TECNOLÓGICO DE MONTERREY®

Protocolos criptográficos

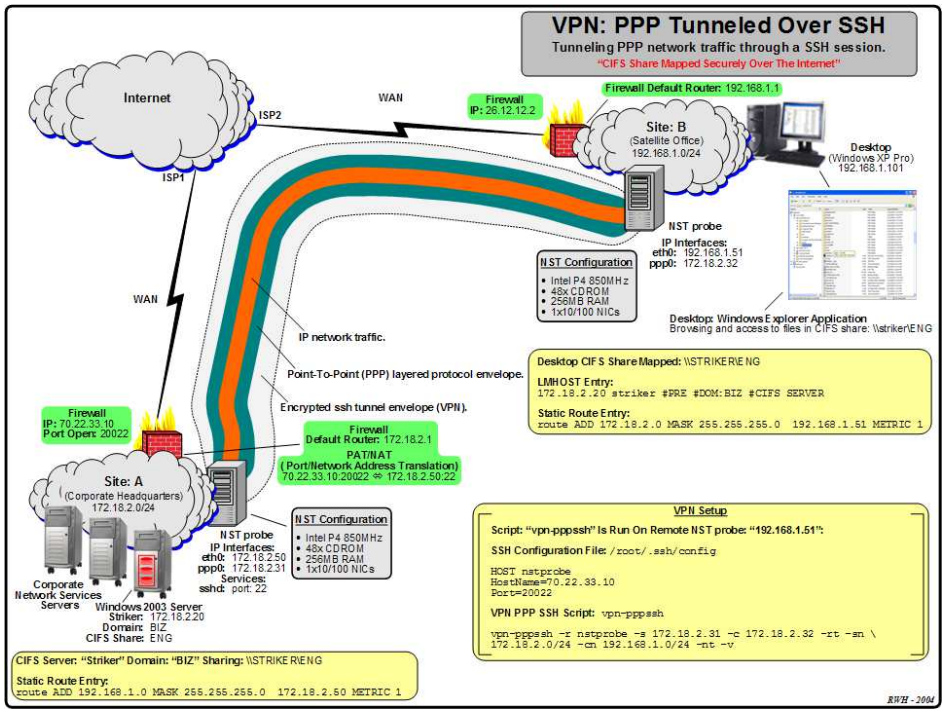
Roberto Gómez Cárdenas

rogoca@gmail.com

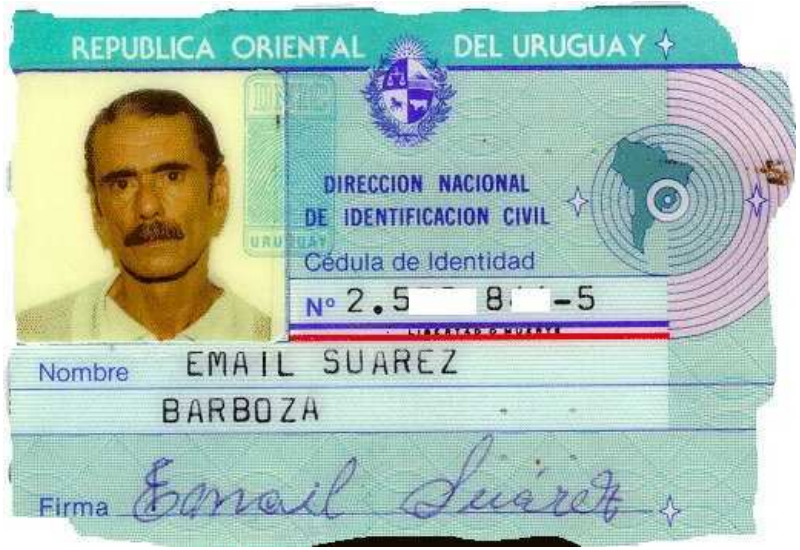
http://cryptomex.org

Protocolos critpograficos

- VPN



- Autenticación



Redes Virtuales Privadas: VPN

- Conexión establecida sobre una infraestructura pública o compartida
  - uso tecnologías encripción o autenticación para asegurar su payload
- Se crea un segmento “virtual” entre cualesquiera dos entidades que tengan acceso.
- Puede darse a través de infraestructura compartida, LAN, WAN o el internet
- Tecnología barata y efectiva para una solución de red remota que cualquiera con Internet puede aprovechar.

TECNOLÓGICO DE MONTERREY®

Metodología VPN básica

- Concepto básico
  - asegurar canal comunicación con encripción
- Comunicación puede asegurarse a diferentes capas:
  - aplicación (PGP o SSH)
    - varios programas trabajan de host a host
    - solo protegen el payload del paquete y no el paquete
  - transporte (SSL)
    - contenido comunicación es protegido, pero paquetes no
  - red (IPSec)
    - no solo encripta el payload sino la información TCP/IP
    - posible si dispositivos usan encapsulación
  - enlace de datos: Layer 2 Tunneling Protocol (L2TP)
    - encripción paquetes sobre PPP

Los protocolos de seguridad

Application Layer

S/MIME, S/HTTP, SET, PEM, PGP
Secure/Multipurpose Internet Mail Extensions
Secure/Hypertext Transfer Protocol
Secure Electronic Transaction
Privacy Enhanced Mail
Pretty Good Privacy

Transport Layer

SSL/TLS
Secure Socket Layer/Transport Layer Security

Internet Layer

IPSEC, GRE
IP Security
Generic Routing Encapsulation

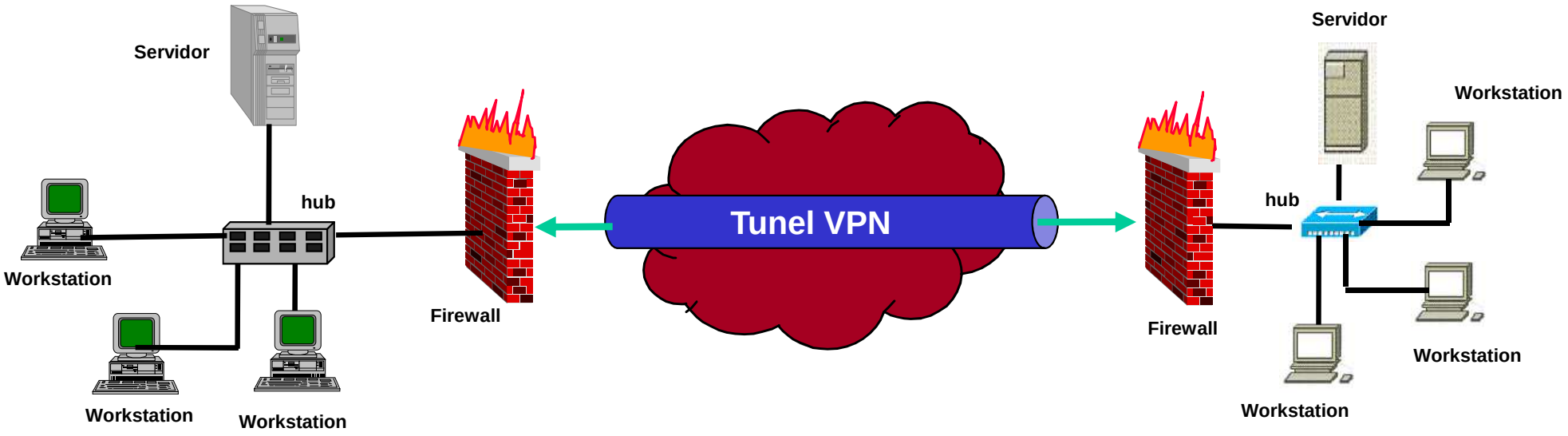
Host to Network Layer

CHAP, PAP
Challenge Handshake Authentication Protocol
Password Authentication Protocol

L2F, L2TP, PPTP
Layer 2 Forwarding, Layer 2 Tunneling Protocol
Point to Point Tunneling Protocol

Concepto: tuneleo

- Tuneleo (tunneling)
  - proceso de encapsular un tipo de paquete dentro de otro para facilitar el transporte de este.



- Ejemplo

00:05:18.671517 192.168.44.129 > 172.16.1.128 AH(spi=580532459, seq=0x3): 1232 > 80: P 1:260(259) ack 1 win 17520 (DF)

TECNOLÓGICO DE MONTERREY®

IPSec

- Este protocolo desarrollado por el grupo de trabajo de seguridad del IETF (Internet Engineering Task Force).
- Surgió a partir del desarrollo de IPv6.
- Empezó siendo una extensión del encabezado en Ipv6
  - debido a que cubría las necesidades de un gran número de clientes, se decidió implantar en parte para Ipv4.
- Consiste de varios protocolos
  - IPSec Protocol Suite
- RFC 2401-2412

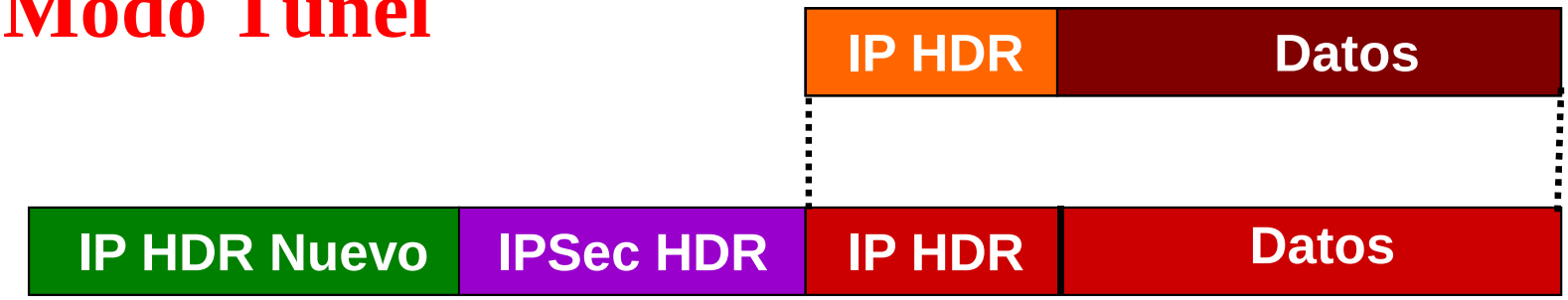
TECNOLÓGICO DE MONTERREY®

Objetivos IPSec

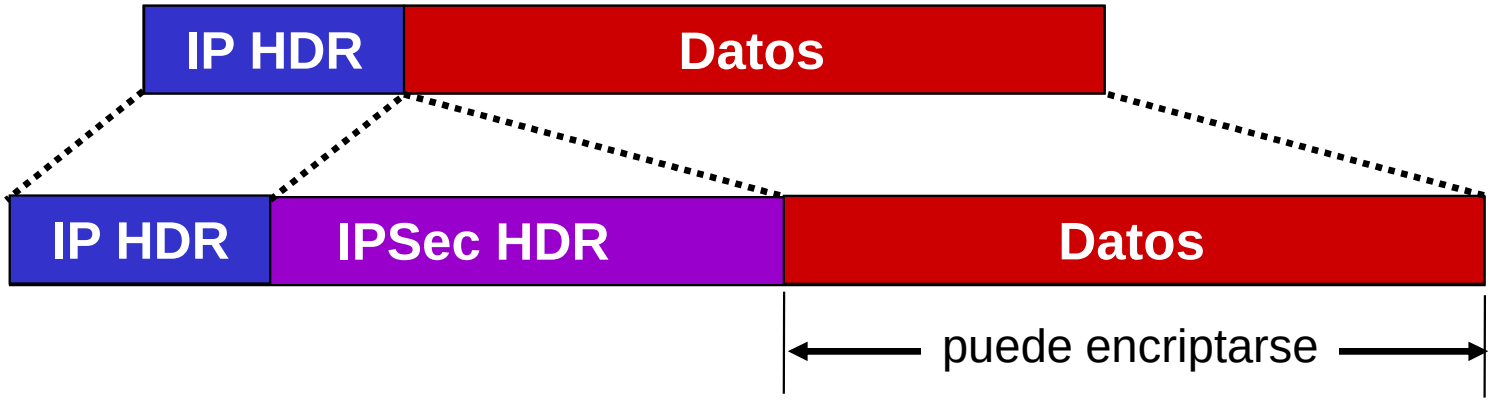
- Soportar los protocolos IP existentes (IPv4, IPv6)
- Incremento pequeño en el tamaño de las tramas
- Permitir implantación progresiva en Internet
- Permitir el establecimiento de túneles
- Ofrecer los siguientes servicios
  - Integridad de los contenidos
  - Confidencialidad de los contenidos
  - Autentificación de los participantes

Modos de operación

- **Modo Túnel**



- **Modo Transporte**



TECNOLÓGICO DE MONTERREY®

Security Association

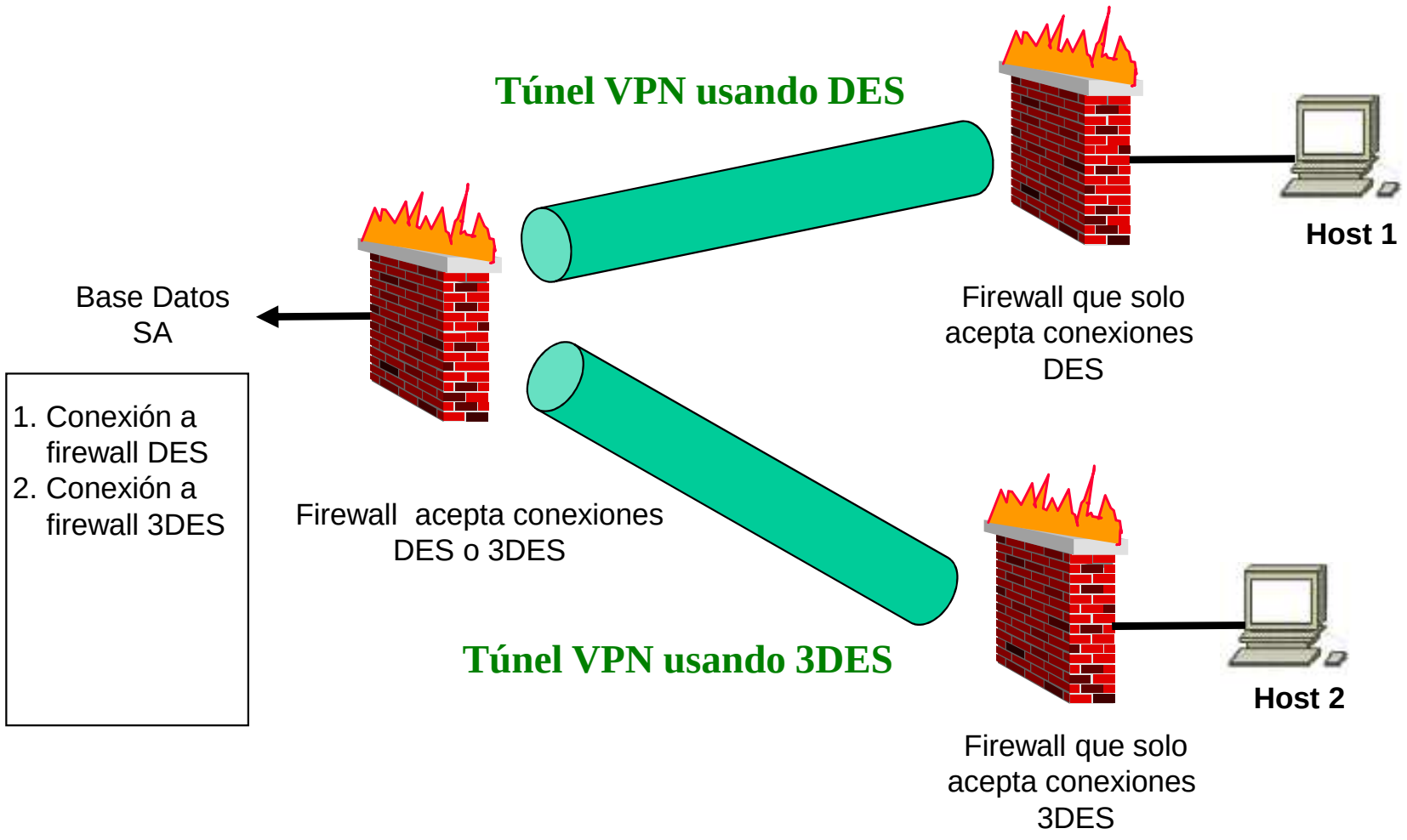
- Se trata de un acuerdo entre dos entidades acerca de cómo se transmitirá información de forma segura.
  - conexión lógica unidireccional entre dos sistemas
- IPSec soporta varios protocolos, diferentes modos de comunicación, así como algoritmos de encripción y de hash.
  - todo esto debe negociarse antes de que la comunicación se lleve a cabo
- El resultado de la negociación es una SA
- Cada sesión de comunicación cuenta con dos SA
  - una para cada participante de la comunicación

TECNOLÓGICO DE MONTERREY®

Base Datos de la SA

- Después de negociar una SA, esta se almacena en una base de datos de SA
- Formadas por una tripleta <*SPI*, *IP-DA*, *SP*>
  - Security Parameter Index (SPI)
    - Identificador único de cada SA
  - IP Destination Address (IP-DA)
    - Dirección del receptor (unicast, multicast, broadcast)
  - Security Protocol (SP)
    - El modo de operación (transporte, túnel)
    - El protocolo usado (ESP, AH)
      - Sólo se puede especificar uno de los dos
      - Pueden ser necesarias hasta 4 SAs para una conexión

Ejemplo negociación



TECNOLÓGICO DE MONTERREY®

Protocolos usados

- AH
  - Authentication Header
  - proporciona un servicio de autenticación a nivel paquete
- ESP
  - Encapsulating Security Payload
  - proporcionar encripción más autenticación
- IKE
  - Internet Key Exchange
  - negocia parámetros de conexión, incluyendo llaves para los otros dos protocolos

TECNOLÓGICO DE MONTERREY®

Protocolo AH

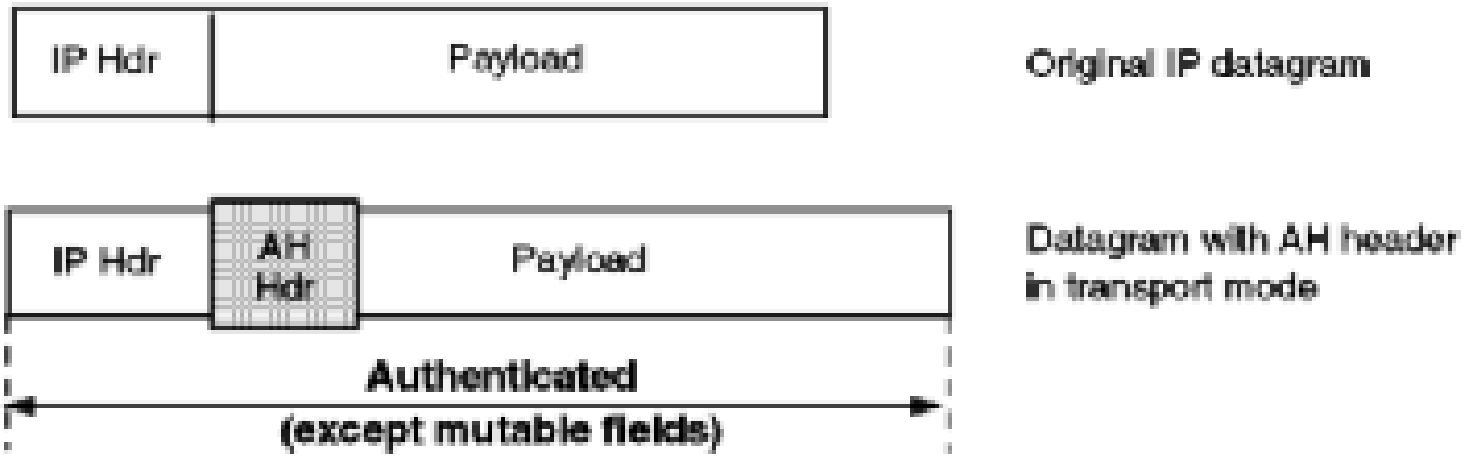
- Proporciona integridad y autentificación
  - opcionalmente protege contra reenvío (replay)
- Añade un encabezado adicional al paquete IP
  - encabezado contiene una firma digital (ICV: integrity check value)
  - garantiza información IP es correcta, pero no se oculta
  - AH usa encabezado IP para calcular la firma digital, dirección fuente es autentica y viene de donde dice
- Soporta números de secuencia para prevenir ataques de tipo replay
  - dispositivos usan números para seguir flujo comunicación
  - atacante no puede re-enviar un paquete capturado para intentar acceder a la VPN

Esquema encabezado AH

- Tipo protocolo del paquete que sigue al encabezado AH
- Longitud encabezado AH
- SPI: a que stream de comunicación SA pertenece el paquete
- Número incremental único para evitar paquetes capturados sean reenviados a una víctima para extraer información
- Contiene ICV y una firma digital

