Grid y Computación de Altas Prestaciones

GRyCAP

P.G.1. Seguridad en un Entorno Grid

Conceptos Básicos de la Computación en Grid y Cloud

Prácticas

Grid y Computación de Altas Prestaciones
GRyCAP

- PRÁCTICA 1: Instalación de una CA
- PRÁCTICA 2: Creación de Certificados Grid (Crear Certificados de Host y de Usuario).
- PRÁCTICA 3: Cifrado y Descifrado Mediante PKI.
- PRÁCTICA 4. Crear Proxies mediante GSI.

Grid y Computación de Altas Prestaciones
GRyCAP

PRÁCTICA 1: Instalación de una CA

P1: Instalación de una CA

Grid y Computación de Altas Prestaciones
GRyCAP

- Sitúate en la carpeta siguiente:

```
[ccgc@XXX~]$ cd /home/ccgc/Evidencias/Grid/01_Seguridad/P1
```

- Todos los ficheros que generes en esta práctica debes de guardarlo en esta carpeta para que consten como evidencia de su realización.

P1: Instalación de una CA

[ccgc@XXX ~]# cd $HOME/Evidencias/Grid/01_Seguridad/P1
[ccgc@XXX ~]# sudo grid-ca-create -force

Certificate Authority Setup

This script will setup a Certificate Authority for signing Globus users certificates. It will also generate a simple CA package that can be distributed to the users of the CA.

The CA information about the certificates it distributes will be kept in:

/var/lib/globus/simple_ca

The unique subject name for this CA is:

cn=Globus Simple CA, ou=simpleCA-damian.ccgc.mastercpd.upv.es, ou=GlobusTest, o=Grid

- Indicar que quieres mantener el DN

Do you want to keep this as the CA subject (y/n) [y]: y

P1: Instalación de una CA

- Indicar el correo de contacto establecido por defecto pulsando INTRO.

```
Enter the email of the CA (this is the email where certificate
requests will be sent to be signed by the CA) [root@damian.ccgc.mastercpd.upv.es]:
```

- Indicar los días que quieres que sea válida la CA (por defecto 5 años).

```
Enter the email of the CA (this is the email where certificate
requests will be sent to be signed by the CA) [root@damian.ccgc.mastercpd.upv.es]:
    The CA certificate has an expiration date. Keep in mind that
          once the CA certificate has expired, all the certificates
          signed by that CA become invalid.  A CA should regenerate
          the CA certificate and start re-issuing ca-setup packages
          before the actual CA certificate expires.  This can be done
          by re-running this setup script.  Enter the number of DAYS
          the CA certificate should last before it expires.
[default: 5 years 1825 days]:
```

P1: Instalación de una CA

Grid y Computación de Altas Prestaciones GRyCAP

- Indicar la contraseña para firmar los certificados

```
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
Installing new CA files to /etc/grid-security/certificates... done
Creating RPM source tarball... done
        globus_simple_ca_XXXXXXXXXX.tar.gz
```

En este punto ya tienes instalado una CA para pruebas

P1: Instalación de una CA
Evidencias

- Al final de esta práctica deberás de haber generado en la carpeta "/home/ccgc/Evidencias/Grid/01_Seguridad/P1"los ficheros siguientes:

globus_simple_ca_XXXXXXXX.tar.gz → certificados y configuración

openssl_req.log – Log de instalación de la simple CA

Grid y Computación de Altas Prestaciones
GRyCAP

PRÁCTICA 2: Creación de Certificados Grid de Usuario

P2: Creación de Certificados Grid de Usuario

Grid y Computación de Altas Prestaciones
GRyCAP

- Sitúate en la carpeta siguiente:

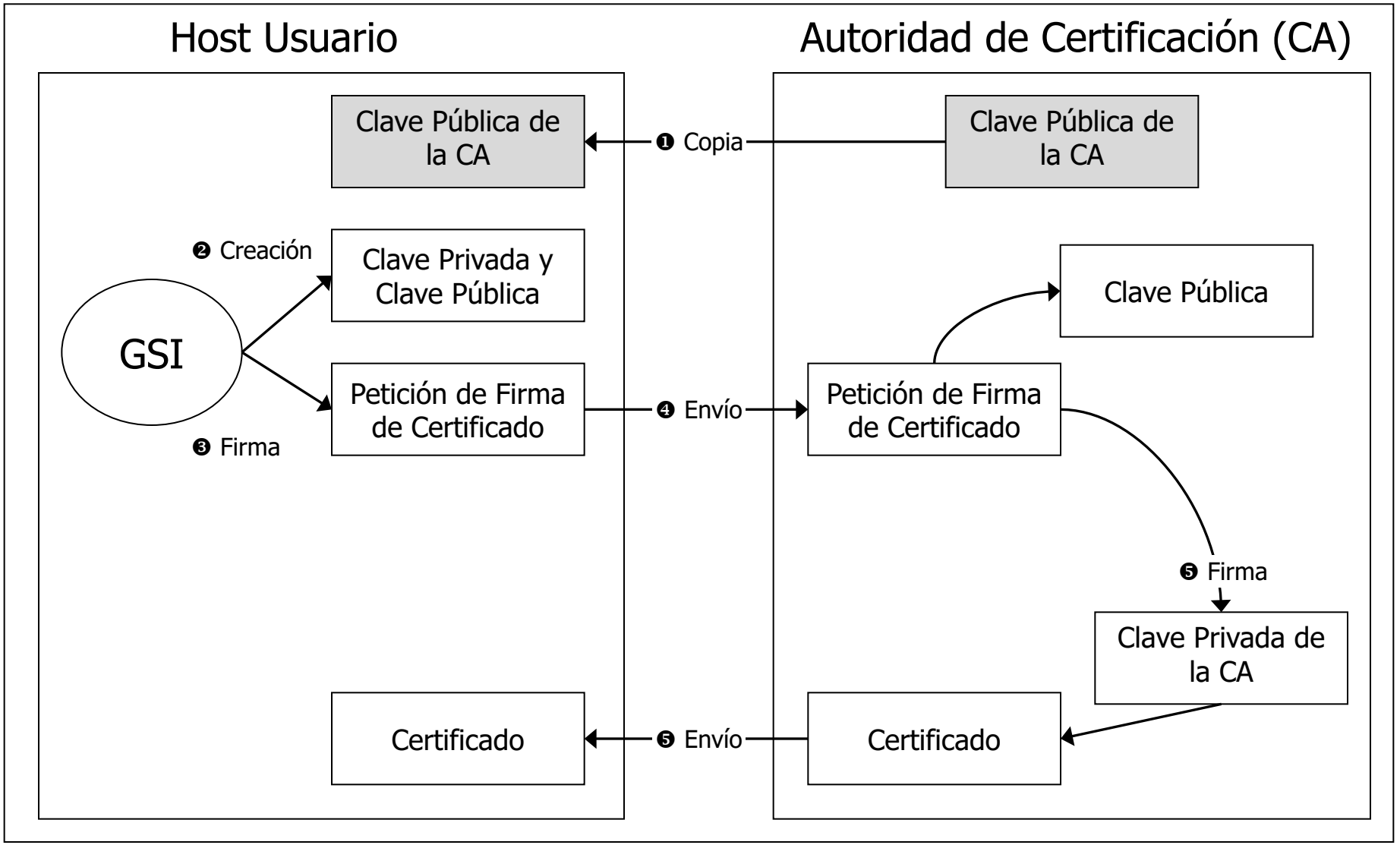
```
[ccgc@XXX~]$ cd /home/ccgc/Evidencias/Grid/01_Seguridad/P2
```

- Todos los ficheros que generes en esta práctica debes de guardarlo en esta carpeta para que consten como evidencia de su realización.

P2: Creación de Certificados Grid de Usuario

- Para Poder Integrar un Recurso en el Grid o Poder **Utilizar algún Servicio o Recurso del Grid como Usuario**, es Necesario Disponer de un Certificado Firmado por una CA Confiable, Además de Disponer de la Clave Pública de Dicha CA.
- Los Pasos son
  1. Copiar la Clave Pública de la CA en el Host Grid Donde se va a Crear la Petición del Certificado.
  2. Crear la Clave Privada (y la Clave Pública) y la Petición para la firma en la CA de la clave pública que contenga la clave publica.
  3. La Usuario Firma la Petición de Certificado con su Clave Privada.
  4. Enviar la Petición del Certificado a la CA por e-Mail, web u Otra Forma Más Segura si es Posible. Al enviar la CA Verifica la Integridad de la Petición del Certificado Descifrando el Hash con la Clave Pública del Usuario (Contenida en el Certificado). De Esta Forma se Verifica que el Solicitante Dispone de la Clave Privada.
  5. La CA verifica la Identidad del Solicitante y Firma la Petición del Certificado y la Envía de Vuelta.

P2: Creación de Certificados Grid de Usuario
Paso 1 – Copiar Certificados de la CA



P2: Creación de Certificados Grid de Usuario
Paso 1 – Copiar Certificados de la CA

