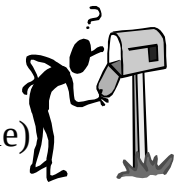
Seguridad en Internet

Nivel del Aplicación

- SSH (Secure Shell)
  - Cifra conexión (autenticación + información)
  - Ideal para teletrabajo y gestión remota
  - http://www.cs.hut.fi/ssh
- Kerberos
  - Autor: MIT
  - Sistema autenticación por tickets
  - Debemos “kereberizar” aplicaciones

Correo electrónico

- PGP (Pretty Good Privacy).
  - Basado en confianza mútua
  - Fácil de instalar e implantar
- S/MIME (Secure/Multipropose Mail Extensions).
  - Utiliza certificados X.509
  - Permite entornos abiertos (escalable)



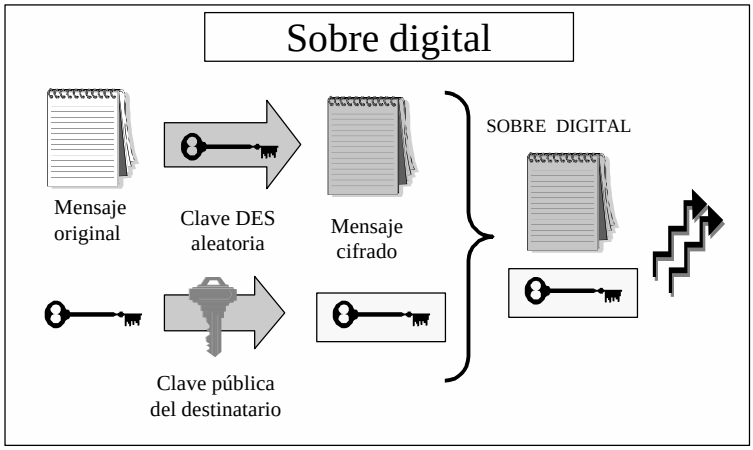
Autoridades Certificación

- FESTE
- ACE
- IPS
- Verisign
- La propia corporación
  - Certification Server (Netscape, IE)

PGP (Pretty Good Privacy).

- Permite intercambiar ficheros con:
  - Confidencialidad.
  - Autenticación.
  - Integridad.
- Permite cifrar y/o firmar los mensajes generados por otra aplicación.
- Proporciona a los mensajes un sobre lacrado e inviolable.

Sobre digital PGP



S/MIME

- Protocolo que añade firmas digitales y cifrado a los mensajes de correo electrónico en formato MIME.
- Puede envolver tanto el mensaje como la firma dentro de un “sobre” de datos cifrados.
- S/MIME asume que todos los participantes confían en alguna autoridad homologada de certificación.
- Fácilmente escalable

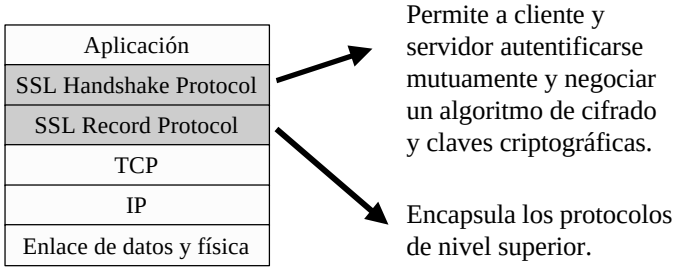
Secure Sockets Layer

SSL

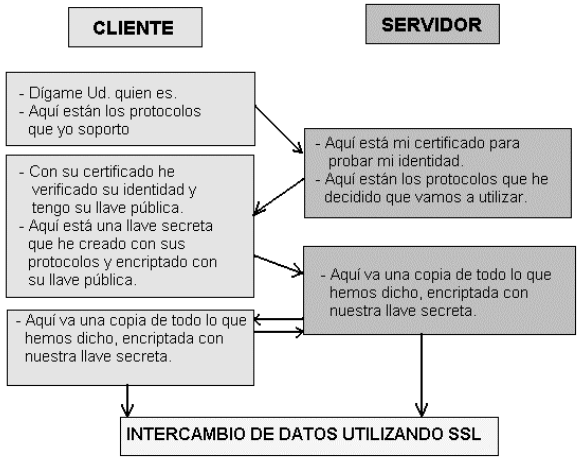
- Protocolo de seguridad creado por Netscape
- Ofrece servicios seguridad a protocolos del nivel de aplicación
- Proporciona confidencialidad, integridad y autenticación
- https: http sobre SSL

SSL (Secure Sockets Layer)

✓ Está situado entre el protocolo TCP y el protocolo de aplicación.



