

# **SEGURIDAD DE LA INFORMACIÓN**

## **TEMA 4**

**SEGURIDAD Y PRIVACIDAD  
EN APLICACIONES TELEMÁTICAS**

# Índice del tema

- Seguridad en e-mail y herramientas
  - PGP
  - S/MIME
  - Conexión remota segura
  - Herramientas de cifrado
- Seguridad en pagos electrónicos
  - Conceptos generales
  - Protocolo SET
  - Protocolo Cyberscash
  - Protocolo iKP
  - Protocolo Millicent
- Privacidad de los usuarios en aplicaciones
  - Conceptos generales
  - Privacidad basada en esquemas avanzados de firma digital
  - Privacidad basada en protocolos criptográficos y de enrutamiento

## SEGURIDAD EN EMAIL Y HERRAMIENTAS

- El correo electrónico es la aplicación más ampliamente utilizada en la gran mayoría de los entornos distribuidos
- El crecimiento en su uso ha conllevado una mayor necesidad de seguridad, y, más concretamente, de la integración de servicios de **autenticación y confidencialidad**
- Entre las soluciones de seguridad en e-mail disponibles en la actualidad, hay dos que destacan por su amplio uso:
  - PGP
  - S/MIME



## PGP (Pretty Good Privacy)

- PGP es una solución diseñada por Phil Zimmerman, que seleccionó algoritmos criptográficos ya existentes y los integró en una aplicación independiente del S.O.
- Proporciona servicios de **autenticidad y confidencialidad** que se pueden usar para:
  - aplicaciones de e-mail
  - almacenamiento de ficheros
- Existen versiones libres para Windows, UNIX y Mac, además de versiones comerciales
- Integra los algoritmos RSA, DSS, Diffie-Hellmann (ElGamal), CAST-128, IDEA, 3DES, SHA-1
- Incluso IETF ha realizado avances con PGP:
  - *RFC 3156: MIME Security with OpenPGP*



# PGP (Pretty Good Privacy)

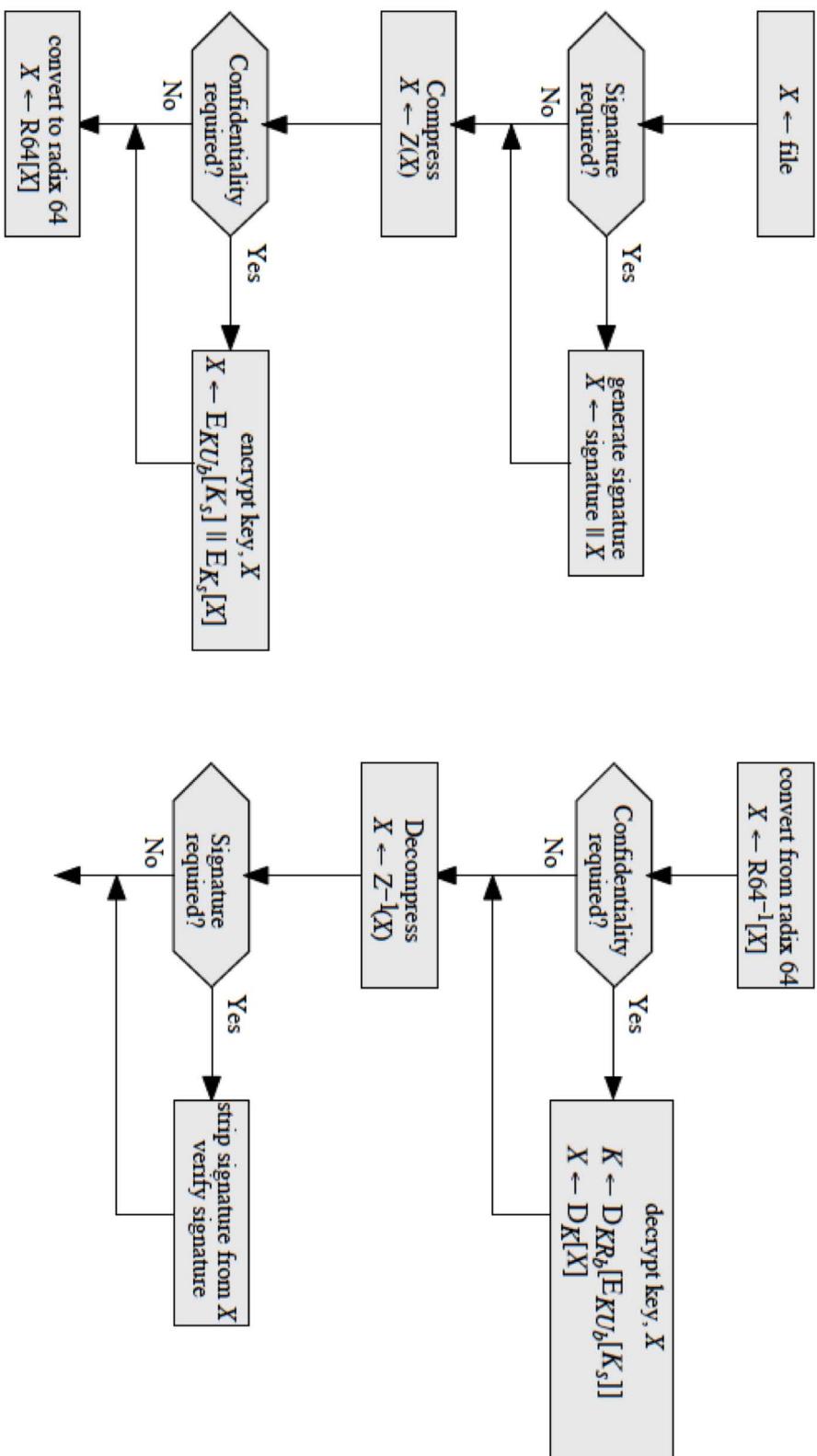
- Las operaciones de PGP incluyen, además de autenticación y confidencialidad, las operaciones de compresión y de compatibilidad de e-mail

Function	Algorithms Used	Description
Digital signature	DSS/SHA or RSA/SHA	A hash code of a message is created using SHA-1. This message digest is encrypted using DSS or RSA with the sender's private key and included with the message.
Message encryption	CAST or IDEA or Three-key Triple DES with Diffie-Hellman or RSA	A message is encrypted using CAST-128 or IDEA or 3DES with a one-time session key generated by the sender. The session key is encrypted using Diffie-Hellman or RSA with the recipient's public key and included with the message.
Compression	ZIP	A message may be compressed, for storage or transmission, using ZIP.
Email compatibility	Radix 64 conversion	To provide transparency for email applications, an encrypted message may be converted to an ASCII string using radix 64 conversion.



# PGP (Pretty Good Privacy)

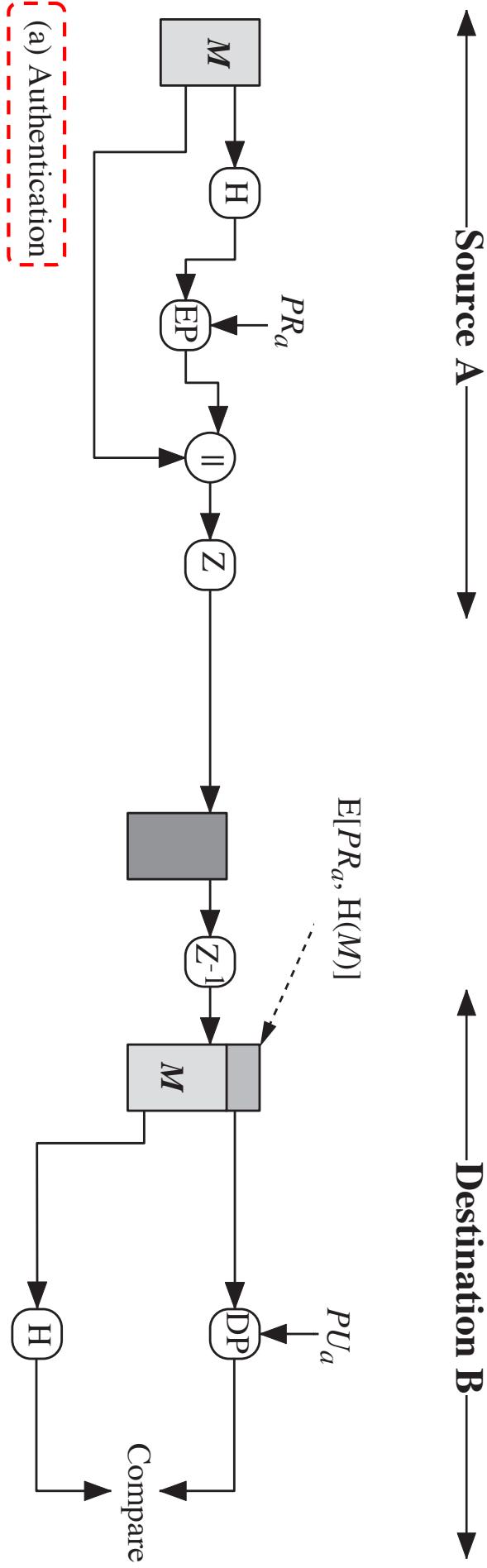
- Esquema de transmisión y recepción de mensajes PGP:



(a) Generic Transmission Diagram (from A)