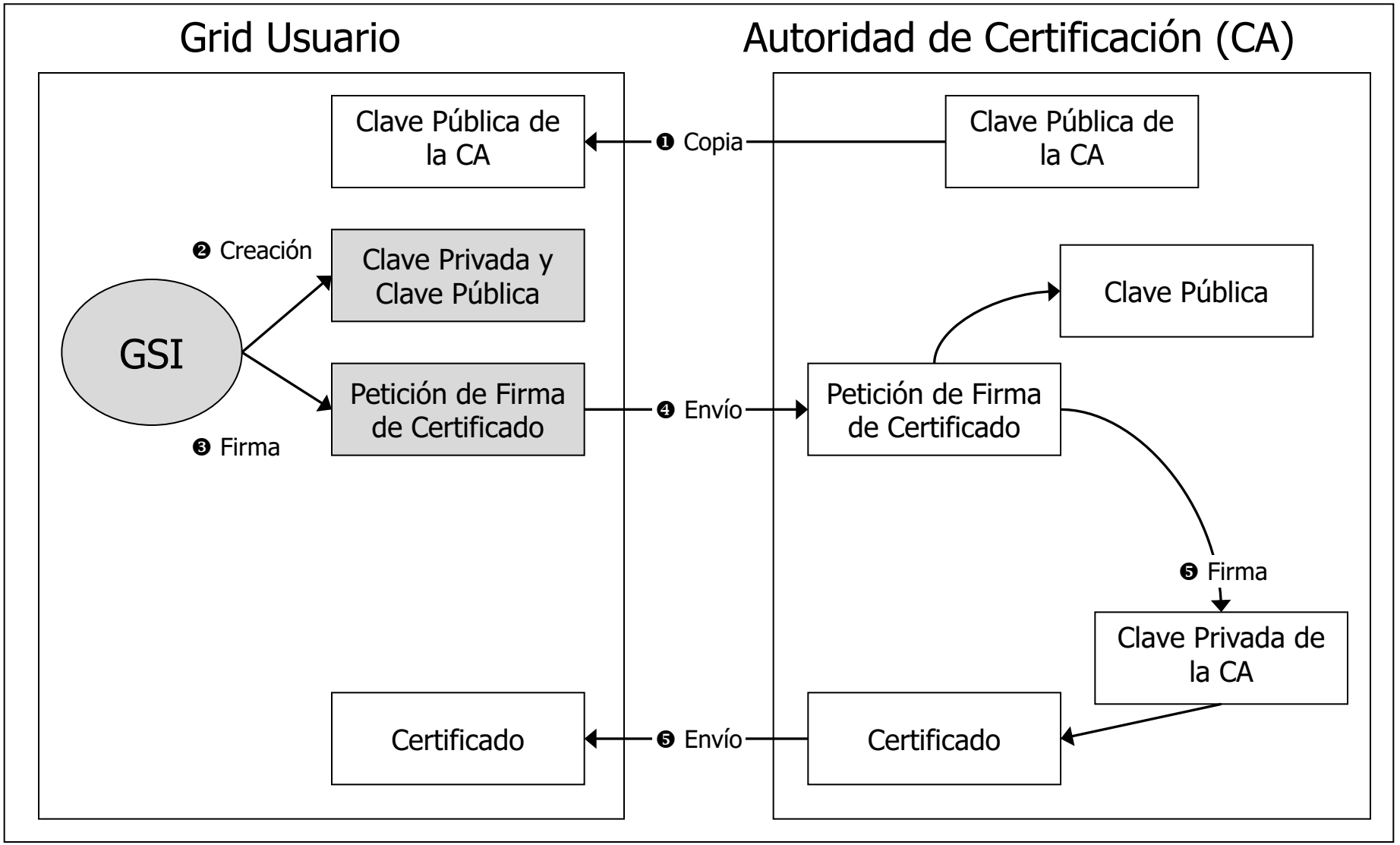
Grid y Computación de Altas Prestaciones GRyCAP

- Inicialmente hace falta una serie de ficheros de la entidad certificadora que queramos utilizar:
  - Certificado de la entidad certificadora: 056e3fca.0
  - Signing Policy: 056e3fca.signing_policy
  - Configuracion general: grid-security.conf.056e3fca
- Todos estos ficheros se deben instalar en las maquinas que vayan a utilizar globus, en la carpeta /etc/grid-security/certificates
- Como veréis tendréis ya estos ficheros que se habrán generado en la P1, que corresponden a vuestra propia CA.
- Si queréis que sea un compañero vuestro quien os firme el certificado, deberíais de instalaros los ficheros de la CA de vuestros compañeros.

P2: Creación de Certificados Grid de Usuario
Paso 1 – Copiar Certificados de la CA

- Dado que tenéis que confiar todos con todos, se deben de transferir todas las claves publicas de las CAs (alumnos) a vuestras maquinas (no os preocupéis, esta tarea la realizará el profesor durante la semana).

P2: Creación de Certificados Grid de Usuario
Paso 2 y 3 – Generar Solicitud de Certificado

