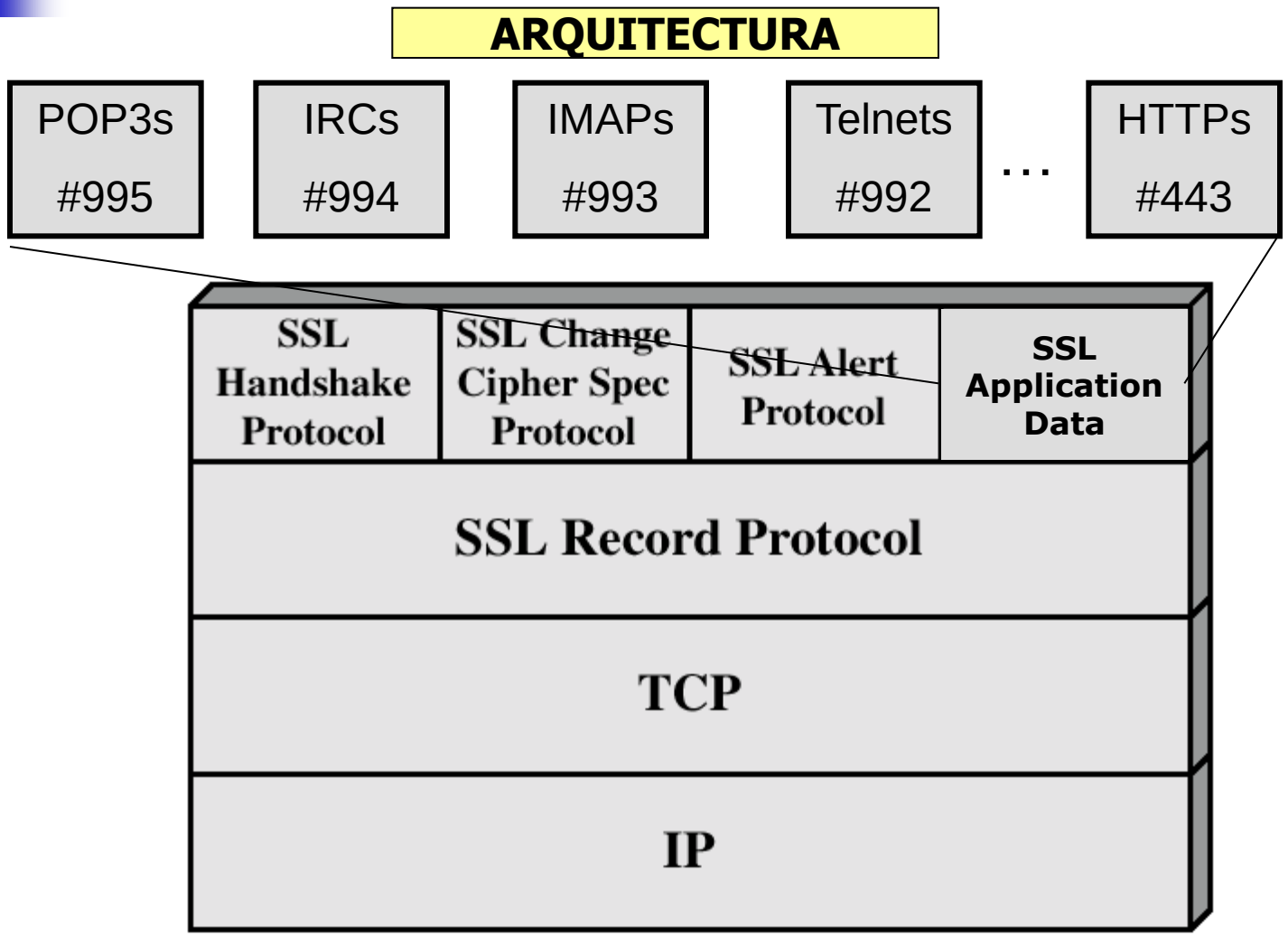
1.3 Secure Socket Layer (SSL) ✓

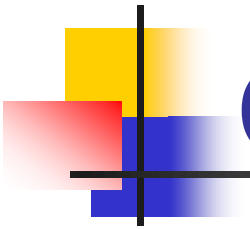
- 1.3.1 Arquitectura
- 1.3.2 Sesiones y conexiones
- 1.3.3 Protocolo Record
- 1.3.4 Protocolo Change Cipher Spec
- 1.3.5 Protocolo Alert
- 1.3.6 Protocolo Handshake
- 1.3.7 Cálculos criptográficos
- 1.3.8 Consideraciones adicionales

1.4 IPSec

- 1.4.1 Protocolos vinculados a IPSec
- 1.4.2 Asociaciones de seguridad
- 1.4.3 Protocolos IPSec
- 1.4.4 Autenticación entre entidades y formación de asociaciones de seguridad

Secure Socket Layer





Contenidos

1.1 Introducción ✓

1.2 Secure Electronic Transactions (SET) ✓

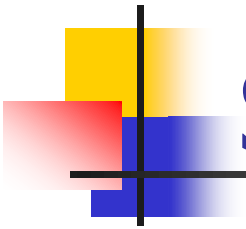
- 1.2.1 Participantes ✓
- 1.2.2 Servicios ✓
- 1.2.3 Secuencia de acciones ✓
- 1.2.4 Firma Dual ✓
- 1.2.5 Transacciones permitidas ✓

1.3 Secure Socket Layer (SSL) ✓

- 1.3.1 Arquitectura ✓
- 1.3.2 Sesiones y conexiones
- 1.3.3 Protocolo Record
- 1.3.4 Protocolo Change Cipher Spec
- 1.3.5 Protocolo Alert
- 1.3.6 Protocolo Handshake
- 1.3.7 Cálculos criptográficos
- 1.3.8 Consideraciones adicionales

1.4 IPSec

- 1.4.1 Protocolos vinculados a IPSec
- 1.4.2 Asociaciones de seguridad
- 1.4.3 Protocolos IPSec
- 1.4.4 Autenticación entre entidades y formación de asociaciones de seguridad

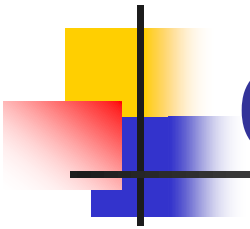


Secure Socket Layer

- **Sesiones**
  - Sesión: asociación entre cliente y servidor
    - Protocolo handshake
  - Parámetros de la fase de sesión
    - Identificador de sesión
    - Certificado de la entidad par
    - Método de compresión
    - Especificación de cifrado
    - Clave maestra
    - Es reanudable

Secure Socket Layer

- **Conexiones**
  - Conexión: servicio de transporte
    - Cada conexión asociada a una sesión
  - Parámetros del estado de la conexión
    - Valores aleatorios del servidor y del cliente
    - Clave secreta MAC de escritura del servidor
    - Clave secreta MAC de escritura del cliente
    - Clave de escritura de servidor
    - Clave de escritura de cliente
    - Vector inicialización (IV) de cliente y servidor
    - Número de secuencia



Contenidos

1.1 Introducción ✓

1.2 Secure Electronic Transactions (SET) ✓

- 1.2.1 Participantes ✓
- 1.2.2 Servicios ✓
- 1.2.3 Secuencia de acciones ✓
- 1.2.4 Firma Dual ✓
- 1.2.5 Transacciones permitidas ✓

1.3 Secure Socket Layer (SSL) ✓

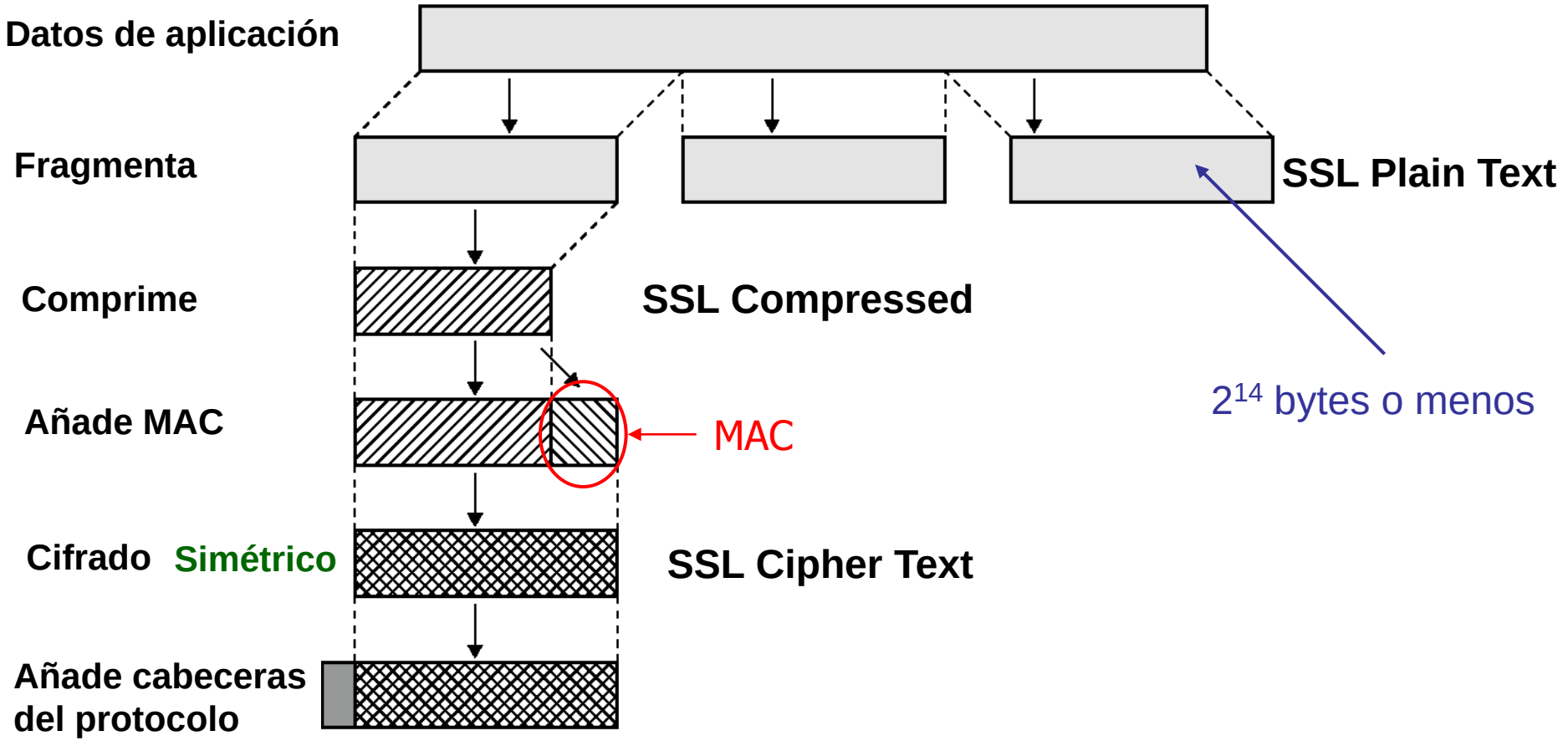
- 1.3.1 Arquitectura ✓
- 1.3.2 Sesiones y conexiones ✓
- 1.3.3 Protocolo Record
- 1.3.4 Protocolo Change Cipher Spec
- 1.3.5 Protocolo Alert
- 1.3.6 Protocolo Handshake
- 1.3.7 Cálculos criptográficos
- 1.3.8 Consideraciones adicionales

1.4 IPSec

- 1.4.1 Protocolos vinculados a IPSec
- 1.4.2 Asociaciones de seguridad
- 1.4.3 Protocolos IPSec
- 1.4.4 Autenticación entre entidades y formación de asociaciones de seguridad