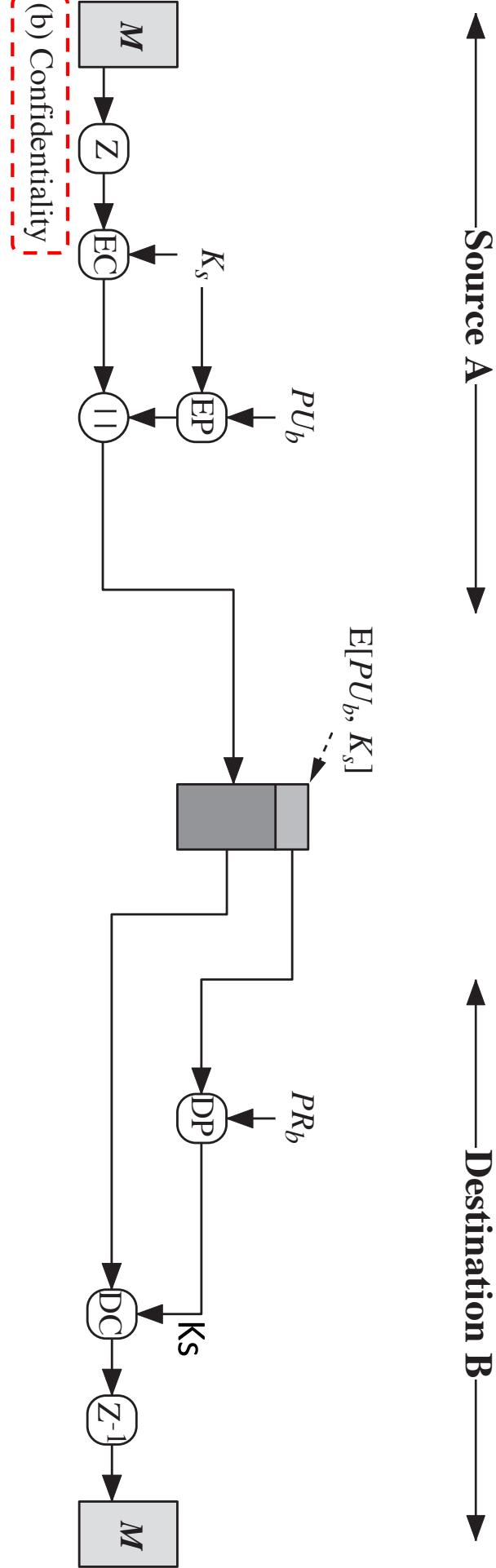
(b) Generic Reception Diagram (to B)

# PGP (Pretty Good Privacy)



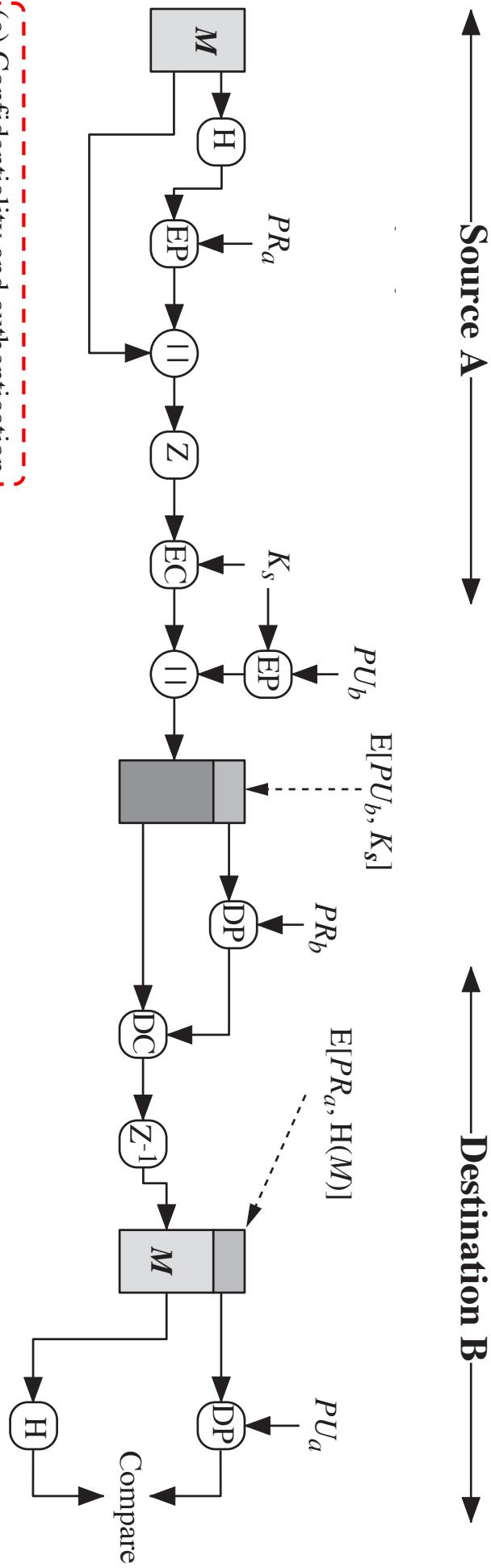
$K_s$  = session key used in symmetric encryption scheme  
 $PR_a$  = private key of user A, used in public-key encryption scheme  
 $PU_a$  = public key of user A, used in public-key encryption scheme  
 EP = public-key encryption  
 DP = public-key decryption  
 EC = symmetric encryption  
 DC = symmetric decryption  
 $H$  = hash function  
 $\parallel$  = concatenation  
 $Z$  = compression using ZIP algorithm  
 R64 = conversion to radix 64 ASCII format

# PGP (Pretty Good Privacy)



$K_s$  = session key used in symmetric encryption scheme  
 $PR_a$  = private key of user A, used in public-key encryption scheme  
 $PU_a$  = public key of user A, used in public-key encryption scheme  
 $EP$  = public-key encryption  
 $DP$  = public-key decryption  
 $EC$  = symmetric encryption  
 $DC$  = symmetric decryption  
 $H$  = hash function  
 $\parallel$  = concatenation  
 $Z$  = compression using ZIP algorithm  
 $R64$  = conversion to radix 64 ASCII format

# PGP (Pretty Good Privacy)



(c) Confidentiality and authentication

- $K_s$  = session key used in symmetric encryption scheme
- $PR_a$  = private key of user A, used in public-key encryption scheme
- $PU_a$  = public key of user A, used in public-key encryption scheme
- EP = public-key encryption
- DP = public-key decryption
- EC = symmetric encryption
- DC = symmetric decryption
- $H$  = hash function
- $\parallel$  = concatenation
- $Z$  = compression using ZIP algorithm
- R64 = conversion to radix 64 ASCII format

# PGP (Pretty Good Privacy)

- PGP proporciona, para cada usuario  $U$ , dos estructuras de datos:
    - **private-key ring**: para almacenar los pares <clave pública, clave privada> del propio usuario  $U$
    - **public-key ring**: para almacenar las claves públicas de los otros usuarios con los que  $U$  se comunica

Private-Key Ring

Public-Key Ring

# PGP (Pretty Good Privacy)

- Cada línea de la tabla del public-key ring puede considerarse en sí misma como un tipo de **certificado digital** (certificado de clave pública) no estándar
  - PGP no usa el estándar X.509, sino un formato propio

Public-Key Ring							
Timestamp	Key ID*	Public Key	Owner Trust	User ID*	Key Legitimacy	Signature(s)	Signature Trust(s)
:	:	:	:	:	:	:	:
:	:	:	:	:	:	:	:
$T_i$	$PU_i \bmod 2^{64}$	$PU_i$	$trust\_flag_i$	$User_i$	$trust\_flag_i$		
:	:	:	:	:	:	:	:
:	:	:	:	:	:	:	:

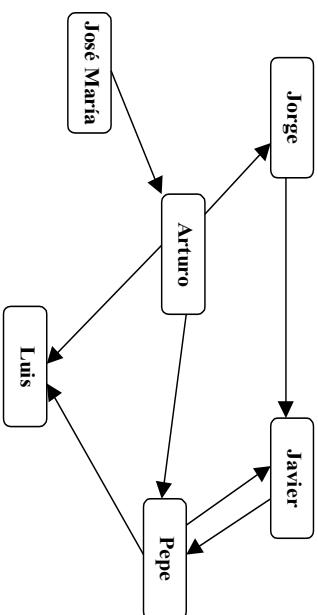


- Tampoco basa su funcionamiento en la existencia de una PKI jerárquica de Autoridades de Certificación, sino en un **modelo de PKI en malla**

- o sea, no existen Autoridades de Certificación al uso, pero **cada usuario del sistema puede emitir certificados al respecto de las claves públicas de los demás usuarios**

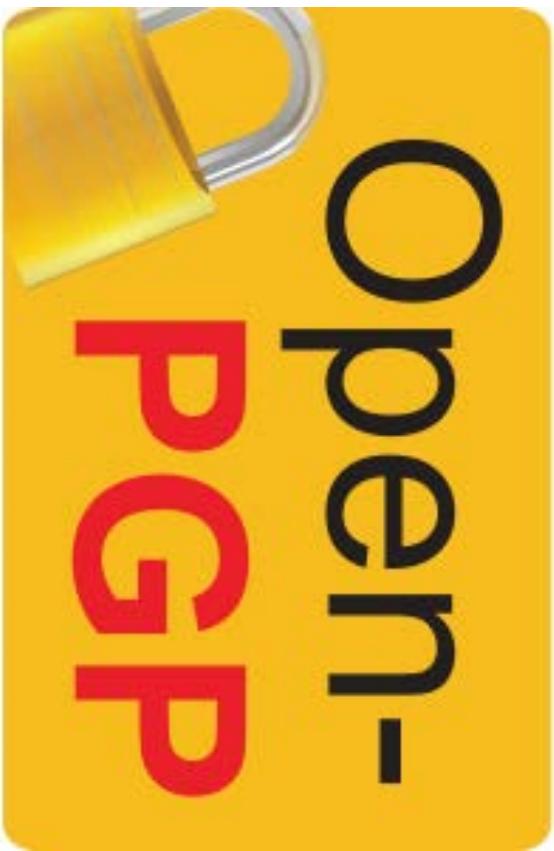
- de ahí los valores de confianza (**trust**)

incluidos en el public-key ring



# PGP con OpenPGP

- El OpenPGP Working Group se creó en 1997 y gracias en parte al Internet Engineering Task Force para definir el estándar
- OpenPGP es una aplicación estándar y libre que permite cifrar emails usando criptografía de clave pública y un específico formato



[Docs] [txt|pdf] [draft-ietf-openpgp...] [diff1] [diff2] [Errata]

Updated by: [5581](#)

PROPOSED STANDARD  
Errata Exist

Network Working Group  
Request for Comments: 4880  
Obsoletes: [1991](#), [2440](#)

J. Callas  
L. Donnerhacke  
H. Finney  
R. Shah  
D. Shaw

PGP Corporation  
IKS GmbH

Category: Standards Track

November 2007

---

**OpenPGP Message Format**

Status of This Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet official protocol standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

**Abstract**

This document is maintained in order to publish all necessary information needed to develop interoperable applications based on the OpenPGP format. It is not a step-by-step cookbook for writing an application. It describes only the format and methods needed to read, check, generate, and write conforming packets crossing any network. It does not deal with storage and implementation questions. It does, however, discuss implementation issues necessary to avoid security flaws.