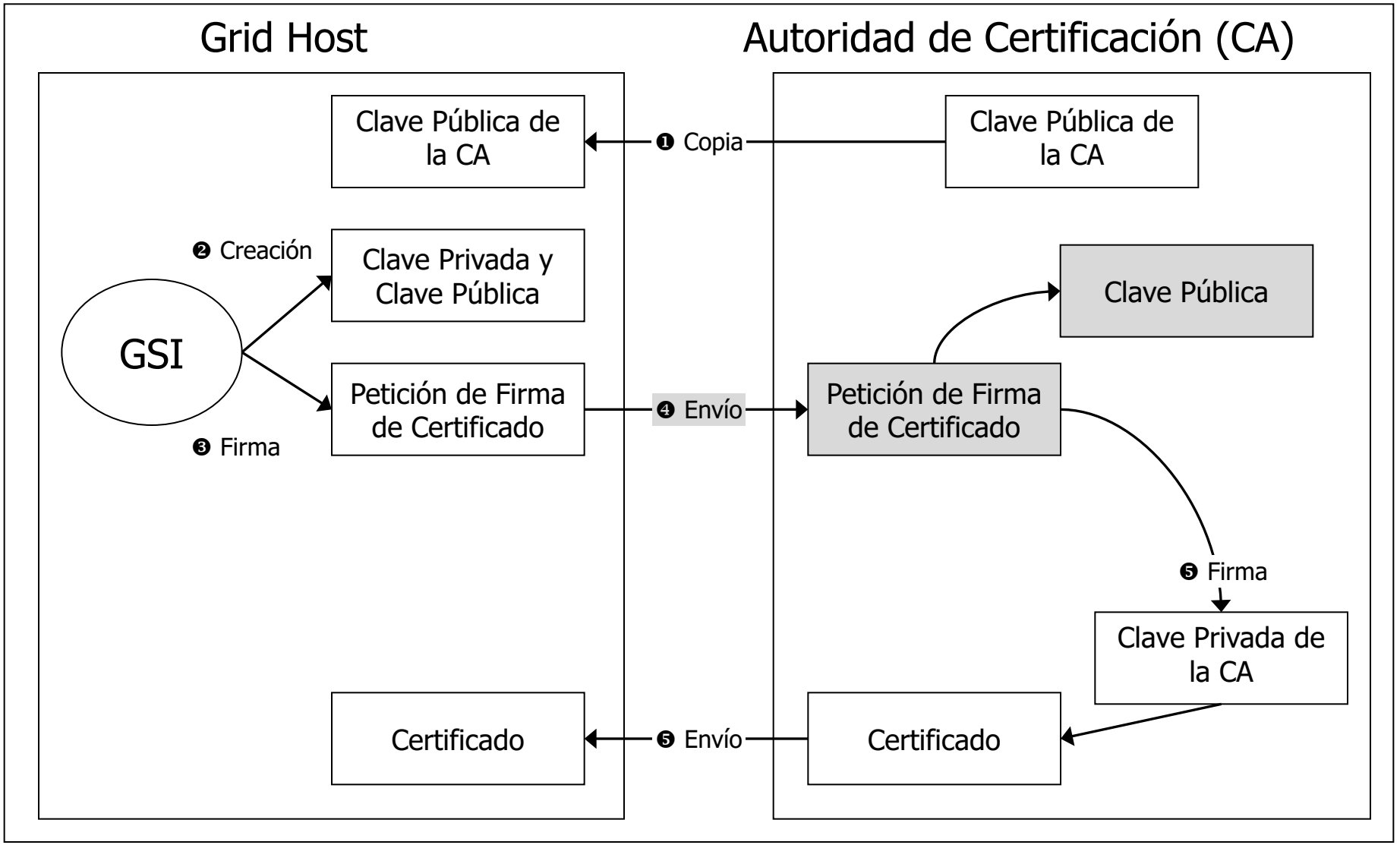


P2: Creación de Certificados Grid de Usuario
Paso 2 y 3 – Generar Solicitud de Certificado

Grid y Computación de Altas Prestaciones GRyCAP

- Crea una petición de Certificado de usuario
  - *grid-cert-request -ca -int -dir .*
    - *Seleccionar de la lista la CA del master*
  - *grid-cert-request -ca* 056e3fca *-int -dir .*
    - *Directamente utiliza la CA del master*
- Al hacerlo se piden una serie de datos, excepto el nombre, el resto pulsar Intro para dar los valores por defecto:
  - Nombre (e.g., John Smith) []: Poner nombre del usuario junto con vuestros apellidos (p.e. J. Damian Segrelles Quilis)
- Este comando crea la clave privada, genera la petición de certificado y lo firma con los datos que se acaban de introducir.
- **Debes de poner una contraseña a tu clave privada!! NO LA OLVIDES!!!!**

P2: Creación de Certificados Grid de Usuario
Paso 4 – Firma Petición Certificado



P2: Creación de Certificados Grid de Usuario
Paso 4 – Firma Petición Certificado

- Cada uno de vosotros va a firmar vuestro propio certificado con vuestra propia CA.

```
[ccgc@XXX P2]$ sudo grid-ca-sign -in usercert_request.pem -out usercert.pem
```

...

- Veras que los ficheros usercert.pem ya tiene la clave pública firmada por la CA.

P2: Creación de Certificados Grid de Usuario
Evidencias

Grid y Computación de Altas Prestaciones
GRyCAP

- Al final de esta práctica deberás de haber generado en la carpeta "/home/ccgc/Evidencias/Grid/01_Seguridad/P2"los ficheros siguientes:

usercert.pem ← Clave pública del certificado de usuario
usercert_request.pem ← Fichero de petición de certificado de usuario
userkey.pem ← Clave privada del certificado de usuario

Grid y Computación de Altas Prestaciones
GRyCAP

PRÁCTICA 3: Cifrado y Descifrado Mediante PKI

P3: Cifrado y descifrado Mediante PKI

- Sitúate en la carpeta siguiente:

```
[ccgc@XXX~]$ cd /home/ccgc/Evidencias/Grid/01_Seguridad/P3
```

- Todos los ficheros que generes en esta práctica debes de guardarlo en esta carpeta para que consten como evidencia de su realización.

P3: Cifrado y Descifrado Mediante PKI

Grid y Computación de Altas Prestaciones GRyCAP

- En la Explicación de la Unidad Temática se Han Visto Varios Modelos de Cifrado, en las que se combinaba el cifrado de datos y la firma.
- Los comandos OpenSSL que implementan estas operaciones son las siguientes:
  - Cifrado de un Fichero (Con Clave Pública)

openssl smime -encrypt -in <fichero_mensaje> -out <fichero_mensaje_cifado> <fichero_clave_publica>

  - Firmado (Con Clave Privada)

openssl smime -sign -text -in <fichero_mensaje> -out <fichero_mensaje_firmado> -inkey <fichero_clave_privada> -signer <fichero_clave_publica>

  - Verificación firma (Con Clave Pública)

openssl smime -verify -in <fichero_mensaje_firmado> -out <fichero_mensaje_sin_firma> -CApath /etc/grid-security/certificates/

  - Descifrado de un Fichero (Con Clave Privada)

openssl smime -decrypt -inkey <fichero_clave_privada> -in <fichero_mensaje_cifrado> -out <fichero_mensaje_descifrado>

P3: Cifrado y Descifrado Mediante PKI
Ejercicios – Tareas Previstas

Grid y Computación de Altas Prestaciones
GRyCAP

- Generar un fichero de texto con un Mensaje, en el que conste vuestro nombre. El fichero debes de llamarlo "mensaje.txt".
- Intercambiar Claves Públicas con un Compañero. El intercambio lo podéis hacer a través del comando scp, pidiendo a vuestro compañero que os diga su <<nombre de maquina>> e introduzca el passwd que utilicen para el usuario ccgc.