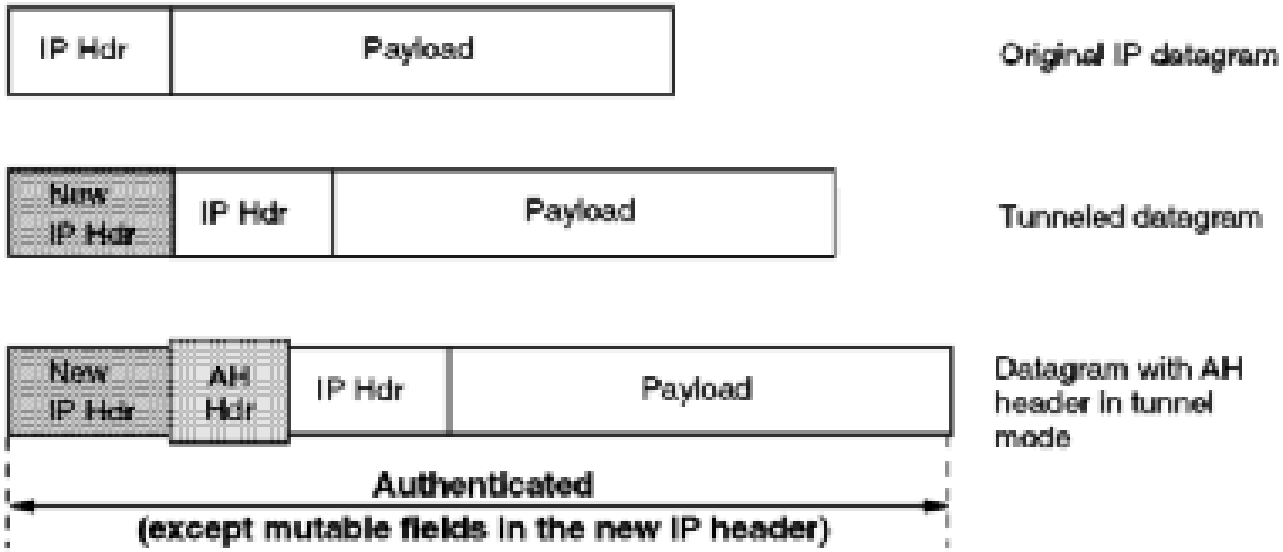
Encabezado AH en modo transporte

- La cabecera AH es insertada justo después de la IP
- Si ya hay cabecera IPSec, se inserta justo antes
- Sólo lo usan los hosts (no los gateways)
  - Ventajas: hay poca sobrecarga de procesamiento
  - Desventajas: los campos mutables no van autentificados



Encabezado AH en modo túnel

- El paquete original se encapsula en uno nuevo IP, al que se le aplica AH en modo de transporte
- Se usa si uno de los extremos es un gateway
  - Ventajas: los campos mutables van autentificados, y se pueden usar direcciones IP privadas
  - Desventajas: hay sobrecarga de procesamiento



```
00:05:18.645054 192.168.44.129 > 192.168.44.128:
➥AH(spi=580532459,seq=0x1): 1232 > 80: S 3631297390:3631297390(0)
➥win 16384 <mss 1460,nop,nop,sackOK> (DF)
0x0000     4500 0048 089a 4000 8033 1797 c0a8 2c81  E..H..@..3....,.
0x0010     c0a8 2c80 0604 0000 229a 38eb 0000 0001  ..,.....".8.....
0x0020     c118 fc19 0124 3688 d1b7 3e13 04d0 0050  .....$6...>....P
0x0030     d871 336e 0000 0000 7002 4000 57cd 0000  .q3n....p.@.W...
0x0040     0204 05b4 0101 0402                      ........

00:05:18.655236 192.168.44.128 > 192.168.44.129:
➥AH(spi=3951698033,seq=0x1): 80 > 1232: S 2981983731:2981983731(0)
➥ack 3631297391 win 17520 <mss 1460,nop,nop,sackOK> (DF)
0x0000     4500 0048 0080 4000 8033 1fb1 c0a8 2c80  E..H..@..3....,.
0x0010     c0a8 2c81 0604 0000 eb8a 2071 0000 0001  ..,........q....
0x0020     24db fdd4 aaa4 0c89 16cf c00c 0050 04d0  $.............P..
0x0030     b1bd 75f3 d871 336f 7012 4470 2b9b 0000  ..u..q3op.Dp+...
0x0040     0204 05b4 0101 0402                      ........

00:05:18.659869 192.168.44.129 > 192.168.44.128:
➥AH(spi=580532459,seq=0x2): 1232 > 80: . ack 1 win 17520 (DF)
0x0000     4500 0040 08a1 4000 8033 1798 c0a8 2c81  E..@..@..3....,.
0x0010     c0a8 2c80 0604 0000 229a 38eb 0000 0002  ..,.....".8.....
0x0020     cbf6 be88 73d7 97a6 a63b a092 04d0 0050  ....s....;.....P
0x0030     d871 336f b1bd 75f4 5010 4470 585f 0000  .q3o..u.P.DpX_..

00:05:18.671517 192.168.44.129 > 192.168.44.128:
➥AH(spi=580532459,seq=0x3): 1232 > 80: P 1:260(259) ack 1 win
➥17520 (DF)
0x0000     4500 0143 08a2 4000 8033 1694 c0a8 2c81  E..C..@..3....,.
0x0010     c0a8 2c80 0604 0000 229a 38eb 0000 0003  ..,.....".8.....
0x0020     3521 0ef0 df8f 17db d87e 7477 04d0 0050  5!.......~tw...P
0x0030     d871 336f b1bd 75f4 5018 4470 0108 0000  .q3o..u.P.Dp....
0x0040     4745 5420 2f20 4854 5450 2f31 2e31 0d0a  GET./.HTTP/1.1..
0x0050     4163 6365 7074 3a20 696d 6167 652f 6769  Accept:.image/gi
0x0060     662c 2069 6d61 6765 2f78 2d78 6269 746d  f,.image/x-xbitm
0x0070     6170 2c20 696d 6167 652f 6a70 6567 2c20  ap,.image/jpeg,.
0x0080     696d 6167 652f 706a 7065 672c 202a 2f2a  image/pjpeg,.*/*
0x0090     0d0a 4163 6365 7074 2d4c 616e 6775 6167  ..Accept-Languag
0x00a0     > truncated for display purposes.
```

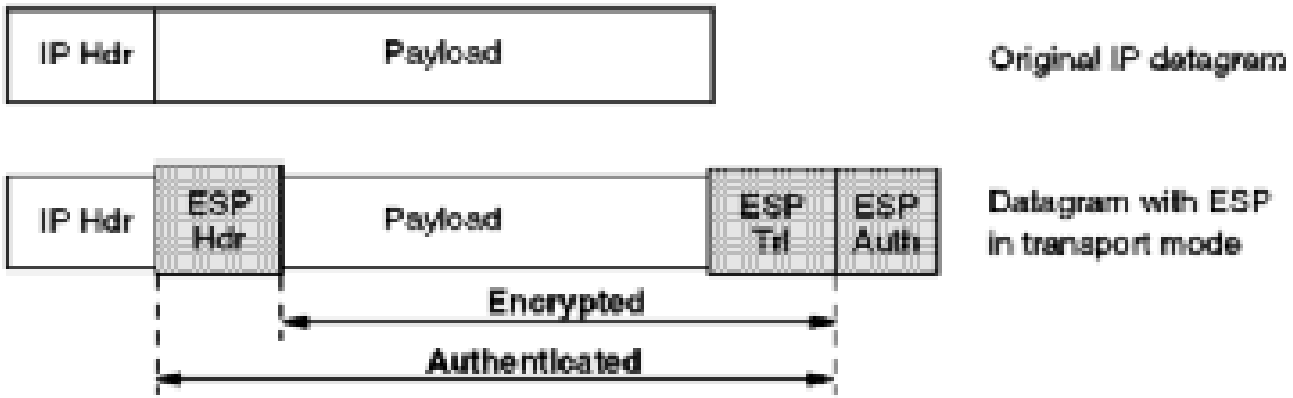
TECNOLÓGICO DE MONTERREY®

Protocolo ESP

- Encapsulating Security Payload (ESP)
- Se utiliza para integridad, autentificación, y cifrado
  - Opcionalmente protege contra reenvío
  - Servicios no orientados a conexión
  - Selección opcional de servicios
    - Al menos uno debe de estar activado
- Encripta el payload de los paquetes IP
- Como varios protocolos IPSec es modular
  - usa diferentes algoritmos encripción DES, 3DES e IDEA
- Trabaja diferente, dependiendo del modo usado

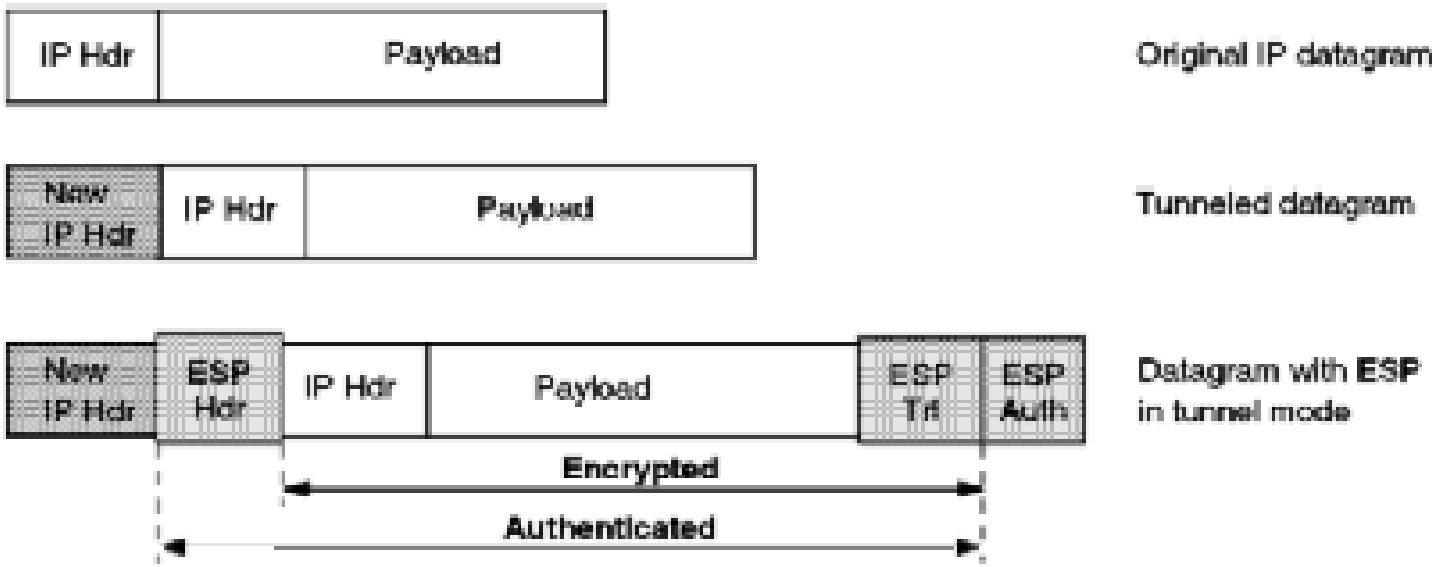
ESP en modo transporte

- Encabezado ESP es insertado justo después de la IP
  - encripta el resto de la información del paquete, de capa 4 para arriba
- Si se especifica servicio de autenticación durante la negociación
  - se añade información del ICV para autenticación e integridad de del paquete
  - contrariamente al protocolo AH el ICV de ESP no es

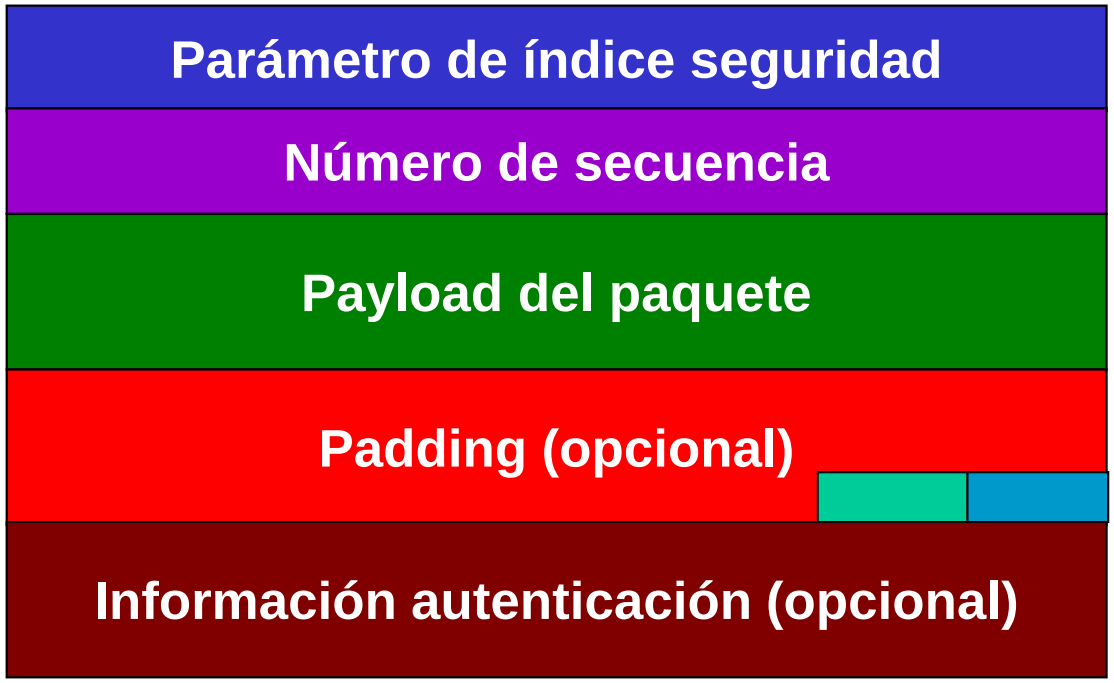


ESP en modo túnel

- El paquete original se encapsula en uno nuevo IP, al que se le aplica ESP en modo de transporte
- Se usa si uno de los extremos es un gateway
  - Ventajas: los encabezados IP van encriptados, y se pueden usar direcciones IP privadas
  - Desventajas: hay sobrecarga de procesamiento



Encabezado ESP



TECNOLÓGICO DE MONTERREY®

Ejemplo ESP

```
00:01:30.031 192.168.44.128 > 192.168.44.129: ESP(spi=1728941913,seq=0x1) (DF)
0x0000     4500 0050 0061 4000 8032 1fc9 c0a8 2c80    E..P.a@..2....,.
0x0010     c0a8 2c81 670d 8f59 0000 0001 0262 5e96  ....,.g..Y.....b^.
0x0020     d238 3af3 c90e c385 fca7 09cf 693a b6cc  .8:.........i:..
0x0030     6d88 5400 d417 a0c4 6f5b df7f 5e96 994f  m.T.....o[..^..O
0x0040     cb03 1624 6668 d10d cf89 f6b0 e4e7 46a9  ...$fh........F.

00:01:30.038 192.168.44.129 > 192.168.44.128: ESP(spi=1302500357,seq=0x2) (DF)
0x0000     4500 0048 06a7 4000 8032 198b c0a8 2c81  E..H..@..2....,.
0x0010     c0a8 2c80 4da2 9405 0000 0002 f22d 2ce7    ....,.M........-,.
0x0020     4dc6 ba58 11e3 333f 0cd5 8079 62d7 7128    M..X..3?...yb.q(
0x0030     0590 3056 085a dd96 3653 ef97 35e1 593c    ..0V.Z..6S..5.Y<
0x0040     8213 a0e7 2516 835b                      ....%..[

00:01:30.105 192.168.44.128 > 192.168.44.129: ESP(spi=1728941913,seq=0x2) (DF)
0x0000     4500 01a8 0062 4000 8032 1e70 c0a8 2c80  E....b@..2.p..,.
0x0010     c0a8 2c81 670d 8f59 0000 0002 5e96 994f    ..,.g..Y....^..O
0x0020     cb03 1624 7da5 0ecb 392f a703 6f53 aa21    ...$}...9/..oS.!
```

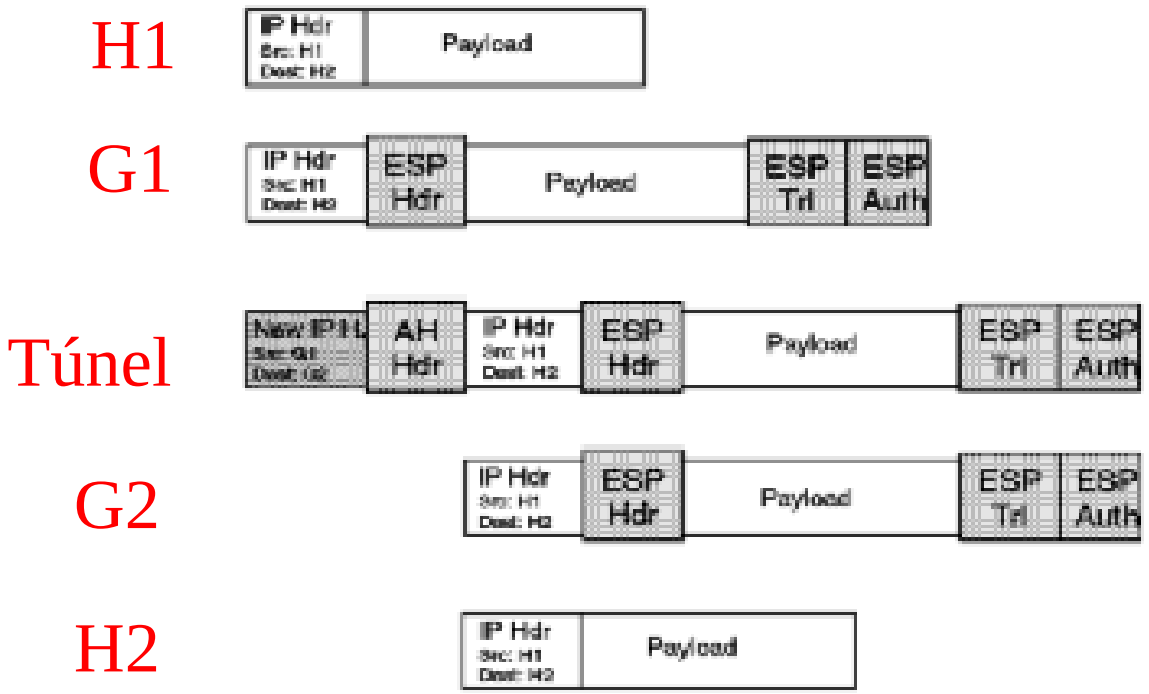
TECNOLÓGICO DE MONTERREY®

¿Porqué dos encabezados/protocolos?

- ESP requiere criptografía fuerte, se use o no, mientras que AH sólo requiere hashing
  - la criptografía está regulada en muchos países
  - la firma no suele estar regulada
- Si sólo se requiere autentificación, AH es mejor
  - formato más simple
  - menor tiempo de procesamiento
- Al tener dos protocolos se tiene un mejor control sobre la red IPSec, así como opciones flexibles

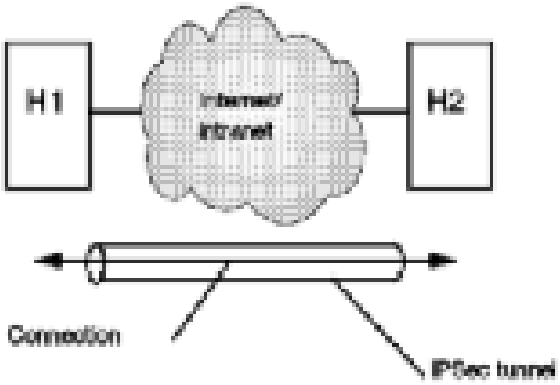
Combinando AH/ESP

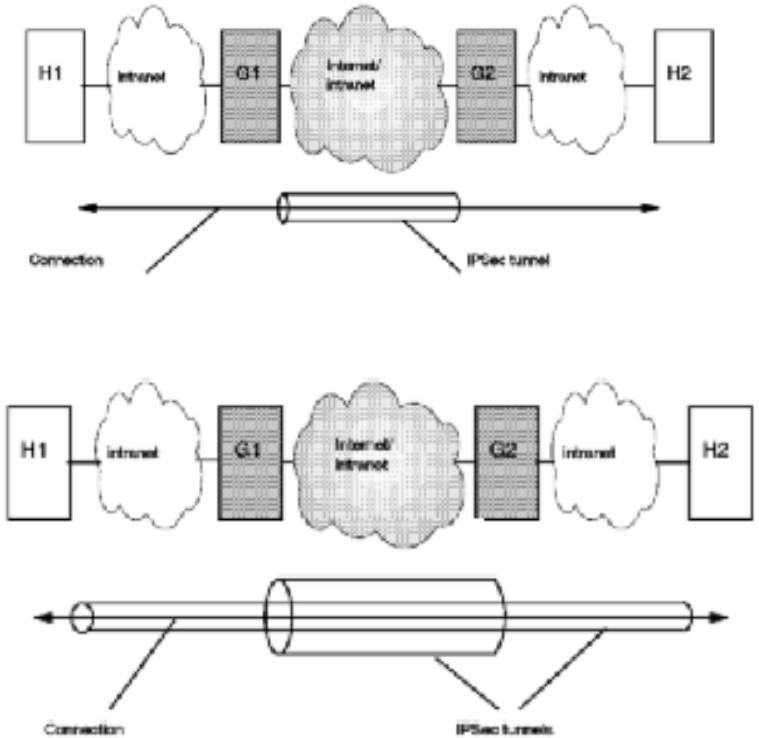
- Si se requiere autenticación de direcciones (AH) y confidencialidad (ESP)
  - posible combinar ambos protocolos
- Hay muchas combinaciones posibles, lo normal:
  - AH en modo túnel
  - ESP en modo transporte

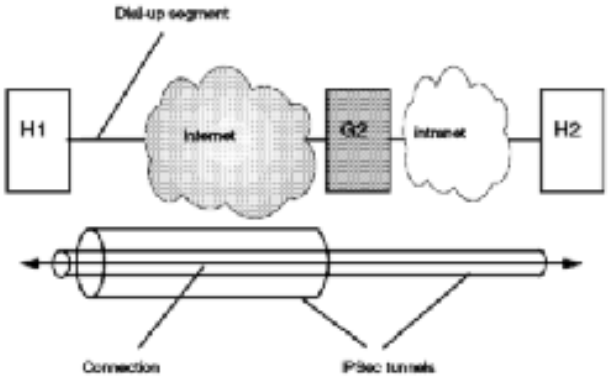


Tuneles IPSec

1. Seguridad de extremo a extremo
2. Soporte básico VPN
3. Seguridad extremo a extremo con soporte VPN
4. Seguridad en acceso remoto







TECNOLÓGICO DE MONTERREY®

El protocolo IKE

- Protocolo autenticador y negociador de IPSec
- Verifica que la parte que desea iniciar una comunicación con un dispositivo, este autorizada a hacerlo.
  - después negocia el tipo de encripción a utilizar
- Es la combinación de dos protocolos
  - ISAKMP: Internet Security Association and Key Management Protocol, maneja las negociaciones de seguridad
  - Oakley: variación Diffie Hellman, responsable del intercambio de llaves

SSL y SSH

TECNOLÓGICO DE MONTERREY®

Secure Sockets Layer

- Es una propuesta de estándar para encriptado y autenticación en el Web.
  - diseñado en 1993 por Netscape
- Es un esquema de encriptado de bajo nivel usado para encriptar transacciones en protocolos de nivel aplicación como HTTP, FTP, etc.
- Con SSL puede autentificarse un servidor con respecto a su cliente y viceversa.