OpenPGP software uses a combination of strong public-key and symmetric cryptography to provide security services for electronic communications and data storage. These services include confidentiality, key management, authentication, and digital signatures. This document specifies the message formats used in OpenPGP.

# PGP con OpenPGP

- Existen varias aplicaciones que soportan OpenPGP:
  - Windows
    - Outlook: gpg4ol, Gpg4win, p=pp
    - Thunderbird: enigmail
  - Mac
    - Apple mail: GPGTools
    - Mutt
    - Thunderbird: enigmail
  - Android
    - K-9 mail: Openkeychain
  - iOS
    - P=pp
    - R2Mail2
  - ....
    - Thunderbird: enigmail

# OpenKeychain

The screenshot displays the OpenKeychain mobile application interface, which includes the following sections:

- OpenKeychain**: The main screen featuring a large green circular icon with a padlock and a key.
- Servidores de claves OpenPGP**: A section for managing PGP servers, showing "keybase.io" as the preferred server at <https://keyserver.ubuntu.com>.
- Administrador servidores de claves OpenPGP**: A section for managing PGP servers, showing "keybase.io" as the preferred server at <https://keyserver.ubuntu.com>.
- Claves**: A section for managing keys, showing a lock icon.
- Cifrar/Descifrar**: A section for encryption/decryption, showing a lock icon.
- Aplicaciones**: A section for applications, showing a grid icon.
- USAR TOKEN DE SEGURIDAD**: A section for using security tokens, showing "Transferencia wifi segura" (Secure WiFi transfer) and "Habilitar Tor" (Enable Tor) with a note that it requires Orbot to be installed.
- IMPORTAR CLAVE DESDE FICHERO**: A section for importing keys from files, showing "Habilitar otro proxy" (Enable other proxy) with a note that it requires Orbot to be installed.
- TRANSFERENCIA WIFI SEGURA**: A section for secure WiFi transfers, showing "Puerto de proxy" (Proxy port) set to 8118 and "Tipo de proxy" (Proxy type) set to HTTP.
- OMITIR CONFIGURACIÓN**: A section for skipping configuration, shown with a red X icon.
- Configuración**: A navigation bar at the bottom right with a back arrow and the text "Configuración".

Texto y ficheros

# iPGMail

Carrier 1:39 PM

**Create Private Key**

**Done** **Create**

Passphrase  
Confirm Passphrase

Key Size:

Expiration:

Real Name: John Q. Smith

Email Addr: user@domain.com

Carrier 1:39 PM

**Edit** **Public** **Private**

**Public Keys**

**Clear** **Sign** **Encrypt** **Both**

+

From:	To:
foobar <foo@bar.com>	info@jpmail.com
Attach: Select Attachments	
Great job!	

From: adele-en <adele-de@gnupg.de>  
4D4B6CC8 RSA(2048) 2013-07-08 2017-07-08  
booo <booo@hoo.com>  
D4C8EB20 RSA(2048) 2013-07-23 (no exp)  
foobar <foo@bar.com>  
C033E7CC RSA(2048) 2013-07-29 (no exp)  
foobar <foo@bar.com>  
F00FFoo <foo@har.com>  
818F5EE0 RSA(1024) 2012-01-03 (no exp)  
Willys <willys@me.com>  
47E5234C RSA(2048) 2011-06-11 (no exp)

Carrier 1:40 PM

**Done** **Public Key Details**

**Public Key Info**

Key ID: 47E5234C  
User ID: Willys <willys@me.com>  
Fingerprint: A5DD EFCG 4A52 B587 E68A 2451 7FEA 1CCB 47E3 234C  
Created: 2011-06-11  
Expiration:   
Algorithm: RSA (enc/sign)  
Image: N/A  
Key Len: 2048

Carrier 1:05 AM

**UID Info**

Willys Ingersoll <willys@gmail.com>  
47E5234C 2011-06-11

**UID Info**

iPGMail Support <info@pgmail.com>  
47E5234C 2011-09-21

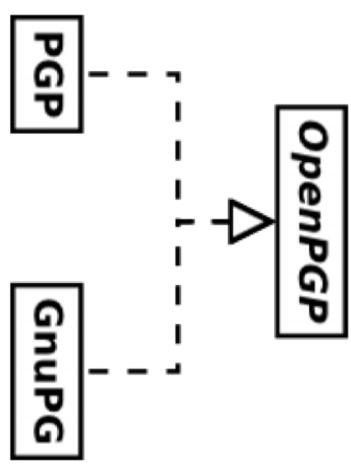
**UID Info**

Willys <willys@me.com>



## GnuPG

- GnuPG es una implementación del estándar OpenPGP que deriva del software criptográfico PGP desarrollado por Philip Zimmermann



- Con GnuPG se puede realizar las siguientes acciones:
  - gestionar y generar claves públicas y privadas
  - visualizar y distribuir las claves públicas, exportándolas e importándolas
  - cifrar y descifrar documentos
  - firmar y validar documentos



# MyPGP

MyPGP (7.5.2016)

new directory refresh secure delete

name	size	date
keys		
secret keys		
lists		
MyKeys		
author		
sample		

/ Users / Cristina / 1234

process encrypt

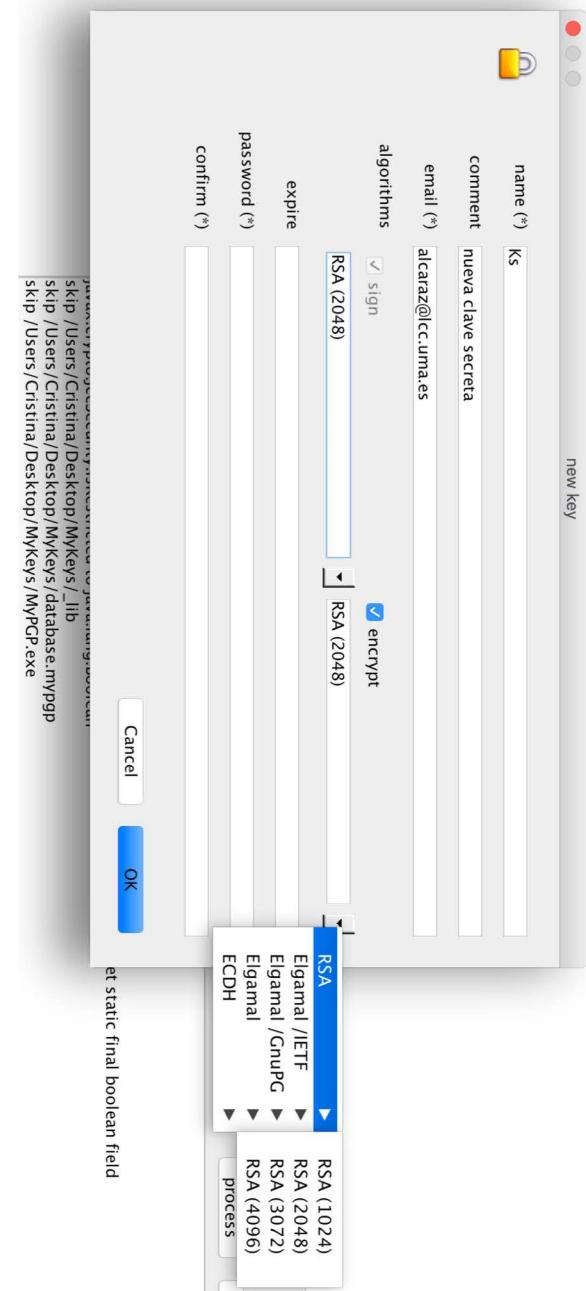
java home: /Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Home  
java version: 1.8.0\_111  
HOME: /Users/Cristina/Desktop/MyKeys

Failed to remove cryptography restrictions: java.lang.IllegalAccessException: Can not set static final boolean field javax.crypto.JceSecurity.isRestricted to java.lang.Boolean  
skip /Users/Cristina/Desktop/MyKeys/.lib  
skip /Users/Cristina/Desktop/MyKeys/database.mypgp  
skip /Users/Cristina/Desktop/MyKeys/MyPGP.exe

secure delete

# MyPGP

Creando una pareja de claves (privada y pública):