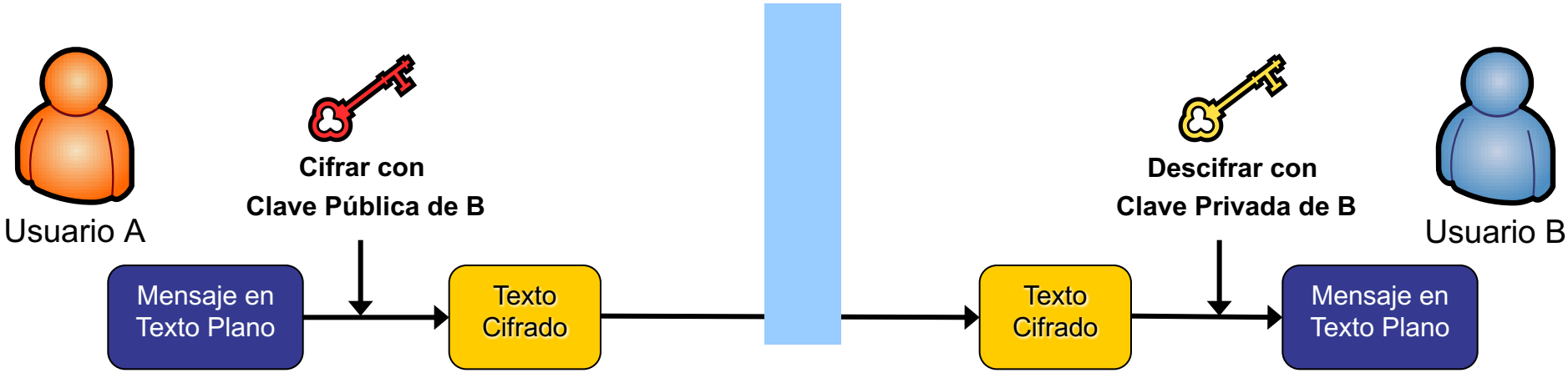
[ccgc@XXXP3]$ scp/home/ccgc/Evidencias/Grid/01_Seguridad/P2/usercert.pem
ccgc@<<nombre_maq_comp>>: /home/ccgc/Evidencias/Grid/01_Seguridad/P3/<<mi_nombre>>_usercert.pem

- En estos momentos, deberás de tener dos ficheros en la carpeta "/home/ccgc/Evidencias/Grid/01_Seguridad/P3" que son los siguientes:

mensaje.txt →Fichero de texto que contiene vuestro nombre
<<nombre_compañero>>_usercert.pem→Fichero con la clave pública de vuestro compañero.

P3: Cifrado y Descifrado Mediante PKI
Ejercicios – Escenario I

- Reproduce el escenario I representado en la figura.
- Crea una carpeta "/home/ccgc/Evidencias/Grid/01_Seguridad/P3/Escenario_I"
- Todos los Ficheros que generes en este ejercicio créalos en la carpeta "../P3/Escenario_I":



P3: Cifrado y Descifrado Mediante PKI

Ejercicios – Escenario I – Pasos a Seguir

Grid y Computación de Altas Prestaciones
GRyCAP

- **Paso 1. Cifrar con la Clave Pública del Receptor.** Utiliza la clave pública de tu compañero para cifrar el mensaje contenido "mensaje.txt" que contiene tu nombre. El fichero cifrado, debes llámalo "mensaje_cifrado_por_<<mi_nombre>>.txt".

  Nota: Guarda la clave pública de tu compañero en la carpeta Escenario_I como clave_publica_<nombre_compañero>.pem

- **Paso 2. Transferencia.** Hazle llegar a tu compañero el mensaje cifrado.

  Nota: Puedes transferirle a tu compañero el fichero cifrado a través del comando scp pidiéndole que introduzca su contraseña.

- **Paso 3. Descifrado con la Clave Privada del Receptor.** Utiliza tu propia clave privada para descifrar el mensaje recibido enviado por tu compañero "mensaje_cifrado_por_<<nombre_compañero>>.txt" que contiene tu nombre. El fichero descifrado, debes llámalo "mensaje_descifrado_por_<<mi_nombre>>.txt".

  Nota: Guarda tu clave privada en la carpeta Escenario_I como mi_clave_privada.pem

P3: Cifrado y Descifrado Mediante PKI
Ejercicios – Escenario I

Grid y Computación de Altas Prestaciones
GRyCAP

- Verifica cuales de estas propiedades se satisfacen en el Escenario I:

a. Autenticación emisor
b. Autenticación del receptor
c. Confidencialidad de los datos
d. Integridad de los datos

- Crear un fichero llamado "conclusiones.txt" en la carpeta "home/ccgc/Evidencias/Grid/01_Seguridad/P3/Escenario_I" donde expliques de forma razonada que propiedades se satisfacen y cuales no (debes de discutirlo con tu compañero).

