

# SEGURIDAD DE LA INFORMACIÓN

## TEMA 4 – PARTE 1

### **SEGURIDAD Y PRIVACIDAD EN APLICACIONES TELEMÁTICAS**

# Indice 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 Cybercash
  - 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 en 1991
  - Básicamente, PGP consiste en seleccionar algoritmos criptográficos ya existentes e integrarlas en una única aplicación SW independiente del S.O.
    - Integra los algoritmos **RSA, DSS, Diffie-Hellman (ElGamal), CAST-128, IDEA, 3DES, SHA-1**
  - 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
- Incluso IETF ha realizado avances con PGP:
  - *RFC 3156: MIME Security with OpenPGP*



# PGP (Pretty Good Privacy)

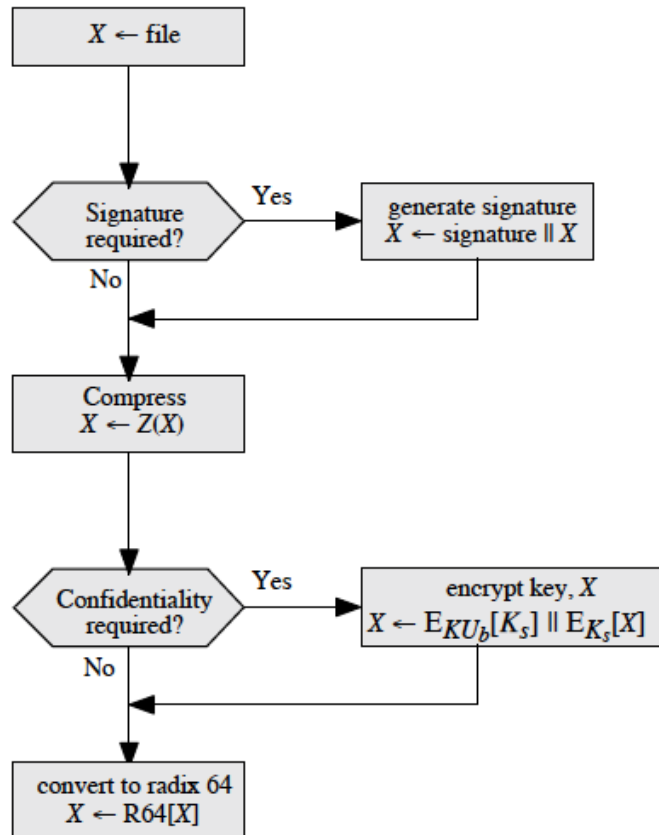
- Las operaciones de PGP incluyen, además de autenticación y confidencialidad, las operaciones de compresión y de compatibilidad de e-mail

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 <u>ASCII string using radix 64 conversion</u> .

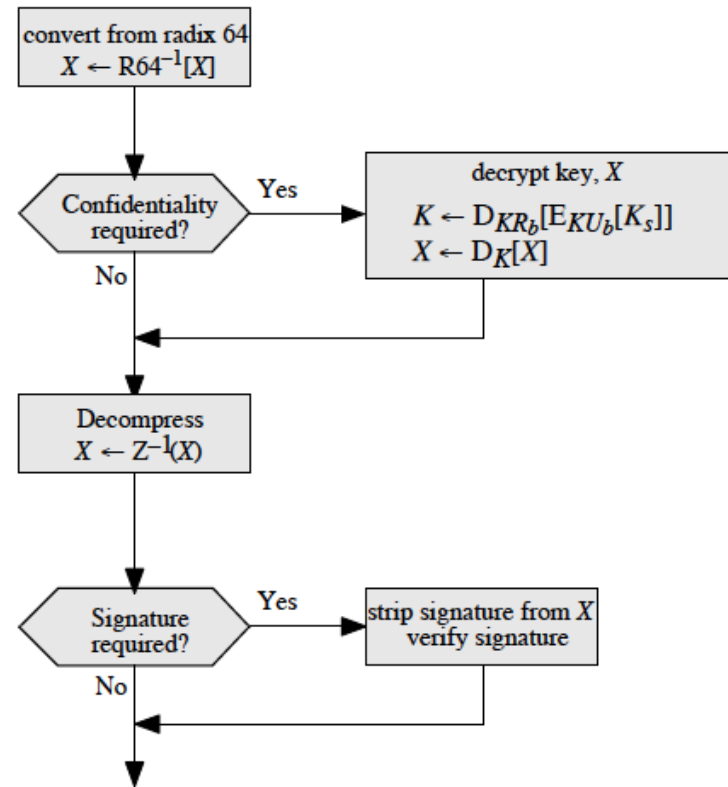


# PGP (Pretty Good Privacy)

- Esquema de transmisión y recepción de mensajes PGP:

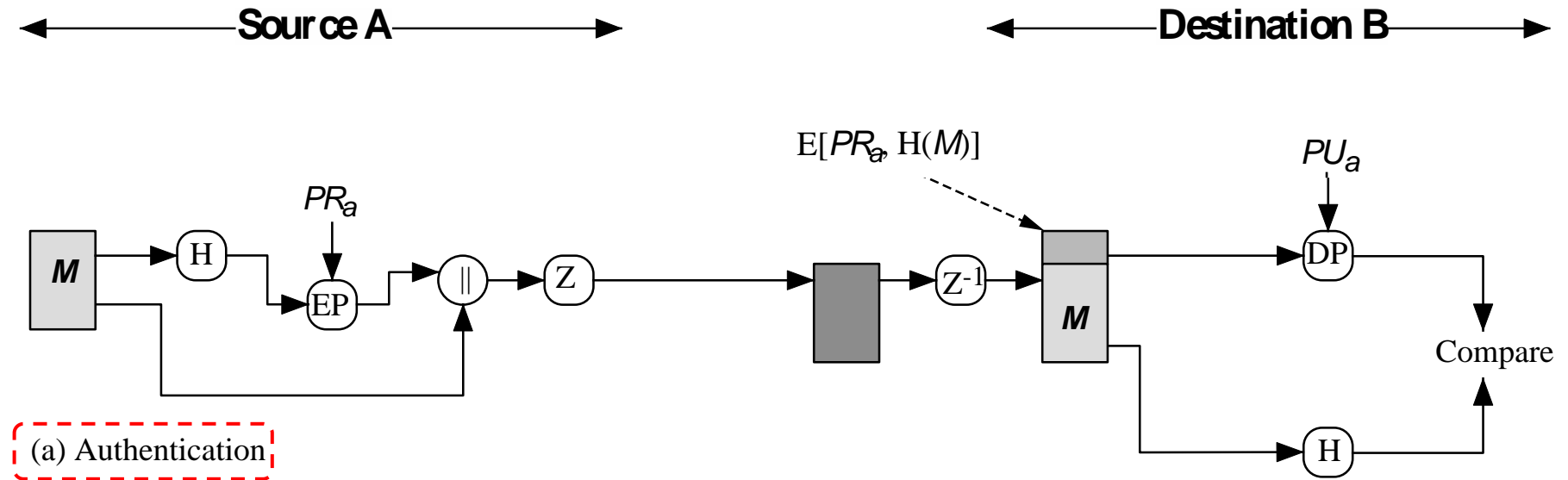


(a) Generic Transmission Diagram (from A)



(b) Generic Reception Diagram (to B)

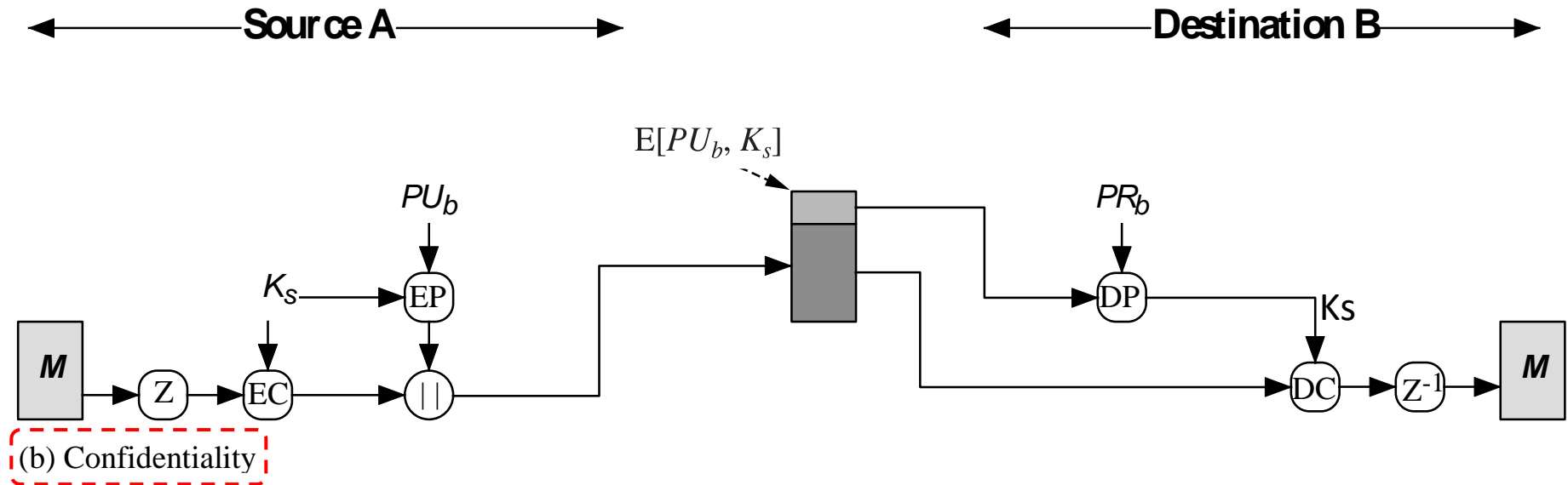
# PGP (Pretty Good Privacy)