Secure Socket Layer

- **Protocolo Record**: Confidencialidad e integridad

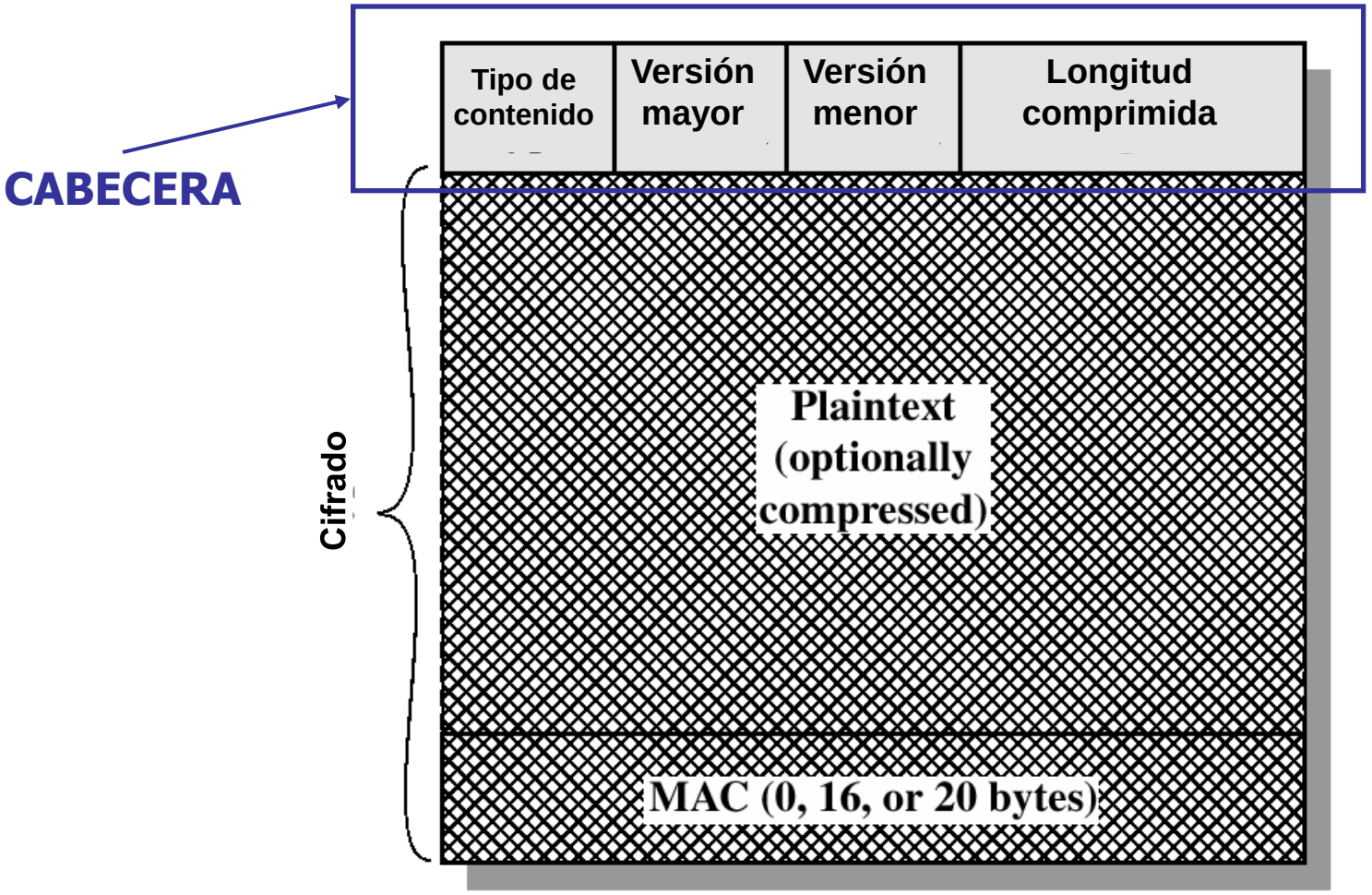


Secure Socket Layer

- MAC
  - Usa clave compartida
  - **Hash (** clave_MAC || opad || **hash (** clave_MAC || ipad || seq_num || SSLCompressed.type || SSLCompressed.length || SSLCompressed.fragment**))**
  - MD5 o SHA1
- Algoritmos de cifrado

Cifrado Bloque		**Cifrado Flujo**	
Algoritmo	**Tamaño K**	**Algoritmo**	**Tamaño K**
IDEA	128	RC4-40	40
DES	56	RC4-128	128
3DES	112		
RSA	1024		
DSA	1024		
FORTEZZA	80		

Secure Socket Layer



Contenidos

1.1 Introducción ✓

1.2 Secure Electronic Transactions (SET) ✓

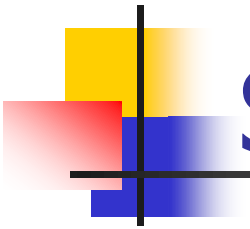
- 1.2.1 Participantes ✓
- 1.2.2 Servicios ✓
- 1.2.3 Secuencia de acciones ✓
- 1.2.4 Firma Dual ✓
- 1.2.5 Transacciones permitidas ✓

1.3 Secure Socket Layer (SSL) ✓

- 1.3.1 Arquitectura ✓
- 1.3.2 Sesiones y conexiones ✓
- 1.3.3 Protocolo Record ✓
- 1.3.4 Protocolo Change Cipher Spec
- 1.3.5 Protocolo Alert
- 1.3.6 Protocolo Handshake
- 1.3.7 Cálculos criptográficos
- 1.3.8 Consideraciones adicionales

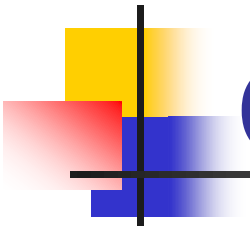
1.4 IPSec

- 1.4.1 Protocolos vinculados a IPSec
- 1.4.2 Asociaciones de seguridad
- 1.4.3 Protocolos IPSec
- 1.4.4 Autenticación entre entidades y formación de asociaciones de seguridad



Secure Socket Layer

- **Protocolo Change Cipher Spec**
  - Un único mensaje de contenido un byte de valor 1
  - Objetivo: pasar de modo pendiente a modo operativo



Contenidos

1.1 Introducción ✓

1.2 Secure Electronic Transactions (SET) ✓

- 1.2.1 Participantes ✓
- 1.2.2 Servicios ✓
- 1.2.3 Secuencia de acciones ✓
- 1.2.4 Firma Dual ✓
- 1.2.5 Transacciones permitidas ✓

1.3 Secure Socket Layer (SSL) ✓

- 1.3.1 Arquitectura ✓
- 1.3.2 Sesiones y conexiones ✓
- 1.3.3 Protocolo Record ✓
- 1.3.4 Protocolo Change Cipher Spec ✓
- 1.3.5 Protocolo Alert
- 1.3.6 Protocolo Handshake
- 1.3.7 Cálculos criptográficos
- 1.3.8 Consideraciones adicionales

1.4 IPSec

- 1.4.1 Protocolos vinculados a IPSec
- 1.4.2 Asociaciones de seguridad
- 1.4.3 Protocolos IPSec
- 1.4.4 Autenticación entre entidades y formación de asociaciones de seguridad

Secure Socket Layer

- **Protocolo Alert**
  - Objetivo: Transmitir alertas
  - Mensaje consta de dos bytes

NIVEL (1 byte)	ALERTA (1 byte)

    - NIVEL: (1) Aviso ó (2) Fatal
    - ALERTA
      - Fatal => Mensaje inesperado, MAC de registro erróneo, fallo de descompresión, fallo de negociación, parámetro ilegal
      - Aviso => Notificación de cierre, no certificado, certificado erróneo, certificado no permitido, certificado revocado, certificado caducado, certificado desconocido

Contenidos

1.1 Introducción ✓

1.2 Secure Electronic Transactions (SET) ✓

- 1.2.1 Participantes ✓
- 1.2.2 Servicios ✓
- 1.2.3 Secuencia de acciones ✓
- 1.2.4 Firma Dual ✓
- 1.2.5 Transacciones permitidas ✓

1.3 Secure Socket Layer (SSL) ✓

- 1.3.1 Arquitectura ✓
- 1.3.2 Sesiones y conexiones ✓
- 1.3.3 Protocolo Record ✓
- 1.3.4 Protocolo Change Cipher Spec ✓
- 1.3.5 Protocolo Alert ✓
- 1.3.6 Protocolo Handshake
- 1.3.7 Cálculos criptográficos
- 1.3.8 Consideraciones adicionales

1.4 IPSec

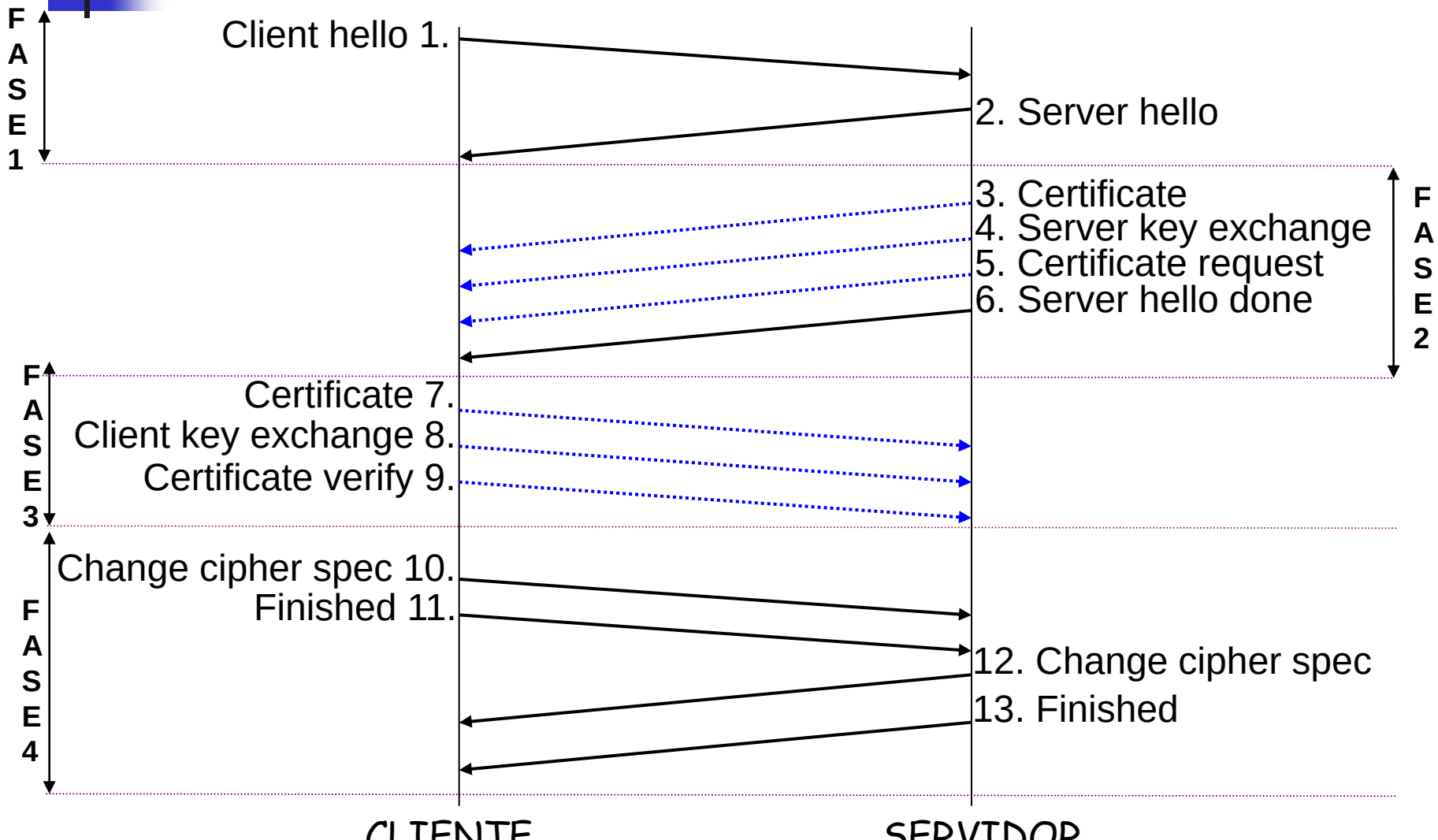
- 1.4.1 Protocolos vinculados a IPSec
- 1.4.2 Asociaciones de seguridad
- 1.4.3 Protocolos IPSec
- 1.4.4 Autenticación entre entidades y formación de asociaciones de seguridad

Secure Socket Layer

- **Protocolo Handshake**
  - Objetivo:
    - Cliente y servidor deben llegar a acuerdo sobre versión de SSL y método de compresión
    - Acuerdo sobre especificaciones de cifrado y creación de claves de cifrado
    - Permite autenticación de cliente y servidor
  - Una sesión SSL siempre comienza con el handshake
  - Mensajes handshake

TIPO (1 byte)	LONGITUD (3 bytes)	CONTENIDO (≥ 1 byte)