TECNOLÓGICO DE MONTERREY®

Protocolo SSL

- El estándar de IETF “Transport Layer Security” (TLS) se basa en SSL.
- Ha pasado por varias versiones
  - las más comunes son las versiones 2 y 3
  - problemas criptográficos conocidos en versión 2, solucionados en la versión 3
- Requiere un transporte confiable.
- Provee seguridad en el canal:
  - Privacía. Se usa un criptosistema simétrico (DES, RC4)
  - Autenticación. Se usa un criptosistema asimétrico (RSA)
  - Integridad:Se usan funciones hash (MD2, MD4, MD5)

TECNOLÓGICO DE MONTERREY®

Protocolos de SSL

- SSL handshake protocol
  - proceso de reconocimiento mutuo y de petición de conexión
  - encargado de establecer, mantener y finalizar las conexiones SSL
- SSL record protocol
  - protocolo de registro de SSL
  - establece el formato de datos que se va a usar en la transmisión encriptada

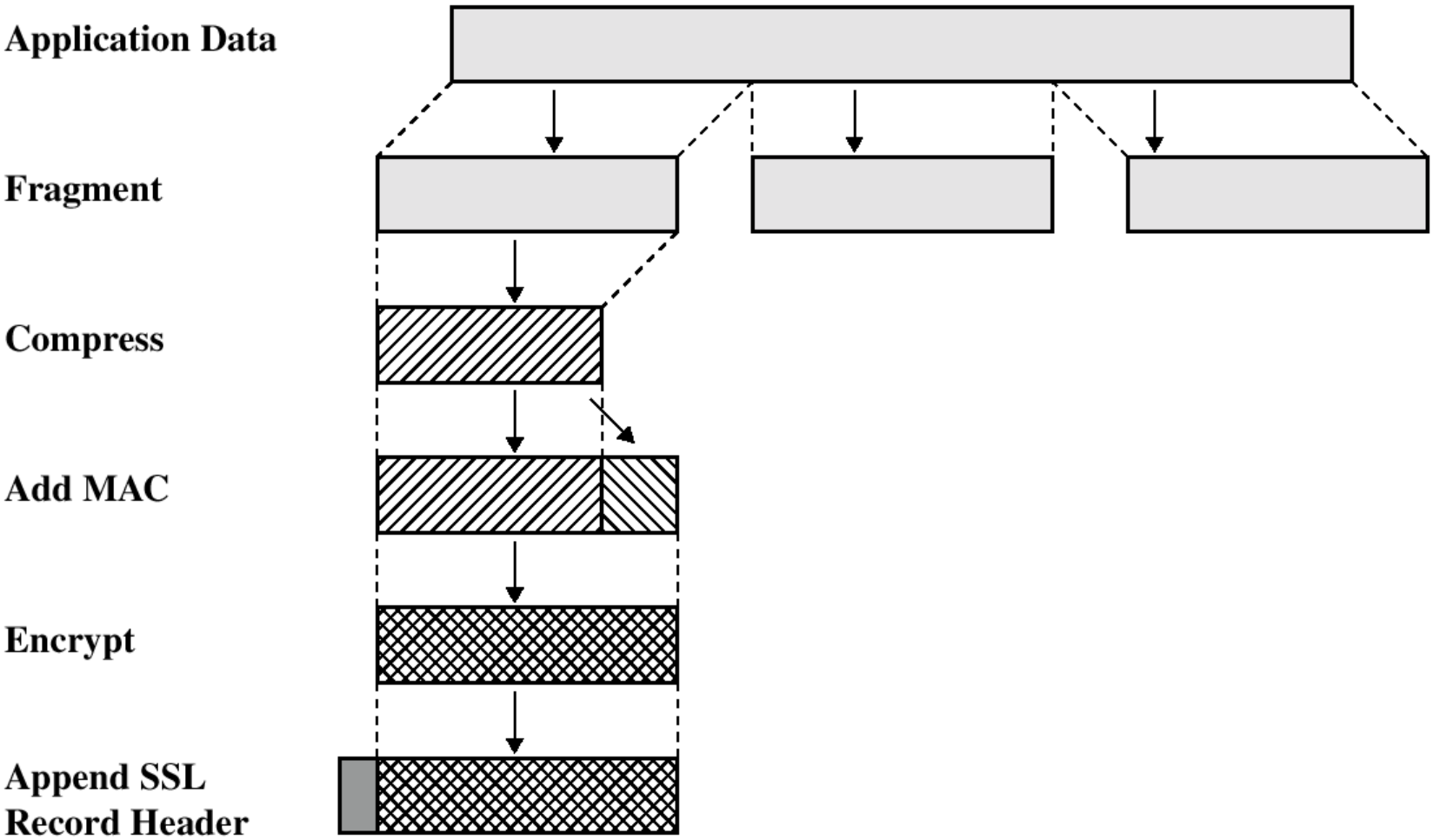
TECNOLÓGICO DE MONTERREY®

SSL record protocol

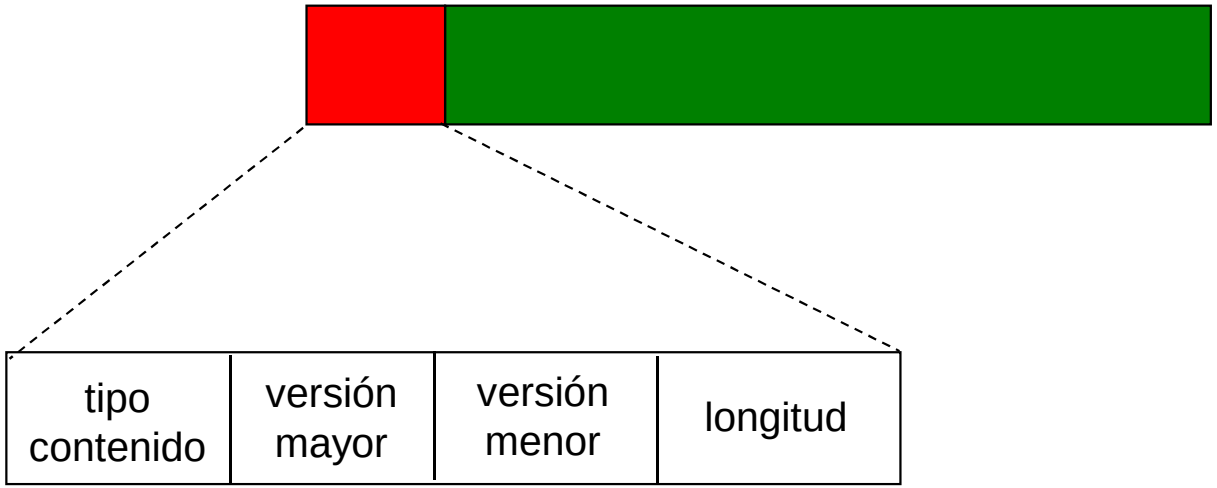
- Construido arriba servicio orientado conexión confiable
  - por ejemplo: TCP
- Define los formatos de los mensajes empleados en SSL.
- Establece tres componentes para la porción de datos del protocolo
  - MAC DATA: código de autenticación del mensaje
  - ACTUAL DATA: datos de aplicación a transmitir
  - PADDING- DATA: datos requeridos para rellenar el mensaje cuando se usa un sistema de encripción en bloque

TECNOLÓGICO DE MONTERREY®

SSL record protocol



SSL record header



- Tipo contenido: protocolo usado para procesar contenido del fragmento
- Versión mayor: versión mayor usada
- Versión menor: versión menor usada
- Longitud: longitud en bytes del fragmento de texto plano

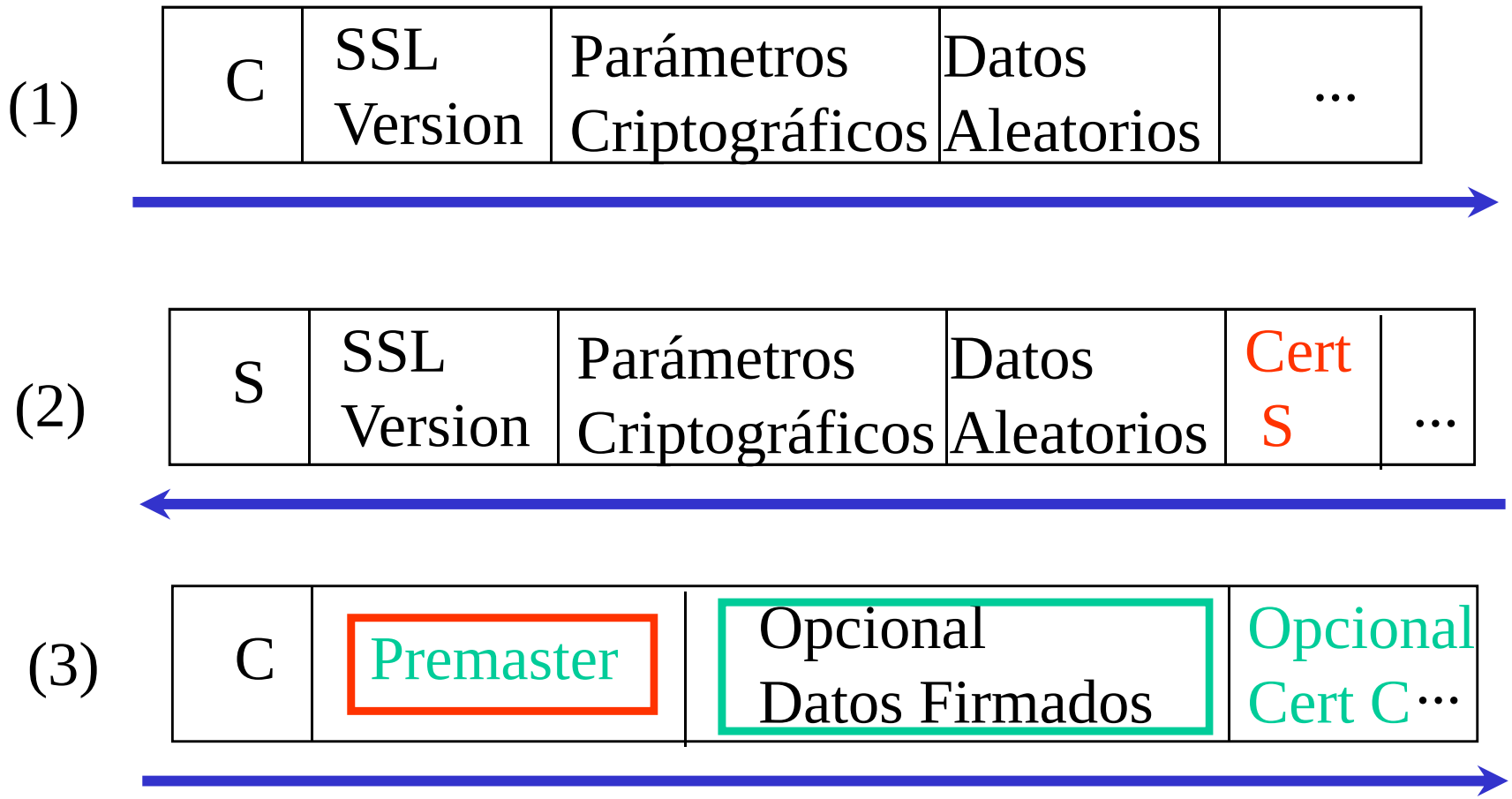
TECNOLÓGICO DE MONTERREY®

SSL handshake protocol

- Autentifica al servidor para el cliente.
- Permite al cliente y servidor seleccionar algoritmos criptográficos, que sean soportados por ambos.
- Opcionalmente autentifica al cliente para el servidor.
- Usa criptografía de llave pública para generar secretos compartidos.
- Establece una conexión SSL encriptada.

Pasos del protocolo handshake

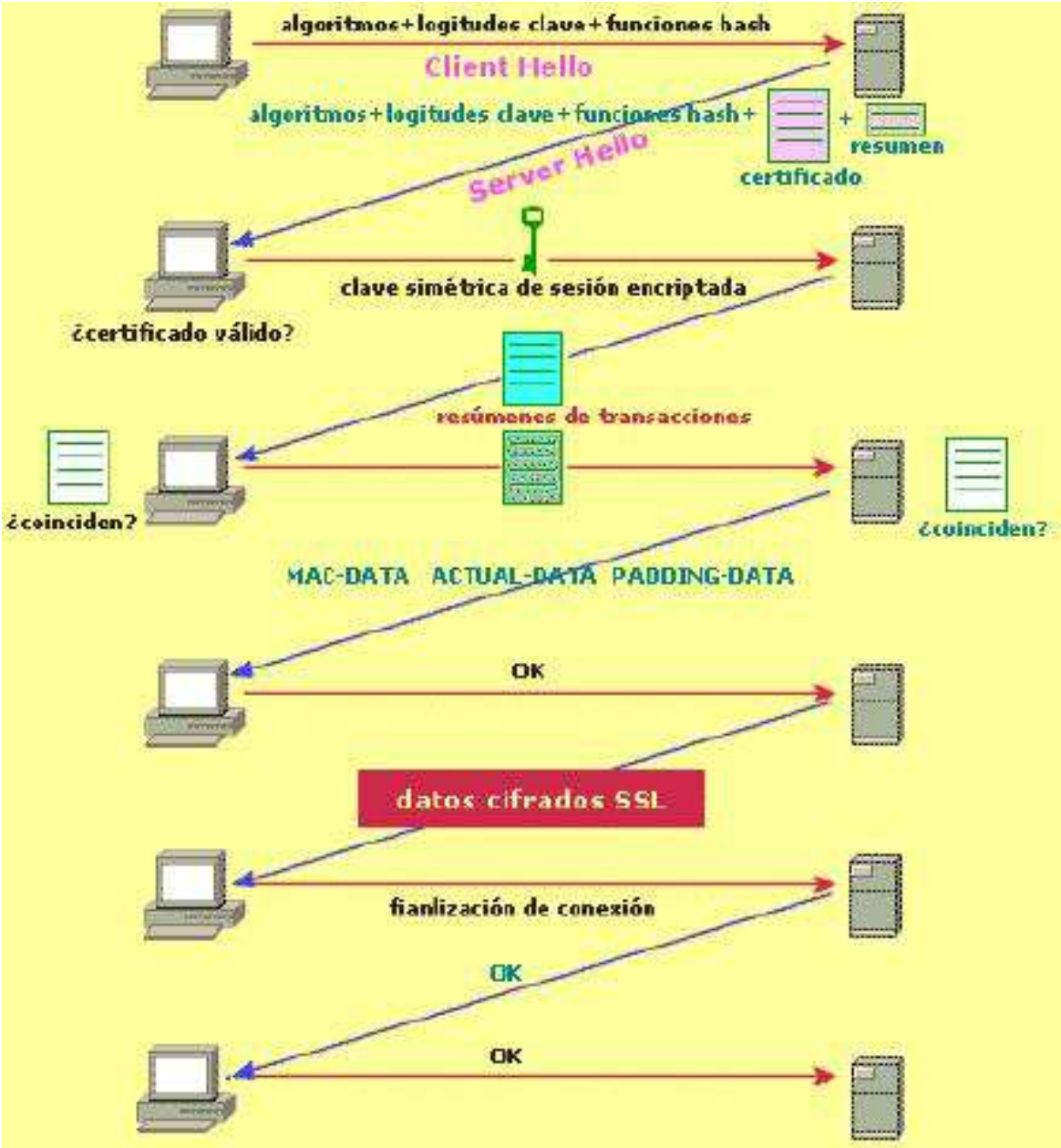
Cliente **Servidor**

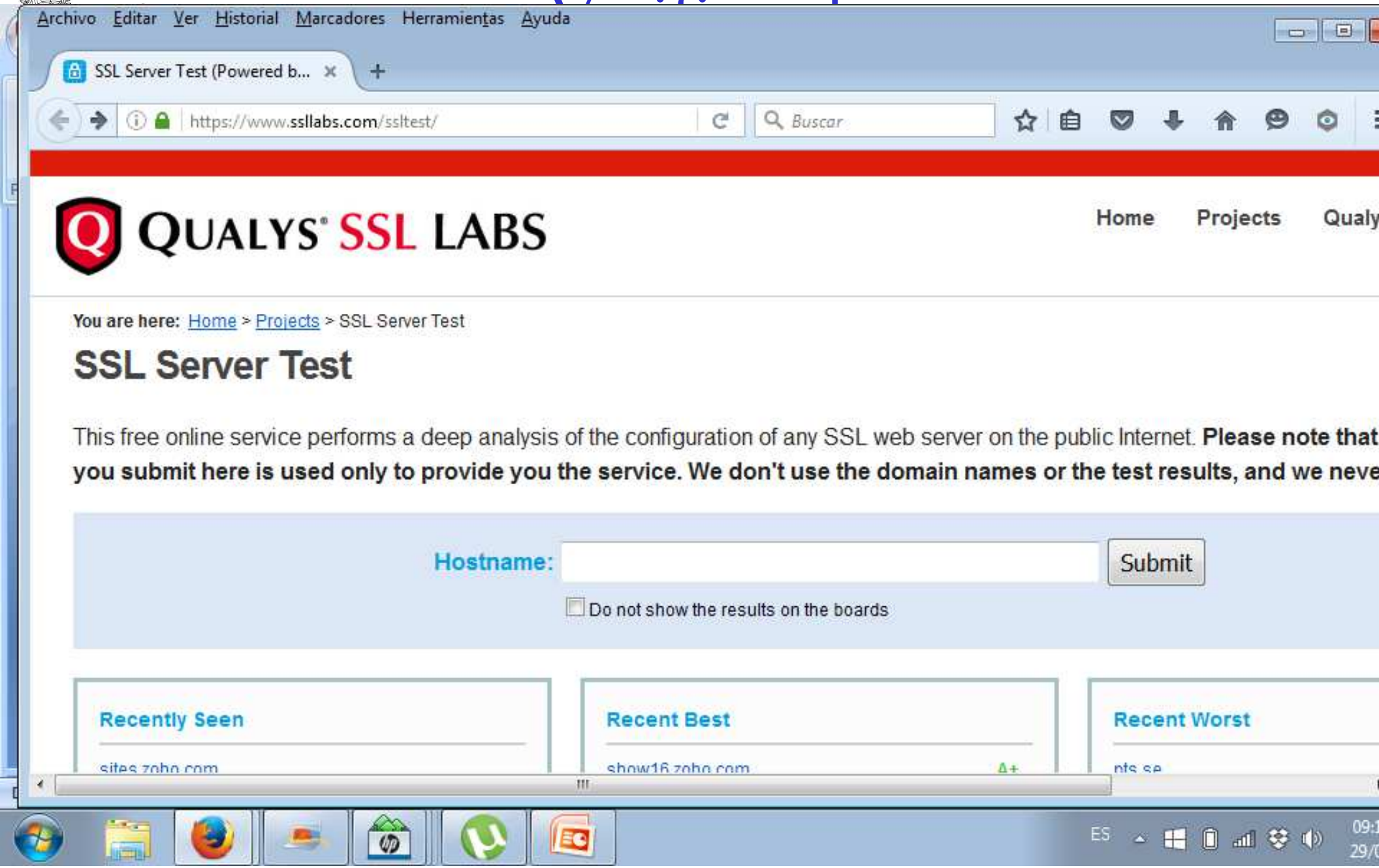


El cliente autentifica al servidor basándose en Cert S
Si falla error
Crea el secreto "Premaster"

TECNOLÓGICO DE MONTERREY®

Todo el protocolo




Archivo Editar Ver Historial Marcadores Herramientas Ayuda
SSL Server Test (Powered b...
https://www.ssllabs.com/ssltest/
Buscar
QUALYS SSL LABS
Home
Projects
Qualy
You are here: Home > Projects > SSL Server Test
SSL Server Test
This free online service performs a deep analysis of the configuration of any SSL web server on the public Internet. Please note that
you submit here is used only to provide you the service. We don't use the domain names or the test results, and we neve
Hostname:
Submit
Do not show the results on the boards
Recently Seen
Recent Best
Recent Worst
ES

TECNOLÓGICO DE MONTERREY®

El protocolo SSH

- Desarrollado por Communications Security Ltd.
- Es un programa (protocolo) para acceder a otra computadora a través de una red, ejecutar comandos a una maquina remota y mover archivos de una computadora a otra.
- Provee una fuerte autenticación y comunicaciones seguras por medio de encripción sobre canales inseguros.
- Es un sustituto para el telnet, ftp, rlogin, rsh, rcp y rdist.