$K_s$  = 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

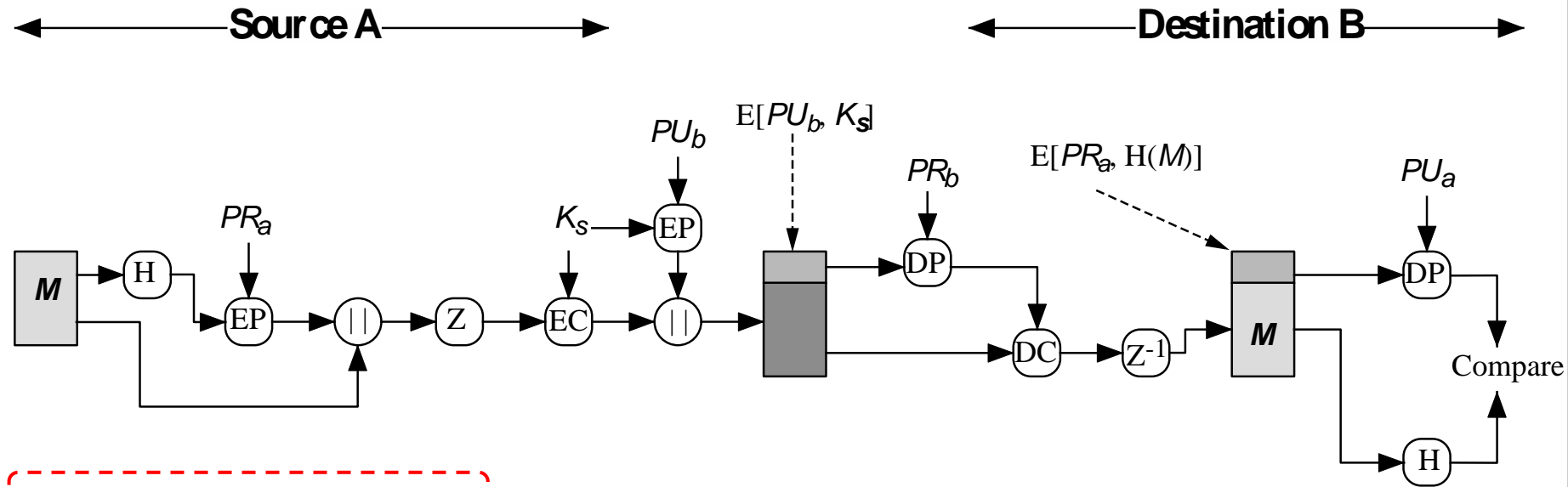


# PGP (Pretty Good Privacy)



$K_s$  = 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  
 $||$  = 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  
 $||$  = 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


Timestamp	Key ID*	Public Key	Encrypted Private Key	User ID*
• • •	• • •	• • •	• • •	• • •
$T_i$	$PU_i \bmod 2^{64}$	$PU_i$	$E(H(P_i), PR_i)$	User $i$
• • •	• • •	• • •	• • •	• • •

## Public-Key Ring

[illegible]

# PGP (Pretty Good Privacy)

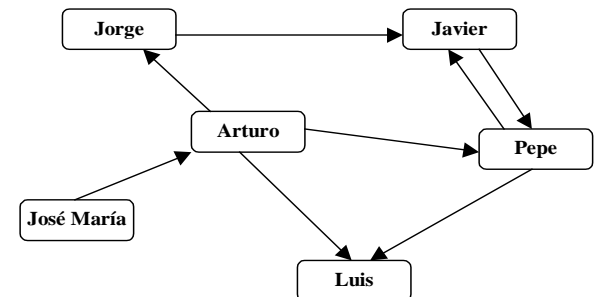
- Cada línea de la tabla del public-key ring puede considerarse en sí misma como un tipo de **certificado digital** (certificado de clave pública) **no estándar**
  - PGP no usa el estándar X.509, sino un formato propio



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. **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
- Está basado en el PGP original



[\[Docs\]](#) [\[txt|pdf\]](#) [\[draft-ietf-openpgp...\]](#) [\[Diff1\]](#) [\[Diff2\]](#) [\[Errata\]](#)

Updated by: [5581](#)

PROPOSED STANDARD

[Errata Exist](#)

Network Working Group

J. Callas

Request for Comments: 4880

PGP Corporation

Obsoletes: [1991](#), [2440](#)

L. Donnerhacke

Category: Standards Track

IKS GmbH

H. Finney

PGP Corporation

D. Shaw

R. Thayer

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

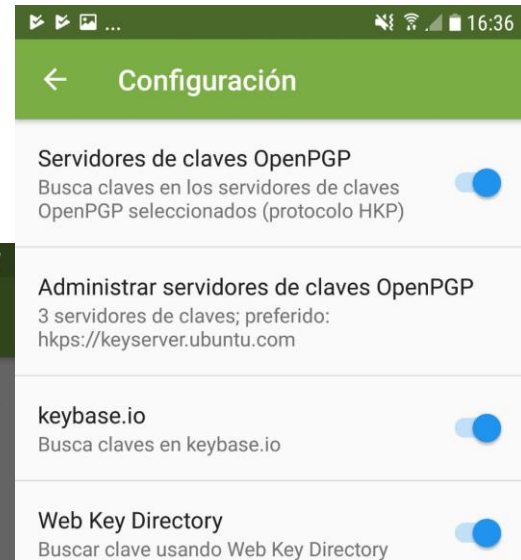
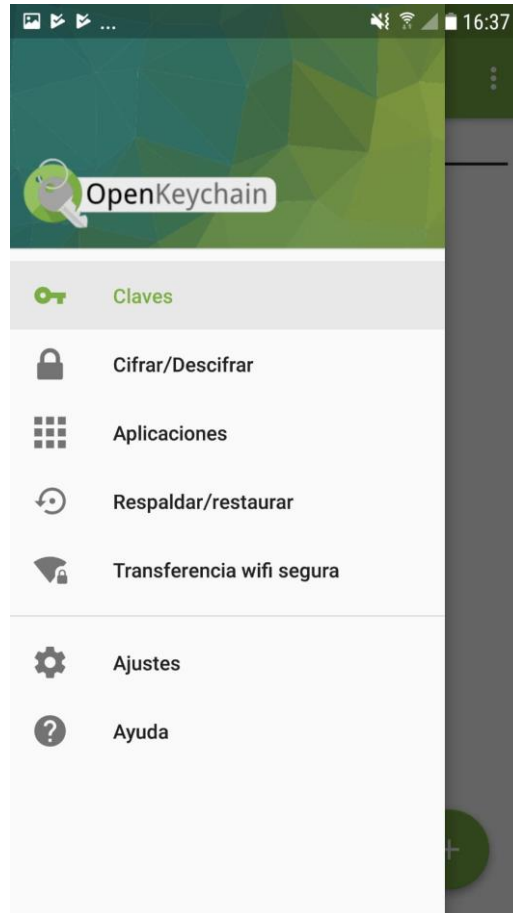
This document is maintained in order to publish all necessary information needed to develop interoperable applications based on the OpenPGP format. It is not a step-by-step cookbook for writing an application. It describes only the format and methods needed to read, check, generate, and write conforming 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: gpg4o1, Gpg4win, p=p
    - Thunderbird: enigmail
  - Mac
    - Apple mail: GPGTools
    - Mutt
    - Thunderbird: enigmail
  - Android
    - K-9 mail: Openkeychain
    - P=p
    - R2Mail2
  - iOS
    - iPGMail
  - Linux
    - Evolution: Seahorse
    - Kmail:Kleopatra
    - Mutt
    - Thunderbird: enigmail
  - Solaris
    - Mutt
    - Thunderbird: enigmail
  - ....