Secure Socket Layer

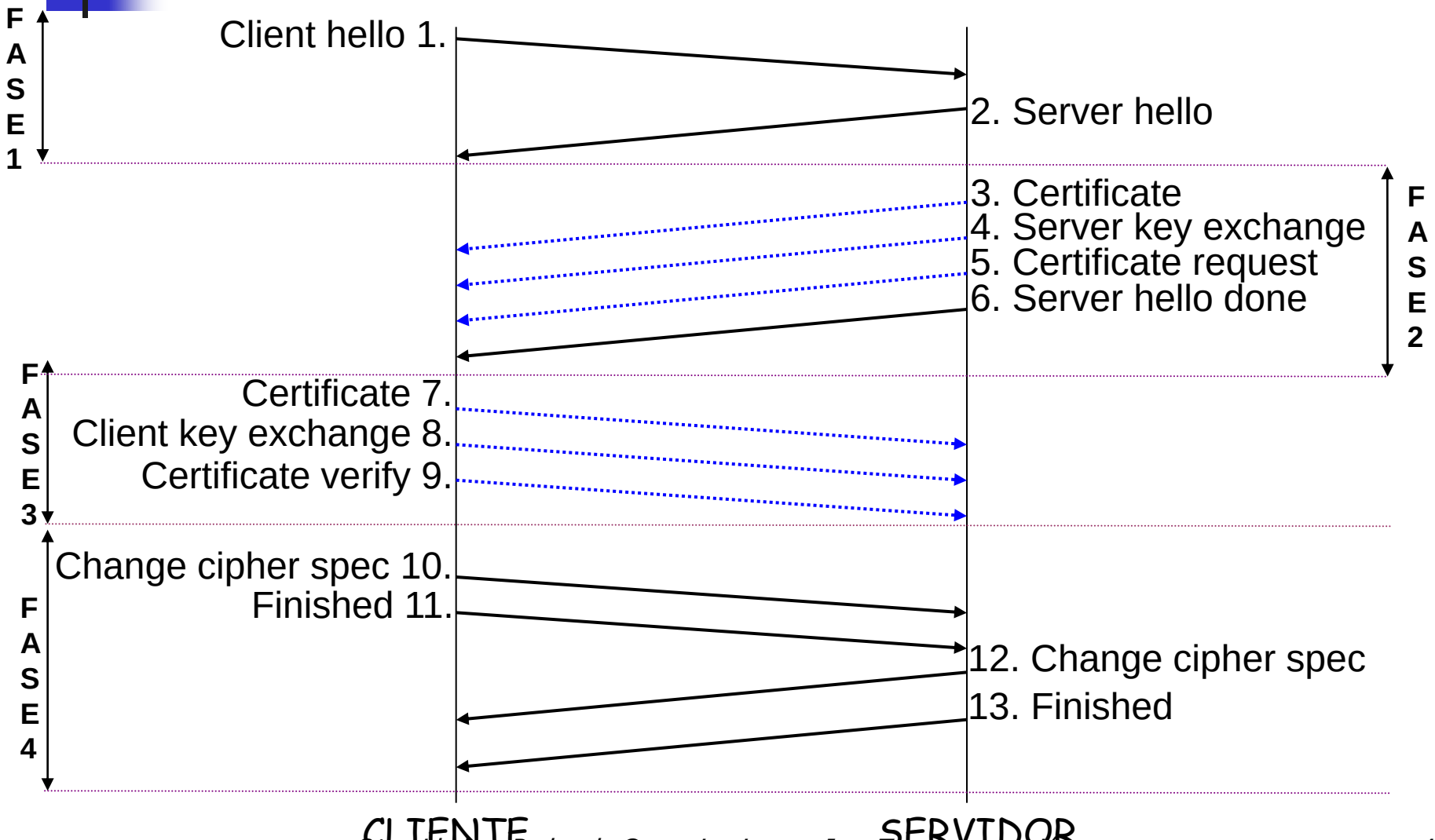


Secure Socket Layer

Fase 1 – Establecimiento de las capacidades de seguridad (versión de protocolo, ID de sesión, suite de cifrado, método de compresión y nº aleatorios iniciales).

- *Client hello*
  - Version, número de versión más alta de SSL que soporta
  - Valor aleatorio
  - Id de sesión, si es ≠ 0 actualizar los parámetros de conexión existente ó crear nueva conexión dentro de esta sesión, si es = 0 indica nueva conexión en nueva sesión
  - Suite de cifrado, lista suites de cifrado que soporta
    - Algoritmo intercambio de claves
    - Especificaciones de cifrado: algoritmo de cifrado, tipo de cifrado, es exportable, tamaño hash, material de clave, tamaño vector inicialización
  - Método de compresión

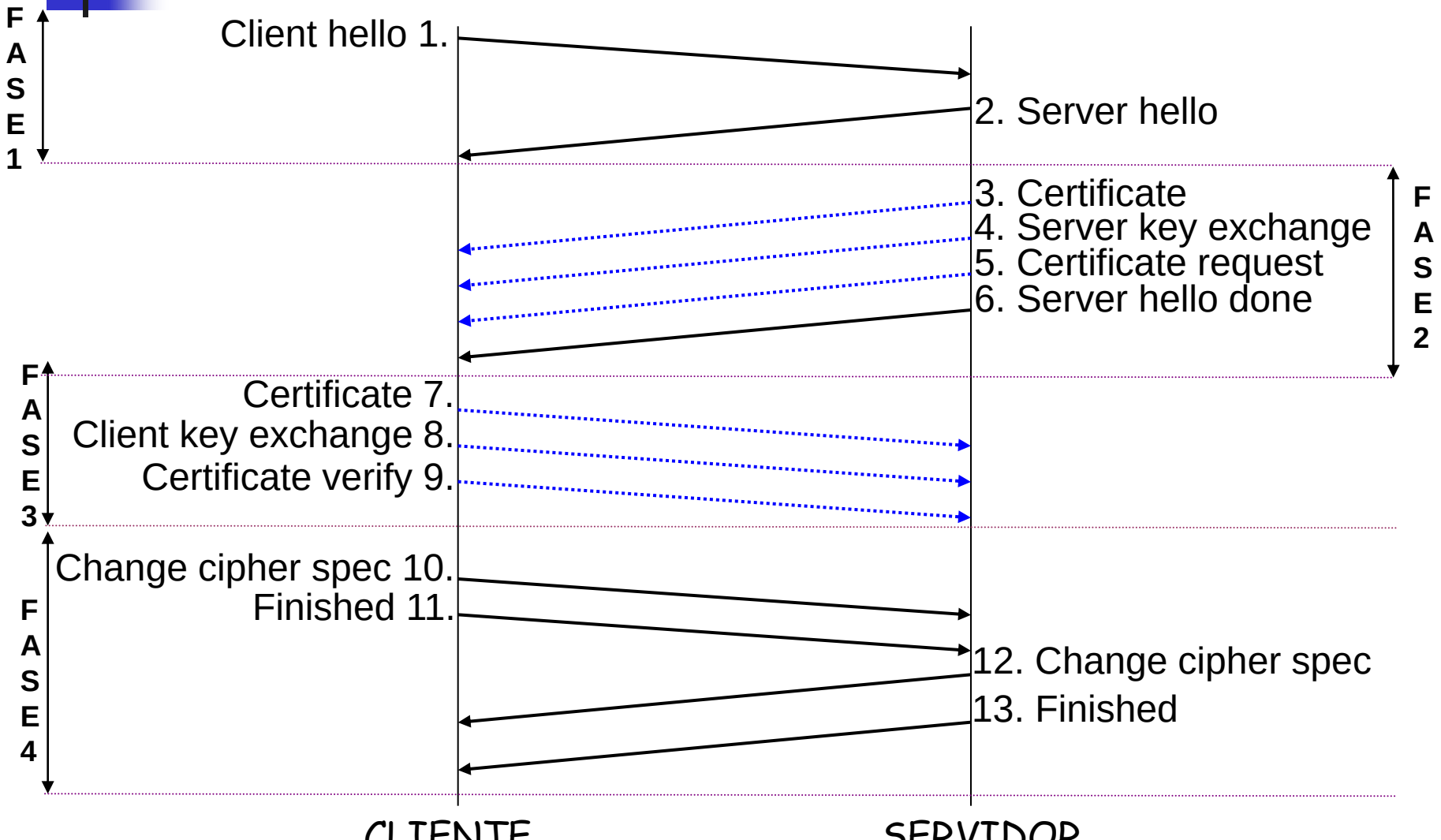
Secure Socket Layer



Secure Socket Layer

- *Server hello*
  - Versión
  - Valor aleatorio
  - Id de sesión
    - Si id sesión de cliente = 0 => id sesión servidor contiene valor distinto indicando que se ha creado nueva sesión
    - Si id sesión cliente ≠ 0 => servidor comprueba en su caché si guarda información sobre esa conexión, si es así y se puede crear nueva conexión responde mismo id sesión cliente
  - Suite de cifrado, escogida de entre las propuestas por cliente
  - Método de compresión, escogido entre los propuestos por cliente

Secure Socket Layer

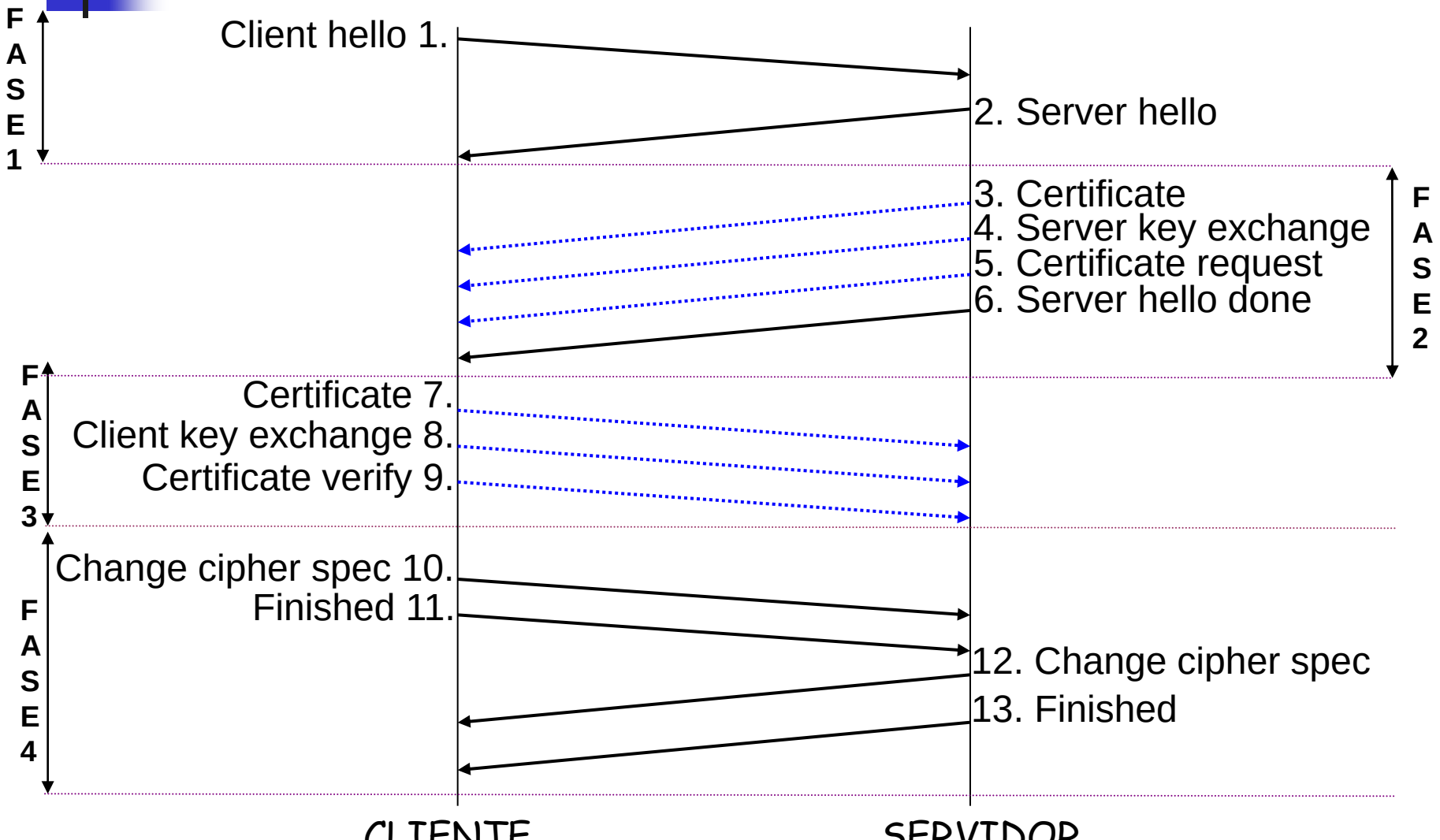


Secure Socket Layer

Fase 2 – El servidor puede enviar un certificado, intercambio de clave y solicitud de certificado. El servidor señala el final de la fase del mensaje hello.