Versiones SSH: SSH v1 y SSH v2

- SSH 1 es la versión original.
- SSH 2 incluye nuevas características
  - soporte protocolo TLS
- SSH 1 es distribuido con todo y código
  - licencia permite obtenerlo gratis para usos no-comerciales
- SSH 2 fue desarrollado por SSH Comm. Security
  - se vende comercialmente, aunque esta disponible para diferentes usos
- Varios programas basados en los protocolos SSH son desarrollados por otra gente.

TECNOLÓGICO DE MONTERREY®

Autenticación servidor

- No se basa en nombre servicio o direcciones IP
- En ambas versiones, criptografia llave pública es usada para probar identidad servidor.
- Primera parte verifica que cliente posee un llave pública correcta del servidor a conectarse.
  - Problema durante desarrollo V1: no existía estándar global para distribuir y verificar llaves públicas
  - SSH V2: puede usar autoridades certificadoras para verificar una llave pública (en base a TLS)
  - SSH V2 también soporta mecanismo desarrollado para V1

TECNOLÓGICO DE MONTERREY®

Solución versión 1

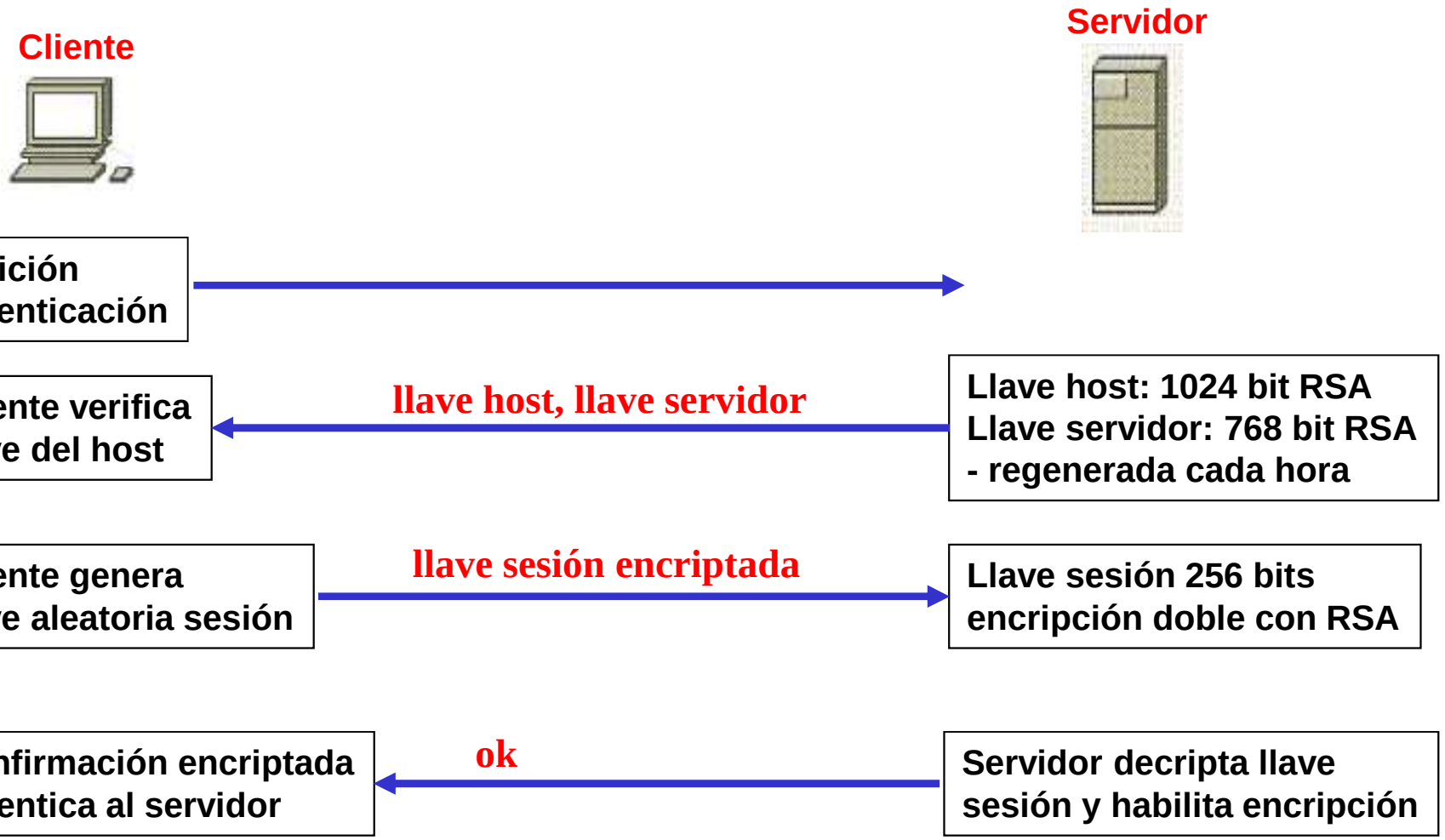
- Cliente retira llave pública del mismo servidor.
- Verifica si conoce una llave para un servidor con el mismo nombre.
  - si no coinciden se imprime una alerta
- Si el cliente no tiene almacenada una llave
  - imprime una alerta y
  - opcionalmente almacena la llave para la proxima vez que se conecte al servidor
- Solución pone al cliente vulnerable a un servidor hostil en la primera conexión
  - más seguridad que tener cliente vulnerable a un servidor hostil en cada conexión

TECNOLÓGICO DE MONTERREY®

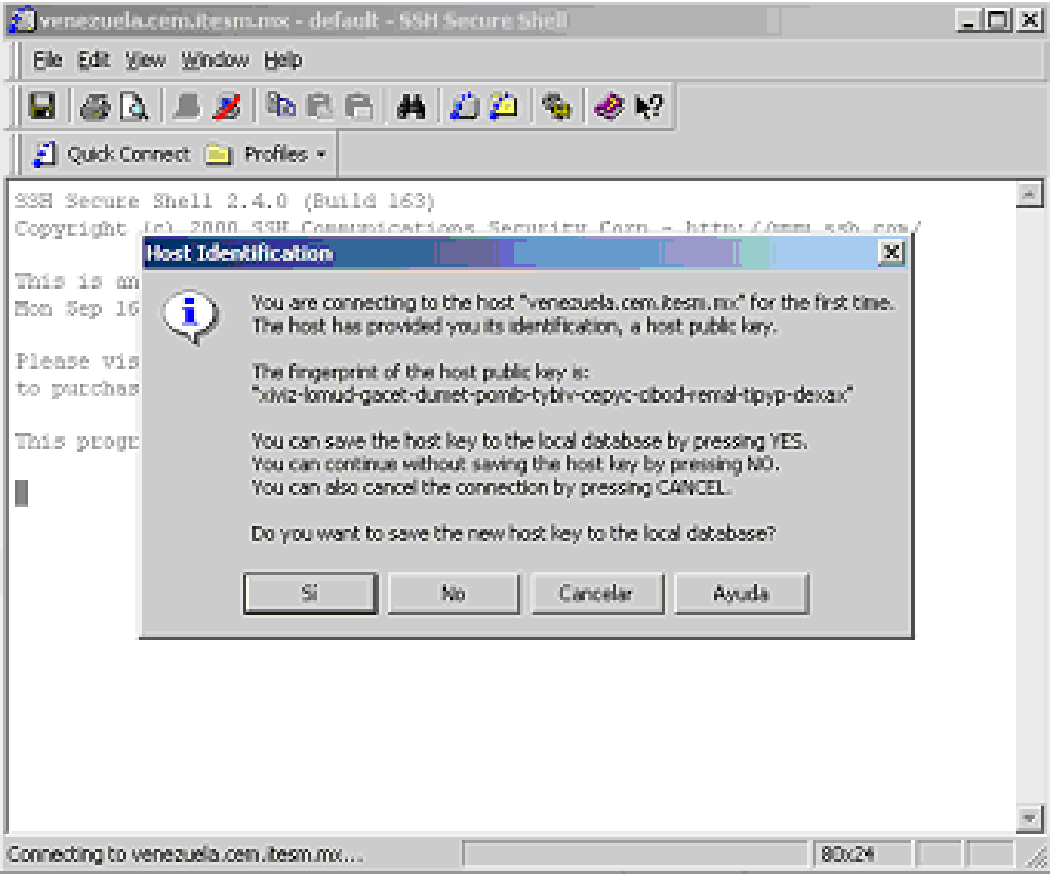
Autenticación usuario

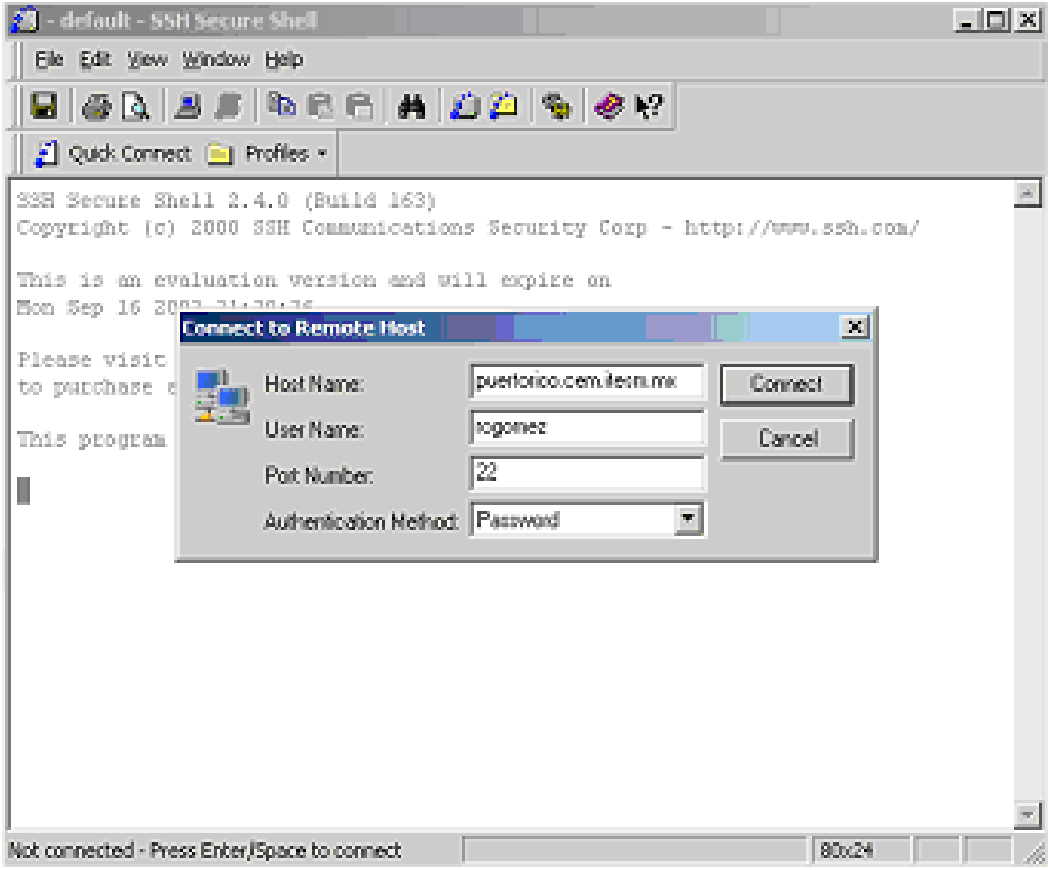
- Puede ser autenticado de diferentes formas
- Dialogo dirigido por el cliente
  - envía peticiones al servidor.
- Primera petición:
  - siempre solicita al usuario su login name.
- Servidor responde peticiones: un éxito o falla.
- Los métodos soportados actualmente son:
  - autenticación de password tradicional
  - combinación de autenticación .rhost con RSA basada en host
  - autenticación RSA pura
  - se incluye soporte para otros métodos

Diagrama autenticación host

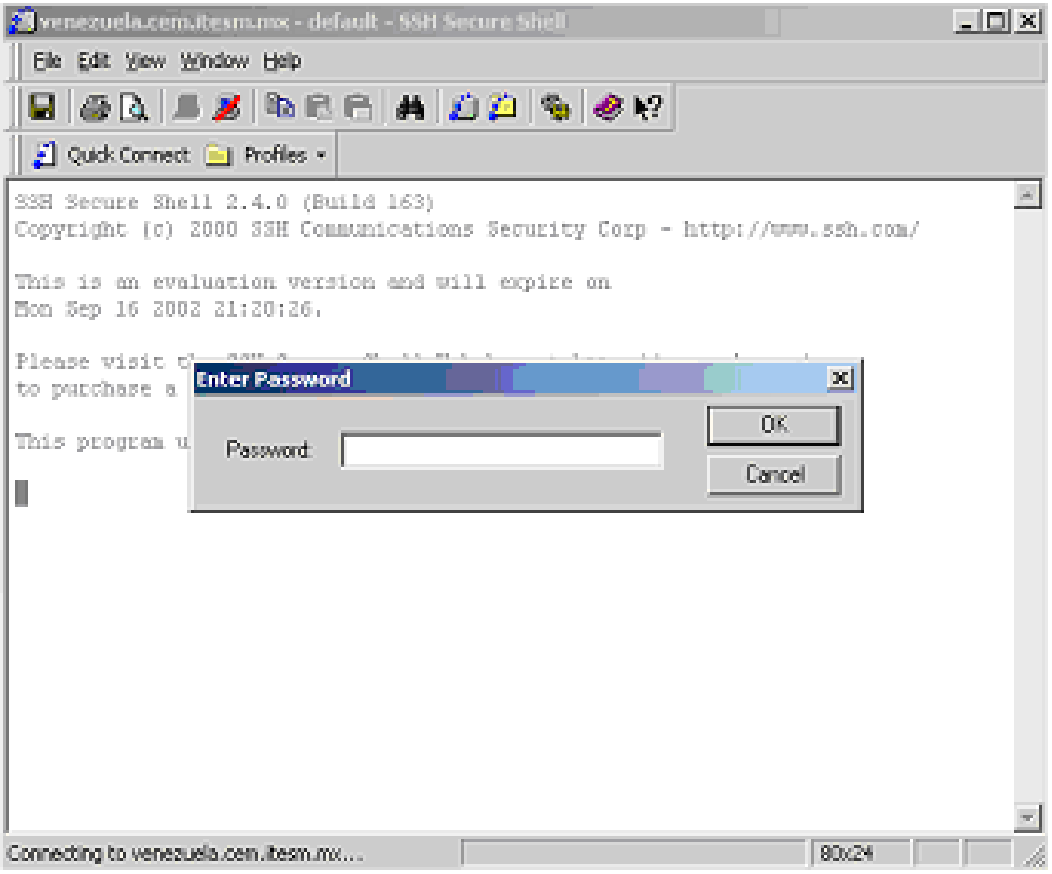


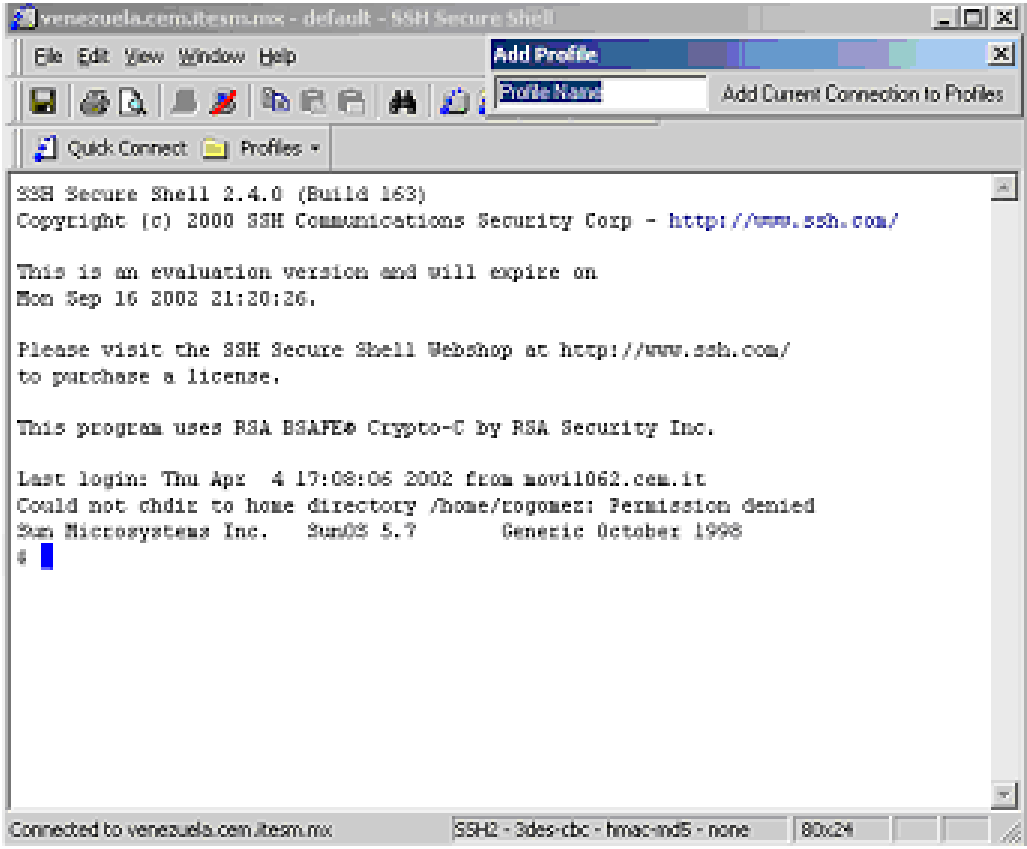
Ejemplo SSH (1/2)





Ejemplo SSH (2/2)





TECNOLÓGICO DE MONTERREY®

SSH vs SSL

- La capa en la que actúan
  - SSH: aplicación
  - SSL: transporte
- El método de autenticación
  - SSH: llaves
  - SSL: certificados

TECNOLÓGICO DE MONTERREY®

El protocolo PPP

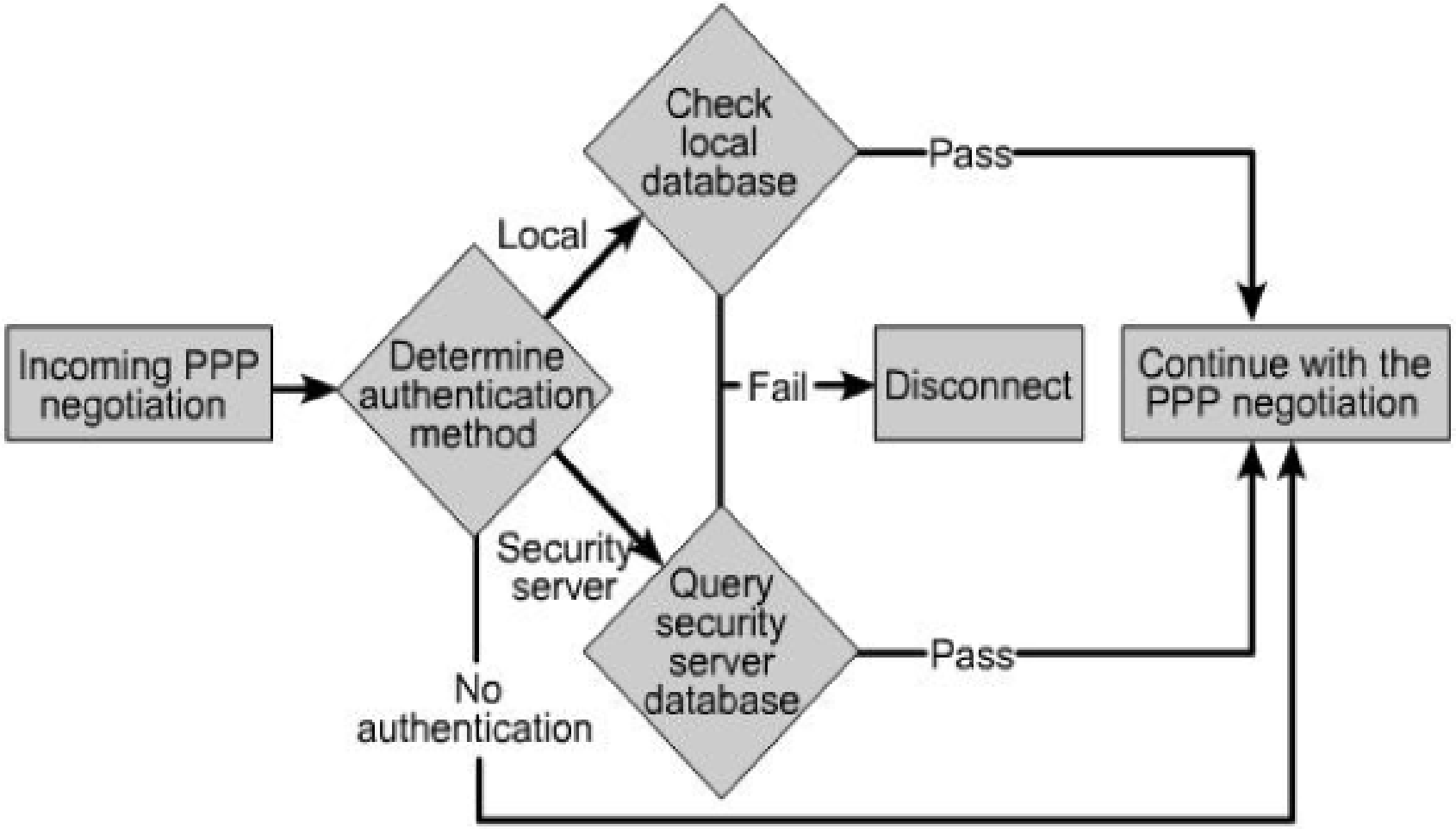
- Point-to-point Protocol se encarga de proveer un método estándar para transportar datagramas de múltiples protocolos sobre enlaces punto a punto.
- Protocolo que opera en la capa del nivel de enlace de datos.
  - se entiende por un enlace punto a punto aquel que conecta dos nodos directamente.
- Se han convertido en el protocolo elegido para conectar a los usuarios de casa con sus ISP’s sobre una conexión telefónica.