P3: Cifrado y Descifrado Mediante PKI

Ejercicios – Escenario I - Evidencias

Grid y Computación de Altas Prestaciones GRyCAP

- En la carpeta "/home/ccgc/Evidencias/Grid/01_Seguridad/P3/Escenario_I" deben de aparecer los ficheros siguientes:

mensaje.txt →Fichero de texto que contiene vuestro nombre.

clave_publica_<<nombre_compañero>>.pem →Fichero con la clave pública de vuestro compañero.

mi_clave_privada.pem →Fichero con mi propia clave privada

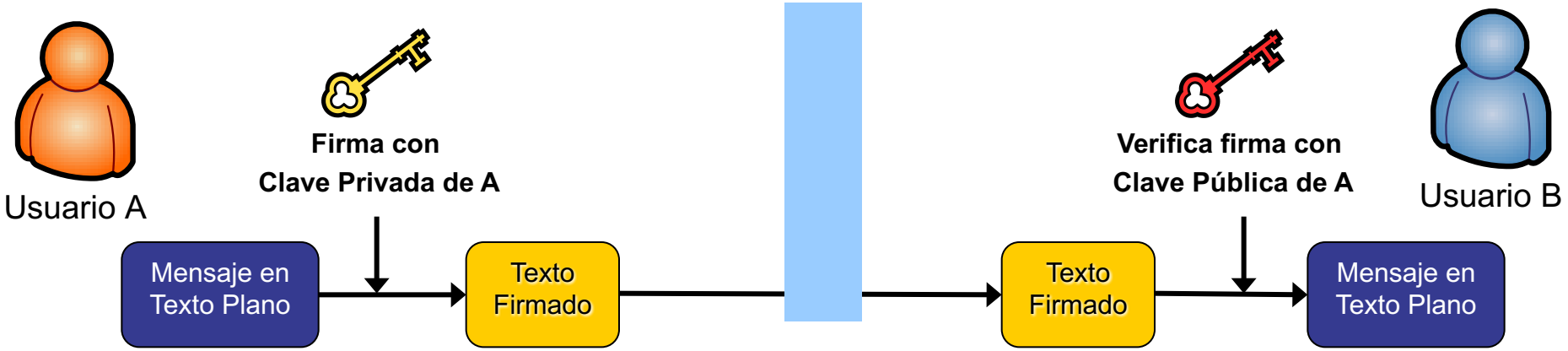
mensaje_cifrado_por_<<mi_nombre>>.txt→Texto cifrado por mi utilizando la clave pública de mi compañero . Contiene mi nombre.

mensaje_cifrado_por_<<nombre_compañero>>.txt→Texto cifrado por mi compañero utilizando mi clave publica y que me ha transferido. Contiene el nombre de mi compañero.

mensaje_descifrado_por_<<mi_nombre>>.txt→Texto descifrado por mi utilizando mi clave privada y que corresponde al fichero cifrado por mi compañero con mi clave publica. Contiene el nombre de mi compañero.

P3: Cifrado y Descifrado Mediante PKI
Ejercicios – Escenario II

- Reproduce el escenario II representado en la figura.
- Crea una carpeta "/home/ccgc/Evidencias/Grid/01_Seguridad/P3/Escenario_II"
- Todos los Ficheros que generes en este ejercicio créalos en la carpeta "../P3/Escenario_II":



P3: Cifrado y Descifrado Mediante PKI

Ejercicios – Escenario II – Pasos a Seguir

Grid y Computación de Altas Prestaciones GRyCAP

- **Paso 1. Firma con la Clave Privada del Emisor.** Utilizo mi clave privada para firmar el mensaje contenido "mensaje.txt" que contiene tu nombre. El fichero firmado, debes llámalo "mensaje_firmado_por_<<mi_nombre>>.txt".

  Nota: Guarda tu clave privada en la carpeta Escenario_II como mi_clave_privada.pem

- **Paso 2. Transferencia.** Hazle llegar a tu compañero el mensaje firmado.

  Nota: Puedes transferirle a tu compañero el fichero cifrado a través del comando scp pidiéndole que introduzca su contraseña.

- **Paso 3. Verificar Firma con la Clave Publica del Emisor.** Utiliza la clave publica de tu compañero para verificar la firma del mensaje recibido enviado por tu compañero "mensaje_firmado_por_<<nombre_compañero>>.txt" que contiene su nombre. El fichero verificado, debes llámalo "mensaje_verificado_por_<<mi_nombre>>.txt".

  Nota: Guarda la clave pública de tu compañero en la carpeta Escenario_II como clave_publica_<nombre_compañero>.pem

P3: Cifrado y Descifrado Mediante PKI
Ejercicios – Escenario II

Grid y Computación de Altas Prestaciones
GRyCAP

- Verifica cuales de estas propiedades se satisfacen en el Escenario II:

a. Autenticación emisor
b. Autenticación del receptor
c. Confidencialidad de los datos
d. Integridad de los datos

- Crear un fichero llamado "conclusiones.txt" en la carpeta "home/ccgc/Evidencias/Grid/01_Seguridad/P3/Escenario_II" donde expliques de forma razonada que propiedades se satisfacen y cuales no (debes de discutirlo con tu compañero).