- *Certificate*, servidor envía su certificado X.509 v.3
- *Server key exchange*,
  - No es necesario si (1) servidor ha enviado certificado con parámetros Diffie-Hellman o (2) se usa RSA para intercambio de claves
- *Certificate request*, solicita certificado a cliente
- *Server hello done*, indica final de la fase 2, no contiene parámetros. Servidor espera respuesta de cliente.

Secure Socket Layer

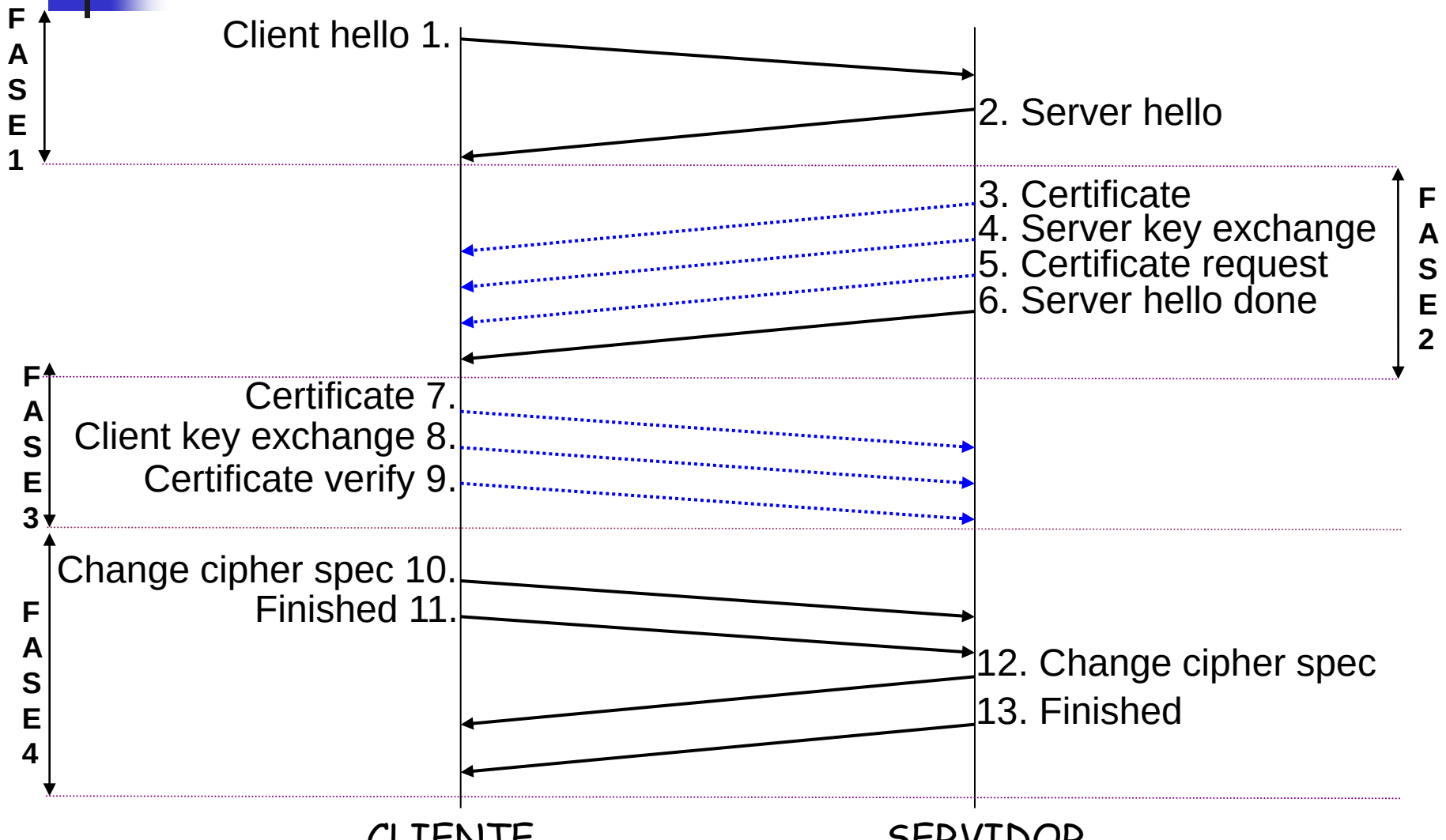


Secure Socket Layer

Fase 3 – El cliente envía certificado si se le solicita, el intercambio de clave, y puede que envíe verificación de certificado.

- Cliente verifica certificado de servidor
- Comprobar que parámetros de fase 1 son aceptables
  - *Certificate*, cliente envía su certificado (si no posee alerta de *no certificado*)
  - *Client key exchange*, depende de tipo de intercambio de clave
    - RSA, envía 48 bytes previos de clave maestra cifrados con clave pública de servidor
    - Diffie-Hellman, parámetros Diffie-Hellman públicos del cliente (si ya en certificado contenido nulo)
  - *Certificate verify*, verifica que cliente posee clave privada en concordancia con certificado de cliente

Secure Socket Layer



Secure Socket Layer

Fase 4 – Intercambio de suite de cifrado y finalización del protocolo handshake.

- Se completa el establecimiento de conexión segura.
  - *Change cipher spec*, se pasa de modo pendiente a operativo (protocolo Change Cipher Spec)
  - *Finished*, cliente y servidor lo envían usando nuevos algoritmos y claves

Contenidos

1.1 Introducción ✓

1.2 Secure Electronic Transactions (SET) ✓

- 1.2.1 Participantes ✓
- 1.2.2 Servicios ✓
- 1.2.3 Secuencia de acciones ✓
- 1.2.4 Firma Dual ✓
- 1.2.5 Transacciones permitidas ✓

1.3 Secure Socket Layer (SSL) ✓

- 1.3.1 Arquitectura ✓
- 1.3.2 Sesiones y conexiones ✓
- 1.3.3 Protocolo Record ✓
- 1.3.4 Protocolo Change Cipher Spec ✓
- 1.3.5 Protocolo Alert ✓
- 1.3.6 Protocolo Handshake ✓
- 1.3.7 Cálculos criptográficos
- 1.3.8 Consideraciones adicionales

1.4 IPSec

- 1.4.1 Protocolos vinculados a IPSec
- 1.4.2 Asociaciones de seguridad
- 1.4.3 Protocolos IPSec
- 1.4.4 Autenticación entre entidades y formación de asociaciones de seguridad

Secure Socket Layer

- **Clave maestra**: valor de un sólo uso (una sesión) de 48 bytes
- Dos pasos
  - Intercambio de valor previo K_{previo}
    - RSA o Diffie-Hellman
  - Cálculo de la clave maestra

$$\mathbf{K_{maestra}} = \mathbf{MD5}\,(\, K_{previo} \,||\, \mathbf{SHA}\,(\, \text{'A'} \,||\, K_{previo} \,||\, \text{clienthello.random} \,||\, \text{serverhello.random}\,)\,) \,||$$
$$\mathbf{MD5}\,(\, K_{previo} \,||\, \mathbf{SHA}\,(\, \text{'BB'} \,||\, K_{previo} \,||\, \text{clienthello.random} \,||\, \text{serverhello.random}\,)\,) \,||$$
$$\mathbf{MD5}\,(\, K_{previo} \,||\, \mathbf{SHA}\,(\, \text{'CCC'} \,||\, K_{previo} \,||\, \text{clienthello.random} \,||\, \text{serverhello.random}\,)\,)$$

Secure Socket Layer

- SSL requiere para cada conexión:
  - clave secreta MAC de escritura del servidor
  - clave secreta MAC de escritura del cliente
  - clave de escritura de servidor
  - clave de escritura de cliente
  - vector inicialización (IV) de cliente y servidor
- Se crean en ese orden a partir de $K_{maestra}$

$$K_{block}=MD5(K_{maestra}||SHA(\text{'A'}||\ K_{maestra} ||clienthello.random||serverhello.random)) ||$$
$$MD5(K_{maestra}\ ||SHA(\text{'BB'}||\ K_{maestra} ||clienthello.random||serverhello.random)) ||$$
$$MD5(K_{maestra}\ ||SHA(\text{'CCC'}||\ K_{maestra} ||clienthello.random||serverhello.random)) \ldots\ldots$$

Contenidos

1.1 Introducción ✓

1.2 Secure Electronic Transactions (SET) ✓

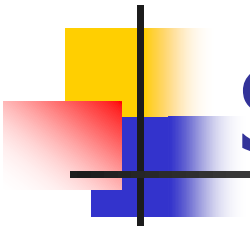
- 1.2.1 Participantes ✓
- 1.2.2 Servicios ✓
- 1.2.3 Secuencia de acciones ✓
- 1.2.4 Firma Dual ✓
- 1.2.5 Transacciones permitidas ✓

1.3 Secure Socket Layer (SSL) ✓

- 1.3.1 Arquitectura ✓
- 1.3.2 Sesiones y conexiones ✓
- 1.3.3 Protocolo Record ✓
- 1.3.4 Protocolo Change Cipher Spec ✓
- 1.3.5 Protocolo Alert ✓
- 1.3.6 Protocolo Handshake ✓
- 1.3.7 Cálculos criptográficos ✓
- 1.3.8 Consideraciones adicionales

1.4 IPSec

- 1.4.1 Protocolos vinculados a IPSec
- 1.4.2 Asociaciones de seguridad
- 1.4.3 Protocolos IPSec
- 1.4.4 Autenticación entre entidades y formación de asociaciones de seguridad



Secure Socket Layer

- Independencia de la aplicación y dependencia del transporte
- Leyes de exportación
- Estandarización
  - **Transport Layer Security**

Transport Layer Security

- 1996, IETF RFC 2246 (SSL con algunas variantes)
  - Formato
    - En TLS versión mayor es 3 y menor 1
  - Código de autenticación de mensaje
    - Algoritmo para calcular código de autenticación es HMAC
    - El HMAC se calcula sobre diferentes campos

Transport Layer Security

- Algoritmo de HMAC

EN SSL v3

Hash (**clave_MAC || opad** || hash (**clave_MAC || ipad** || seq_num || SSLCompressed.type || SSLCompressed.length || SSLCompressed.fragment))

EN TLS

$HMAC_K = H[(K^+ \oplus opad) || H[(K^+ \oplus ipad) || X]]$

H≡ función hash MD5 o SHA1

X ≡ Texto plano

K^+≡ clave secreta con relleno de ceros a la izquierda hasta que iguale longitud del bloque de entrada de funciones hash

ipad ≡ 00110110 repetido

opad ≡01011100 repetido

Transport Layer Security

- Campos sobre los que calcular el HMAC

EN SSL v3

Hash (clave_MAC || opad || hash (clave_MAC || ipad || seq_num || SSLCompressed.type || SSLCompressed.length || SSLCompressed.fragment))

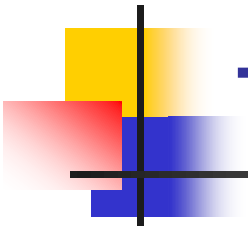
EN TLS

HMAC (clave_MAC, seq_num || TLSCompressed.type || **TLSCompressed.version** || TLSCompressed.length || SSLCompressed.fragment))

Versión de protocolo que se está usando

Transport Layer Security

- **Códigos de Alerta**:
  - Todos las de SSL v.3 excepto alerta de *no-certificate*
  - Alertas adicionales:
    - Fallo de descifrado (*decryption-failed*)
    - Autoridad de certificación desconocida (unknown-ca)
    - Seguridad insuficiente (insufficient_security)



Transport Layer Security

Otras diferencias:

- Suite de cifrado: Todas las técnicas de intercambio de clave y cifrado simétrico disponibles en SSL v.3 a excepción de Fortezza.
- Certificados: no incluye Fortezza
- Relleno:
  - En SSL relleno mínimo para que el tamaño total de los datos que se van a cifrar sea múltiplo de la longitud del bloque cifrado (DES -> 512 bits)
  - Con TLS puede ser cualquiera (máx 255 bytes = 2040 bits)

Transport Layer Security

- TLS emplea la función PRF (Pseudo Random Function) para expansión de clave maestra

PRF (secret, label, seed) = P_MD5 (S1, label || seed) ⊕ P_SHA-1 (S2, label || seed)

P_hash = HMAC_hash (secret, A(1) || seed) || HMAC_hash (secret, A(2) || seed) || HMAC_hash (secret, A(1) || seed) || …

A(n):

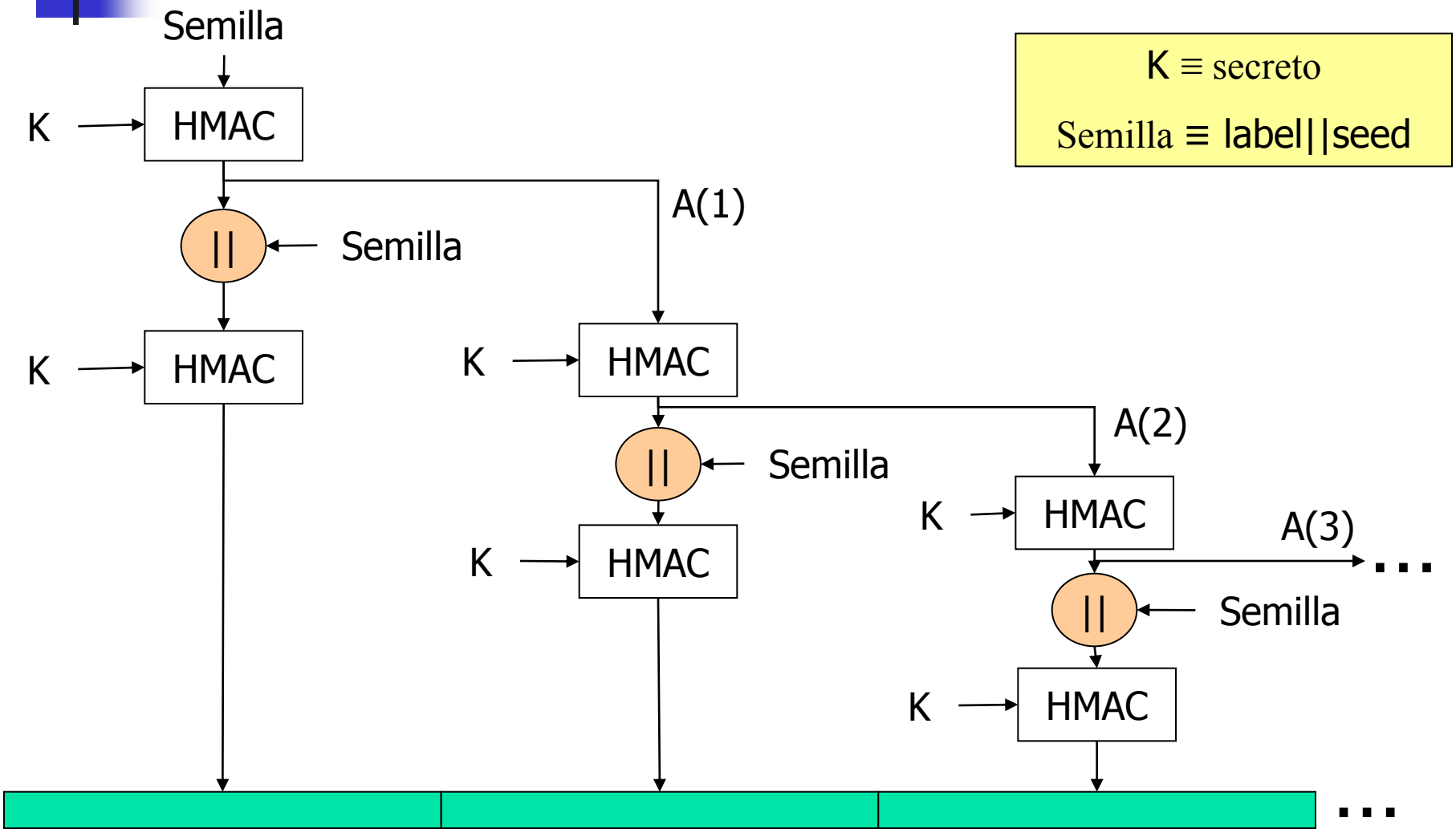
A(0) = seed

A(1) = HMAC_hash (secret, A(0))

…

A(i) = HMAC_hash (secret, A(i-1))

Transport Layer Security



FUNCIÓN P_HASH

Transport Layer Security

Creación de clave maestra

- Pre_master_secret K_{previa} igual que en SSL v.3
- Clave maestra $K_{maestra}$ 48 bytes:

$K_{maestra}$= PRF (K_{previa}, "master secret", clienteHello.random || servidorHello.random)

K_{block}= PRF ($K_{maestra}$, "key expansion", SecurityParameters.server_random || SecurityParameters.client_random)

Contenidos

1.1 Introducción ✓

1.2 Secure Electronic Transactions (SET) ✓

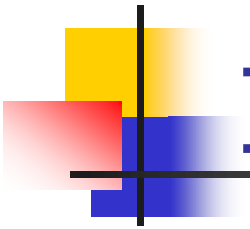
- 1.2.1 Participantes ✓
- 1.2.2 Servicios ✓
- 1.2.3 Secuencia de acciones ✓
- 1.2.4 Firma Dual ✓
- 1.2.5 Transacciones permitidas ✓

1.3 Secure Socket Layer (SSL) ✓

- 1.3.1 Arquitectura ✓
- 1.3.2 Sesiones y conexiones ✓
- 1.3.3 Protocolo Record ✓
- 1.3.4 Protocolo Change Cipher Spec ✓
- 1.3.5 Protocolo Alert ✓
- 1.3.6 Protocolo Handshake ✓
- 1.3.7 Cálculos criptográficos ✓
- 1.3.8 Consideraciones adicionales ✓

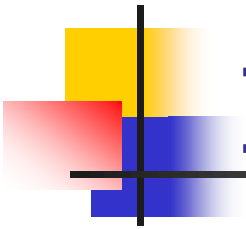
1.4 IPSec

- 1.4.1 Protocolos vinculados a IPSec
- 1.4.2 Asociaciones de seguridad
- 1.4.3 Protocolos IPSec
- 1.4.4 Autenticación entre entidades y formación de asociaciones de seguridad



IPSec

- IPSec (IP Security Protocol) es un conjunto de estándares abiertos que trabajan de forma conjunta para garantizar entre entidades pares en el nivel de red:
  - Confidencialidad
  - Integridad
  - Autenticación



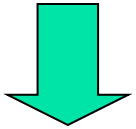
IPSec

- Protocolos IPSec:
  - **Authentication Header (AH)**
  - **Encapsulation Security Payload (ESP)**
  - Cifrado: DES, 3DES, AES, …
  - Funciones resumen: HMAC, MD5 ó SHA1
  - Firma digital: RSA o secreto compartido
  - Intercambio de claves: mediante CA (certificados) o Diffie-Hellman
  - Negociación de asociaciones de seguridad:
    - IKE (Internet Key Exchange)
    - ISAKMP (Internet Security Association and Key Management Protocol)

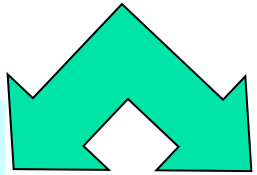
IPSec

ASOCIACIONES

- Entidades deciden qué servicios de seguridad necesitan
- Comienza proceso de negociación entre entidades
  - Conjunto de algoritmos comunes de autenticación, cifrado y/o funciones resumen + periodo de validez



ASOCIACIÓN DE SEGURIDAD
(SA, Security Association)



Protocolo IKE (ISAKMP)

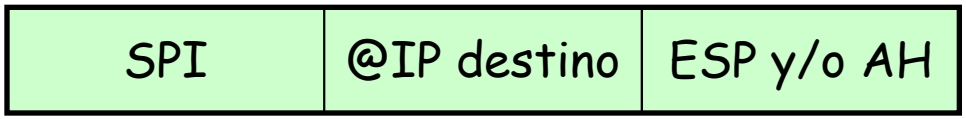
Entidades que quieren establecer una conexión

Protocolo IPSec

Usadas con cada paquete seguro

IPSec

- Asociaciones
  - Simplex
  - Asociaciones IPSec dependen del tipo de protocolo
  - Security Parameter Index (SPI)



Identificación única de la asociación de seguridad

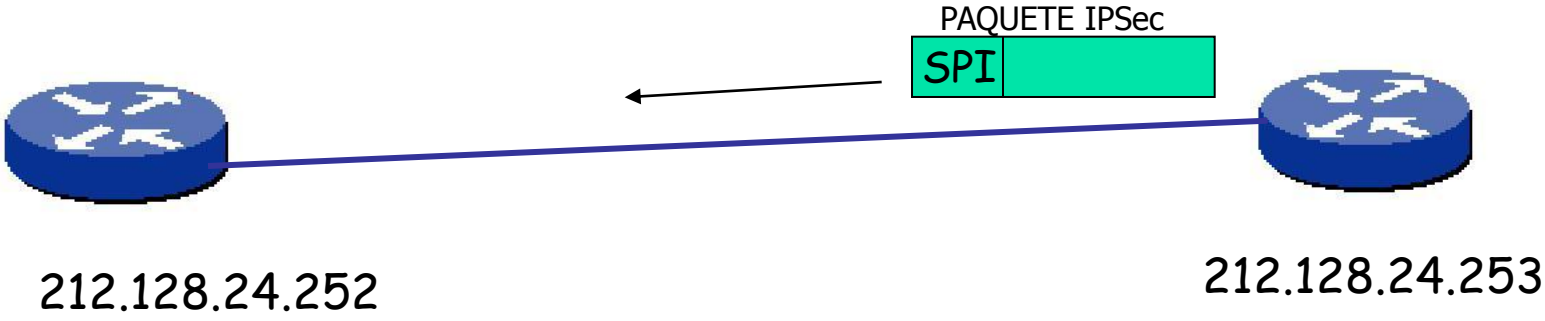
  - Security Association Database

IPSec

1. SPI+@IPdestino +protocolo IPSec
2. Consulta SAD

1. ¿SA? -> SPI
2. SPI

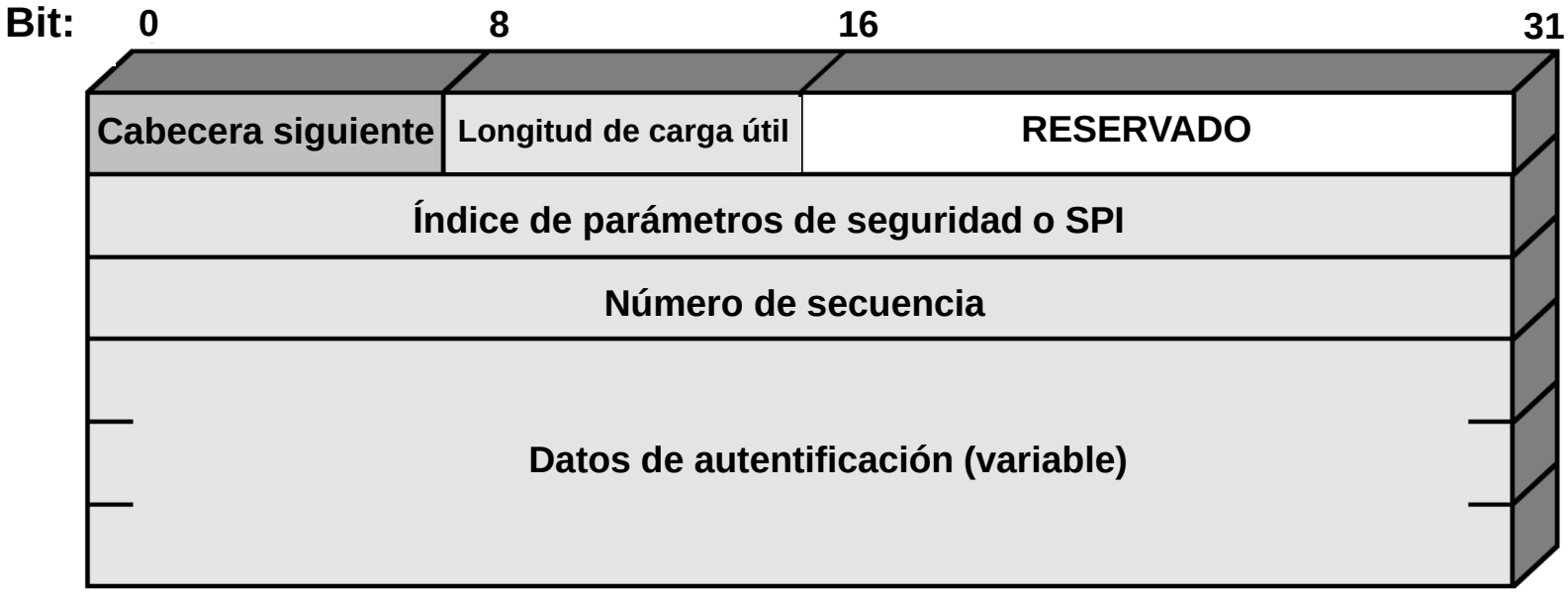
PAQUETE IPSec



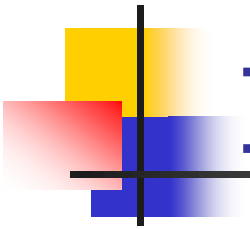
IPSec

- **Protocolo AH** (RFC 2402)
  - Integridad de datos
  - Autenticación del origen de datos
  - Servicio contra reenvío de paquetes (opcional)
- Tráfico de Interés ≡ cabecera añadida por AH