SSL Handshake Protocol



IPSEC

IPSEC

- RFC 1825
- Ampliación del protocolo IP para ofrecer servicios de seguridad estandar sobre redes TCP/IP
- Compatible con IPv6
- Los principales fabricantes evolucionan hacia productos IPSec

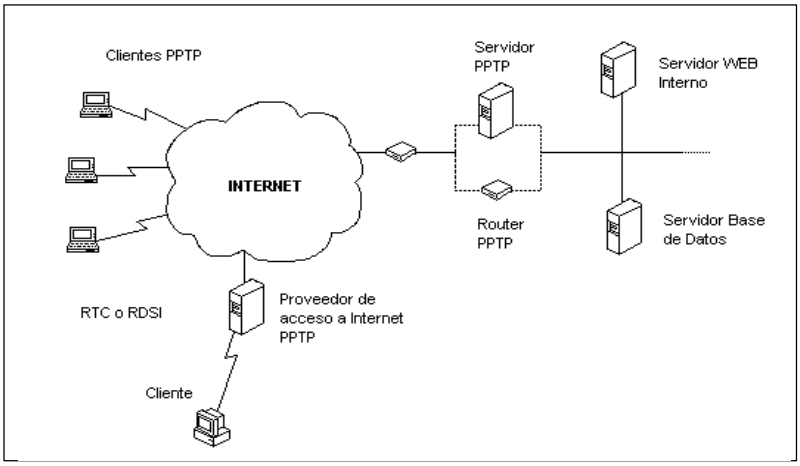
IPSEC

- Existen dos mecanismos de seguridad criptográficos para proporcionar seguridad en IP:
  - Cabecera de autenticación (AH): proporciona integridad y autenticación sin confidencialidad.
  - Encapsulado de seguridad de la carga útil (ESP): proporciona confidencialidad y, dependiendo del algoritmo y del modo, integridad y autenticación.

Gestión de claves

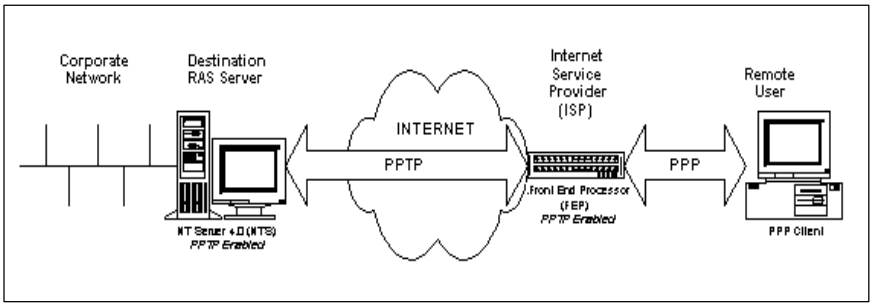
- **Internet Key Exchange (IKE)**
- **Permite negociación de mecanismo de seguridad y claves para ofrecer los servicios de seguridad**
- **Es la parte más compleja de IPSec y que menos fabricantes superan**

Entunelado



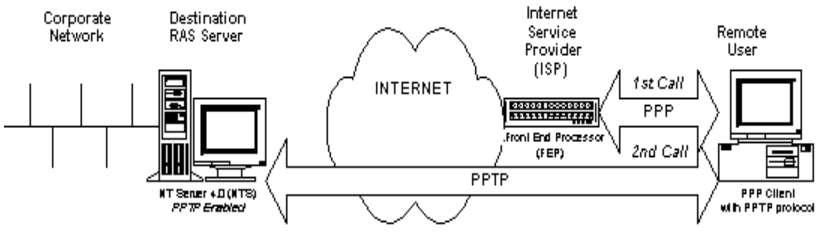
Entunelado PPTP

- El ISP proporciona PPTP



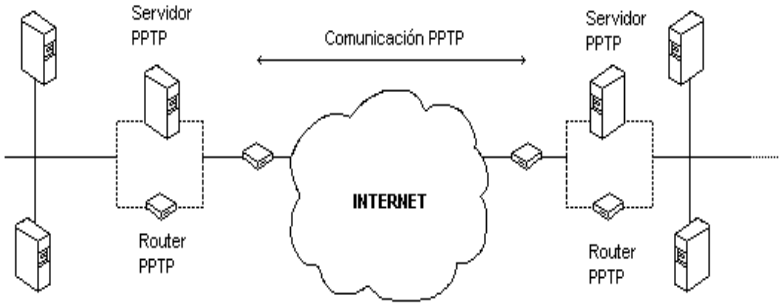
Entunelado PPTP

- La corporación proporciona PPTP



Creación de RPV

- Utilización de PPTP para construir el tunel



PPTP

- Soporta túneles extremo a extremo y entre servidores
- Cifrado RC4, de RSA
- No proporciona autenticación de puntos finales de túnel
- En desarrollo integración con IPSec

L2F (Layer 2 Forwarding)

- Soportado por la gran mayoría de fabricantes
- Habilita entunelado multiprotocolo
- No posee cifrado
- Autenticación débil

L2TP

- Entunelado a nivel 2
- Acuerdo Microsoft - Cisco
- Ofrece lo mejor de PPTP y L2F
- Estándar Internet
- Será adoptado por lo fabricantes una vez completo el proceso de estandarización
- Posible utilización conjunta con IPSec para reforzar seguridad