P3: Cifrado y Descifrado Mediante PKI
Ejercicios – Escenario II - Evidencias

Grid y Computación de Altas Prestaciones GRyCAP

- En la carpeta "/home/ccgc/Evidencias/Grid/01_Seguridad/P3/Escenario_II" deben de aparecer los ficheros siguientes:

clave_publica_<<nombre_compañero>>.pem → Fichero con la clave pública de vuestro compañero.

mi_clave_privada.pem →Fichero con mi propia clave privada

mensaje.txt → Fichero de texto fuente que contiene vuestro nombre.

mensaje_firmado_por_<<mi_nombre>>.txt→Texto firmado por mi utilizando mi clave privada. Contiene mi nombre.

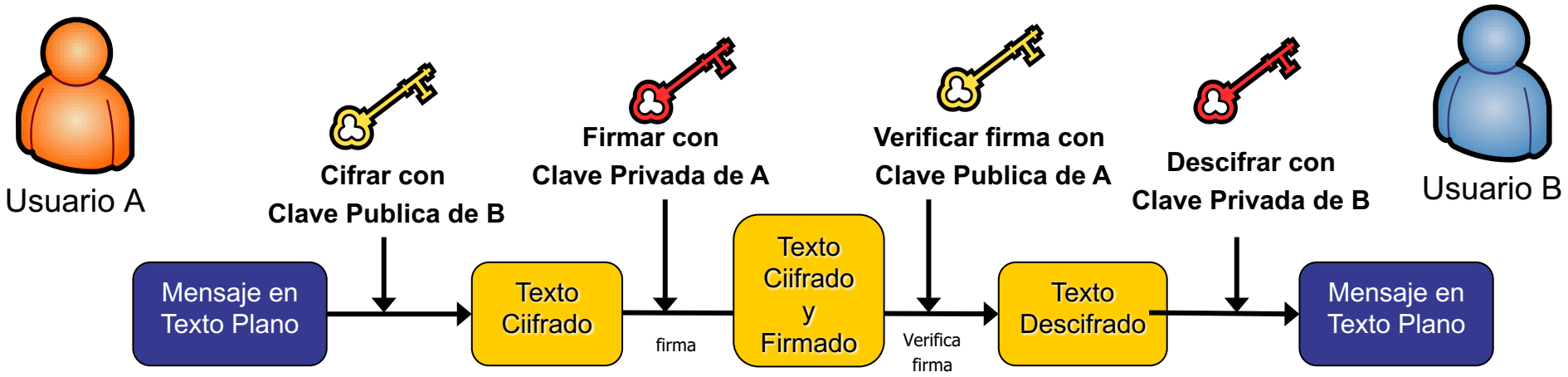
mensaje_firmado_por_<<nombre_compañero>>.txt→Texto firmado por mi compañero utilizando su clave privada y que me ha transferido. Contiene el nombre de mi compañero.

mensaje_verificado_por_<<mi_nombre>>.txt→Texto verificado por mi utilizando la clave publica de mi compañero y que corresponde al fichero firmado por mi compañero con su clave privada. Contiene el nombre de mi compañero.

conclusiones.txt →Explicación razonada de las propiedades que se satisfacen en el escenario.

P3: Cifrado y Descifrado Mediante PKI
Ejercicios – Escenario III

- Reproduce el escenario III representado en la figura.
- Crea una carpeta "/home/ccgc/Evidencias/Grid/01_Seguridad/P3/Escenario_III"
- Todos los Ficheros que generes en este ejercicio créalos en la carpeta "../P3/Escenario_III":



P3: Cifrado y Descifrado Mediante PKI
Ejercicios – Escenario III – Pasos a Seguir

Grid y Computación de Altas Prestaciones
GRyCAP

- **Paso 1. Cifrar con Clave Pública del Receptor.** Genera el fichero "mensaje_cifrado_por_<<mi_nombre>>.txt".

  Nota: Guarda la clave pública de tu compañero en la carpeta Escenario_III como clave_publica_<nombre_compañero>.pem

- **Paso 2. Firmar con Clave Privada del Emisor.** Genera el fichero "mensaje_cifrado_y_firmado_por_<<mi_nombre>>.txt".

  Nota: Guarda tu clave privada en la carpeta Escenario_III como mi_clave_privada.pem

- **Paso 3.** Transferencia.

- **Paso 4. Verificar con Clave Publica del Emisor.** A partir del mensaje recibido de vuestro compañero, genera el fichero "mensaje_verificado_por_mi_ y_cifrado_por_<<nombre_comp>>.txt". A este fichero debes quitarle la primera línea antes de descifrar.

- **Paso 5. Descifrar con Clave Privada del Receptor.** Genera el fichero "mensaje_verificado y_descifrado_por_<<mi_nombre>>.txt".

P3: Cifrado y Descifrado Mediante PKI
Ejercicios – Escenario III

Grid y Computación de Altas Prestaciones
GRyCAP

- Verifica cuales de estas propiedades se satisfacen en el Escenario III:

a. Autenticación emisor
b. Autenticación del receptor
c. Confidencialidad de los datos
d. Integridad de los datos

- Crear un fichero llamado "conclusiones.txt" en la carpeta "home/ccgc/Evidencias/Grid/01_Seguridad/P3/Escenario_III" donde expliques de forma razonada que propiedades se satisfacen y cuales no (debes de discutirlo con tu compañero).