## Si se visualiza la clave privada:

-----BEGIN PGP PRIVATE KEY BLOCK-----  
Version: BCPG v1.55 (7.5.2016)  
Comment: MyPGP (7.5.2016)

```
LQGBFg8ccABCACchl2mdceC4gKKyPR0W2YKbm08u+g/+0c+rFy90q28p7a61EX  
LQmRer0ffFeech1hx/17DmKLH-n5ca/0m10H-x2xvewvt/mwksqGFByP1986bpoW  
jps6/KJm9x1PusCenkob-B-TMAnoU/6E/CPrNQWm/DE9j6SG39gZoeg_6hz  
14kNakc2rcRfTzLwnt8R1ujFLjnkUXwahnX-qj/0pLingLyT0r5z1z1AYH  
dKbmwhLRzRxapKt5UmG1n9B7TVuK99909rth-0nHjczcr0j010r5132.vb69ko  
0x+TQ00X11VY-PY796uLl94E765CEKUJABE8AH-COM1971ZLUGUsBAU26m  
0x711Uj16tskb881hwpg9kbpLV77G.lv3.007mt21cikYmVn3VIR4054XNrn  
90wAr9imXif99g0eamW8ieb@eEUJ-99990n39gtWkgTPN1rqgf8pxpjlUBYD  
T5163011QJcKtVnsplCn02>J5evb0uWESvA40D1YKxcwms.WakDore653.5w  
5/LV7zatedlar0EKN1CSq9r71+bwsL/TDjhcrGZhs-XkvLUkLUk2asgPbzZ  
MTf4M1K62ED/P4-FG1Gr6swxLUFfBn08/w78c316puvJ0x77AF01nc2of  
12310wn29.9/11K1o-TWm8Y2GBa8s1sae+D2kQ9-puxmicaLRKcuaLowlBemqSg  
/JTrv40xvqyMdagf46PnpeU0XPruG6-7Vj-09tP+flmVqd0L1Tqxidw483JJU  
trd67-YKv541Xqzb0T4xuJmG43KZ46Jp0T92NbuSRUWmA1s3.Cmld/bDJx  
CSWic2J1ncqod11866mMdnF.E4rCctq1IWSf52d1-K7G/a9.g8nRnRg1.RQie  
moXW21JZLb0o1WPw265iph.Lcu+se+AU.crvng.Uawd1.94011.0ze-n8P5  
tK510ThqJt4271hkQm1052zu2t0Xs20Inr412H1S0p990ahgF0ckJXIn2months  
t0UE51f1LSCf3J0s3KuYSXBj11J0m0R69J7110eo1LGENek/17YNGYNN  
zWeXvJuunmJF42J08171/PkT69w/5.ca.ccw9gk790J01rrngtt2coCwof3x1  
+L19k80uSho9tC1LcvABWkYXJhekb5Y2MuW1nLmVzP4obhny\dmIE92xh0mug  
c2Vjcm10Y5m1AtUEwE1ABFA1g8cEcGmGwKtBwNCBVCAwEGFG1Jg.Cahb  
Aa0E011VKKtchutAry.Rhore1obs+4gJ9H510d48rRoxinOylLNsAGcPSK/  
B8XW7r7qEB899GICt6299gln3PBa8H0Nz710qmn13r0d0uNb5CT0f0TTL8G  
a408GEWw7h'sFVCBHvFRv0r0zzJ0B105C05pdAnB.DMK17M8FA  
0VvNzJ1+16CVt109.yQd1.K1-49.94XWmZ7NmK7/03JYVJUStTnSkAV.KmkDm/G  
Hd129qvYt9EowTpb0qwnjWRxarVzczkV15.Ha31m7b16w0d0SPcGqY680J9XvJ  
1PAuN02Zetm14nFlzRzXZj0EKAhoJavbeonhijidABUEw0xwAEATkmbdwt  
70515E-0upLIX577e10M1ecuMIGf0oXpRv1f0t5shuf8SBsB1Gt1s93r  
VFTW9jX1-1SSh0135E01rbbb-Z49ZLNU10M01060p  
t0k-07gtJg.aobE1Efxkh+HmOs62ZfX.0MBKScP+GwHx0d0LtkAn2b7nQLB8TLo  
50229En0C1-1Bq6enWkX1Kw4d211BqKX1TV  
6HFnGn0SS1CwLAX-8XmrtA0vY11Qb/Gycdts0fg9.2p267jnaf93Y1mgnQ  
SQm9gB33512rMXuAf0EAAf4JAwiruNn0427CsA802kSAV.L6nXk1sh7Bpr6ut  
11057R9m12hmrh02z-TRK18k1MKp2XKzKzKzKzKzKzKzKzKzKzKzKzKzKz  
RCp9bT0TEmpHa0m1+07YF-UNrCzah0VsLw2d00815MjKTT91D.RX0m61rVIA  
jE50t09q30m7tx5hkv0j1np0e41n2zGK1d02+B.IV0JVa0n421L8.UhgM0  
60rPm1z9n1.Iws413av81t1c91Hw70P-0SS9q0EP01MDL0613V/7N1  
qVR177zHa2B-4h9uUXx9-ri1.Sb03BwMcRwLuNqkyZ0/7w2.7saV.tOp3D1.  
4/Law.Tsdvtr749smLE001p4ExkzxcVmtA2mB1t6156gokTegm9a2XcG0H/Y  
1Nds910F48-1TLL0010mtz1ay1z+HmW0j52K1.K1THF6v6ANXKUtfXmLP092Y  
KoghdID1N2AKGegeK6X00mm1j9B.KsZz.BA1qw1nT.Pm0r12g+pedz.4nwq  
UkPuzTod911ql9pbyo5ctkwk1s1aemnajqt1.18b0c16pxHmFRTYV14.13eq1v8yq  
bCCDCL47L09+jx.in/0/bwmstV65ncj19PSB01281AtIn1ur3RVMyB65C8k/mnkok3  
Ex-165405YCGEd21J0n9.6ewpwkLc190nQ-W7Z210cNCTYKmNE2Wf2Jj0X/  
1H7Nam45h0S65Y7nu9jLtwghb0Kt1swavX88ABrB61.JabK33Ba1zL1+mnXKUp  
tswuBD+ZY2CIBX0ZHHPlmjiCST/09c1m94B9tZyy-h102hnu3M70E01  
E99wuhb.fmkwBRBwW00z2m69hdwUJ.ZUUr+TfHebaUnR74o.wb7akBhwQaQa  
CQwdwkw1QjbDAKer0DcCCL471.0s1biwub.9601TfJwz.rTccha90euRSvV5/7F  
r4QmukXckKopPw6559.L15c47KkP92mrxX1CguLo0e1t.ZmxXNWKtNto4vVns/1D  
HNGs0/1fNSUk0m1bRmkPfX0gJkmt05.bSGAAKmWtPlJUDeF.bh3LP/H  
QEJm0o0dL+bo1nrhttjb1mW.VD0m4-qlx37.0lgvef.0-0+0bK0dAtrWnLl0  
1dbbfh0p19fSXmGex.W1Iu255ccCS600XH1ywU3x09jY.LH77mGZ51dUL+d6  
1027So1rT76Wm0c00+RyTnL5F+40f2B6+7auw5ING16CggpXW  
=m3c+  
-----END PGP PRIVATE KEY BLOCK-----
```

# MyPGP

MyPGP (7.5.2016)

Main keys lists clipboard files language

keys  
secret keys  
Ks <alcaraz@lcc.uma.es>  
Ks2 <a@lcc.uma.es>  
[28.11.2016] Ks2 <a@lcc.uma.es>  
[179701F4] fingerprint: 03ca 09a4 c6db 5175 1351 1fff e344 548c 1797 01f4

view encrypt sign encrypt & sign decrypt & verify

new directory refresh secure delete

name prueba.txt  
prueba.txt.asc

MyPGP (7.5.2016)

Main keys lists clipboard files language

keys  
secret keys  
Ks <alcaraz@lcc.uma.es> (nueva cla  
Ks2 <a@lcc.uma.es>  
[28.11.2016] Ks2 <a@lcc.uma.es>  
[179701F4] fingerprint: 03ca 09a4 c6db 5175 1351 1fff e344 548c 1797 01f4  
RSA (2048) / RSA (1024)  
encrypt: AES 256, AES 192, AES 128, CAST5 (128), 3DES (112/168)  
Publius Cornelius Scipio Africanus <publius@roma.imperium> (password: password)

encrypt sign encrypt & sign decrypt & verify  
secure delete

new directory refresh secure delete

name prueba.txt  
prueba.txt.asc

# Enigmaill

**Inicio - Mozilla Thunderbird**

**Administrador de claves Enigmaill**

Mostrar por defecto todas las claves

Identifí...

Adjuntos

Nuevo mensaje

Adminstrador de actividad

Filtros de mensajes

Adjuntos

Buscar

Complementos

Editar

Preferencias

Imprimir...

Enigmaill

Rearrugar nombre

**Redacción: Mensaje secreto**

De: Alejandro Luna  Responder  Reenviar

Asunto: Mensaje cifrado con thunderbird

Mensaje cifrado con thunderbird

Información de seguridad Enigmaill

Mensaje descifrado SIN CONFIANZA La firma de es correcta

Identificador de clave: 0x32CEEDBB Firmada el: 13/01/16 16:50 Huella digital de la clave: 1D8B 4C4A EA01 2C5D 4EFC 0183 BD90 3534 32CE EDDB

Nota: el mensaje está cifrado con los siguientes identificadores de usuario o claves:

0xF959CB776B55D1B ( ), 0x153342368713423 ( )

**Thunderbird Correo - erc**

Nombre

Buscar por:

Recibir mensajes  Redactar  Charlar  Direcciones  Etiqueta  Filtro rápido

Archivo  Editar  Ver  Servidor de claves  Generar

Correo electrónico

Leer mensajes

Adjunto

Adjuntar mi clave pública

Este mensaje se firmará y cifrará

De:

Para:

Para:

Asunto: Mensaje secreto

Preformato  Anchura fija

Hola

# Enigmail

Support for OpenPGP encryption and signing messages is provided by Enigmail. You need to have GnuPG (gpg) installed in order to use this feature.