TECNOLÓGICO DE MONTERREY®

Autenticación PPP

- PPP provee básicamente dos esquemas de autenticación, en líneas asincrónicas se debe siempre configurar algún esquema de autenticación a diferencia que si esta usando PPP sobre enlaces punto a punto.
- Los dos esquemas básicos de autenticación que maneja PPP son:
  - PAP (Password Authentication Protocol, rfc 1334)
  - CHAP(Challenge-Handshake Authentication Protocol, rfc 1334)

Pasos para el proceso de autenticación

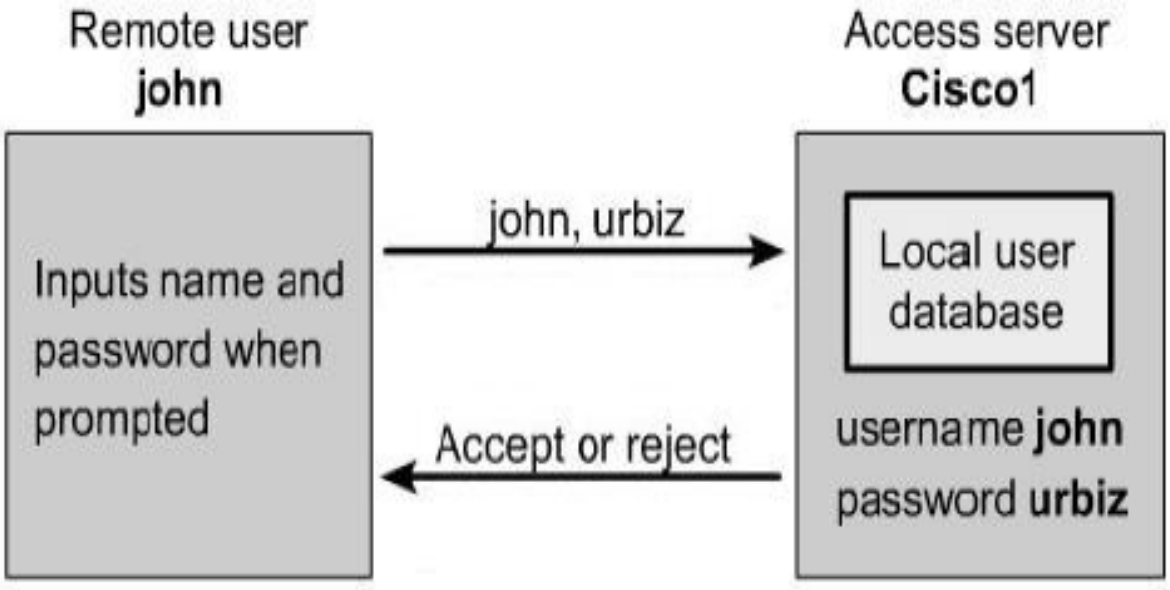


TECNOLÓGICO DE MONTERREY®

Protocolo PAP

- Password Authentication Protocol
- Provee un simple método de autenticación para que un peer (en un enlace punto a punto) se autentique utilizando un saludo de dos vías (two-way handshake).
- PAP no es un protocolo seguro de autenticación.
  - el enlace el password es enviado en texto claro
- De igual forma el control del número de intentos de conexión lo tiene el peer remoto mas no el servidor.
- PAP no provee ningún esquema de protección para intentos de un hacker de ensayo/error.
- PAP soporta autenticación bidireccional o unidireccional .

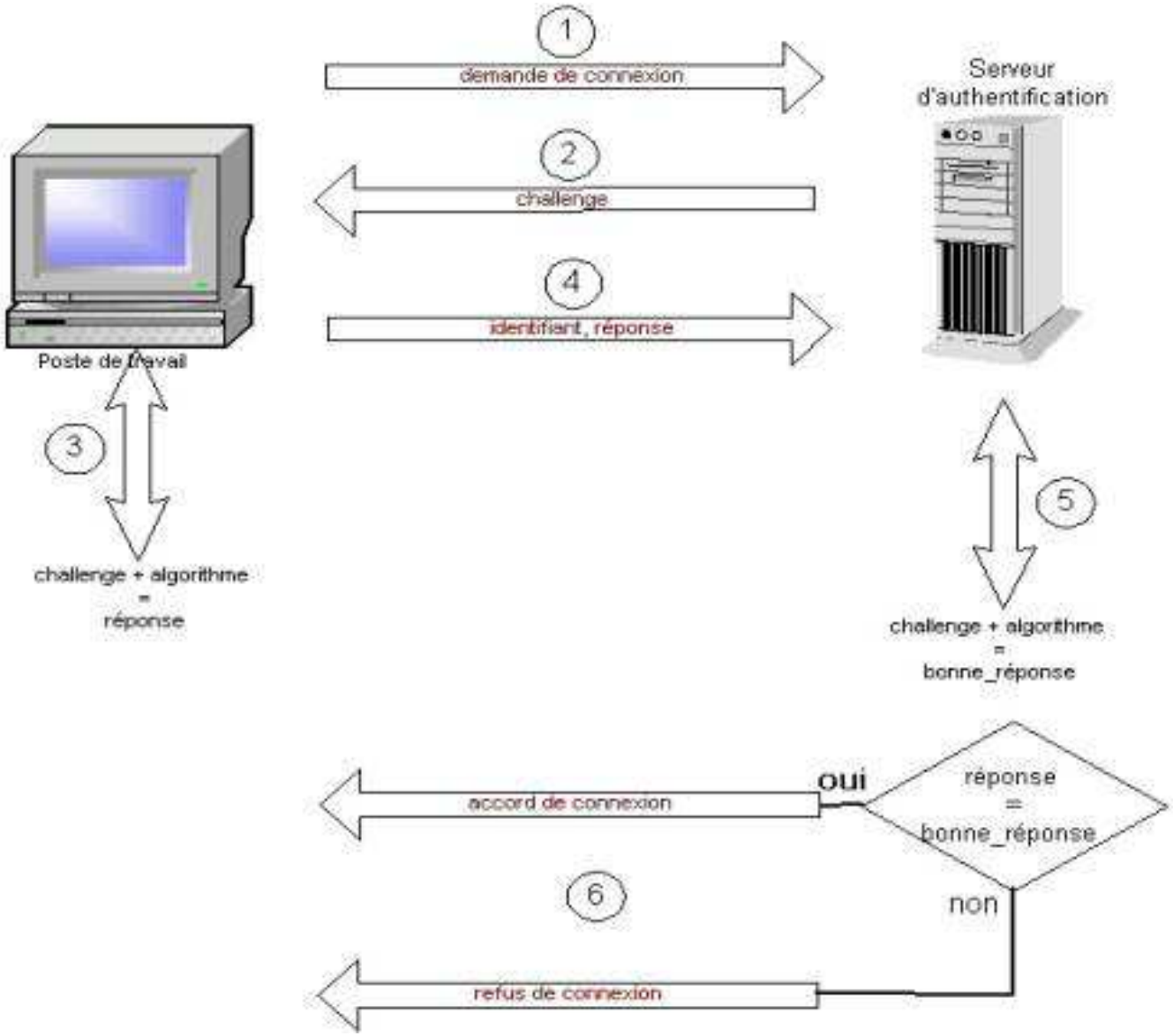
Esquema funcionamiento PAP



CHAP

- Challenge Handshake Authentication Protocol
- A diferencia de PAP, CHAP es usado para verificar periódicamente la identidad del peer usando un “3-way handshake”.
- Esto es hecho al inicio del establecimiento del enlace y puede ser repetido en cualquier momento después de que el enlace ha sido establecido.
- CHAP es considerado un protocolo mas seguro y debe ser usado cuando sea posible.
  - solo se recomienda utilizar PAP cuando los equipos no soporten CHAP.
- Con CHAP el control del número de intentos para autenticarse no lo tiene el nodo remoto si no el server.
- Este método de autenticación depende de un “secreto” que solo es conocido por los peers y que en ningún momento es enviado sobre el enlace.

Funcionamiento CHAP



TECNOLÓGICO DE MONTERREY®

Desventaja CHAP

- Los clientes estándar de CHAP usan la versión de texto claro del password (i.e. password decriptado) para crear el reto del CHAP challenge response
- Debido a lo anterior los passwords deben ser almacenados “en claro” dentro del servidor, para poder calcular la respuesta.

TECNOLÓGICO DE MONTERREY®

MS-CHAP v1

- Microsoft Challenge Handshake Authentication Protocol
- Variante de CHAP que no requiere que una versión “en claro” del password sea almacenada en el servidor.
- El servidor remoto solo requiere el hash MD4 del password para validar la respuesta del reto.
- En Windows 2000, el password del usuario es almacenado como un hash MD4 (NT hash).

TECNOLÓGICO DE MONTERREY®

MS-CHAP v2

- Proporciona autenticación mutua
  - cliente autentica al servidor
  - servidor envía también un challenge al cliente y este lo verifica
- El hash LAN Manager ya no es utilizado junto con el hash NT
  - prevenir que software de crack de passwords como L0phtcrack rompan el hash débil de LAN Manager y después usen esta información para romper el hash NT que es más fuerte
- Modificación en los paquetes de cambio de passwords

TECNOLÓGICO DE MONTERREY®

Diferencias entre MS-CHAP v1 y v2

MS-CHAP v1	MS-CHAP v2
Negocia CHAP con valor algoritmo 0x80	Negocia CHAP con valor algoritmo 0x81
Servidor envía un valor de challenge de 8 bytes	Servidor envía un valor de 16 bytes para ser usado por el cliente para crear un valor de challenge de 8 bytes
Cliente envía 24 bytes LANMAN y 24 bytes NT response al challenge de 8 bytes	Cliente envía 16 bytes de challenge que fue usada en crear el challenge de 8 bytes y los 24 bytes de NT response
Servidor envia una respuesta de éxito o fracaso-	Servidor envía una respuesta de éxito o falla y “piggybacks” un Authenticator Response al challenfe de 16 bytes de la contraparte
Cliente decide si continua o termina de acuerdo a la respuesta anterior.	Cliente decide continuar o terminar de acuerdo a la respuesta anterior. Aparte el cliente verifica la validez del Authenticator Response y se desconecta si no es el valor correcto

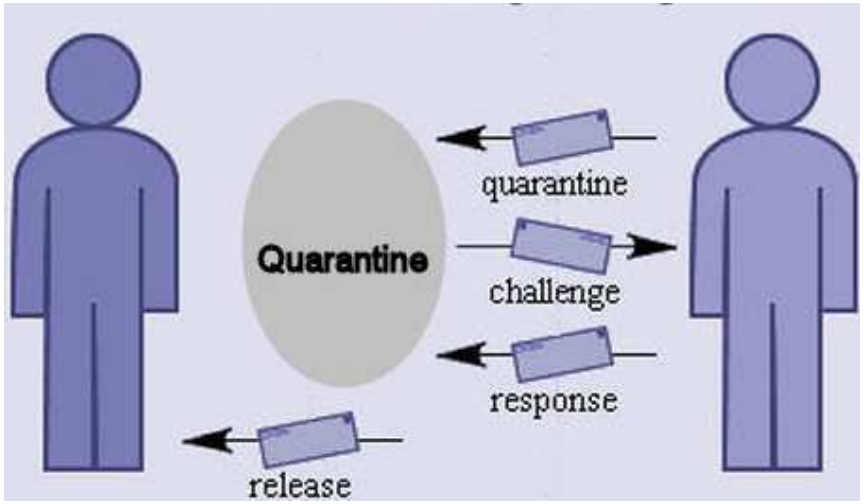
Protocolos de autenticación

- Alicia proporciona su identidad a Beto realizando una operación criptográfica en un número que Beto le proporciona
- La operación criptográfica realizada por Alicia se basa en el secreto de Alicia

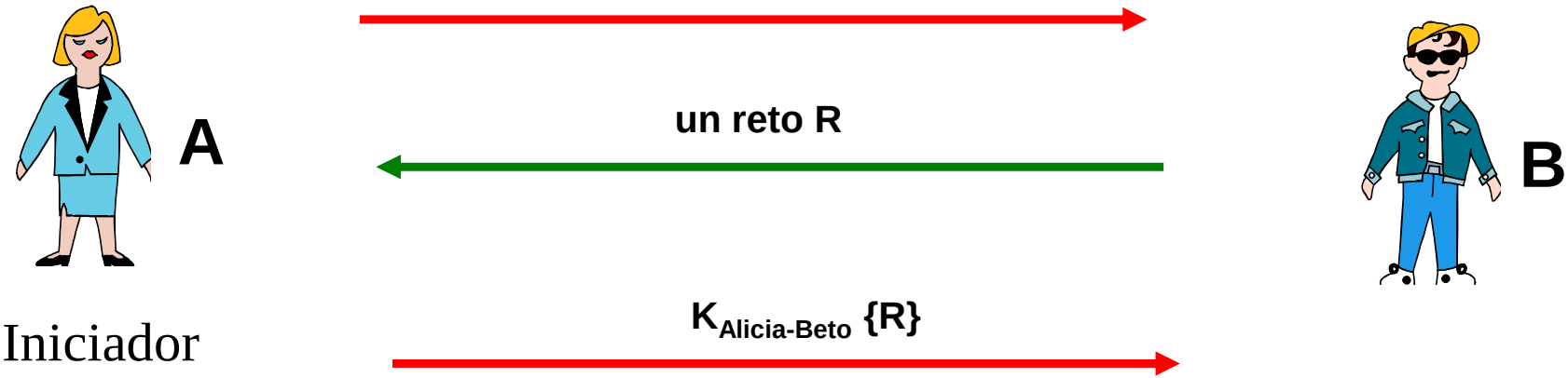
Protocolos de autenticación

- Secreto compartido

- Reto/respuesta (challenge/response)



Secreto compartido (shared secret)



Two one way authenticacion protocolos

Iniciador

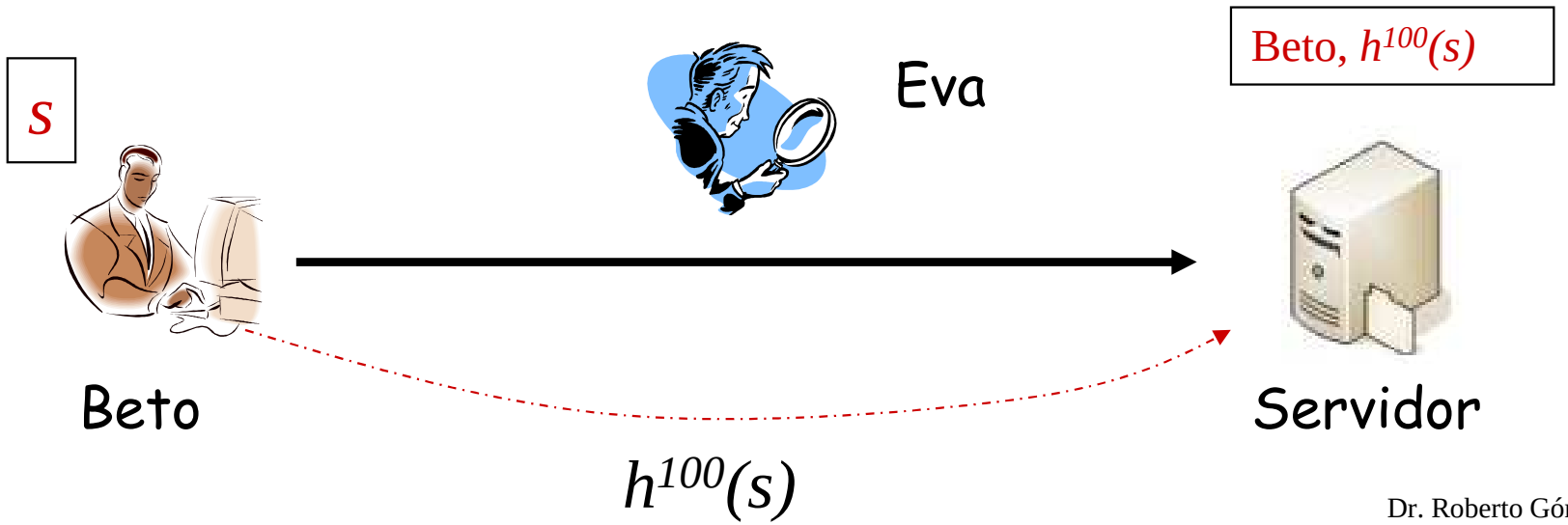
Beto autentica Alicia basado en la firma de Alicia del reto que envía

Iniciador

Beto autentica Alicia si ella puede decriptar un mensaje encriptado con su llave pública

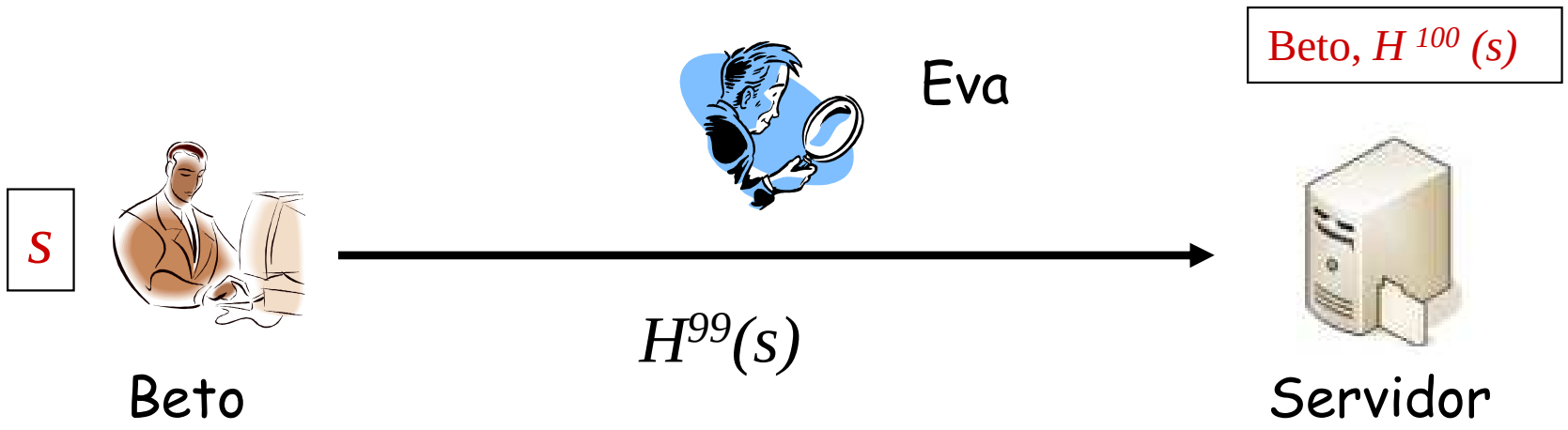
El hash de Lamport

- Autenticación basada en funciones hash.
- Fase de registro:
  - Usuario elige un secreto s.
  - Calcula $h^n(s)$
    - $h^n(s) = h(h(... \text{ n veceses...}(h(s))...))$
  - Almacena, o envía de forma segura, este valor en el servidor.