# OpenKeychain



Texto y ficheros

# iPGMail

Carrier 1:39 PM

Done Create Private Key Create

Passphrase

Confirm Passphrase

Key Size: 1024 2048 4096

Expiration: 0 D W M Y

Real Name: John Q. Smith

Email Addr: user@domain.com

Carrier 1:39 PM

Edit Public Private +

Public Keys

adele-en <adele-de@gnupp.de>  
4D486CC8 RSA(2048) 2013-07-08 2017-07-08

boo <boo@hoo.com>  
D4C8EB20 RSA(2048) 2013-07-23 (no exp)

foobar <foo@bar.com>  
CC33E7CC RSA(2048) 2013-07-29 (no exp)

FooFoo <foo@bar.com>  
818F5EE0 RSA(1024) 2012-01-03 (no exp)

Wyllys <wyllys@me.com>  
47E3234C RSA(2048) 2011-06-11 (no exp)

Keys Compose Decode Files Settings

Carrier 1:40 PM

Clear Sign Encrypt Both

From: foobar <foo@bar.com>

To: info@ipgmail.com

Attach: Select Attachments

Great job!

Keys Compose Decode Files Settings

Carrier 11:05 AM

Done Public Key Details

Public Key Info

Key ID  
47E3234C

User ID  
Wyllys <wyllys@me.com>

Fingerprint  
A5D0 EFBC 4A52 B587 E68A 2451 7FEA 1CCB 47E3 234C

Created  
2011-06-11

Expiration  
-----

Algorithm  
RSA (enc/sign)

Image  
N/A

Key Len  
2048

UID Info

Wyllys Ingersoll <wyllys@gmail.com>  
47E3234C 2011-06-11 -----

UID Info

iPGMail Support <info@ipgmail.com>  
47E3234C 2011-09-21 -----

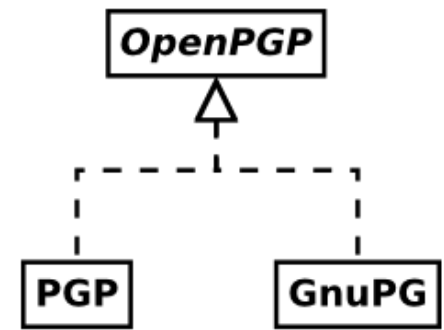
UID Info

Wyllys <wyllys@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)

keys

secret keys

lists

MyKeys

author

sample

new directory

refresh

secure delete

name	size	date
------	------	------

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

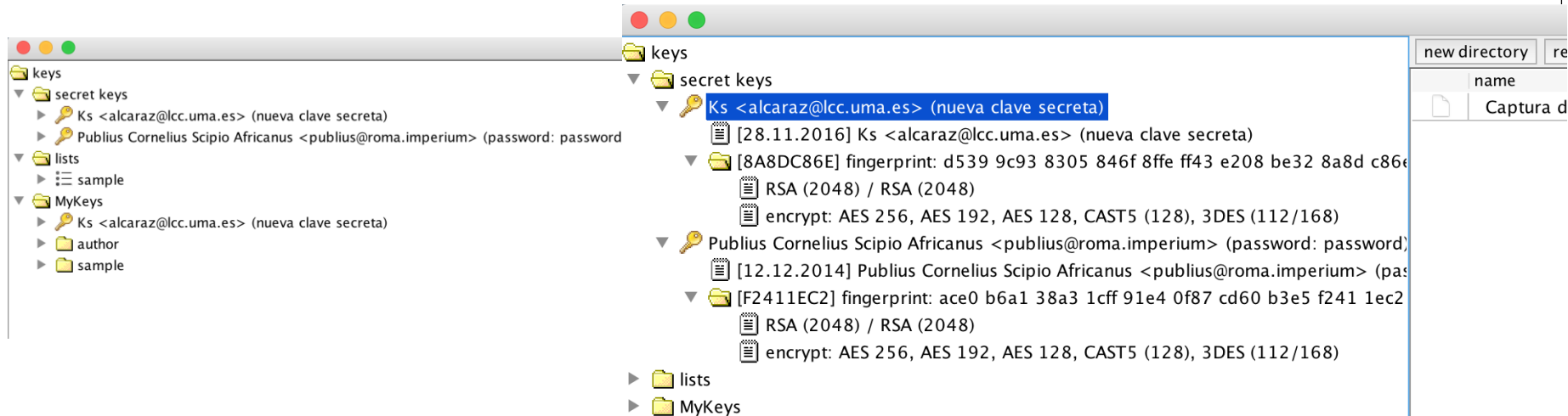
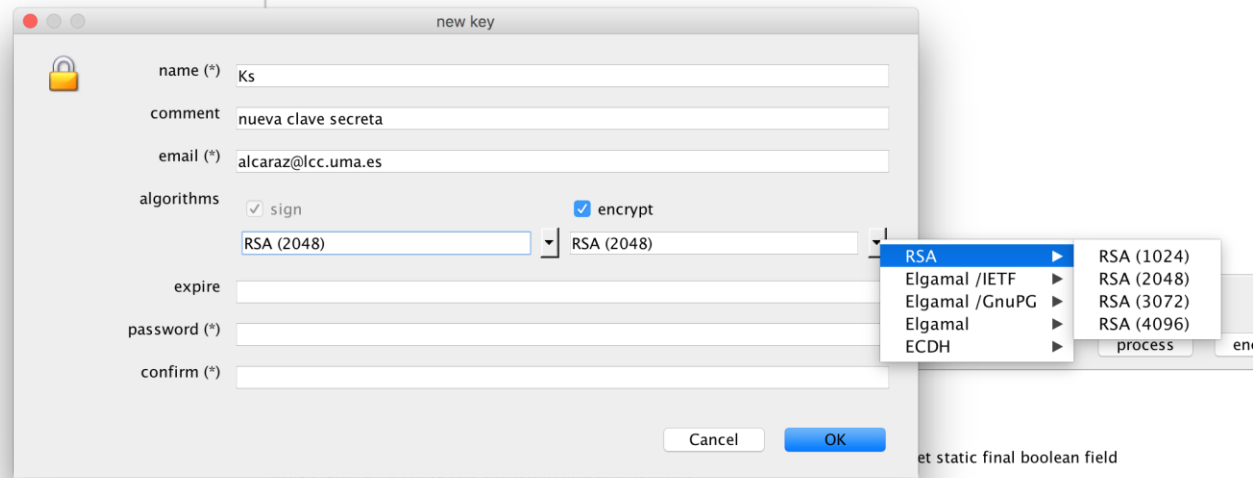
skip /Users/Cristina/Desktop/MyKeys/database.mypgp

skip /Users/Cristina/Desktop/MyKeys/MyPGP.exe

secure delete

# MyPGP

Creando una pareja de claves (privada y pública):



# MyPGP

Si se visualiza la  
clave privada:

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

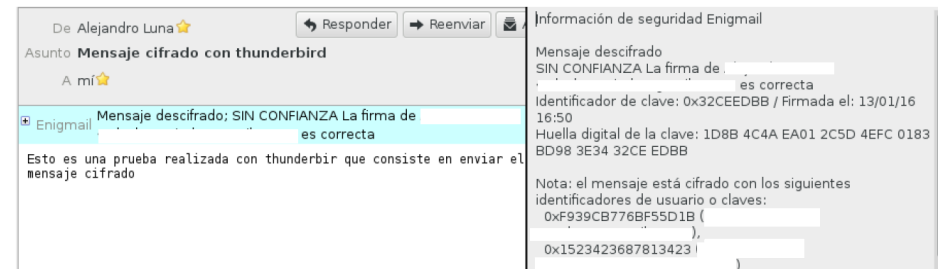
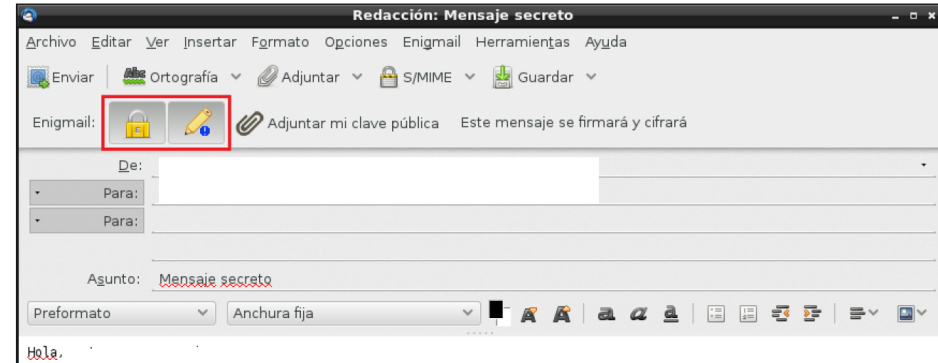
lQPBFg8cCABCAChL2mdceC4GKvyPROW2Y9Kbmo8u+g+/0C+rFy90g28P7a6JIEX
LQxhERg0FFFFeeCiHix/h7DmKLH+n5Ga0mHQHx2xyevvT/HWKKgGfByPt98i6boW
5pSa/k1mngx1Pw5CaNckoEB+TnAYNDu/6E/cPNNbqWn7nEBJ6dcG3ogZGweG/6hz
I4ksNak2rccRif0ZLwnt8RIuIFLihKUx0waWhX+GjY0pLhgiiyTQRr5ZiZiAYH
dKbnWhLRzQXqpKJsLHWG1N9BTfVUyqqa0Iqthz0nHJctzcR0Jo105n32vD6gko
0x+fqU0XIjvvyrPyT96cUL49E76P5aEKUueLABEBAAH+CQMiq7LzTuGUsbAU26m
6X7hiUj6tskb8Bjh+Wpa9k8bPLVfZz7Glv3007mt2icVKYhVhN3VfR4054XTNRn
qQwARrhgmXnFoa9o6aMW8ieB0eEUJ+gga0n3qatVw9TPNiRaaF8bpyliuBYDrr2D
20/iv2ub32jTysdzLYKbeT/L5A+GP5czQ3TMPNiYd5PqIgMwiiod6/PXd4Nku5PY
TsiC63qIlaVJCWtVnsPiCNOzJ5eVbQRVWESVb40DtYkxcw7MsLWaKLP0Ke6535w
5/LViZATedLaR0E0KNjvCSg4orzi+bwsL/TDJHcxRGZ1Hs+XkVLukU2asgPibizz
MTrh4M1K6pzEp/P4+F6lGre5wxluFFBQV08jW78zu3U6PvuvJn0x7TAFQ1nCz0fs
iZ3vbnw29y9IIXlosTW8Y2dGBQ8I3ae+LD2k09+uxnWcalRgkcUq10wFBeMGiSg
/TjRv4XvQUYQagf46PnoeU0XP7uGz67iYjn0tP+HmIvQd00LTtqx4dwI4R8JJJu
trdF67zYKV541Xqzib00T4xwUwaG4xKZA6JpoT92NbuSRUVW4Is3jCmWd/bD1cx
CSNVcz3jhcqodulBG6MgmDNvE4HccMaYMw5Fg2d1+K7G/arg8tNRhkqirJPdIEv
moXWEZLJZLBo0CWpW265lphlTcJ+se/+A0/crtVmgl9awdYiq4KQI0Ize+nR0E/5
tkSOTHTqJ1427lHKQmLOSziuzfQX4S0Unr4izHLS0P90aHGfDfckJXIHJ2monhs
t0L/E5YfYysCfY3USe3YkVv5XBjaipLQmd4RC69yR7MpioLGSNe4KJ1r7rYGYNN
Zw6eXv1UuUmqJFK42JU8V1/PYKfG9W/5calCawC9GK790JQJ1RNqT2aCbCwdF3xf
+Lh9k8uShoYatC1LcyA8YwxiYXJhekBsY2MudW1hLmVzPiAobnVldmEqY2xhdmUq
c2VjcmV0Ym5tATUEEwIAB8FAq8CECGwG6CwkIBwMCBBYCAwEFGQJCsCAh4B
AAoJE0iVjKKjchuFtAH/RHURetobj+GJR9MSID848RboXhfoYLKsAgsCqAsK/7
B8XvrZaE/B89G1CIG29ghgn3PB48HQNYZT0qWmN13r0ADuqNh5rCToSfC0fTL8Gs
a40RGEMy57h/sFVCBH/VFRbvjdZJUaBe7vvnX/05vcaEa5pd4N8j0Wkt7MF8FAr
0vynzJj+IdCvthQ9vqD1k1+49T94XMwZ7KmkR/oa3JYvJU5trh5ukAvYkmkDBm/G
HDM2qyFt9EowTtpbrqWhlWRsaxrVzcKvX15rHa3Im7b16wD05pCqA968DJr9xyi
lPAmZQW2zehuA4nFqIR3xRZJQEKzhgIavUbeonpNijidA8UEWdxwIAEIAKm0duWt
7dh51E+UpEHXf7/eY00M1eCu/M4GF0oVxZPR7Vjfd/issHbFMy8SB+iGN1sk93R+
vfffw91XT+S5h913sEQiRbb+ZqsADZZdsDQovTFdc0vPZhng9EILkNLnQMU060p
t0k+d7gtJG/aoBElkfxkkih+UMqs6z2fXL0MBKScP+GMVHXbDLIKam2bTnQLB8TLQ
5qpZ9eNQC+ld8m6enBvxtHkXw4dzIHBGTyKaKxjrvj8A9pmvc9ux7FZJYEJWENU0
6HFnNgW5s51Cw1Ax28XmwAd0YlTqB/Gydc5ts0TGaI2pY26TJnayFq3jIhmghk
SQMm9qR3512rMXUAEQEAf4JAwiruXN04ZTCxsAG802KhS+V16NHXUSH78pru6ut
w1u6s7RNWbHouq2znRku8kiVQab7XRkrtjZ0dkZ0iIOPX9ctaJIH4WmuYWG2mLoTJ
RCp3bt07EMPhAbmzH+07LYE+LNYczAHuV0sLw2db08T5MjKKT9LDrCX0w6iFuYIA
jE5nfnboq3gm7mxz5hk0VJi1npl0e41nziGKjdI0Z+B/RVQJV90nd2Lx8LHgmL0
60rnpMtzJqN1JWS4uf3aV8jtvcI9lu7Hw70PpP1zSEM9J9DEP01MLD6h3h/7N11
qyRtrPszHaZZB+M9uUX9+rjYsBq3BvWCWiu5Nqakyz0/76w2Y2saivlqp30E1ff
4/lAw/fsdhVT49sMiE0d1pxExksZxcRvMTA2NIBiET6n556okfEqMo9a1XcG0H/Y
1Nos9l0F48+1TILTi0mIxzVaYjzx+qRWQjS2KLk1ITHEV6+xNxxutufxMLPYD92Y
KdGwhDnDjN2AKGgeWx6Jv0hmnjGBK5xZ7BAPlqww1MErPMBRiWzq+3eDdzf4MwUq
UkPuzfoDqL9pHyOeCtMKWJ51qiaemzuLatiJ8bUC16pXhmFRYyEYL4L3eq1v8yg
bCcDCLA7loqj+7x1m0/dbWh5TV65nCi9P5BQI2BtLatln1ur3Rvmy8DC8k/mhK03k
Exr65A05qyGE0o2IJdna/6ew3DkWKJC90XH0+W7XzM0cvNC7YSWESZwfE2J10xz/