Enable OpenPGP support (Enigmail) for this identity

**OpenPGP Security**

Use email address of this identity to identify OpenPGP key  
 Use specific OpenPGP key ID (0x1234ABCD):  
0xC218F36

**Message Composition Default Options**

Encrypt messages by default  
 Sign messages by default  
 Use PGP/MIME by default

After application of defaults and rules:

sign non-encrypted messages  
 sign encrypted messages

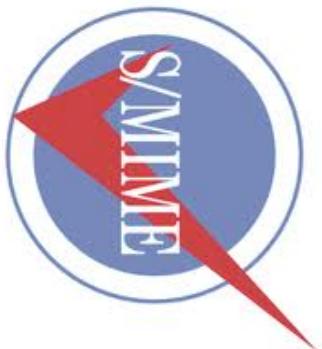
Encrypt draft messages on saving

**Enigmail Preferences...**

**Account Actions**

## S/MIME (*Secure/Multipurpose Internet Mail Extension*)

- S/MIME es una mejora en el ámbito de seguridad del formato MIME para correo electrónico
  - el cual a su vez es una mejora de SMTP
- Algunos de los documentos que describen S/MIME son:
  - RFC 5652: Cryptographic Message Syntax (CMS)
  - RFC 5750: Secure/Multipurpose Internet Mail - Version 3.2 - Certificate Handling
  - RFC 5751: Secure/Multipurpose Internet Mail Extensions – Version 3.2 - Message Specification



## S/MIME (*Secure/Multipurpose Internet Mail Extension*)

- Aunque tanto PGP como S/MIME están en vías de llegar a estándar, todo apunta a que **S/MIME se va a consolidar como estándar para uso comercial**
  - mientras que PGP quedará para uso personal
- En términos de funcionalidad, S/MIME es similar a PGP en el sentido de que ambos ofrecen la posibilidad de **firmar y/o cifrar mensajes**
- S/MIME usa certificados de clave pública con formato **X.509v3**, con un **modelo de PKI híbrido** entre la jerarquía estricta de Autoridades de Certificación y el modelo en malla
  - Utiliza los algoritmos criptográficos de la siguiente tabla:

# S/MIME (Secure/Multipurpose Internet Mail Extension)

Function	Requirement
Create a message digest to be used in forming a digital signature.	MUST support SHA-1. Receiver SHOULD support MD5 for backward compatibility.
Encrypt message digest to form a digital signature.	Sending and receiving agents MUST support DSS. Sending agents SHOULD support RSA encryption.
Encrypt session key for transmission with a message.	Receiving agents SHOULD support verification of RSA signatures with key sizes 512 bits to 1024 bits.
Encrypt message for transmission with a one-time session key.	Sending and receiving agents SHOULD support Diffie-Hellman. Sending and receiving agents MUST support RSA encryption with key sizes 512 bits to 1024 bits.
Create a message authentication code.	Sending and receiving agents MUST support encryption with tripleDES. Sending agents SHOULD support encryption with AES. Sending agents SHOULD support encryption with RC2/40.

# Thunderbird

## Seguridad

Para enviar y recibir mensajes firmados o cifrados, debe especificar tanto un certificado para firma digital como uno para cifrado.

### Firmado digital

Usar este certificado para firmar los mensajes que envíe:

Seleccionar... Limpiar

Firmar mensajes digitalmente

### Cifrado

Usar este certificado para cifrar/descifrar mensajes enviados a Uds.:

Antonio Gamarrero

Seleccionar... Limpiar

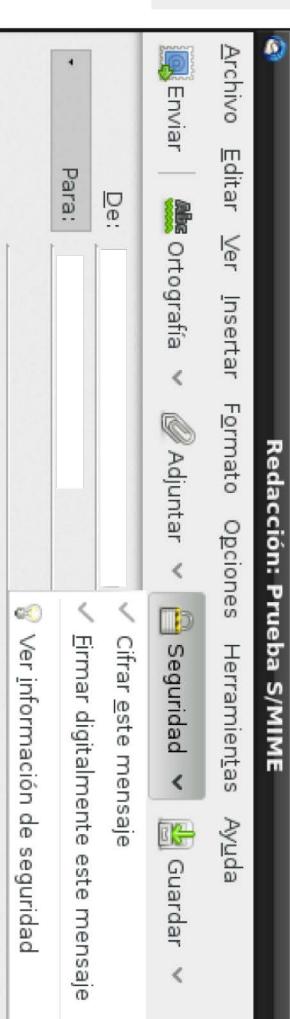
Cifrado elegido para enviar mensajes:

Nunca (no usar cifrado)

Siempre (no podrá enviar si algún receptor carece de certificado)

### Certificados

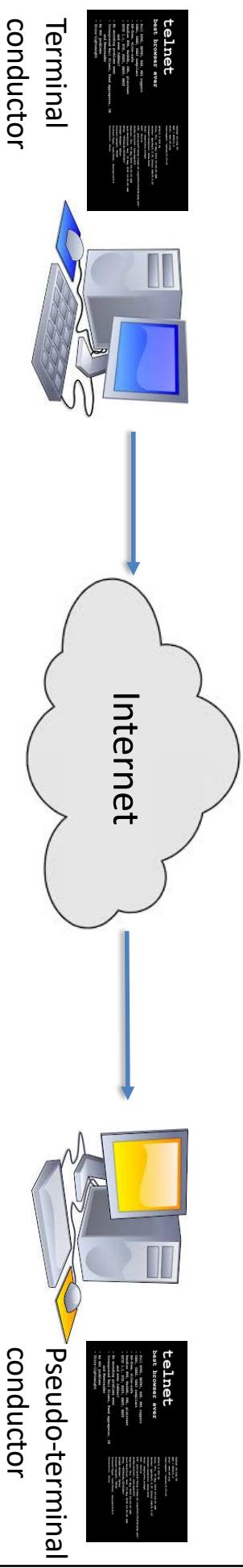
Ver certificados Dispositivos de seguridad



```
smime.p7m x
-----BEGIN PGP MESSAGE-----
1   0ACK *HT
2   SOHBELDETX <0ESTXSOHNULL, SOHS0, SOH STXSOHNND0-0,1VTO ACKETXUEOTI
3   ACKETXUEOTBSDC3ACKMalaga1ST0
4   ACKETXUEOTBElDC3ACKMalaga1FF0
5   ACKETXUEOT
6   DC3ETXUMA1FF0
7   ACKETXUEOTVTD3ETXUMA1DC20DLEACKETXUEOTETXDC3 Cristina 1!0USA
8   SOH SOH$NDC2a1caraz@lcc.unma.esSTXSOH$T0
9   ACK *HT-
10  SOH$OHSOHNODU EONE'8>, `NAKE'#i-c-ò-, -jò- (»,,dEò"DC1[2v, SUBDòUSO
11  \í,íNADE4ièòOCANià<GDLE=TX:FF/séS16NAKI DIFEFJg\zsfjòauñ!ETBK
12  SOHBELUSOHD4ACKBS*tHT-
13  ETXBELBOTBSLP*t-ag eEON,
14  @`ES3ñ-*P±SUBñ2, Ð/[\ø,4äG*E`*!i@GShfç23ñ] GSLjETX<%xñBELWACK&C_
15  æíDC4aâðe1=ÑøGP2"ÖVÜB<"Vñcfoå"US<"âñÍ-íðñEvý6èëDC1ZoÈ\3[írtkny>
```

# Telnet (TELetype NETwork) y FTP (File Transfer Protocol)

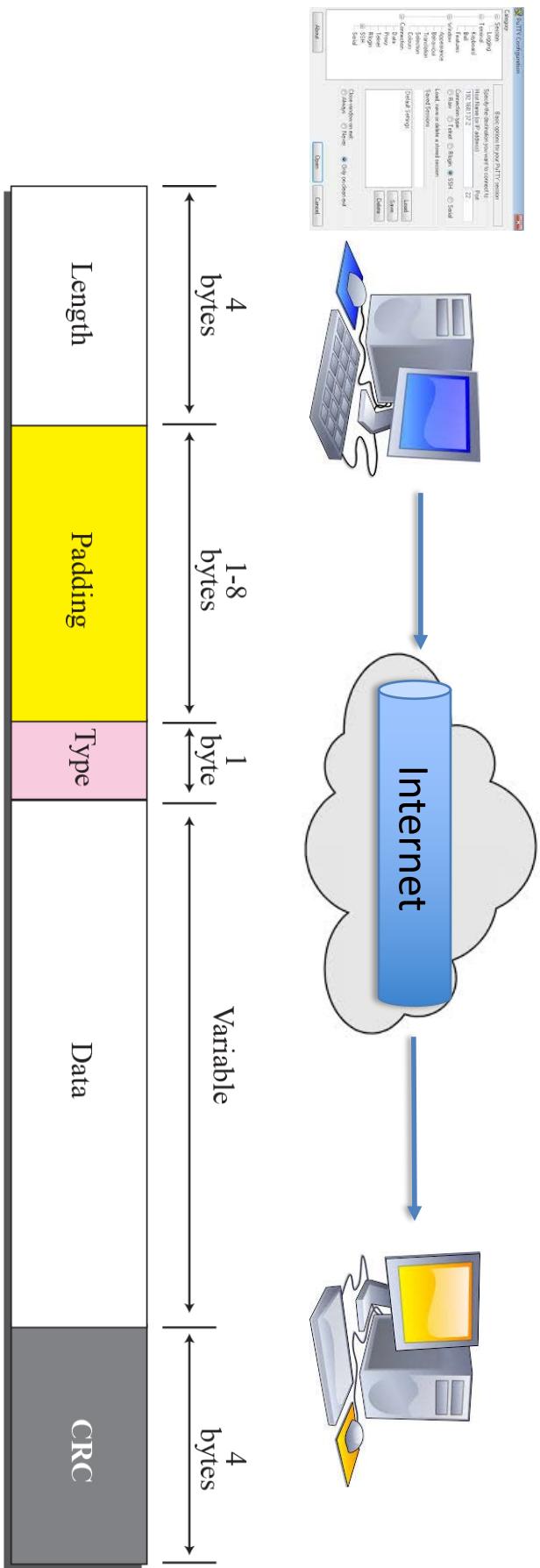
- Características funcionales:
  - **Telnet** (puerto 23): facilita el acceso remoto a otros sistemas y sobre TCP, de forma que el terminal local aparece ser el terminal del sistema remoto



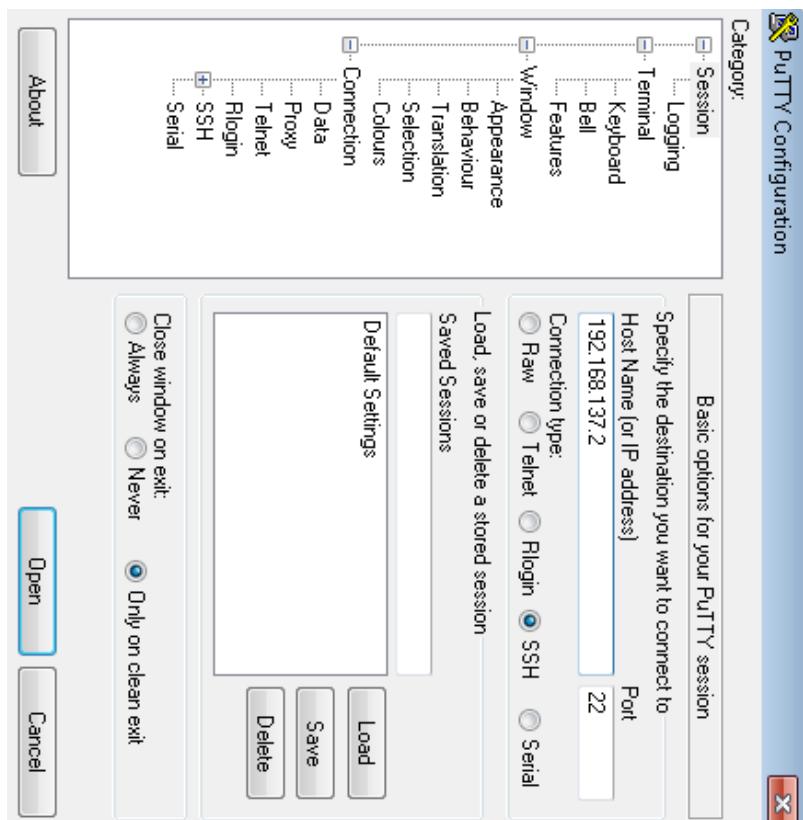
- Problemas:
  - **FTP** (puerto 20/21): permite la transferencia de ficheros entre diferentes recursos remotos