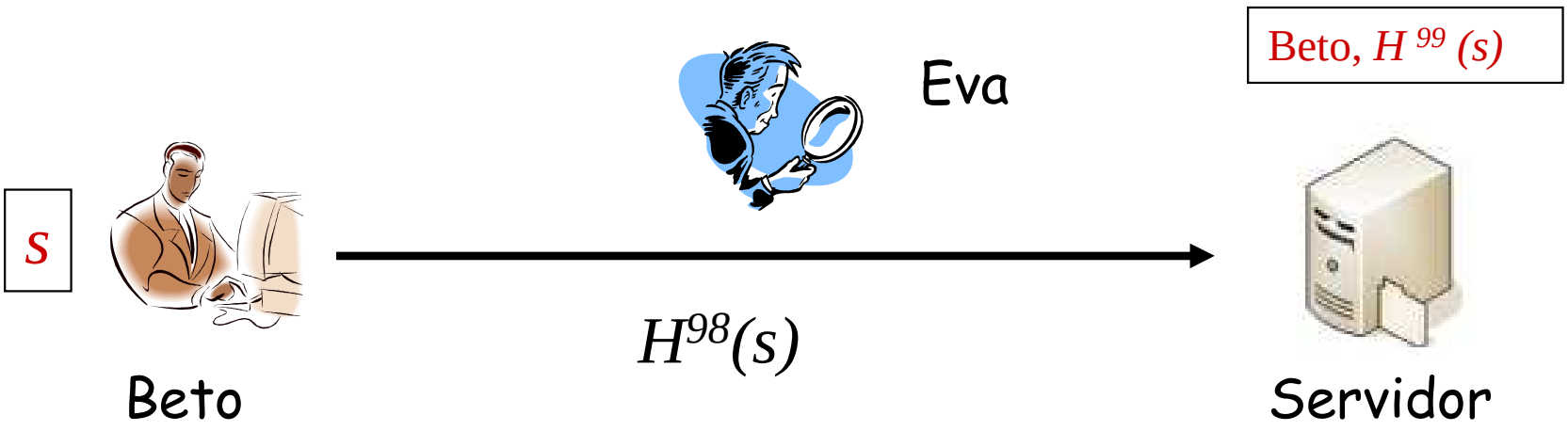
Primera autenticación

- Asumiendo un valor de n=100.
- Beto envía su primera contraseña, $p_1=h^{99}(s)$ al servidor.
- Servidor autentica a Beto verificado que $h(p_1) = h^{100}(s)$
- Si la autenticación tiene éxito, el servidor reemplaza $h^{100}(s)$ con $p_1=h^{99}(s)$

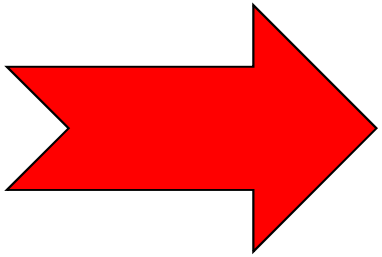


Segunda autenticación

- Beto envía su segunda contraseña, $p_2=h^{98}(s)$ al servidor.
- Servidor autentica a Beto verificado que $h(p_2) = h^{99}(s)$
- Si la autenticación tiene éxito, el servidor reemplaza $h^{99}(s)$ con $p_1=h^{98}(s)$



Ambiente humano y de papel: SKEY



PASSWORD01
PASSWORD02
PASSWORD03
PASSWORD04
PASSWORD05
PASSWORD06
PASSWORD07
PASSWORD08
PASSWORD09
PASSWORD10
PASSWORD11
PASSWORD12

Ejemplo fase de registro

- Sea una semilla S = 71890 y n = 5

Sistema calcula los hash

$h^1(s) = h(71890) = 8a9ef$
$h^2(s) = h(8a9ef) = 71821$
$h^3(s) = h(71821) = 47aef$
$h^4(s) = h(47aef) = 12345$
$h^5(s) = h(12345) = 67890$

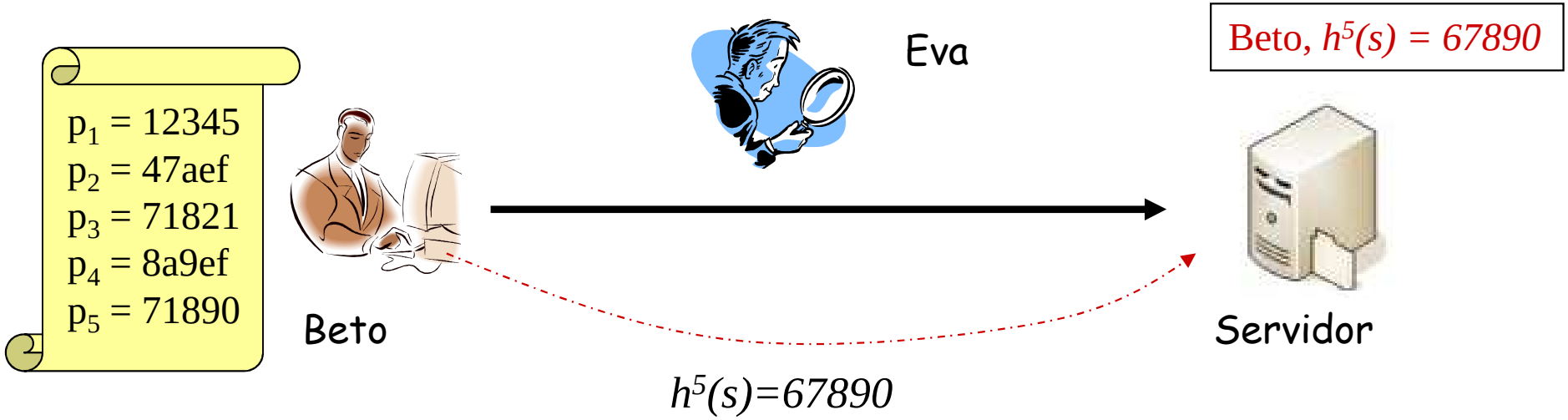
Se entregan los passwords al usuario

$p_1 = 12345$
$p_2 = 47aef$
$p_3 = 71821$
$p_4 = 8a9ef$
$p_5 = 71890$

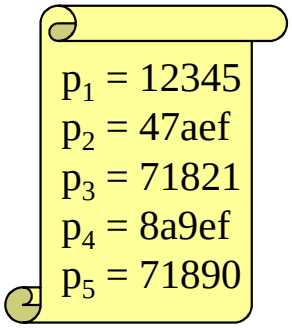
Sistema almacena

$h^5 = 67890$

y valor de n = 5



Ejemplo autenticación



Beto

Eva

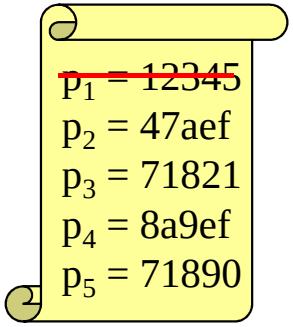
Servidor

Beto, 67890

$h^4(n) = 12345$

¿h(12345) = 67890?

Se substituye 67890 por 12345



Beto

Eva

Servidor

Beto, 12345

$h^3(n) = 47aef$

¿h(47aef) = 12345?

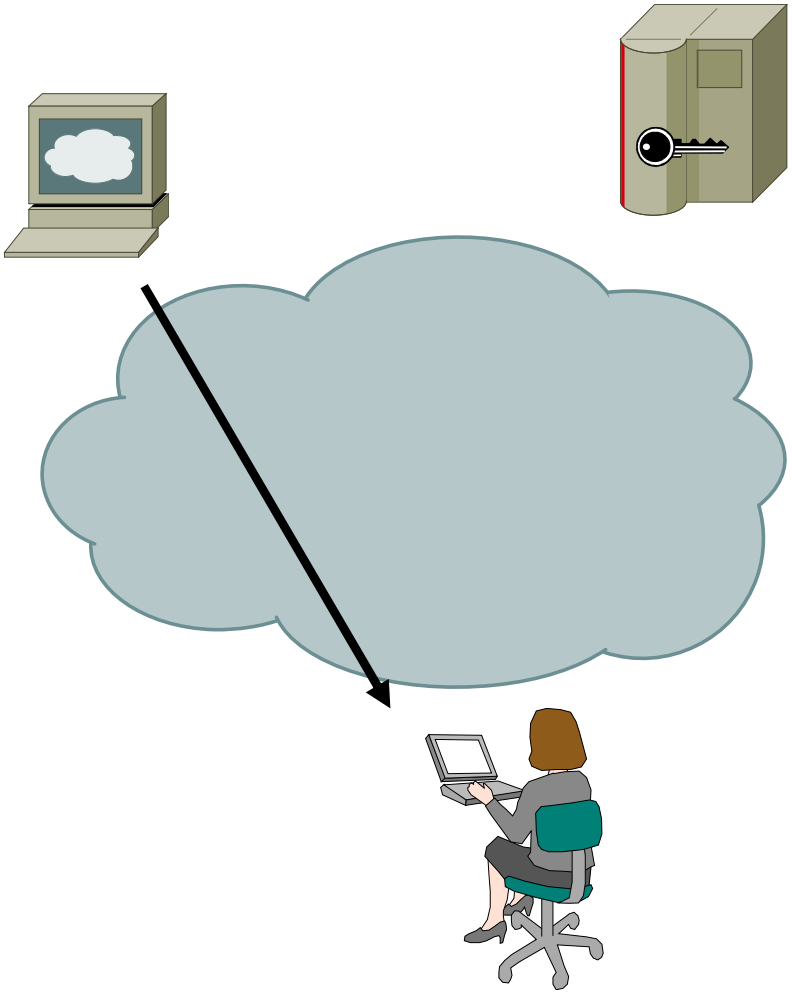
Se substituye 12345 por 47aef

TECNOLÓGICO DE MONTERREY®

OTP: One Time Password

- RFC 2289, extensiones OTP: RFC 2243
- Un sistema OTP garantiza un nuevo password en cada conexión
  - usuario establece secreto en el servidor remoto
  - usuario tiene una calculadora en software o en hardware
  - al autenticarse, el servidor envía su reto en forma de string
  - usuario responder calculando reto+secreto
  - resultado (password) copiado en la ventana de login
  - servidor verifica la respuesta

Tokens: OTP Challenge-response



System

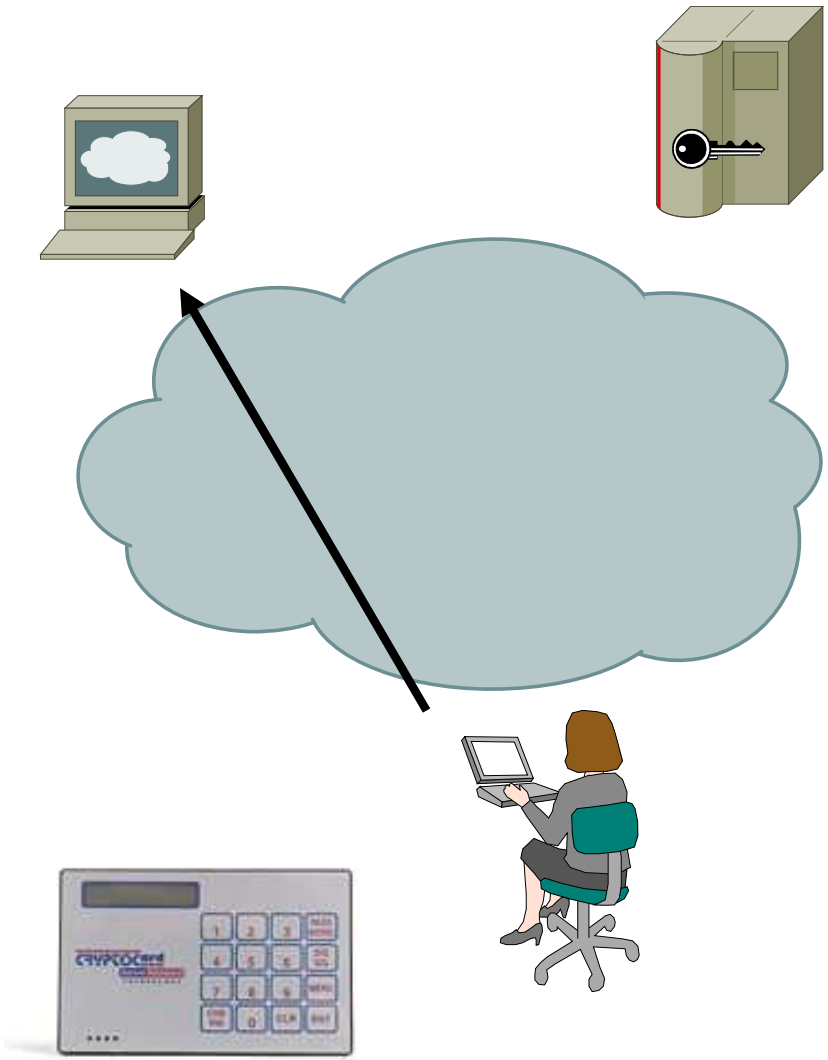
1) Request username:

3) Challenge (4230618)
4) Request password:

User

2) Enter: toto

Tokens: OTP Challenge-response



System

1) Request username:

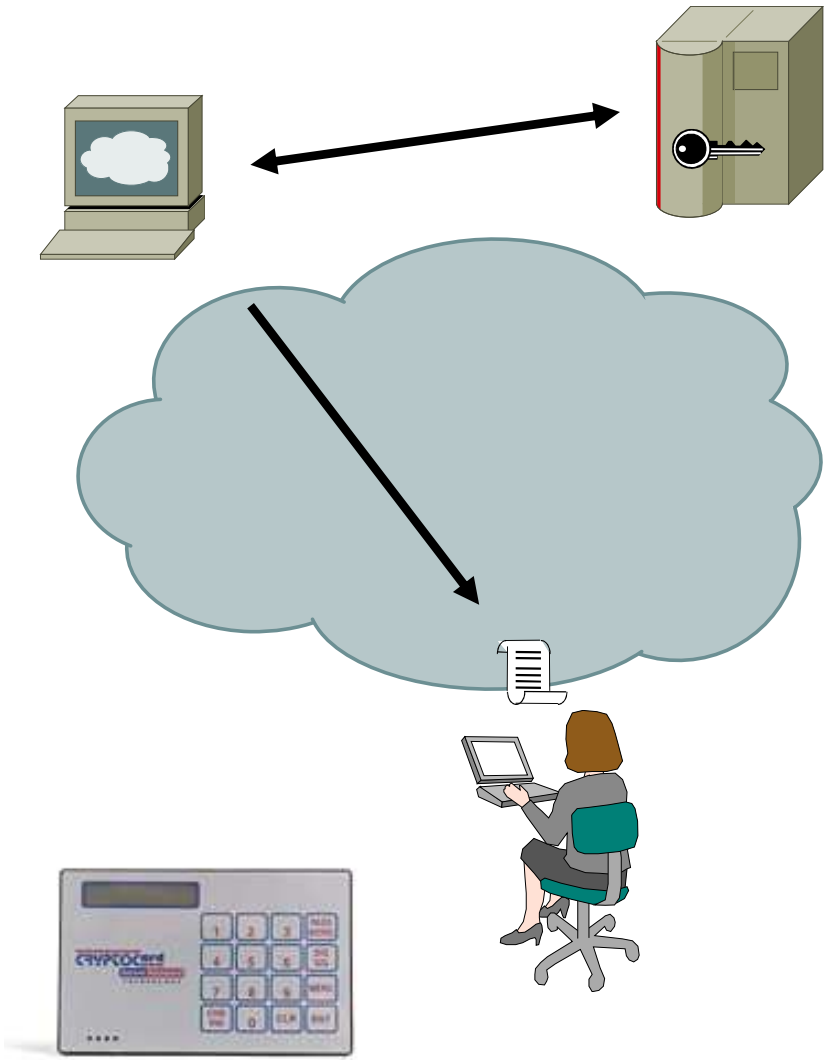
3) Challenge (4230618)
4) Request password:

User

2) Enter: toto

5) Unlock token with PIN
6) Enter challenge in token (4230618)
7) Token responds with OTP password (0923735)
8) Enter: 0923735

Tokens: OTP Challenge-response



System

1) Request username:

User

2) Enter: toto

3) Challenge (4230618)
4) Request password:

5) Unlock token with PIN
6) Enter challenge in token (4230618)
7) Token responds with OTP password (0923735)
8) Enter: 0923735