IPSec



- Next header (6 -> TCP, 17 -> UDP)
- Payload Length, longitud de cabecera en palabras de 32 bits (-2)
- Reserved
- Security Parameters Index (SPI)
- Sequence Number Field, evitar ataques de reenvío de paquetes
- Authentication Data, contiene valor de comprobación de integridad (ICV, Integrity Check Value) (múltiplo de 32 bits siempre -> relleno)

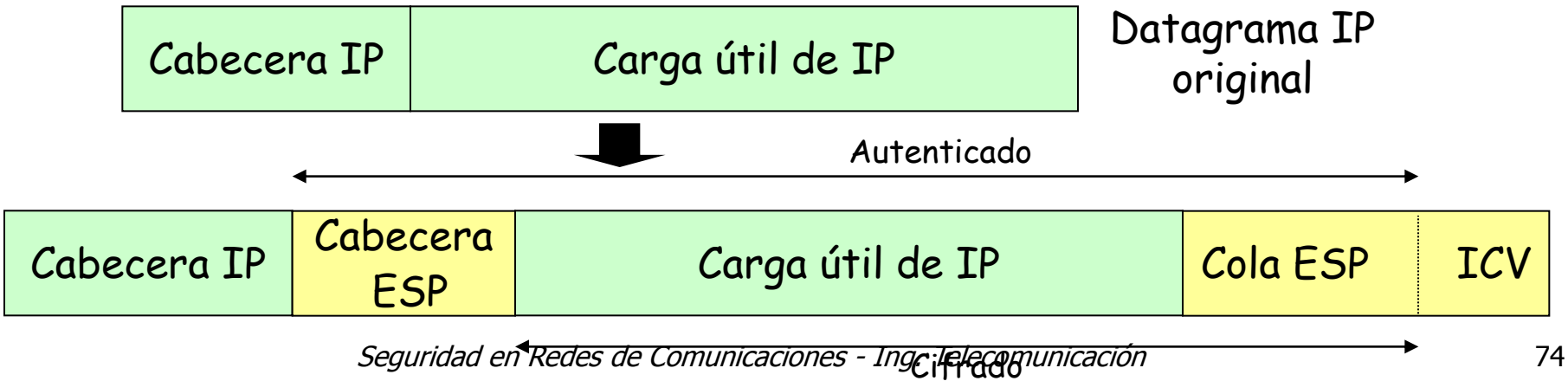


IPSec

- ICV se calcula usando MAC:
  - Emplea DES, 3DES o AES
  - Emplea MD5 o SHA1
  - Emplea clave compartida
  - MAC de paquete IP completo (incluidos campos cabecera AH) obviando campos mutables como TTL que irían a cero
  - Cada entidad de la asociación segura calcula el ICV por separado y luego comprueba

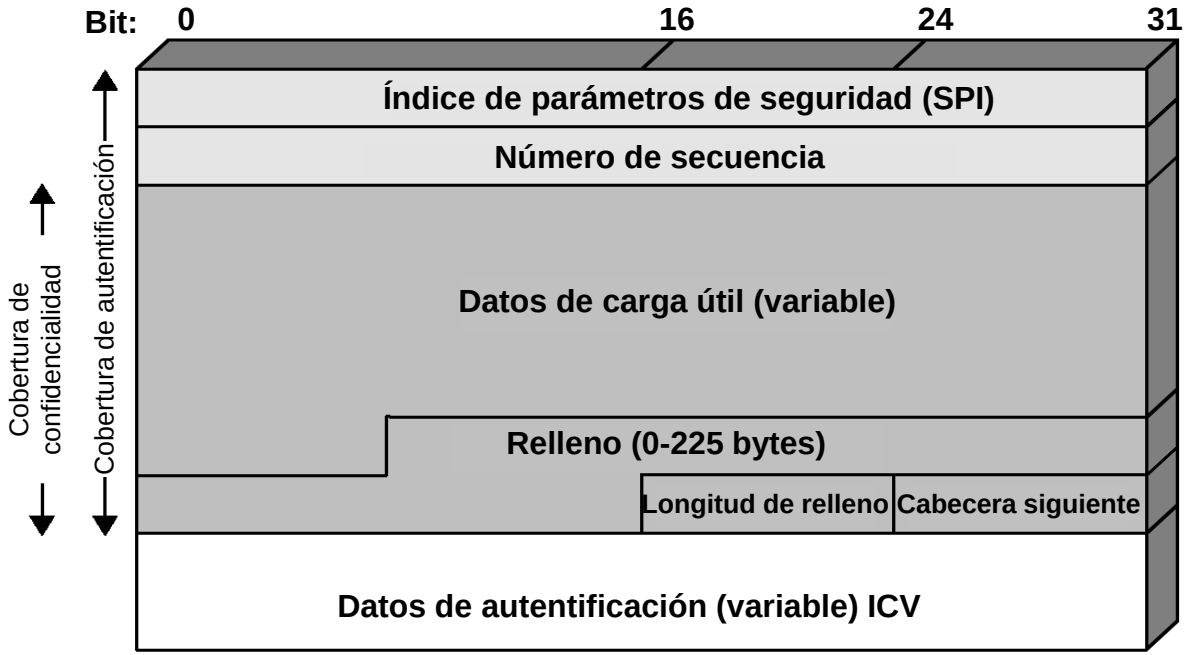
IPSec

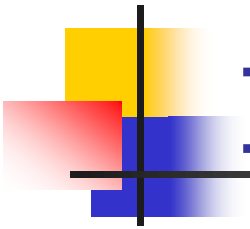
- **Protocolo ESP** (RFC 2406)
  - Confidencialidad
  - Autenticación del origen de datos (opcional)
  - Integridad (opcional)
  - Servicio contra reenvío (opcional)
- ESP encapsula el datagrama IP original (completo o no)



IPSec

- Cabecera ESP
  - SPI
  - Sequence Number
- Datos de carga útil (datagrama IP original o parte de él)
- Cola ESP
  - Padding
  - Padding Length
  - Next Header
  - ICV



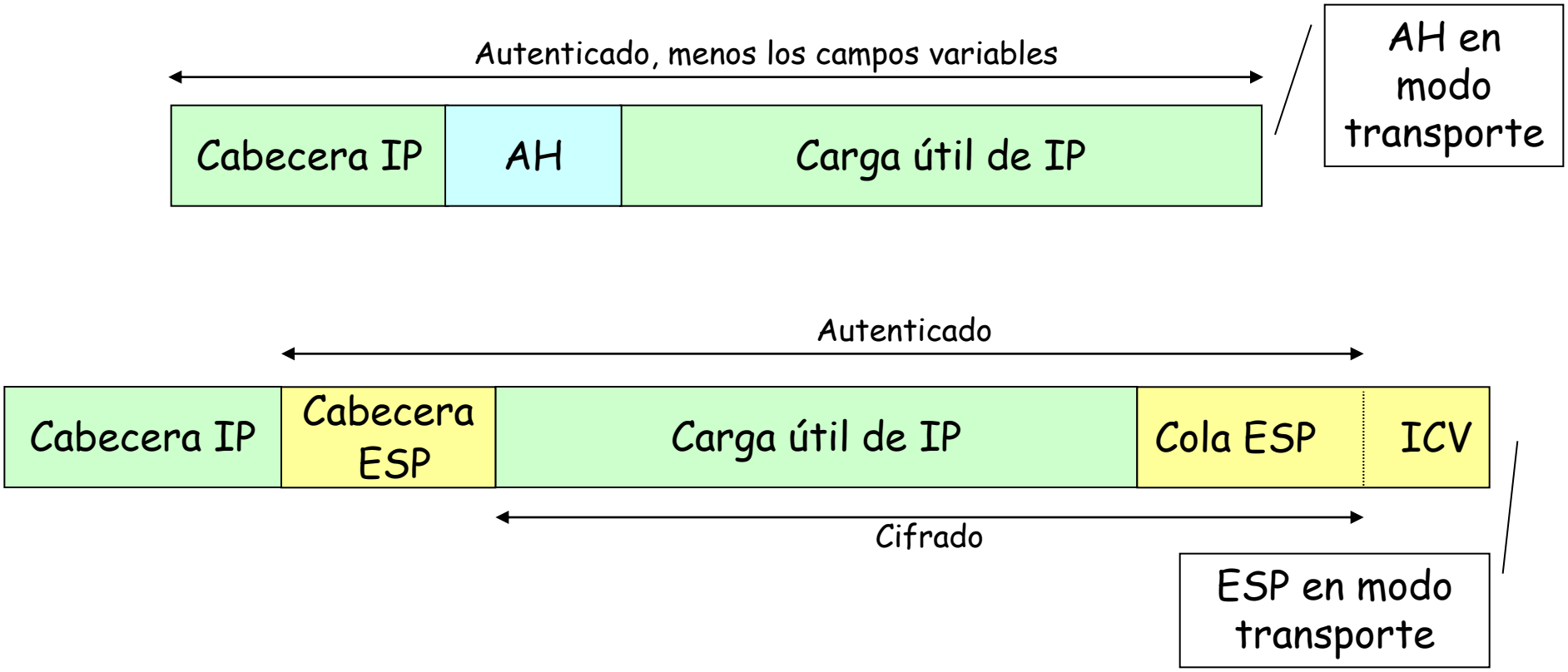


IPSec

- **Modo Transporte**
  - Conexiones extremo a extremo entre un host y un dispositivo que actúa como tal
- **Modo Túnel**
  - Entre pasarelas, o entre un host que se conecta a una pasarela de seguridad
  - Cabecera IP se copia y se desplaza a la izquierda
  - Se forma nueva cabecera IP con la copia