# SSH: Secure Shell (v2)

- SSH es una herramienta similar al telnet funcionando en el puerto **22**
- Permite el acceso remoto sobre TCP a otros sistemas usando el concepto de cliente/servidor pero cifrando las transacciones usando **criptografía pública**
- Características funcionales:
  - Después de realizar la conexión inicial, el cliente puede verificar que está conectado al mismo servidor por el que se conectó anteriormente



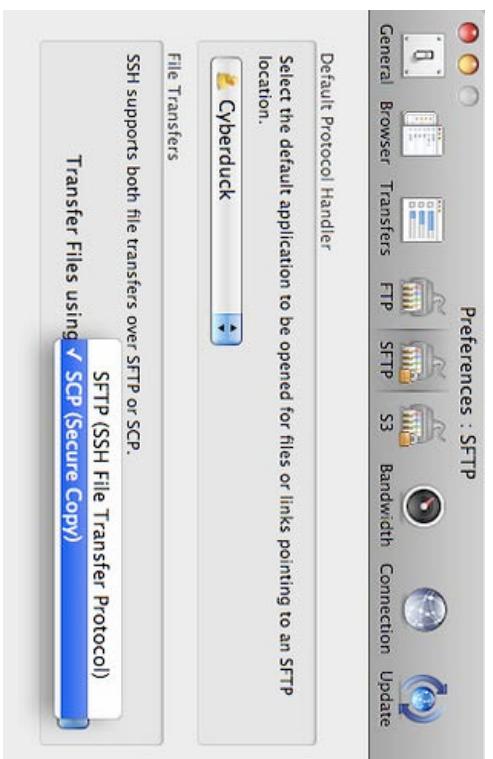
# PUTTY



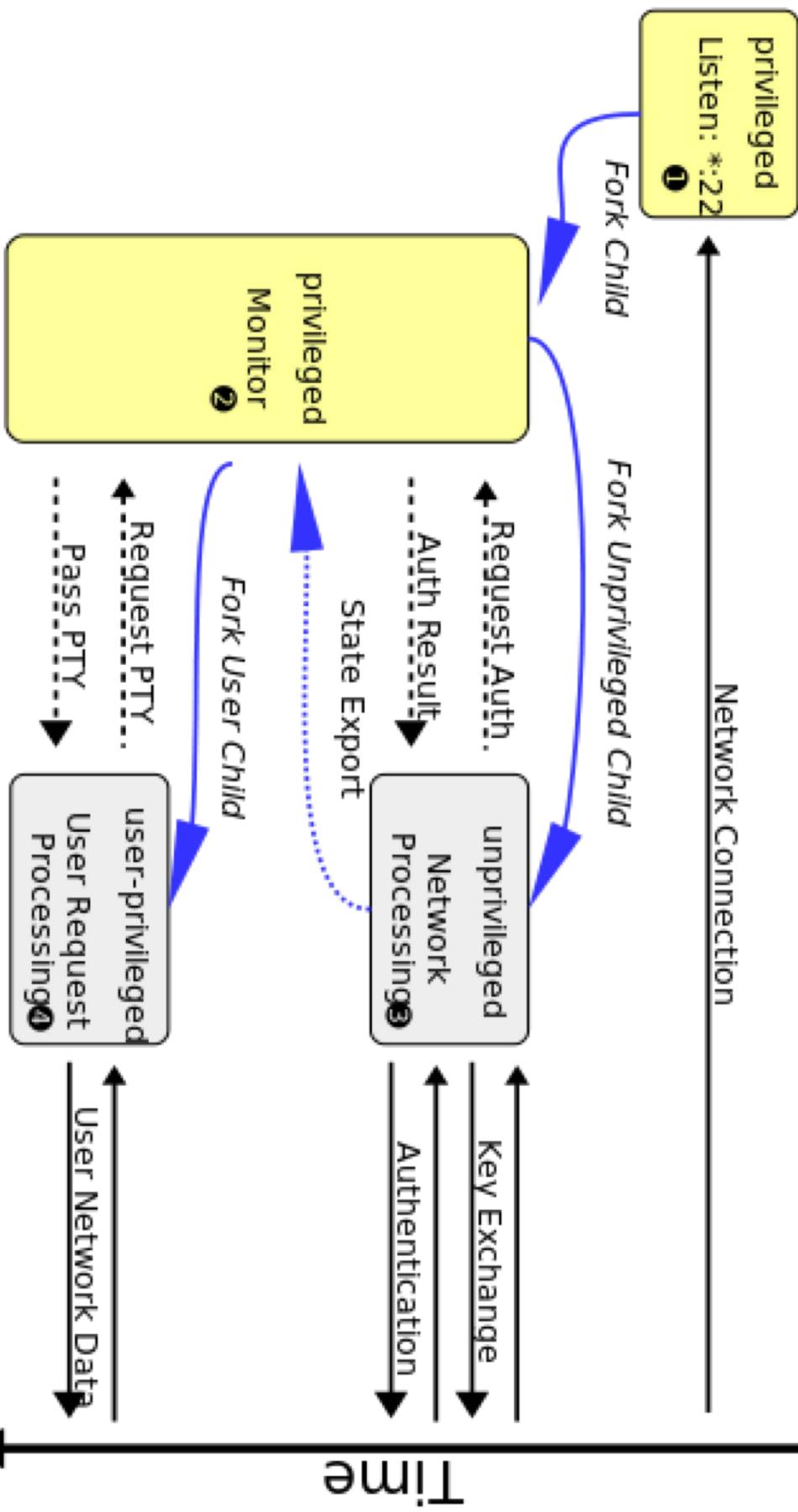
# OpenSSH

```
vdi-6E20:~ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/Users/
[Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in hola.
Your public key has been saved in hola.pub.
The key fingerprint is:
[SHA256:GX02RHZboy@wveGG14B1emRoo2TxY2degHktiuK3vA
The key's randomart image is:
+---[RSA 2048]---+
| . o+ooo o |
| + +Boo.=+ |
| ...=B .+oo |
| o+o*+.+ |
| S+o-oo . |
| . . o... |
| o . . .. |
| . + o. |
| . E .. |
+---[SHA256]---+
```

- Funcionamiento general:
  - Capa de aplicación:
    - Gestiona la autenticación del cliente haciendo uso de un user/password o de criptografía de clave pública
  - Capa de transporte:
    - Gestiona e intercambia las claves iniciales
    - Establece los modos de cifrado y de comprensión
  - Capa de red:
    - Establece una “conexión directa” entre el cliente-servidor y redirige el tráfico entre estos puntos de conexión. Modo túnel (en base a cifrado simétrico)
  - Mitiga o evita ataques específicos:
    - spoofing de IP o suplantación de identidad: remotos nodos intentan suplantar la identidad de otro nodo de la red
    - spoofing de DNS en donde el atacante trata de suplantar el nombre del servidor
    - SSH puede ser usado también para transferir ficheros como una alternativa a FTP, conocido como SFTP (SSH File Transfer Protocol) y SCP (Secure Copy)