jH7MaMT45Hg565YFWU9ULIwDgh80kTVsw0vx88A6RBZ6Li4bK93Bd1LzL+nWUXP
tsuw1BD+zYl2CIBXZHWPMijCst/OvqLNSXh7Z6mrcG4BqfZv+u1pZhwU3MFOe0j
Ee9NwjbhfmkwbRBvW03ZW69hdwuUjZUur+tyFHEB4UnUr740/WbT4k8HwQYA0gA
COUCWdxwIQIBDAKCRD1CL4yio3IbiwuB/9GbtTfXjWVzrFicAa90GuRSvVfS/7F
r4QHuKXxKoPnw6SSgLIsc4YkkPRgzmxkKiC6uLoe1tZmxxNwKTNoy4vnsY/LD
HNqS0/LFN5UkpmLbcRmKkPtX0grUK6MT2q5/b5GnAAxmwW1tpU1UDDEfxbH3LP/H
QEJMD09dL7+bo1nrgHtIubIMwVlVZDR0M+qLx570QGvcFu+0+bBKDAfrFWNi1johx
idJBHfupv0k19FSXEmGPexJW1Iuz55ccY560uXH1yuW3xq5jyLHTmWGZSiDuL+D6
IQqzSolrI7R6Wlm0cLo30++RyIdnL5F+4DfZB6+70UW5INg16CcaqhXw
=m3c+
-----END PGP PRIVATE KEY BLOCK-----
```

# MyPGP

The screenshot shows the MyPGP application window with the title bar "MyPGP (7.5.2016)". The menu bar includes "Main", "keys", "lists", "clipboard", "files", and "language". The "clipboard" menu is open, showing options: "view", "encrypt", "sign", "encrypt & sign", "decrypt & verify", and "decrypt & verify". The left sidebar shows a tree view of keys under "secret keys", including "Ks <alcaraz@lcc.uma.es>" and "Ks2 <a@lcc.uma.es>". The right sidebar shows a file list with "prueba.txt" selected and "prueba.txt.asc" below it. Buttons for "new directory", "refresh", and "secure delete" are visible.

The screenshot shows the MyPGP application window with the title bar "MyPGP (7.5.2016)". The menu bar includes "Main", "keys", "lists", "clipboard", "files", and "language". The "files" menu is open, showing options: "encrypt", "sign", "encrypt & sign", "decrypt & verify", and "secure delete". The left sidebar shows a tree view of keys under "secret keys", including "Ks <alcaraz@lcc.uma.es> (nueva clave)", "Ks2 <a@lcc.uma.es>", and a folder "[179701F4] fingerprint: 03ca 09a4 c6db 5175 1351 1fff e344 548c 1797 01f4". The right sidebar shows a file list with "prueba.txt" selected and "prueba.txt.asc" below it. Buttons for "new directory", "refresh", and "secure delete" are visible.

# Enigmail



# Enigmail

▼

Server Settings

Copies & Folders

Composition & Addressing

Junk Settings

Synchronization & Storage

OpenPGP Security

Return Receipts

Security

▼

Server Settings

Copies & Folders

Composition & Addressing

Junk Settings

Synchronization & Storage

OpenPGP Security

Return Receipts

Security

▼

Local Folders

Junk Settings

Disk Space

Outgoing Server (SMTP)

Account Actions ▼

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

☐ Use email address of this identity to identify OpenPGP key

☒ Use specific OpenPGP key ID (0x1234ABCD):

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

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

# 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 Vd.:

Antonio Gamarro

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

Redacción: Prueba S/MIME

Archivo Editar Ver Insertar Formato Opciones Herramientas Ayuda

Enviar Ortografía Adjuntar Seguridad Guardar

De:

Para:

☒ Cifrar este mensaje

☒ Firmar digitalmente este mensaje

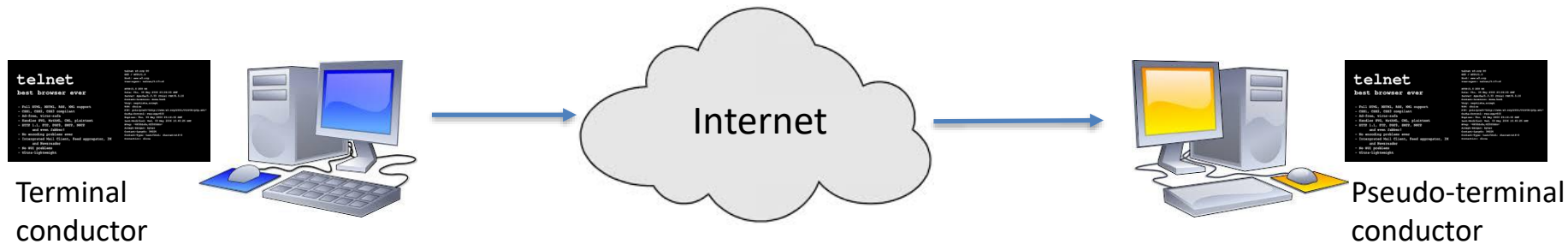
Ver información de seguridad