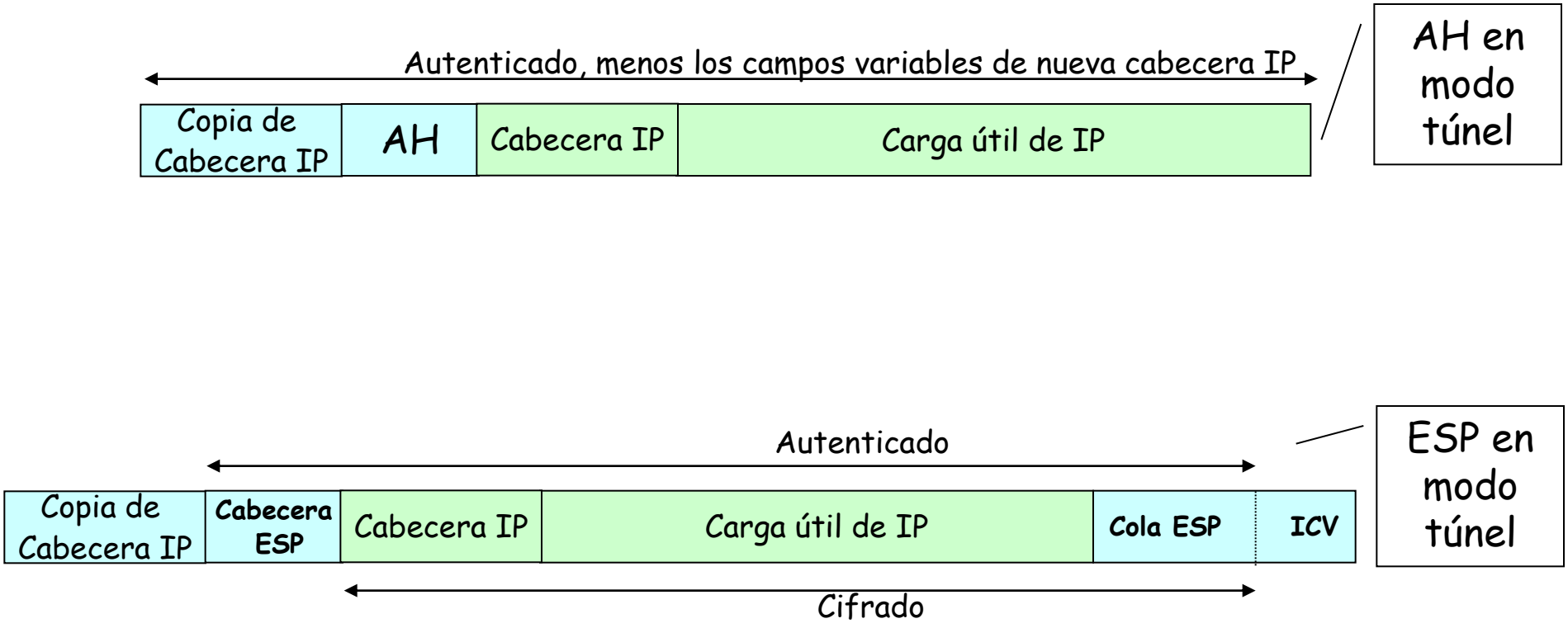
IPSec

- AH y ESP en modo transporte



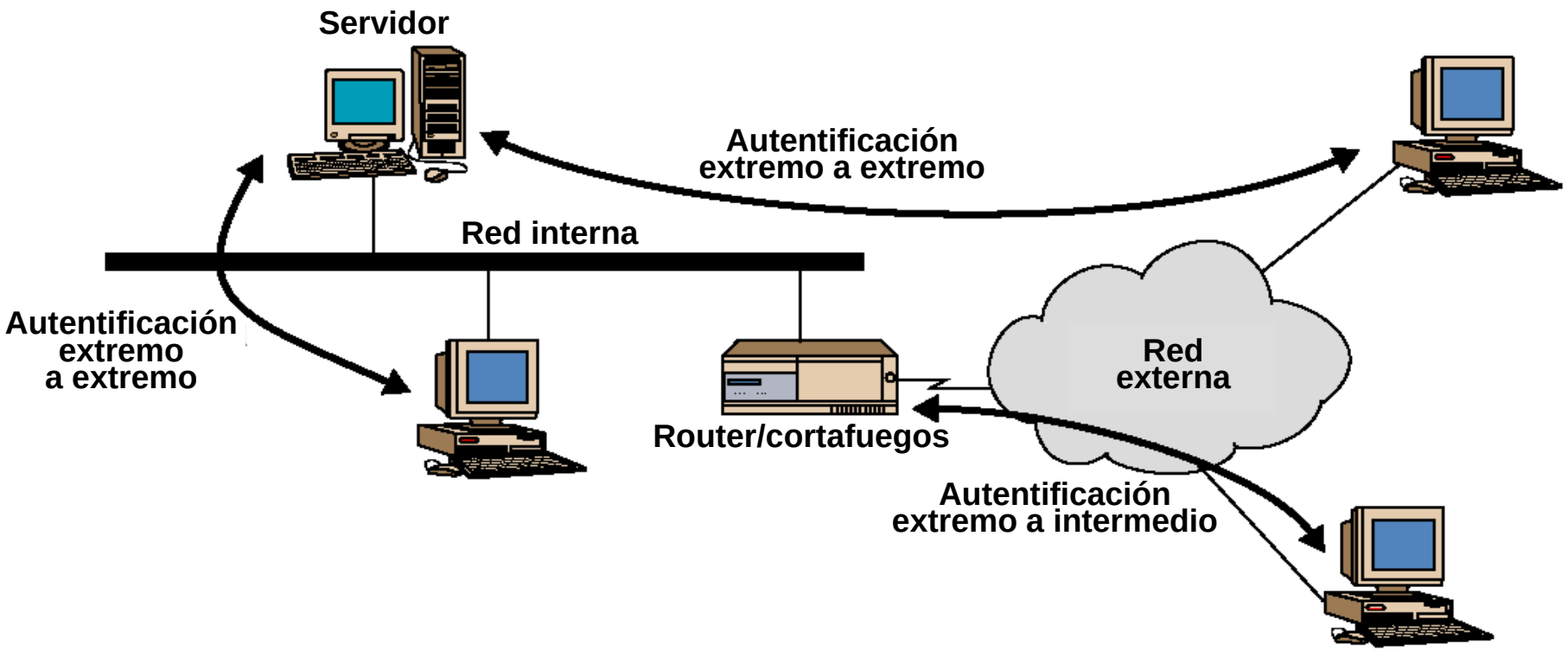
IPSec

- AH y ESP en modo túnel

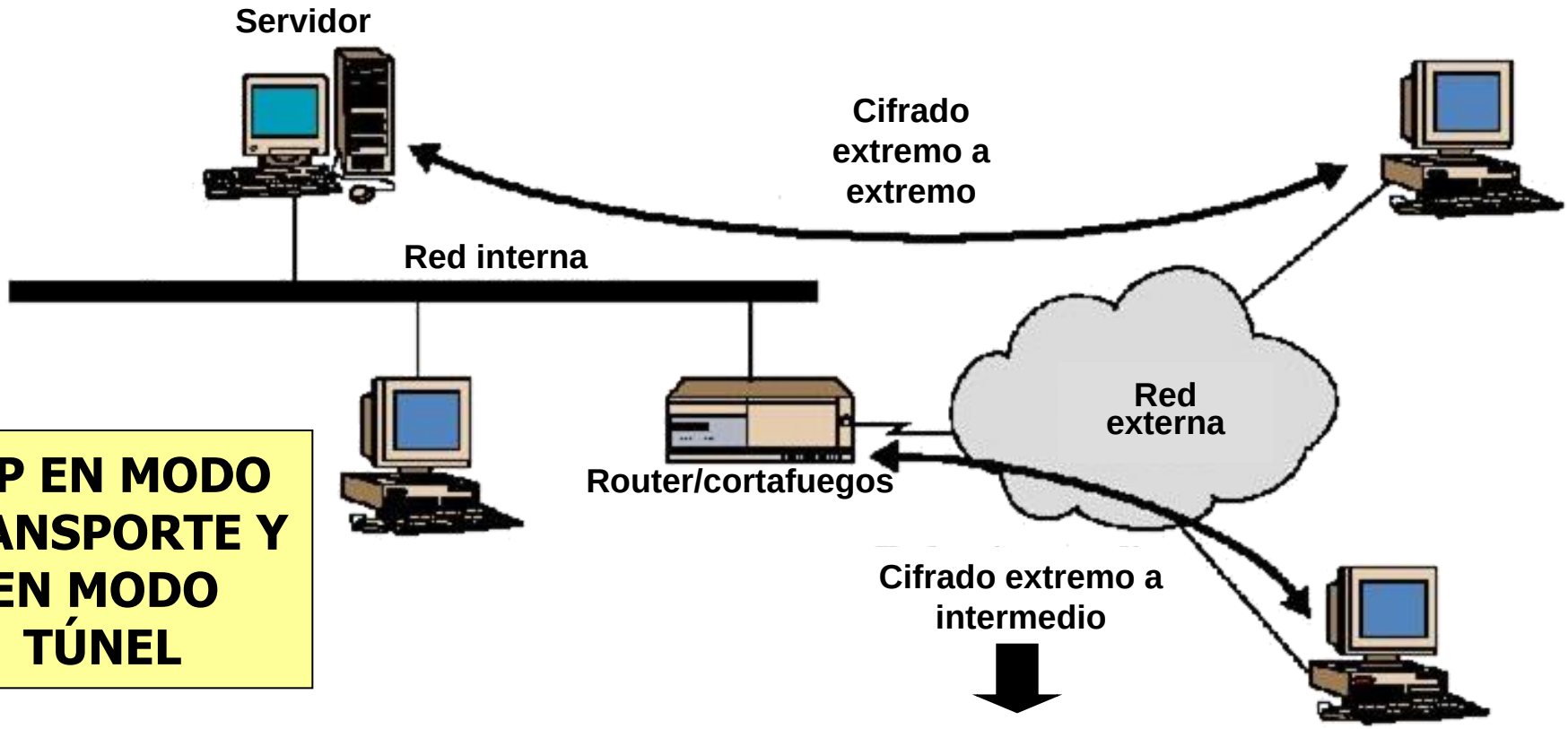


IPSec

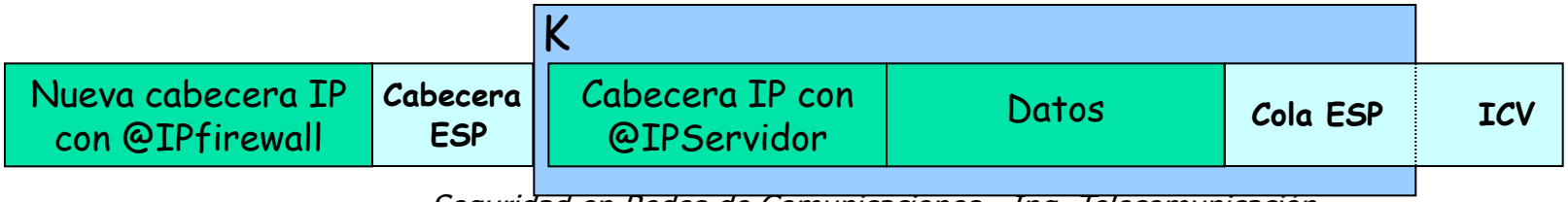
AH EN MODO TRANSPORTE Y EN MODO TÚNEL



IPSec

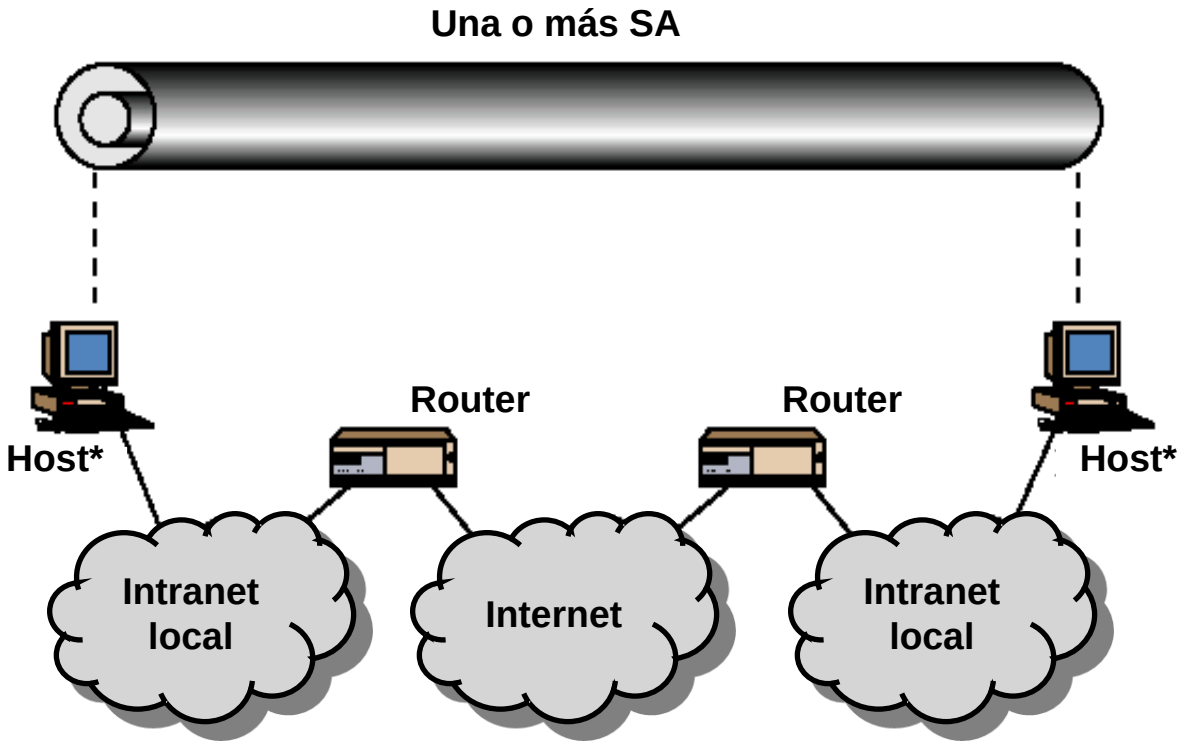


ESP EN MODO TRANSPORTE Y EN MODO TÚNEL



IPSec

COMBINACIONES BÁSICAS DE ASOCIACIONES DE SEGURIDAD



- AH en modo transporte
- ESP en modo túnel
- AH seguida de ESP en modo transporte
- Cualquiera anterior dentro de una AH o ESP en modo túnel