9) Checks with authentication sever
10) Login successful/not

Ejemplo calculadora: Token

```
Login:    JSMITH
Passcode: 2468234836
```

PASSCODE = PIN + TOKENCODE

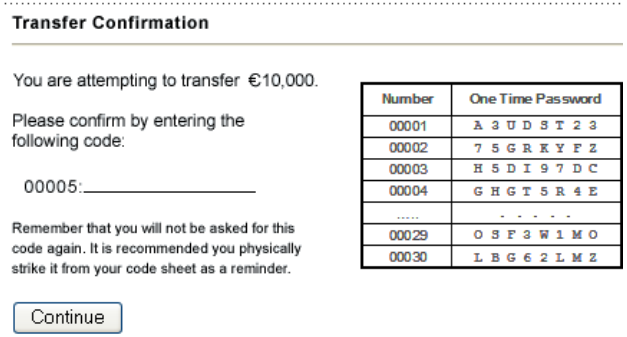
Token code: Changes every 60 seconds

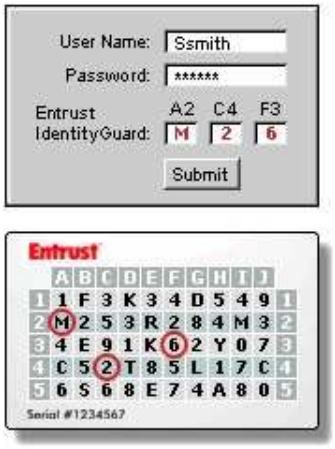
Clock synchronized to UCT

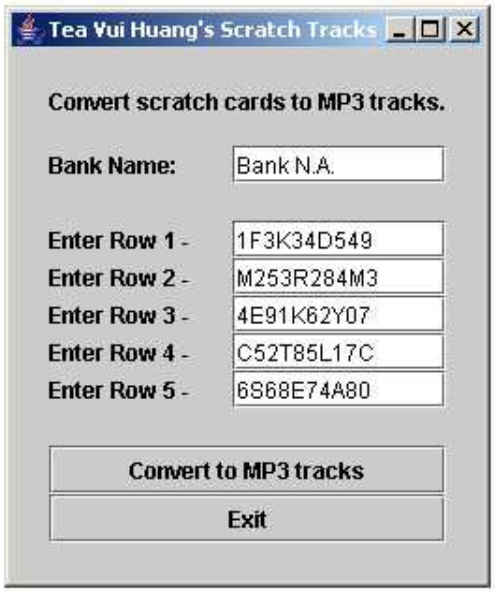
Unique seed

Tipos One Time Password

- Time based
- Event based
- Challenge-response based

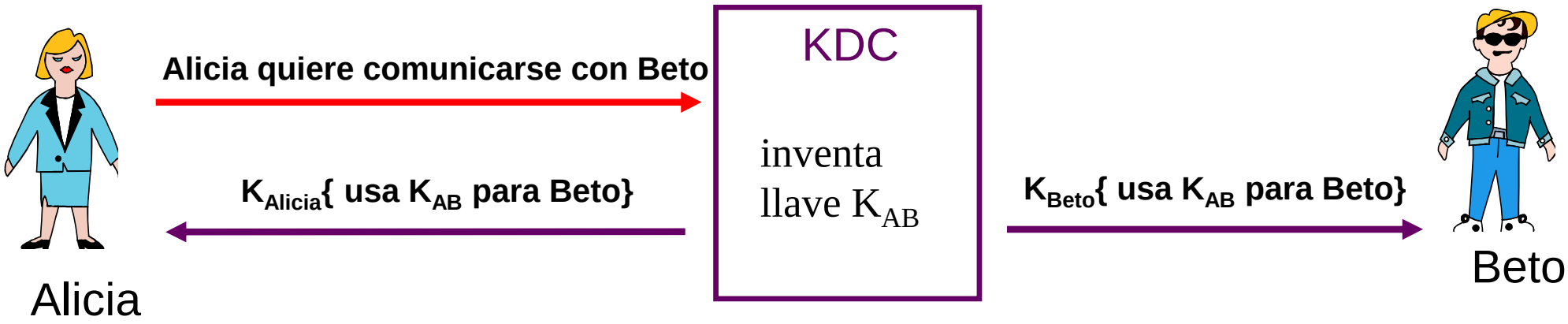




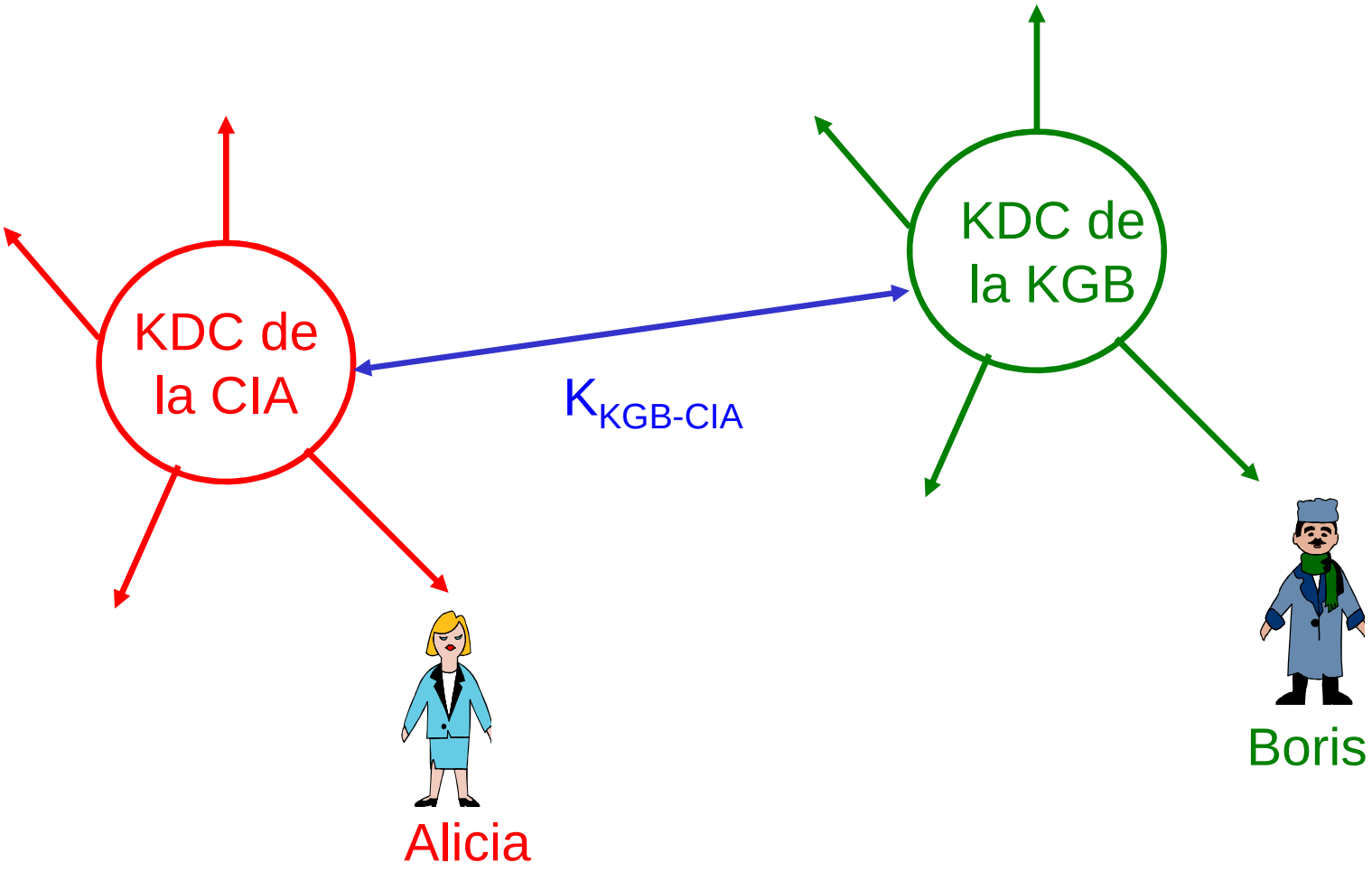


Key Distribution Center

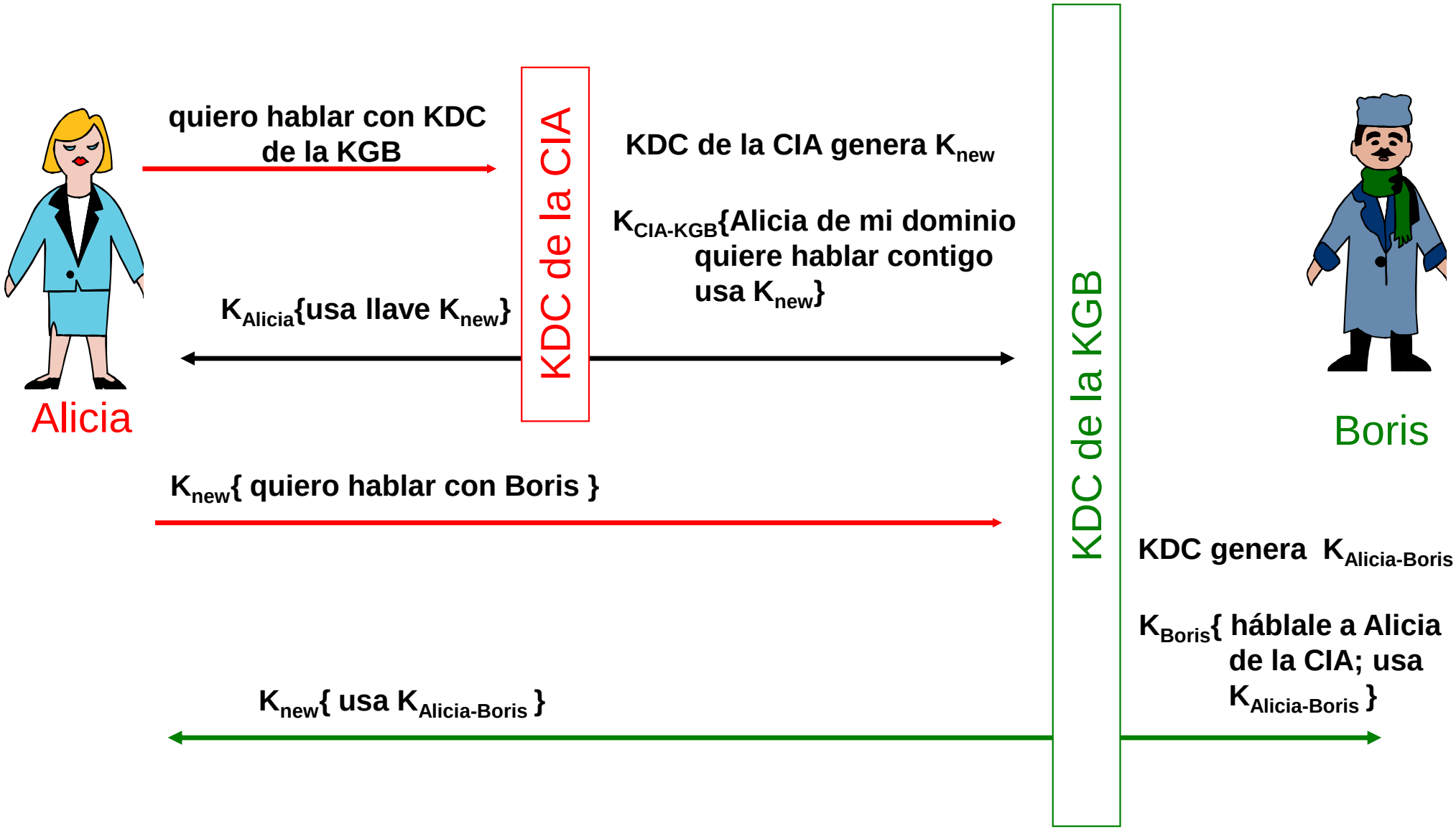
- El KDC conoce las llaves de todos los nodos.
- Si un nuevo nodo es instalado en la red, solo ese nuevo nodo y el KDC necesitan ser configurados con la llave para ese nodo.



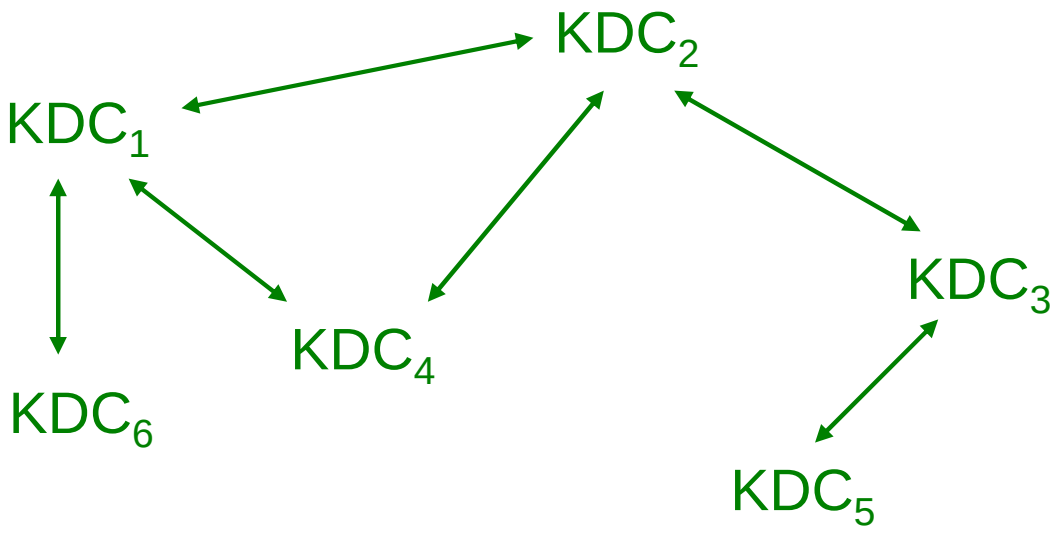
Multiple domain example

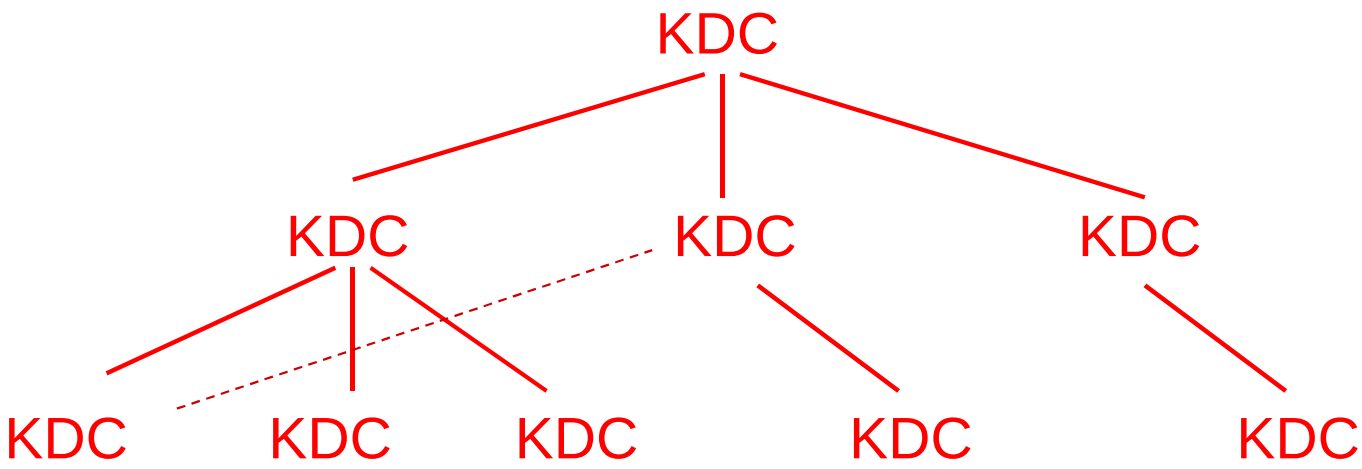


Protocolo múlti-dominio

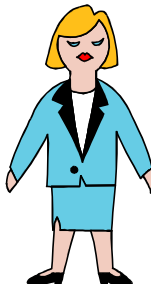


Topological KDC structures





Uso de tickets



Alicia

Alicia quiere comunicarse con Beto

K_{Alicia}{ usa K_{AB} para Beto}
ticket Beto = K_{Beto}{usa K_{AB} para Alicia}

KDC

inventa llave K_{AB}

Beto

"Soy Alicia", ticket = K_{Beto}{ usa K_{AB} para Alicia}

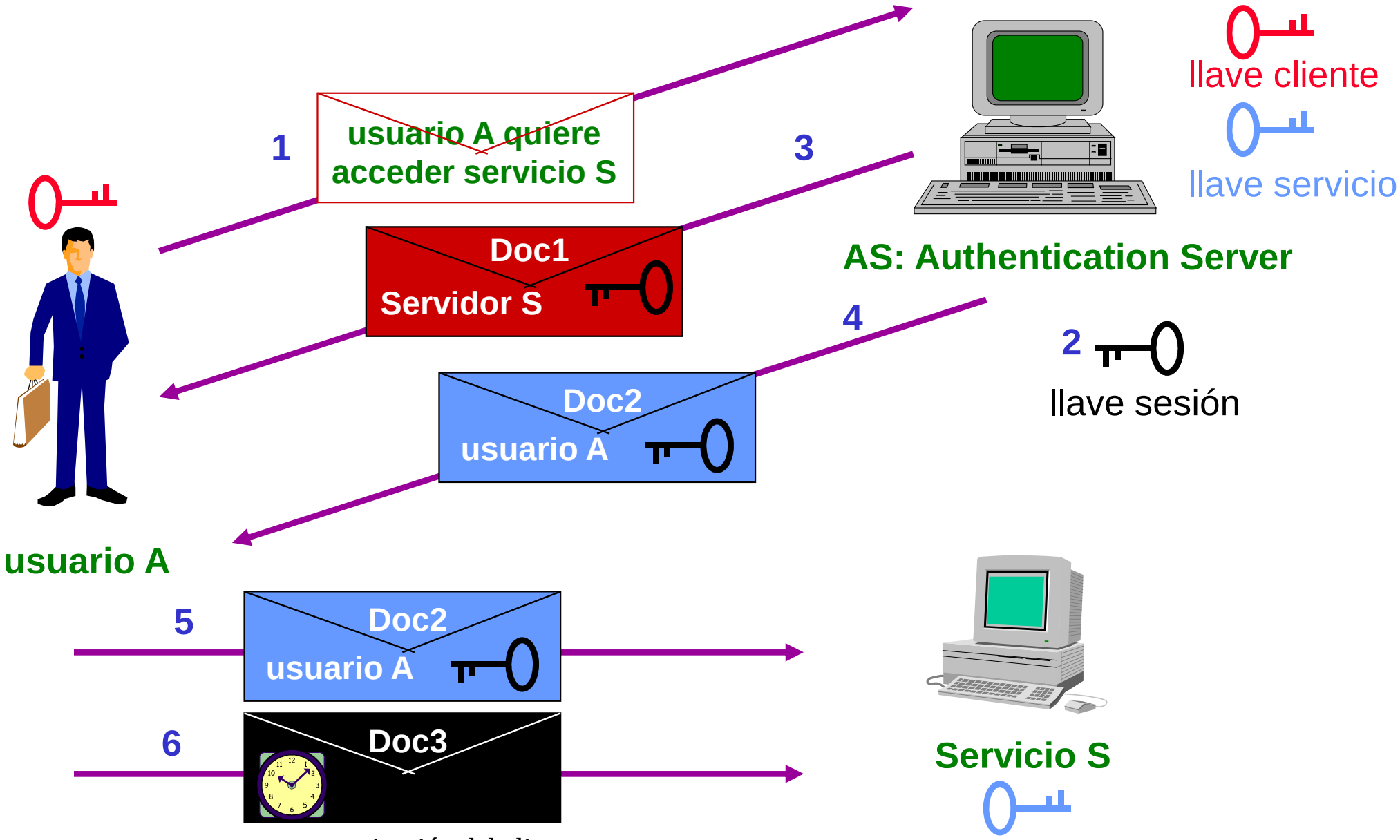
KERBEROS

Kerberos o Cancerbero (de can y cerbero) .

Mit. Perro de tres cabezas que, según la fábula, guardaba la puerta de los infiernos.

Real Academia Española, Diccionario de la Lengua Española.

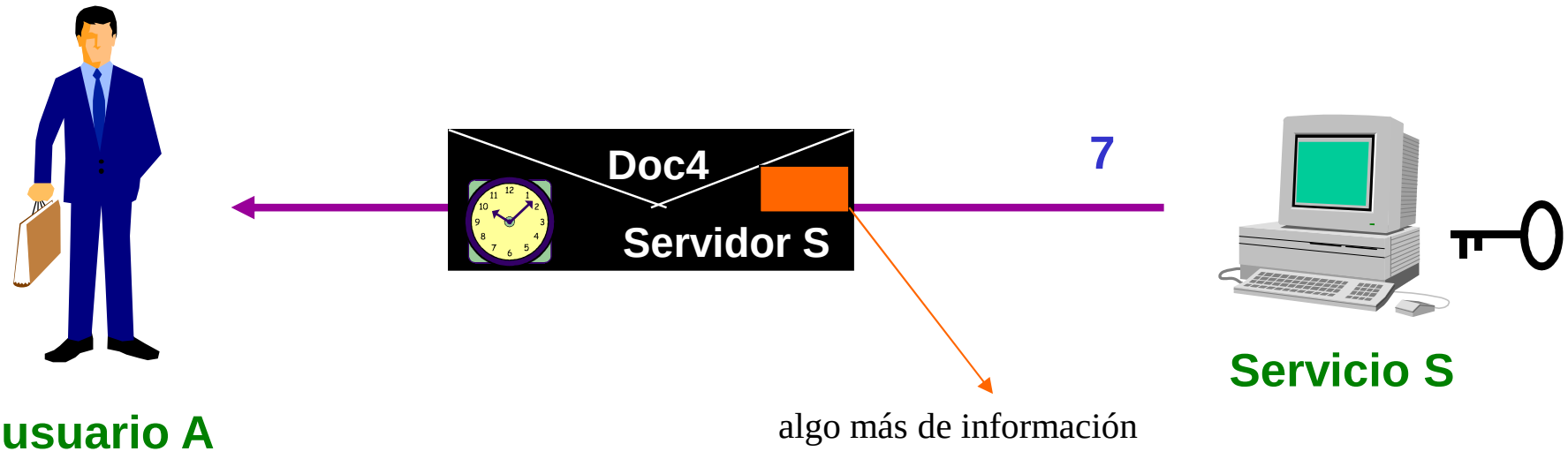
Principio base Kerberos



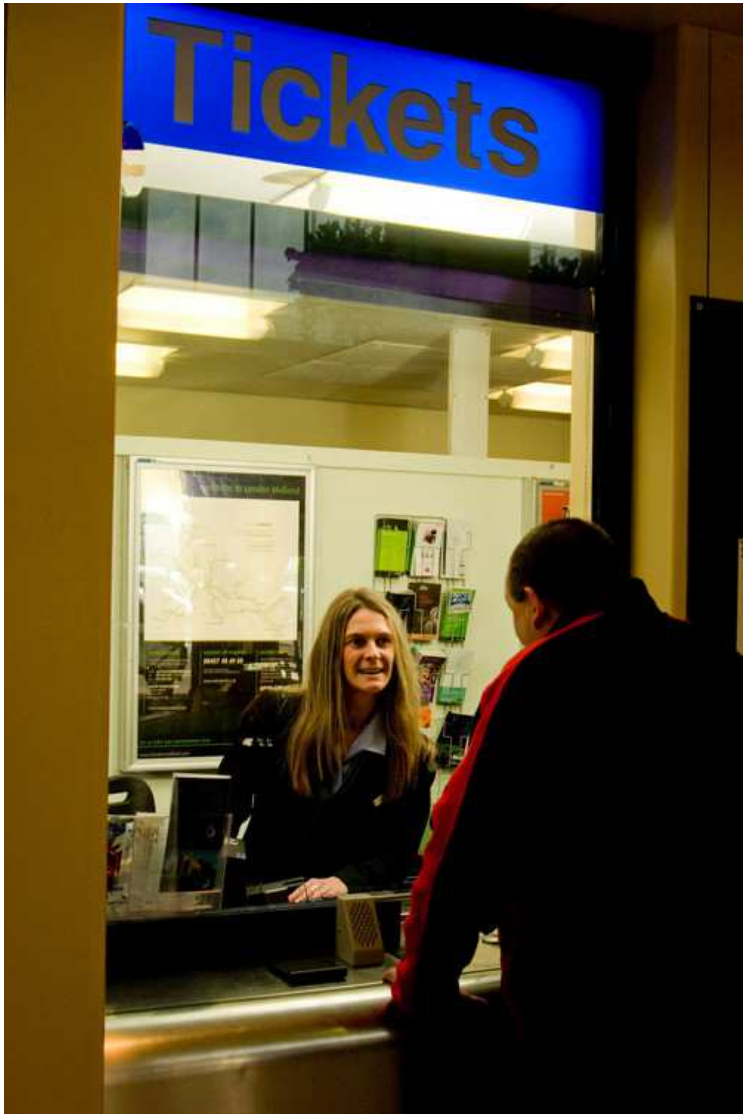
para autenticación del cliente

¿¿Y??