```
smime.p7m
1 0EACK *tHt÷
2 SOHBELETX €0€STXSORNU1,SOH$0,SOH STXSORNU0^0,1V0 ACKETXUEON!
3 ACKETXUEOTESDC3ACKMalaga1$10
4 ACKETXUEOTESDC3ACKMalaga1$30
5 ACKETXUEOT
6 DC3ETXUMA1$30
7 ACKETXUEOTVTD3ETXUMA1DC20DLEACKETXUEOTETXDC3 Cristina 1!0US2
8 SOH SOHSYNDC2alcaraz@lcc.uma.esSTXSORSTX0
9 ACK *tHt÷
10 SOH SOH SOHENONNULEOT€'8>,'NAK@'#i-c-ò*,~jÕj («„d£ò~DC1[2v, SUBÕ0úSOi
11 \Iq„iñÀDC4iè80CANiA<GDLE=IX'EE/$éeSI66NAKI DLEF8Jg\%Sf]ÓáuâI)ETBK
12 SOHBELESOH0DC4ACKES*tHt÷
13 ETXBELEOTESCP+t`aG €EOT,
14 @'ES3ñ`*p+SUBâ2,D/[0,4â3G*E`t`!i@GShf923Í]GSLjETX«`%*iBMVACKx8Ç_
15 eiDC4aA@e)1=NøÇP2^OVÜB<~Vúcf0â`US«`âÄí-iôûEvY6è¥DC1ZcE\3[ÍrT<h#Kný.
```

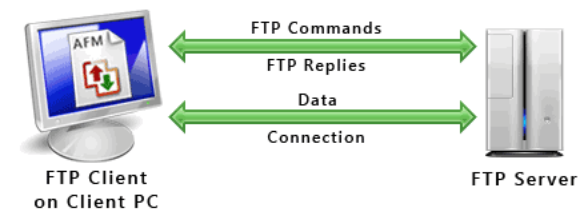
# Telnet (TELeType NETwork) y FTP (File Transfer Protocol)

- Características funcionales:

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



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

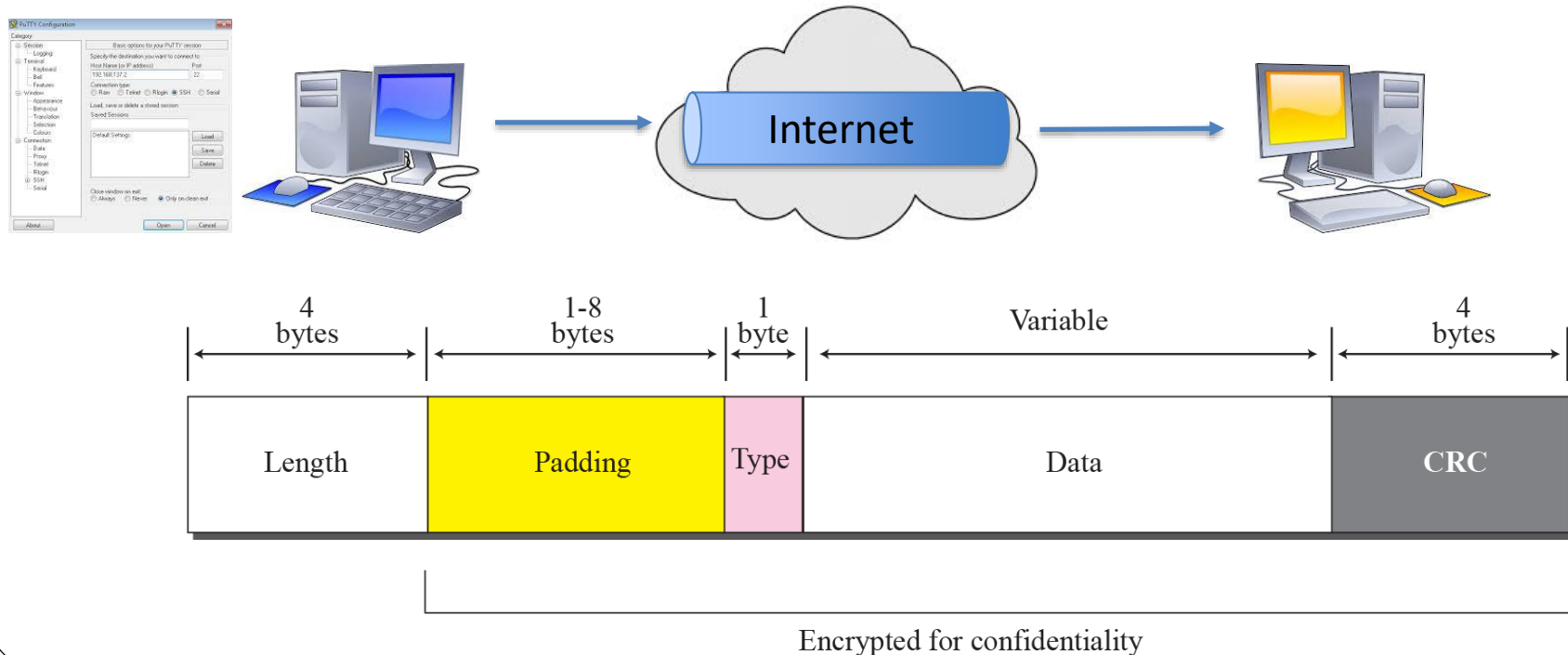


- Problemas:

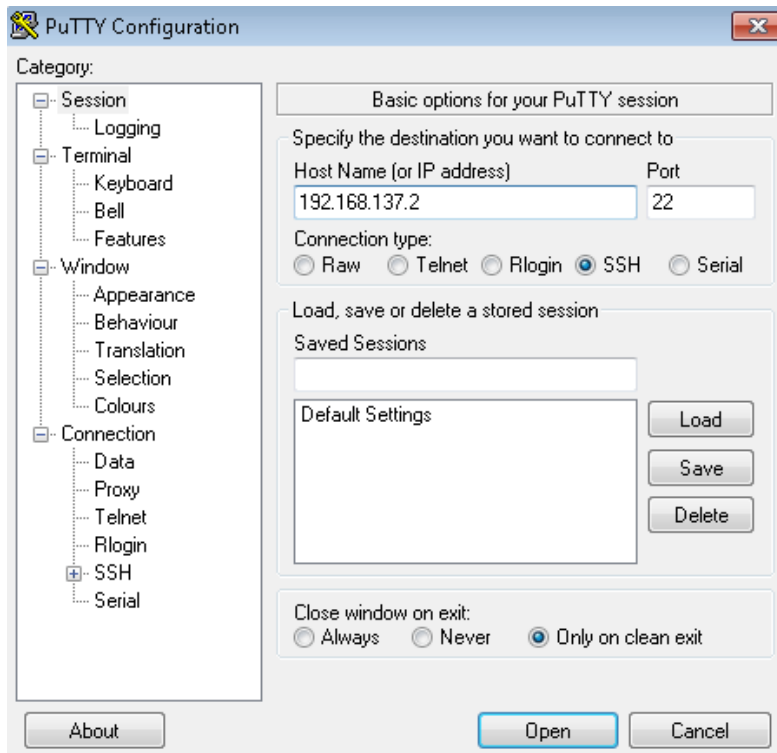
- La información transferida y las acciones remotas se realizan en claro, por lo que no se recomienda su uso

# 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



- Funcionamiento general:
  - **Capa de aplicación:**
    - Gestiona la autenticación del cliente haciendo uso de un usuario/contraseña o aplicando 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**
    - nodos remotos intentan suplantar la identidad de otro nodo de la red
  - **spoofing de DNS** en donde el atacante trata de suplantar el nombre del servidor



# PuTTY

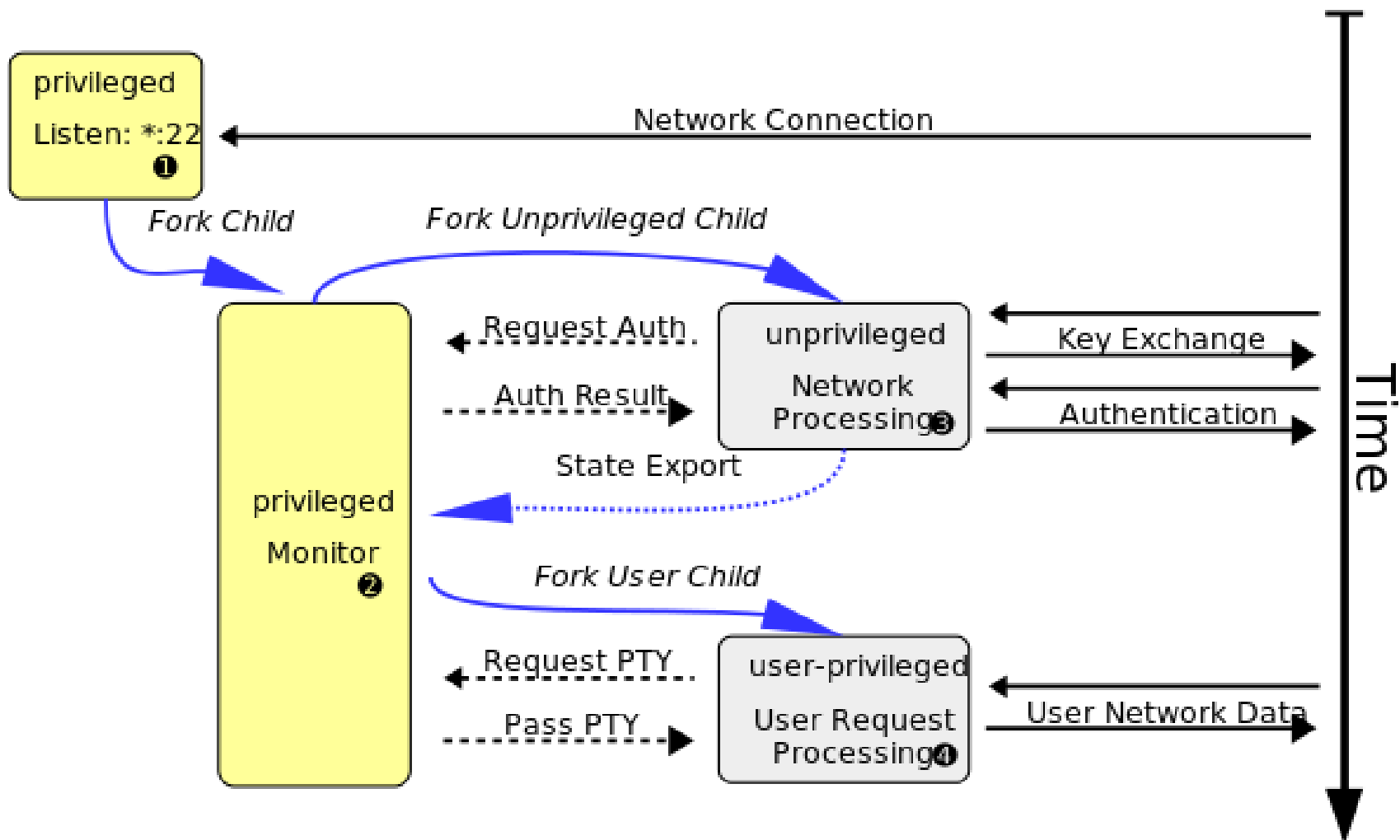
# OpenSSH