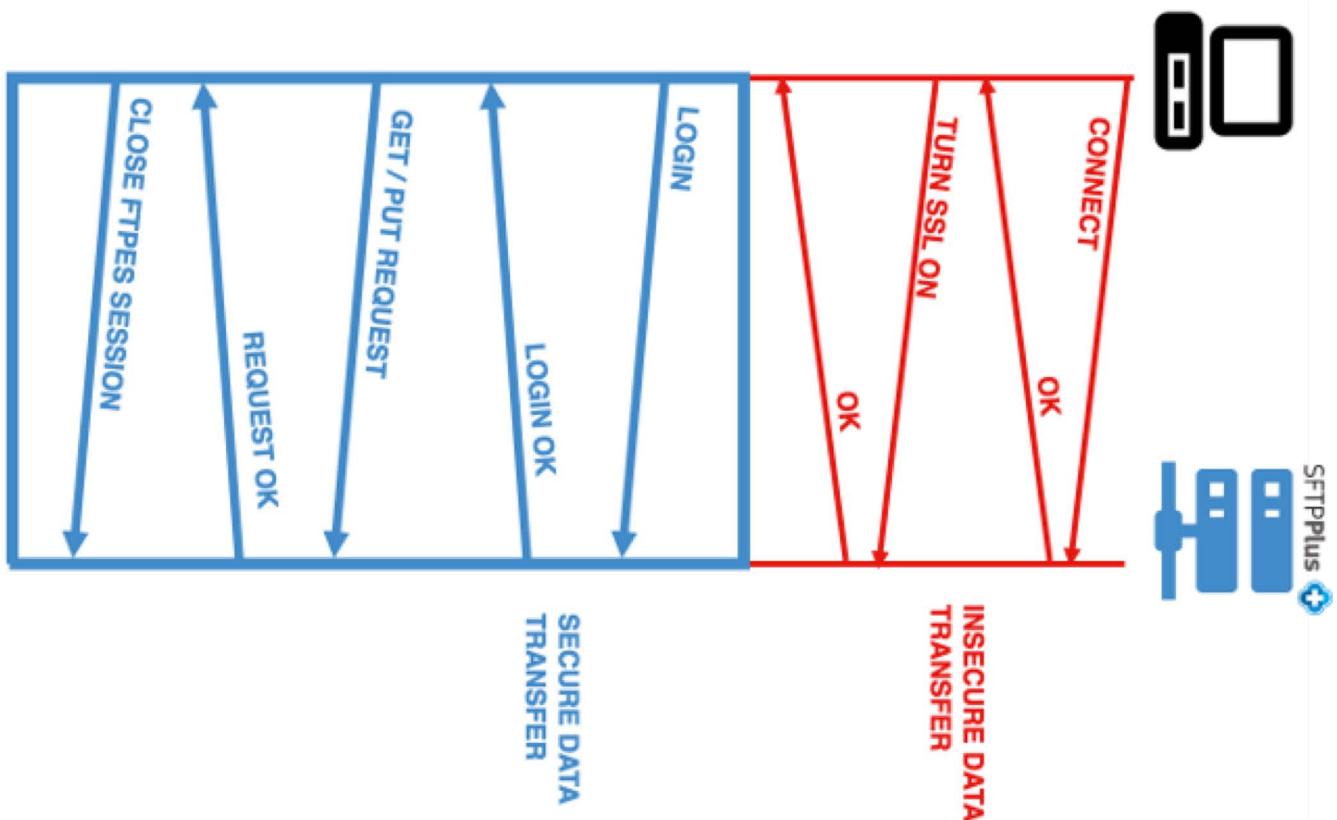


- SFTP (FTP sobre SSH) # FTPS (FTP sobre SSL)
- Funcionamiento:
  - Se puede basar de diferentes modos de autentificación para conectar con el servidor SFTP:
    - Modo básico: usuario y contraseña
    - Modo avanzado: usando las claves públicas de SSH, previamente generadas, y compartiendo dichas claves públicas con el servidor SFTP
  - De esta forma, cuando el cliente quiere establecer conectividad con el sistema remoto, el proceso software del cliente tendrá que transmitir su clave pública al servidor para su autenticación
  - Todas las conexiones SFTP están cifradas



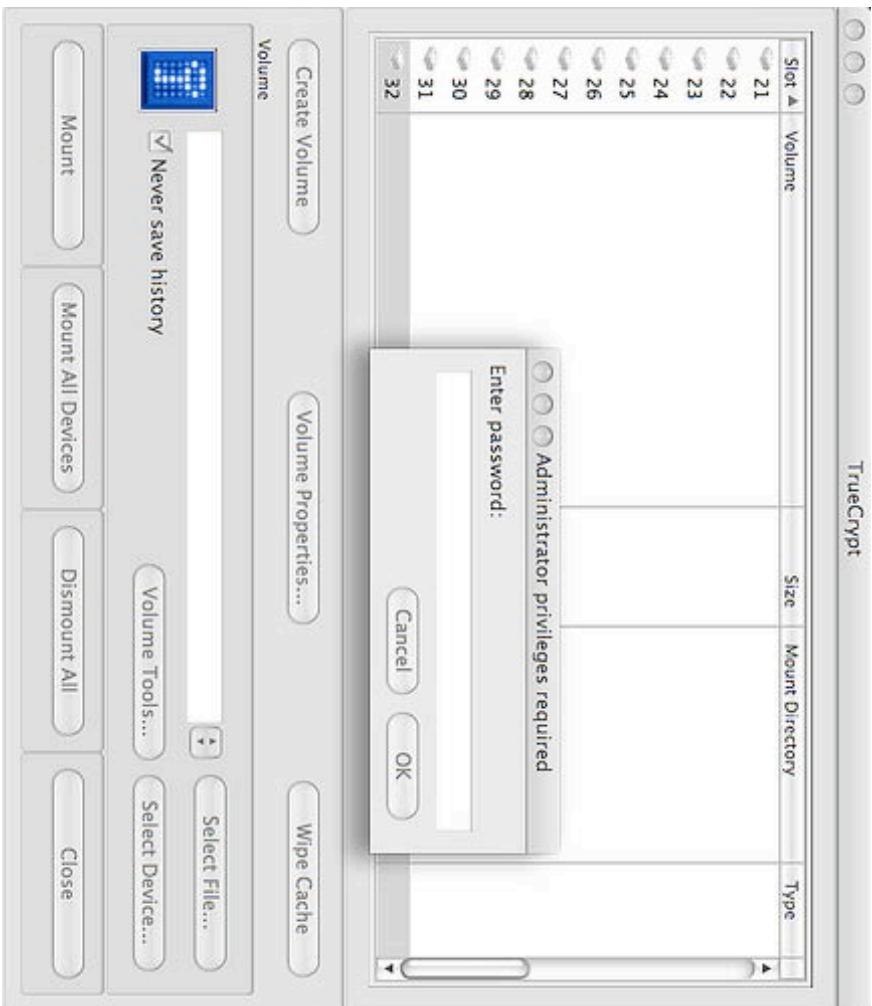
# FTPS (FTP Secure)

- FTPS proporciona un soporte adecuado para TLS (Transport Layer Secure) y SSL (Secure Sockets Layer)
- Funcionamiento:
  - Se basa de usuario, contraseña y certificados, de forma que:
    - las credenciales de seguridad (usuario y contraseña) son cifrados a lo largo de la conexión FTPS
    - Para ello, el cliente primero verifica que el certificado del servidor es correcto y de confianza para hacer uso de su clave