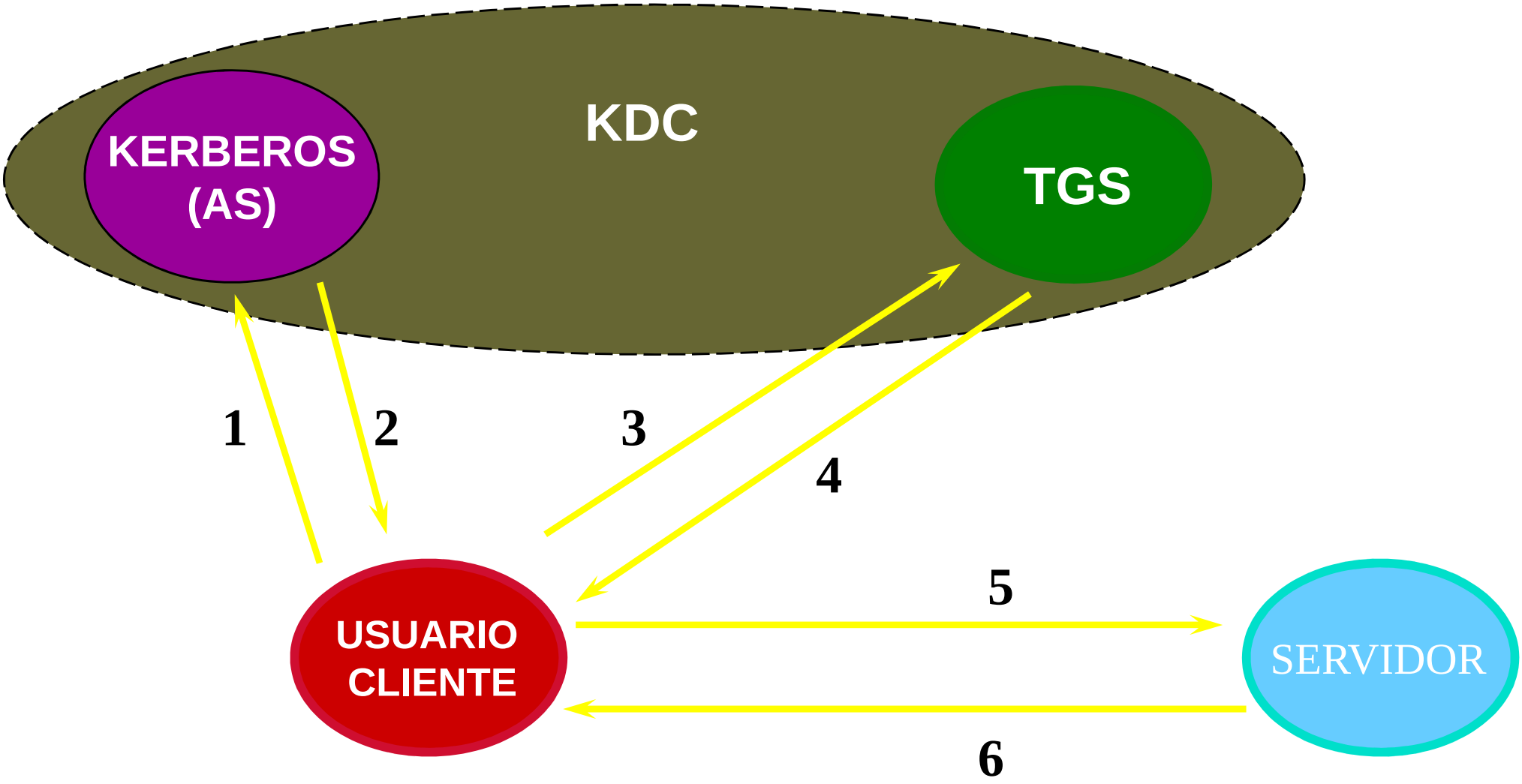
- Desde el punto de vista del protocolo de Kerberos:
  - Doc2 es el ticket
  - Doc3 es el autenticador
- Posible autenticar al servidor:



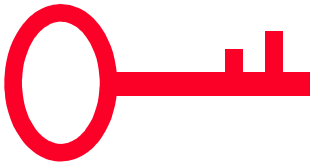
El TGS

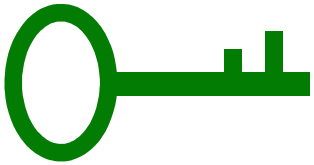


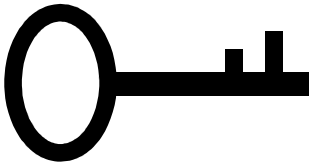
El protocolo Kerberos

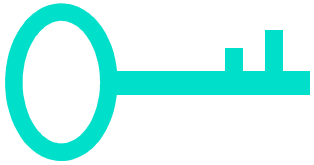


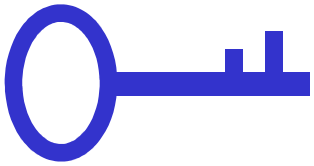
Tipos de llaves

1  Llave secreta del Cliente

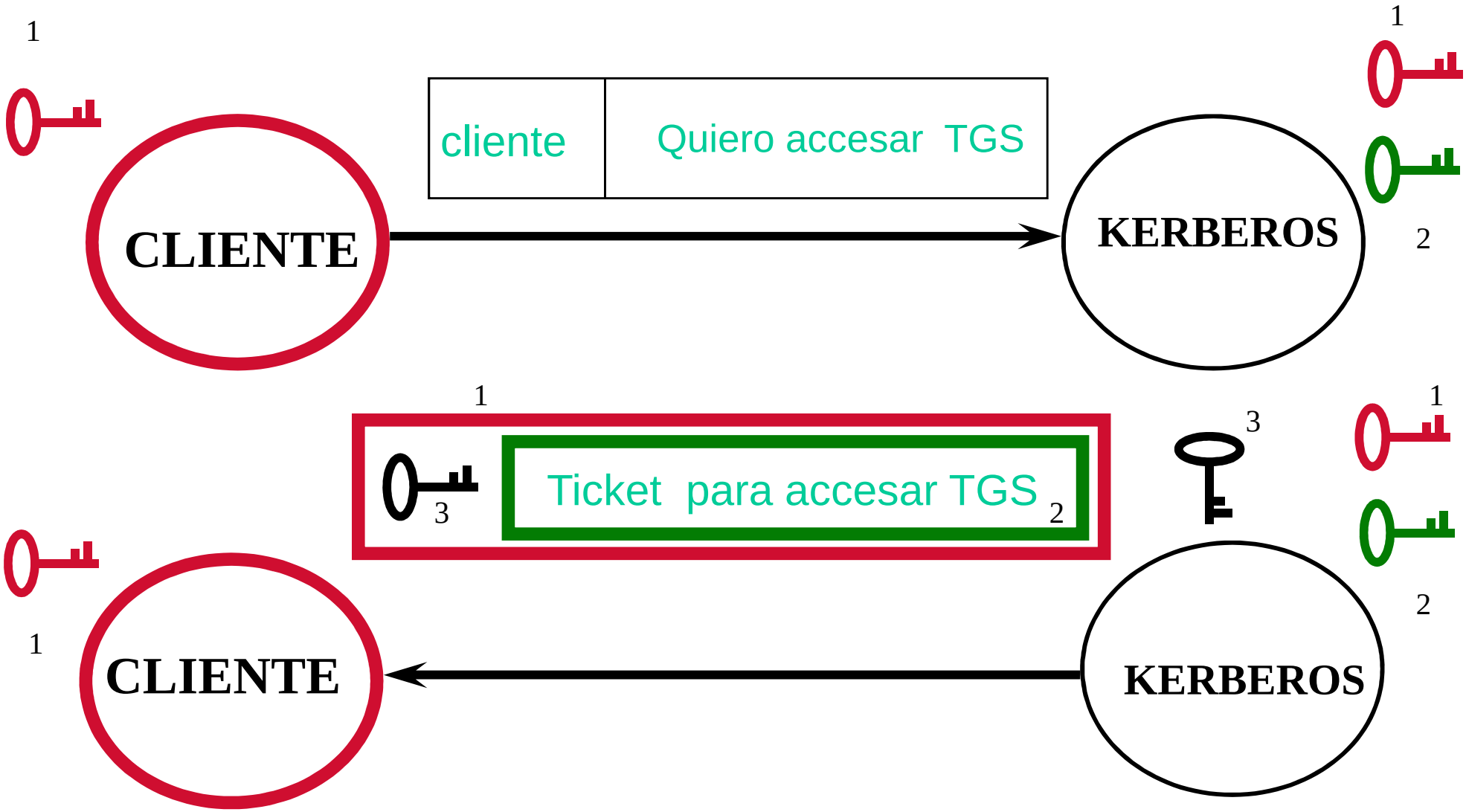
2  Llave secreta del TGS

3  Llave de sesión entre el Cliente y el TGS

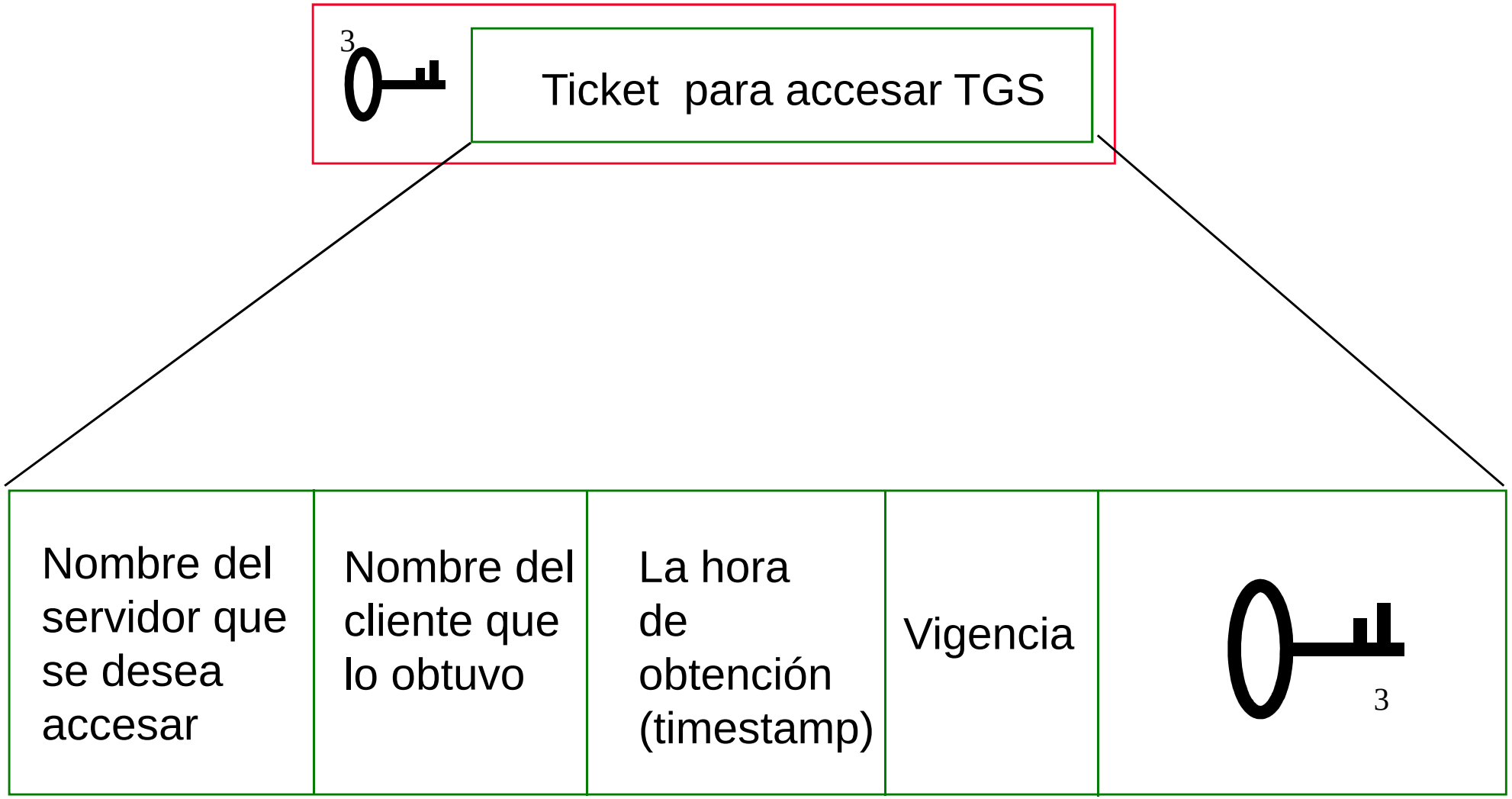
4  Llave secreta de un Servidor

5  Llave de sesión entre el Cliente y un Servidor

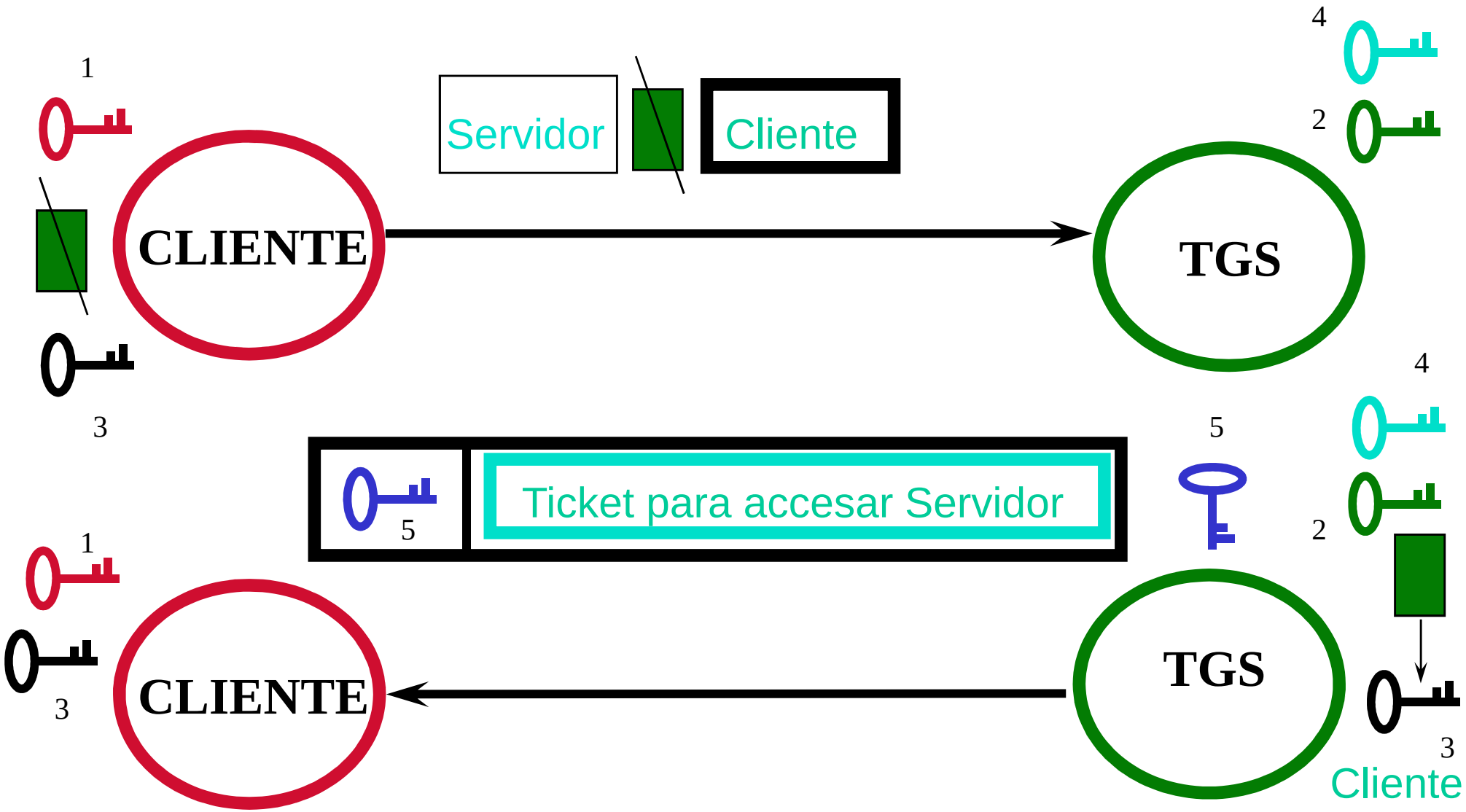
Solicitud de Ticket Inicial



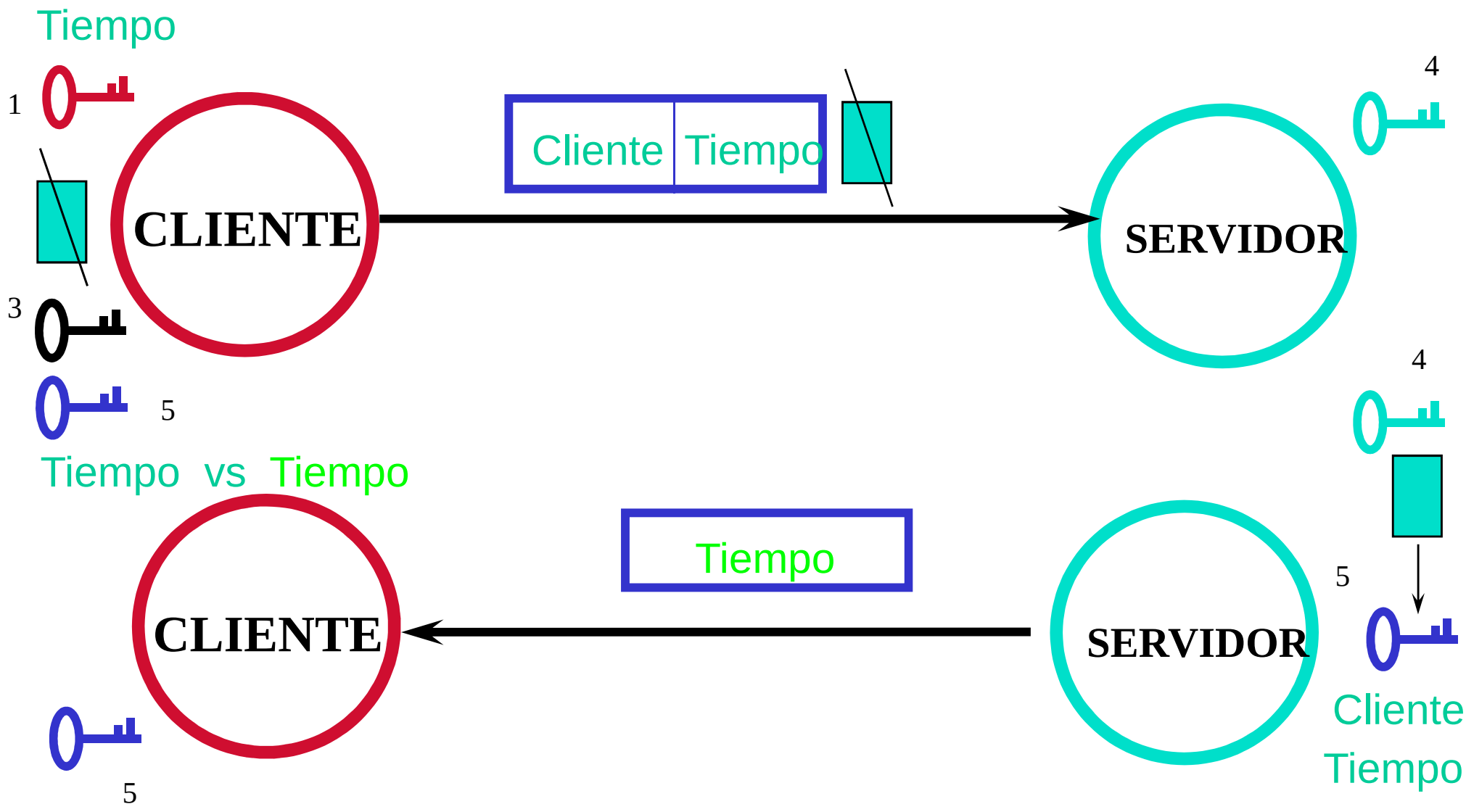
¿Qué tiene el TICKET del TGS?



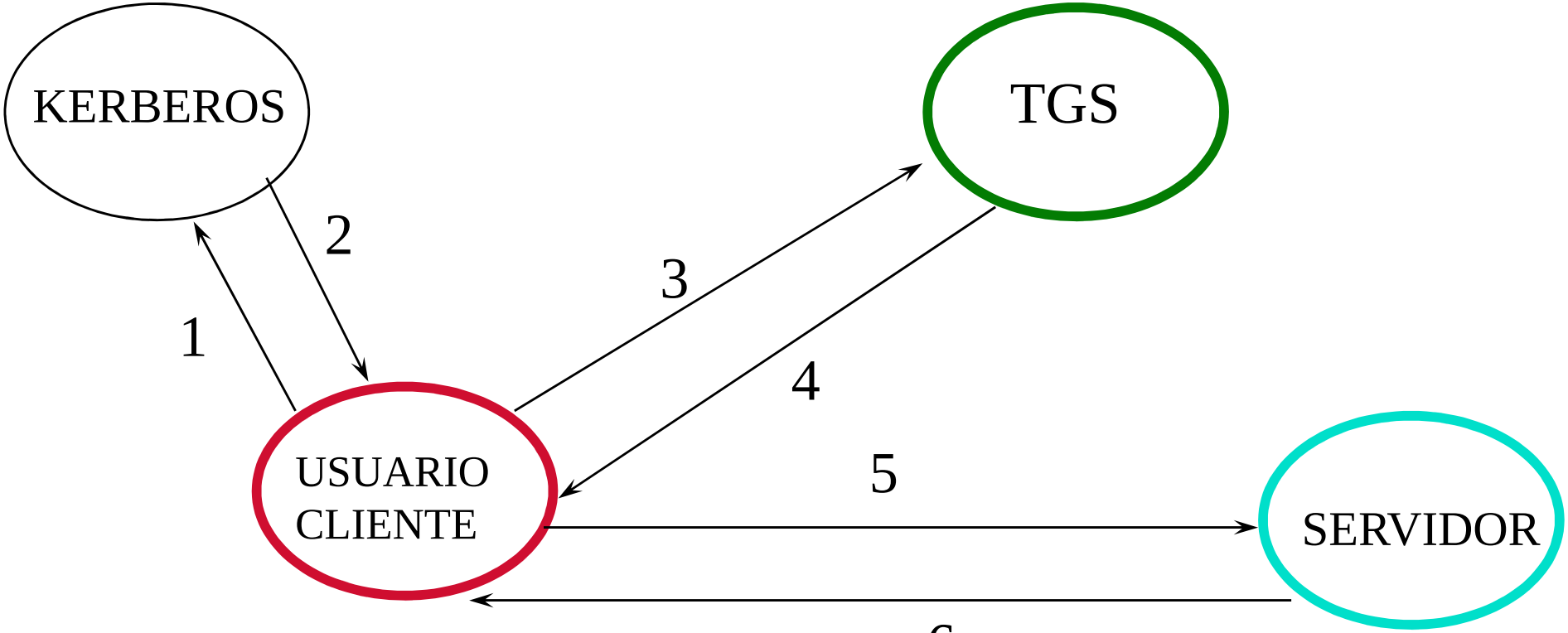
Solicitud de Ticket de Servidor



Solicitud de Servicio y Autentificación Mutua



Resumiendo ...



1) SOLICITUD DE TICKET PARA TGS
2) TICKET PARA EL TGS
3) SOLICITUD DE TICKET PARA SERVIDOR
4) TICKET PARA SERVIDOR
5) SOLICITUD DE SERVICIO
6) AUTENTIFICACION DEL SERVIDOR

Realms o Reinos

TECNOLÓGICO DE MONTERREY®

Algunas adecuaciones a Kerberos

- Kerberos de llave pública
- Kerberos y smart cards
- Kerberos y biómetricos
- SESAME
  - extensión kerberos con servicios adicionales
  - proporciona servicios de autenticación y autorización y asignación de derechos de acceso
  - soporta tanto autenticación en base a passwords o en base a llave pública