```
vdi-6E20:~ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/Users/ /ssh/id_rsa): hola
[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:GXD2RJHZboy0wveGP14B1emRo0zTxY2degkktiuK3va
The key's randomart image is:
+---[RSA 2048]-----+
|  . o.+0oo o |
| + +Boo.=+. |
| ...=B .+oo |
| o++o*+. |
| S+o=oo . |
| . . o.o.. |
| o . . . |
| . + o. |
| . E . . |
+---[SHA256]-----+
```

- 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 de SFTP:
  - Se puede basar de diferentes modos de autenticación 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

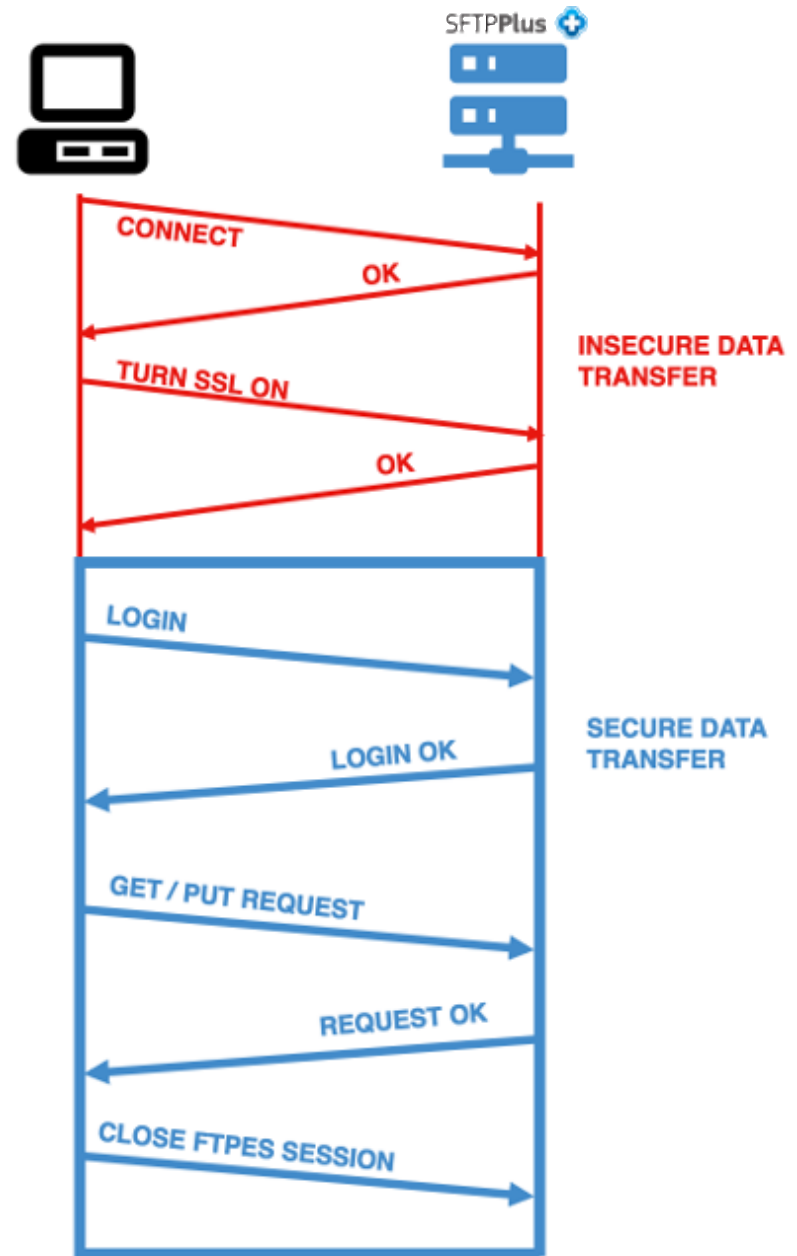






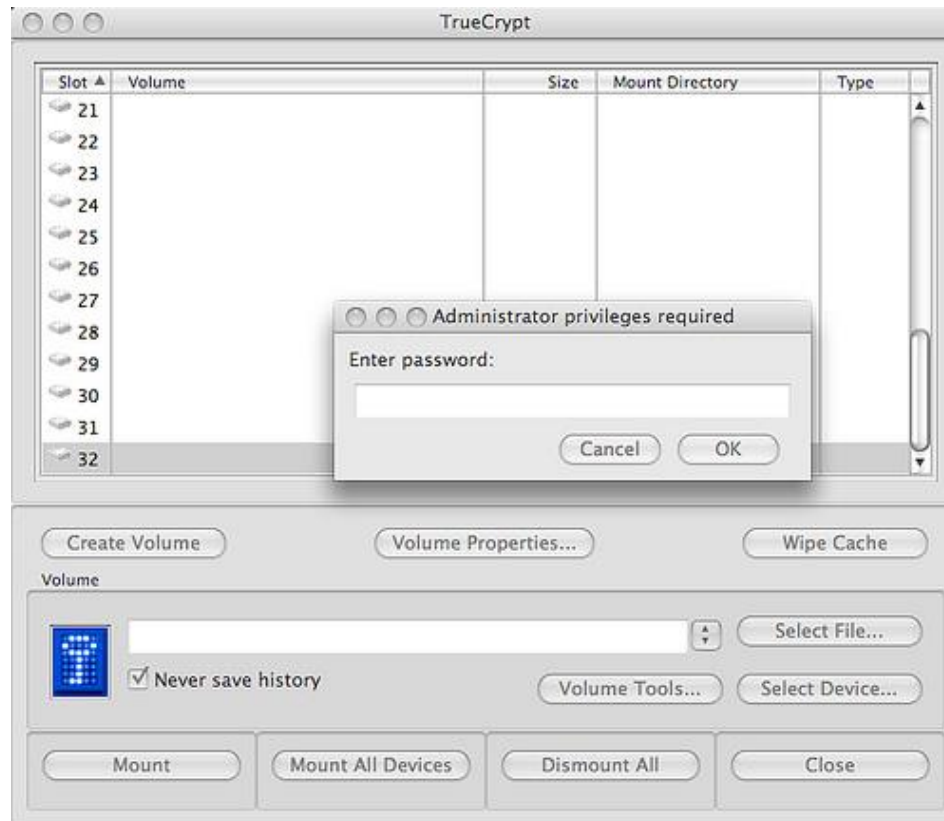
# FTPS (FTP Secure)

- 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

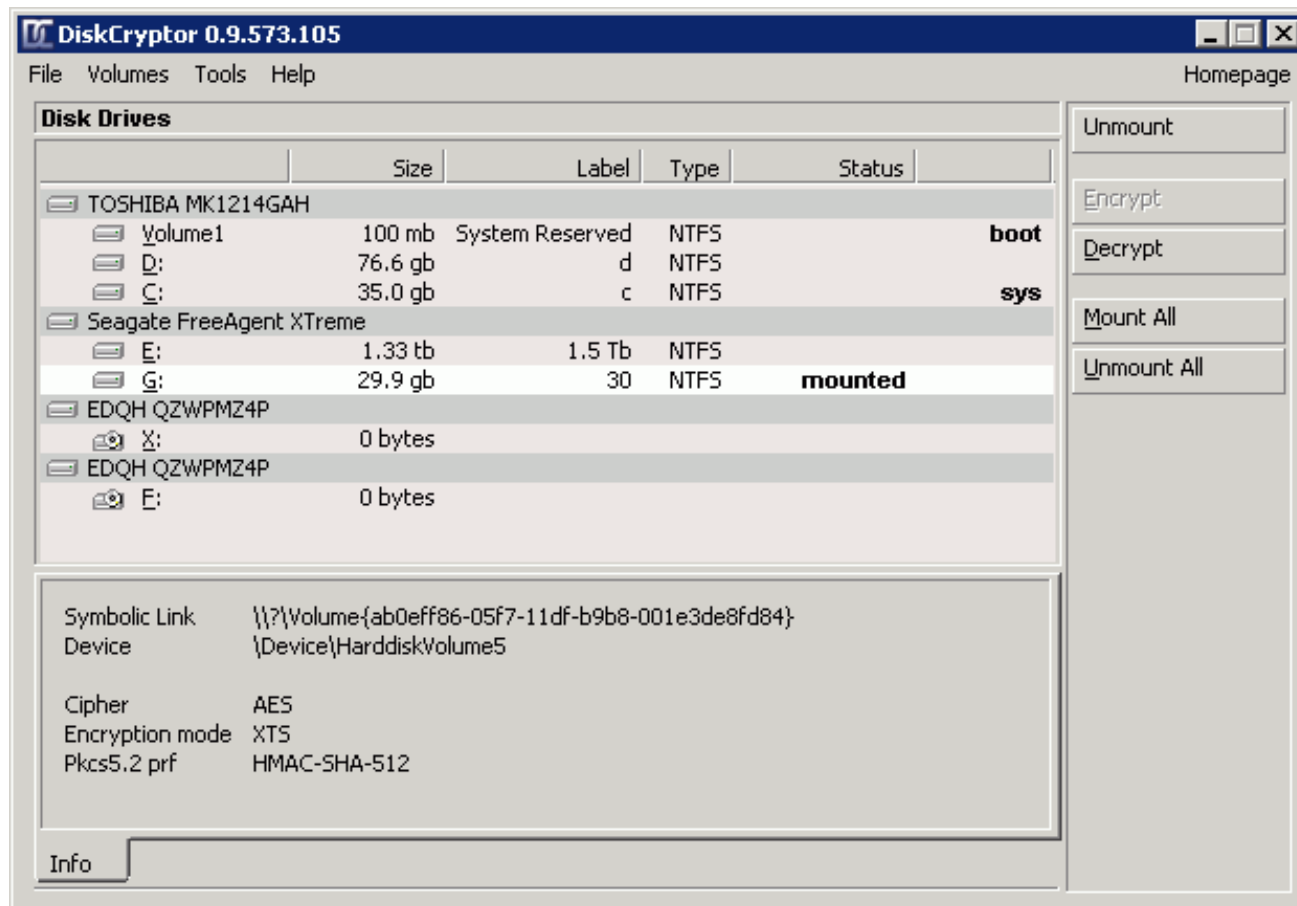


# Herramientas de cifrado open-source

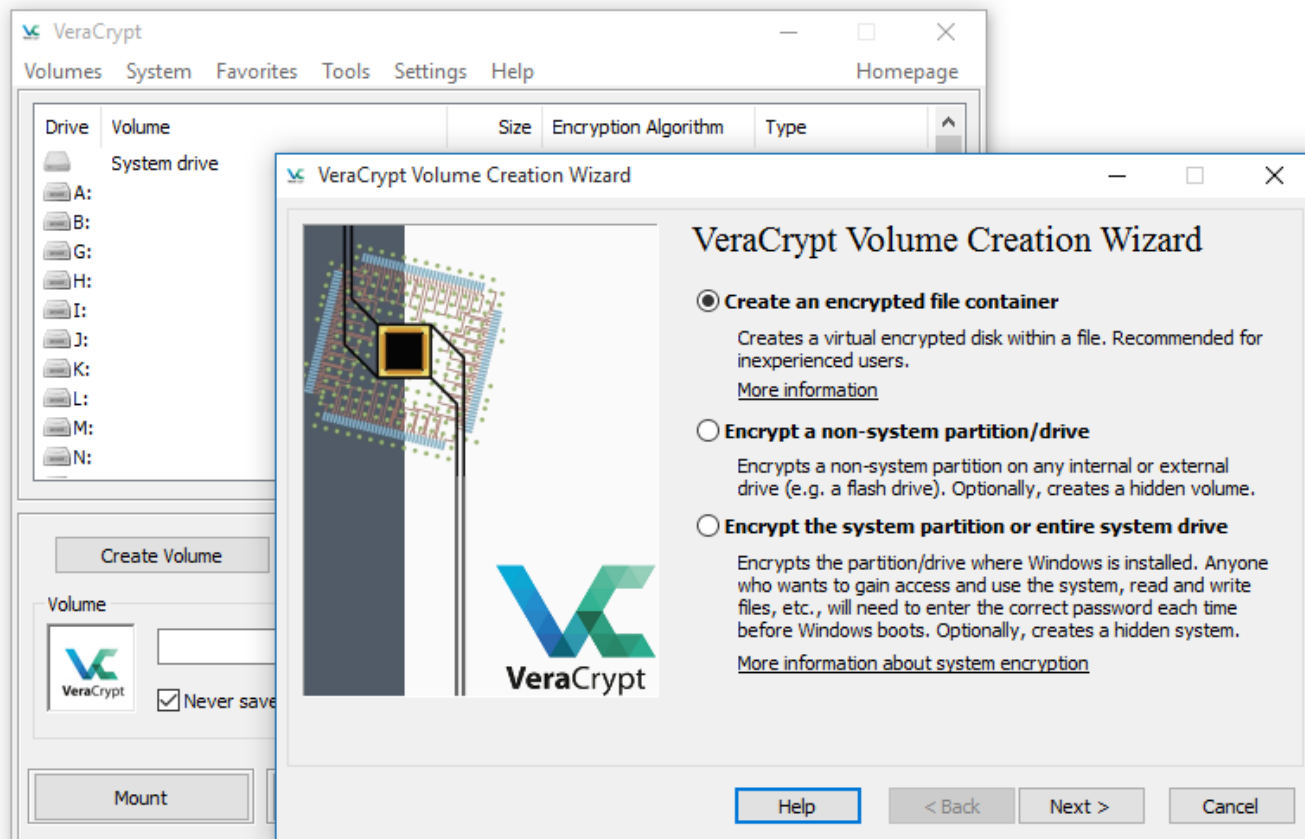