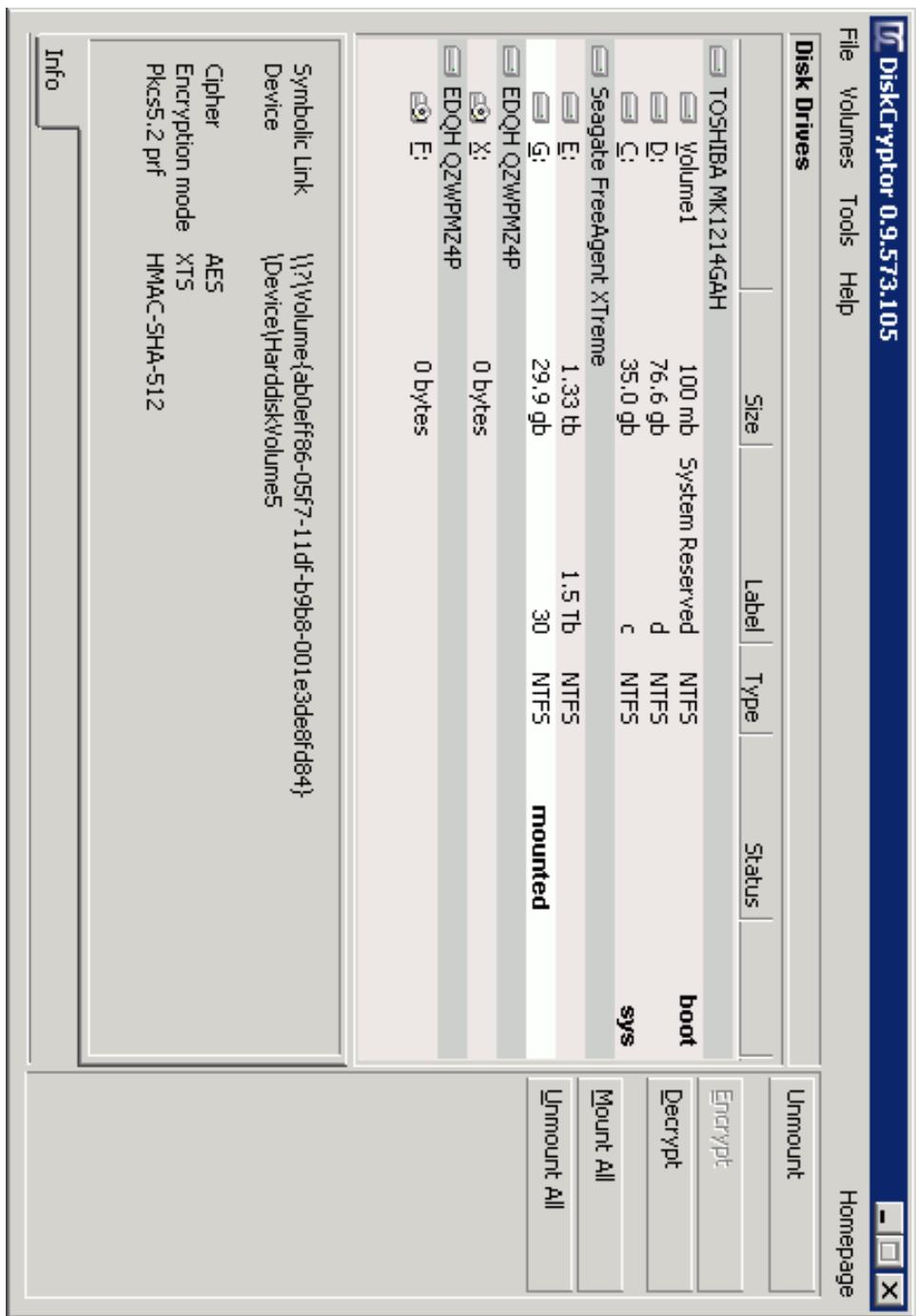


# Herramientas de cifrado open-source

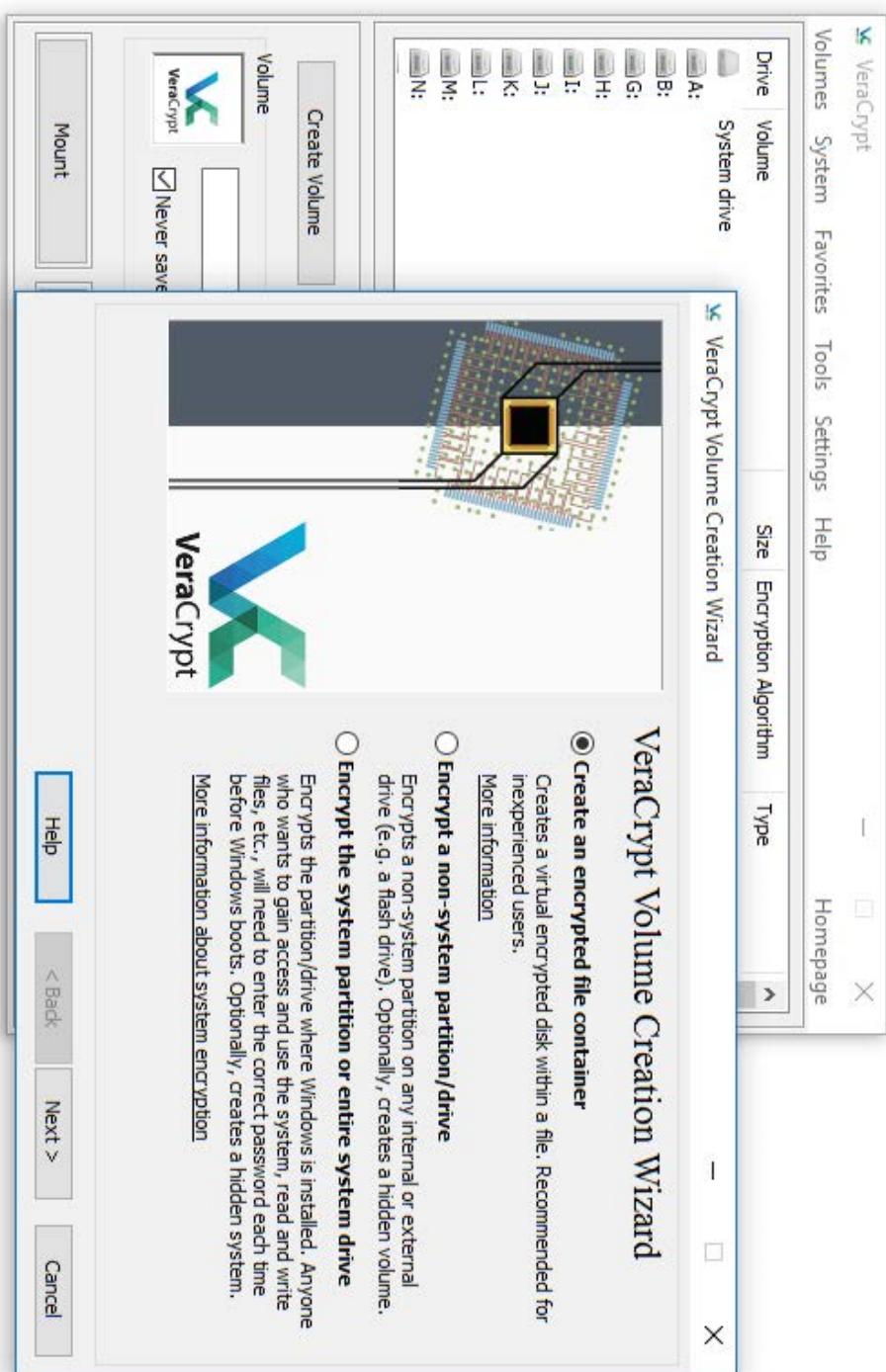
- **TrueCrypt:** herramienta de cifrado de discos duro disponible para Windows (XP/2000/2003) y Linux, haciendo uso de AES-256, Blowfish, CAST5, Serpent, Triple DES y Twofish
  - También permite ocultación de particiones haciendo uso de cifrado y aleatoriedad de la información



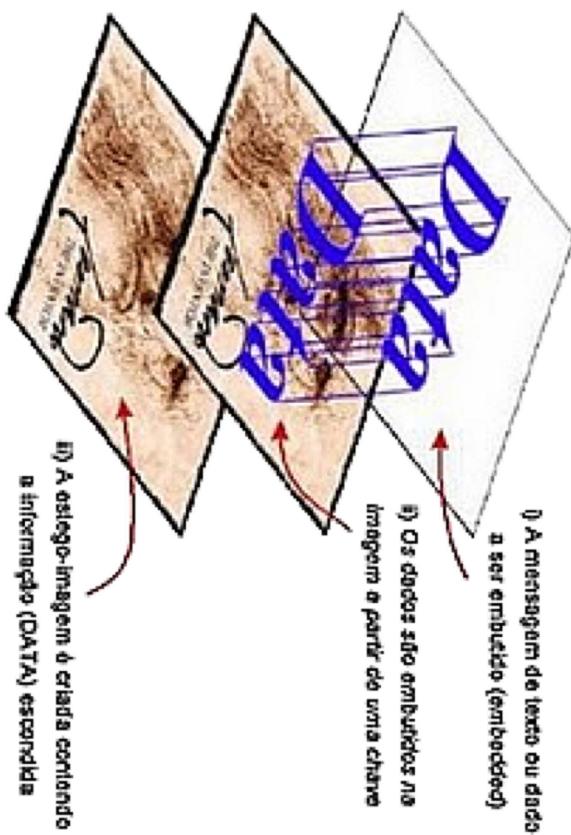
- **DiskCryptor**: similar a TrueCrypt pero con capacidad de cifrar dispositivos de almacenamiento externo USB
  - También incluye algoritmos de cifrado como AES, Twofish y Serpent



- **VeraCrypt**: similar a TrueCrypt pero con la diferencia que incluye un número específico de iteraciones para el cifrado, incrementando la lentitud del sistema durante los procesos de lectura y escritura en el disco
  - Como TrueCrypt, aplica AES, Twofish y Serpent

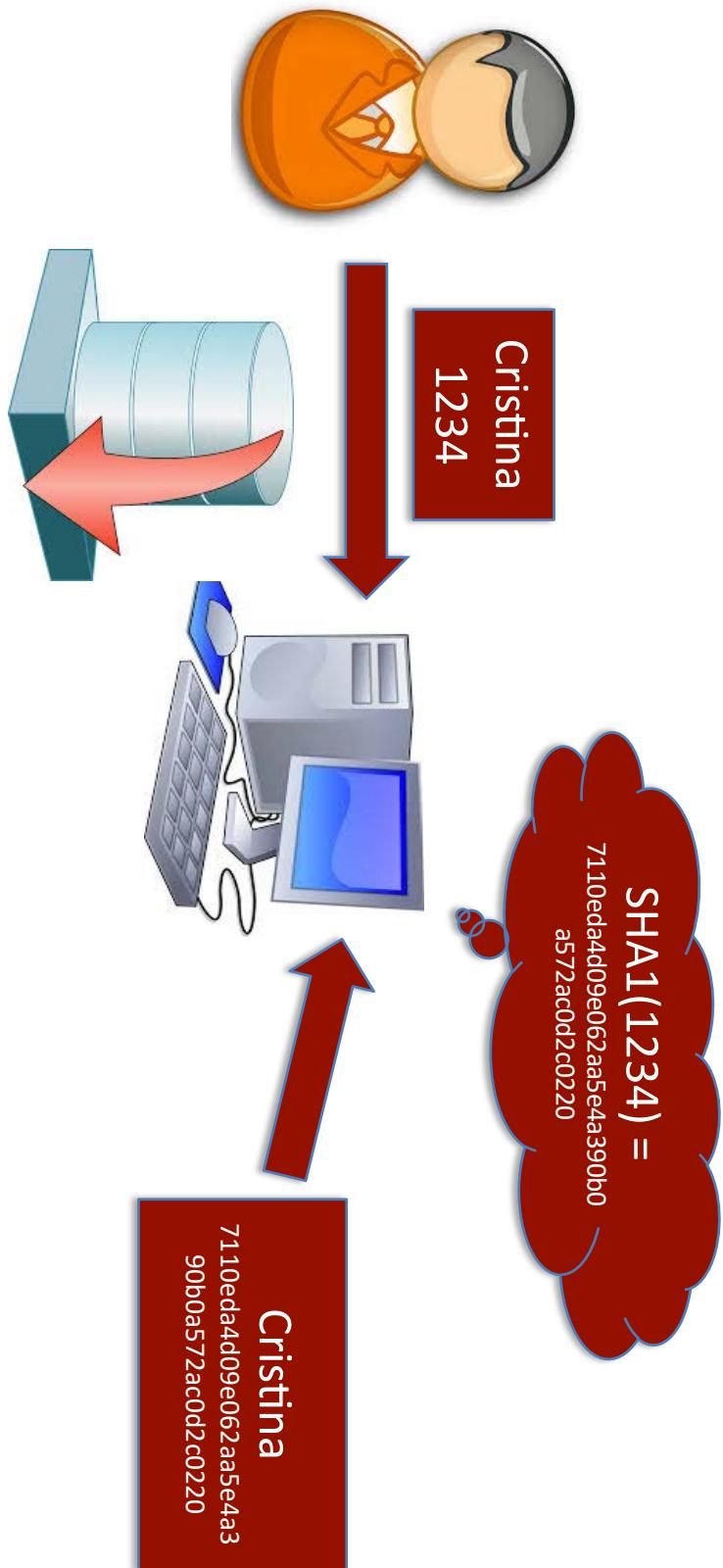


- **OpenStego**: aplica técnicas de Esteganografía para ocultar información haciendo uso de imágenes o cualquier archivo multimedia
- **OpenPuff**: es similar a OpenStego para Windows con soporte para BMP, JPG, MP3, WAV y MPG4



0001 80  
C02001 80 DF038  
C809 DE038  
21B2C809 DF038  
EE8EE 4F511C  
CB3EE8EE 4F511C  
B75 C820E  
CB3EE8EE 4F511C  
04143B75 C820E  
B51C659E 9A36  
~ B51C659E 9A51  
~ B51C659E 9A51  
~ B51C659E 9A51

## Salt: Contraseñas con Salt



- Las cuentas almacenadas en un disco duro de un sistema y protegidas con contraseñas, suelen tener asociado un HASH a dichas contraseñas. **¡Nunca se debe almacenar las contraseñas en claro!**
- Cuando el usuario quiere entrar al equipo se le pide la contraseña, se hace el hash y se compara con el hash almacenado

- Si alguien roba el fichero con los HASH puede hacer fácilmente un ataque de diccionario
- Para dificultar los ataques de diccionario se usa una “**Sal**” → valores aleatorios que se asocia al HASH