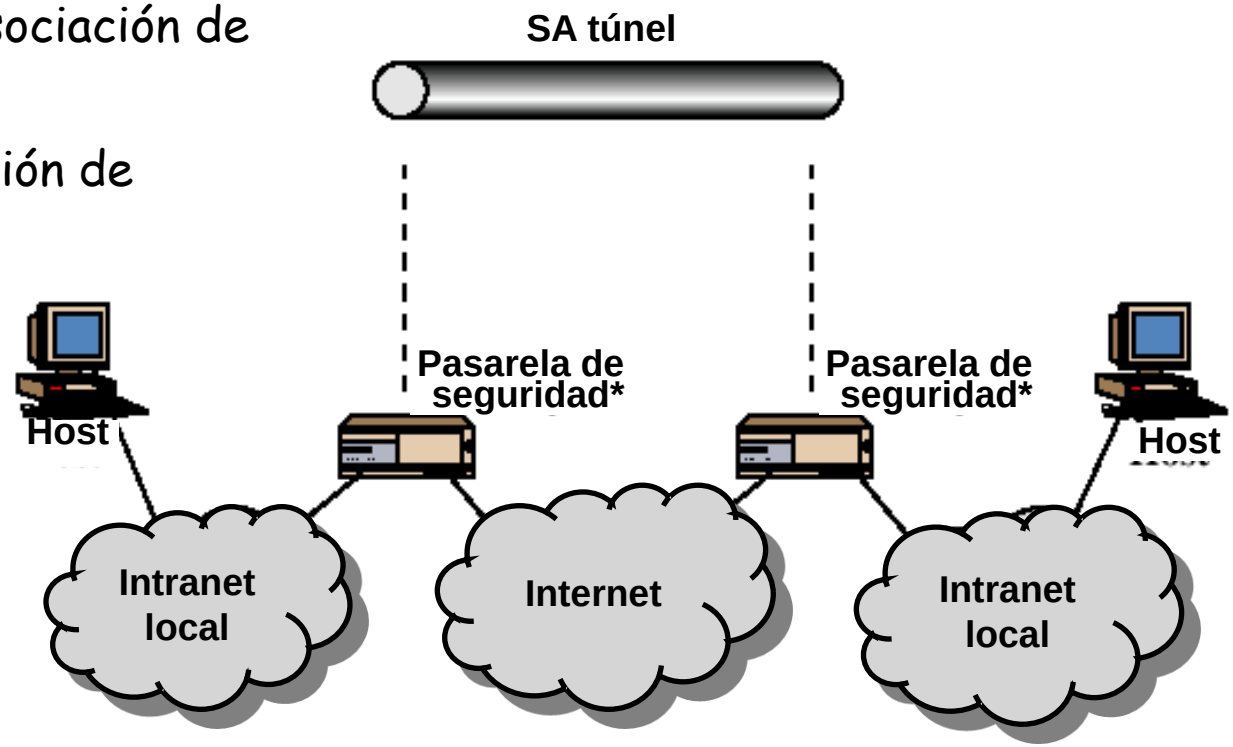
IPSec

COMBINACIONES BÁSICAS DE ASOCIACIONES DE SEGURIDAD

-Ilustra modo túnel en una red privada virtual (VPN)

-Sólo se necesita una asociación de seguridad

-AH, ESP o ESP con opción de autenticación

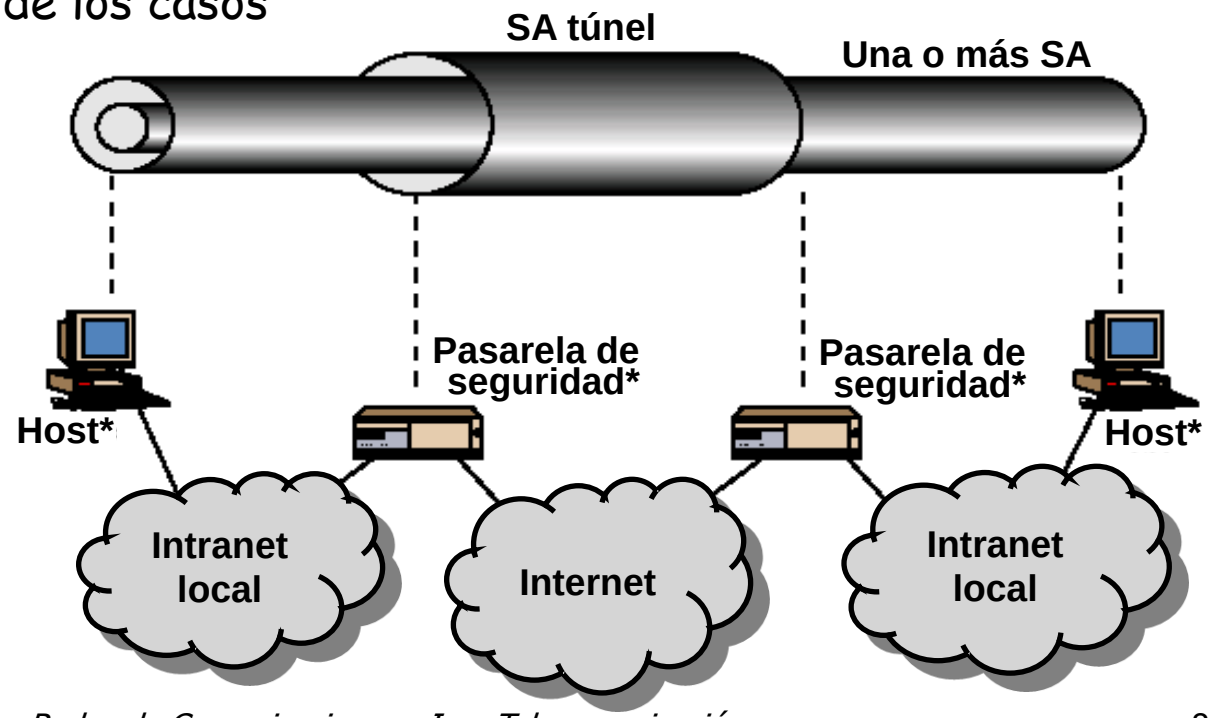


IPSec

COMBINACIONES BÁSICAS DE ASOCIACIONES DE SEGURIDAD

- Se construye sobre caso anterior añadiendo seguridad extremo a extremo

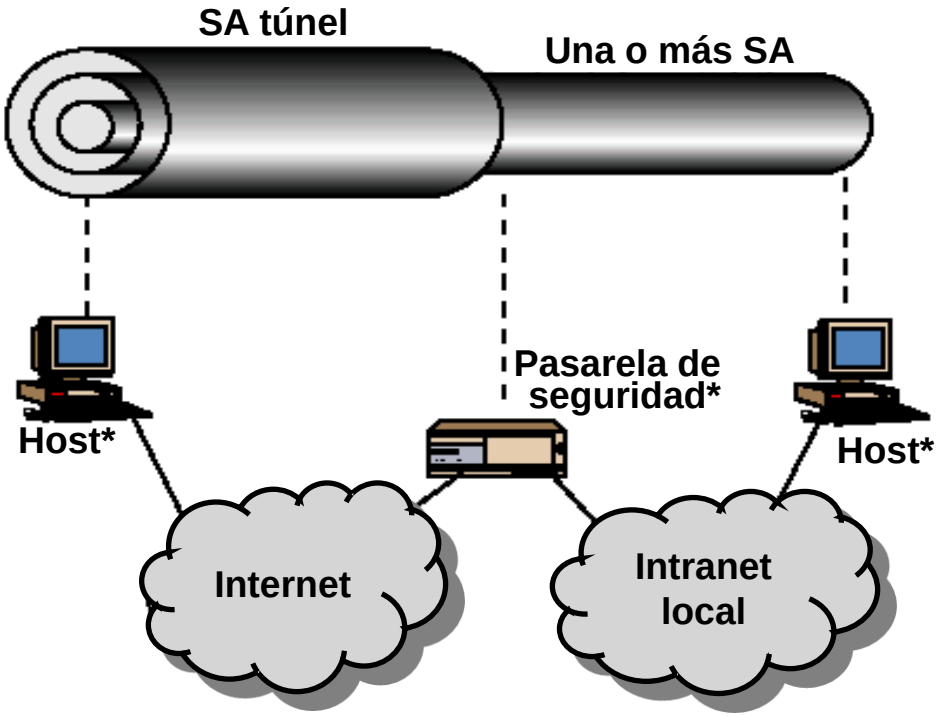
- Todas las combinaciones de los casos anteriores



IPSec

COMBINACIONES BÁSICAS DE ASOCIACIONES DE SEGURIDAD

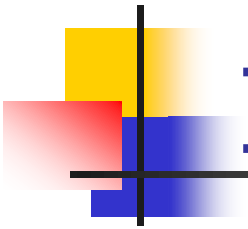
- Soporte para un host remoto que desea acceder a una organización con cortafuegos y luego acceder a algún servidor detrás del cortafuegos



IPSec

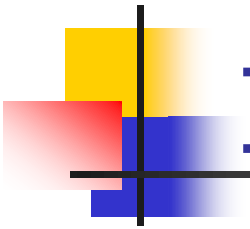
- Formación de asociaciones de seguridad
  - Protocolo IKE en dos fases

Fase 1. Autenticación entre entidades, negociación de AS e inicialización de túnel IPSec (ISAKMP)	**Fase 2.** Negociación parámetros seguridad de túnel IPSec, creación de túnel IPSec.
PARÁMETROS: alg. cifrado, alg. hash, método autenticación, método intercambio claves, validez.	PARÁMETROS: protocolo IPSec, alg. cifrado, alg. hash, validez.



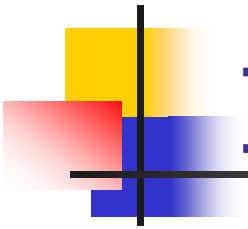
IPSec

- IPSec sólo funciona con tráfico *unicast*
- Túneles IPSec son túneles punto a punto
- Encapsulaciones de IPSec: HDLC, PPP, ATM o Frame Relay
- Si usamos NAT y AH => NAT antes de encapsulación IPSec
- USAR AH cuando
  - Se requiere sólo autenticación
- USAR ESP cuando
  - Se requiera confidencialidad



IP v.6

- Nueva versión del protocolo IP
- Motivos
  - Agotamiento de direcciones IP (~2008)
  - Crecimiento exponencial de tablas de rutas BGP
  - Nuevas funcionalidades: QoS, movilidad, seguridad, …
- Principales características
  - Direcciones IP de 128 bits
  - Direccionamiento con estructura jerárquica
  - Ubicuidad
  - QoS
- Seguridad en IP v.6: IPSec es obligatorio



IP v.6

- **Protocolo Neighbor Discovery** (RFC 2461 y 2462)
  - Descubrir nodos en la red
  - Determinar dirección física de otros nodos
  - Localizar *routers* vecinos
  - Autoconfigurar direcciones
  - Descubrir direcciones duplicadas
- Se propone uso de AH => problemas
- SEcure Neighbor Discovery (SEND)
  - Sellos temporales y *nonces*
  - Cadenas de certificados
  - Direcciones generadas criptográficamente