- **TrueCrypt:** herramienta de cifrado de discos duro disponible para Windows (XP/2000/2003) y Linux, haciendo uso de AES-256, Blowfish, CAST5, Serpent, Triple DES y Twofish
  - También permite ocultación de particiones haciendo uso de cifrado y aleatoriedad de la información



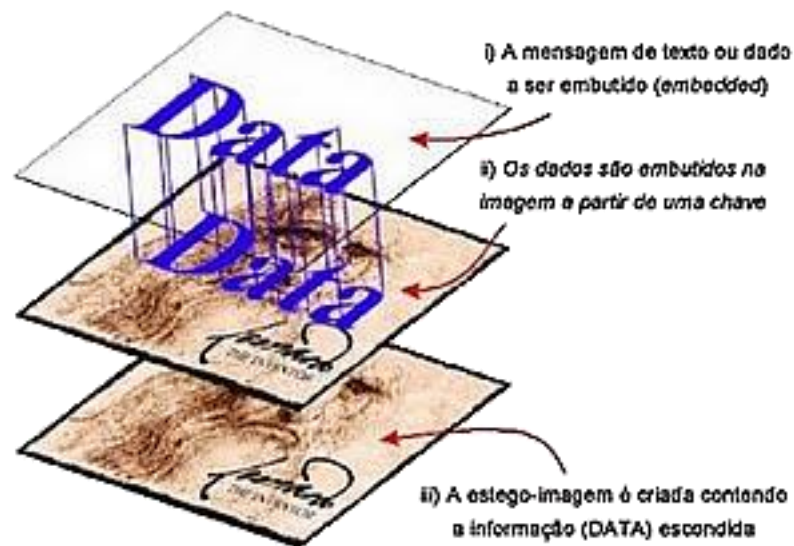
- **DiskCryptor**: similar a TrueCrypt pero con capacidad de cifrar dispositivos de almacenamiento externo USB
  - También incluye algoritmos de cifrado como AES, Twofish y Serpen



- **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 Serpen

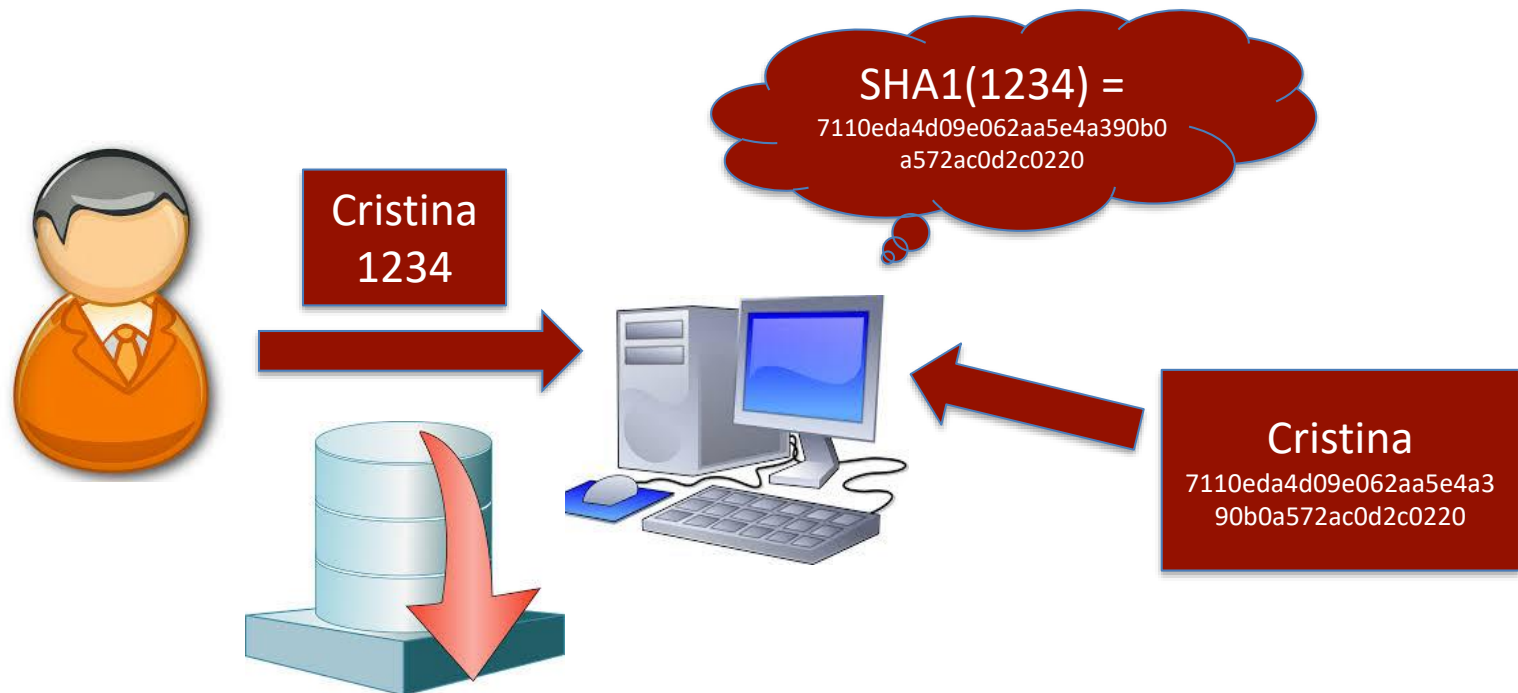


- **OpenStego**: aplica técnicas de **Esteganografía** (del griego "cubierto" u "oculto", y "escritura") para ocultar información haciendo uso de imágenes o cualquier archivo multimedia
- **OpenPuff**: es similar a OpenStego para Windows con soporte para BMP, JPG, MP3, WAV y MPG4



# 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



- Sin embargo, 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