P3: Cifrado y Descifrado Mediante PKI
Ejercicios – Escenario III - Evidencias

Grid y Computación de Altas Prestaciones
GRyCAP

- En la carpeta "/home/ccgc/Evidencias/Grid/01_Seguridad/P3/Escenario_III" deben de aparecer los ficheros siguientes:

clave_publica_<<nombre_compañero>>.pem → Fichero con la clave pública de vuestro compañero.
mi_clave_privada.pem →Fichero con mi propia clave privada
mensaje.txt → Fichero de texto fuente que contiene vuestro nombre.

mensaje_cifrado_por_<<mi_nombre>>.txt→Texto cifrado por mi utilizando la clave pública de mi compañero . Contiene mi nombre.
mensaje_cifrado_y_firmado_por_<<mi_nombre>>.txt→Texto firmado por mi utilizando mi clave privada. Contiene mi nombre cifrado con la clave pública de mi compañero.
mensaje_verificado_por_<<mi_nombre>>_y_cifrado_por_<<nombre_compañero>>.txt→Texto verificado por mi utilizando la clave publica de mi compañero y que corresponde al fichero firmado por mi compañero con su clave privada. Contiene el nombre de mi compañero cifrado con mi clave pública.
mensaje_verificado_y_descifrado_por_<<mi_nombre>>.txt→Texto descifrado por mi utilizando mi clave privada y que corresponde al fichero cifrado por mi compañero con mi clave publica y verificado por mi. Contiene el nombre de mi compañero.
conclusiones.txt →Explicación razonada de las propiedades que se satisfacen en el escenario.

Grid y Computación de Altas Prestaciones
GRyCAP

PRÁCTICA 4: Crear Proxies Mediante GSI

P4: Crear Proxies Mediante GSI

- Sitúate en la carpeta siguiente:

```
[ccgc@XXX~]$ cd /home/ccgc/Evidencias/Grid/01_Seguridad/P4
```

- Todos los ficheros que generes en esta práctica debes de guardarlo en esta carpeta para que consten como evidencia de su realización.

P4: Crear Proxies mediante GSI

Grid y Computación de Altas Prestaciones GRyCAP

- Desde el punto de vista de un usuario Grid, los requisitos para poder ejecutar un trabajo en un Grid son:
  - Disponer de una Cuenta en una Máquina con Globus Instalado (Las máquinas virtuales).
  - Disponer de un Certificado Válido (Los certificados de usuario generados en la P2).
  - **Crear el Proxy Correspondiente.**
  - Pertenecer a una VO (Disponer de Autorización en los Recursos a Utilizar).

P4: Crear Proxies mediante GSI

Grid y Computación de Altas Prestaciones GRyCAP

- Comandos Relativos al Certificado y al Proxy
  - `grid-cert-info[-help] [-file certfile] [OPTION]...`

    `-all` **whole certificate**

    `-subject | -s` **subject string**

    `-issuer | -i` **Issuer**

    `-startdate | -sd` **Start of validity**

    `-enddate | -ed` **End of validity**
  - grid-proxy-init, Creación del Proxy Válido a Todos los Efectos por un Tiempo Limitado.
  - grid-proxy-destroy, Destrucción de un Proxy Activo.
  - grid-proxy-info, Información Sobre un Proxy Creado.

P4: Crear Proxies mediante GSI

Grid y Computación de Altas Prestaciones GRyCAP

- Syntaxis: grid-proxy-init [opciones] ...

-help, -usage	Muestra Ayuda.
-version	Muestra Versión.
-verify	Verifica el Certificado.
-limited	Crea un Proxy Limitado.
-valid <h:m>	Crea un Proxy Válido por h horas y m minutos (12:00 por Defecto).
-cert <certfile>	Ubicación del Certificado (si no es la estándar)
-key <keyfile>	Ubicación de la Clave Privada (Si no es la Estándar)
-out <proxyfile>	Ubicación del Proxy (Si no es la Estándar).

P4: Crear Proxies mediante GSI

Grid y Computación de Altas Prestaciones GRyCAP

- Otros Comandos
  - Sintaxis: grid-proxy-destroy [opciones] …
    - -help, -usage Información sobre el Uso
    - -all Destruye Todos los Proxies del Usuario
  - Syntax: grid-proxy-info [-opciones]
    - -help, -usage Información sobre el Uso
    - -file <proxyfile> Ubicación No Estándar del Proxy.
    - -subject Nombre Distintivo del Proxy.
    - -issuer Nombre Distintivo del Firmante.
    - -identity Nombre Distintivo del Usuario Representado.
    - -type Tipo de Proxy (Completo o Limitado)
    - -timeleft Tiempo (en Segundos) Hasta la Expiración.
    - -strength Longitud de la Clave (en Bits)
    - -all Toda la Información Anterior.
    - -text Toda la Información Existente y en Texto.
    - -path Ubicación del Fichero Proxy.

P4: Crear Proxies mediante GSI
Ejercicio

Grid y Computación de Altas Prestaciones
GRyCAP

- Crear un proxy Válido por 10 Minutos y llámalo *proxy_10_min.pem* y comprueba su validez y su datos Mediante grid-proxy-info.
- Preguntas:
  - ¿Cuál es el DN del Proxy?
  - ¿Cuál es el DN del firmante del proxy?
- Crea un fichero respuestas.txt en la carpeta de la Practica P4 con las respuestas.

P4: Crear Proxies mediante GSI
Ejercicios - Evidencias

- En la carpeta "/home/ccgc/Evidencias/Grid/01_Seguridad/P4" deben de aparecer los ficheros siguientes:

proxy_10_min → Proxy de 10 minutos generado con vuestras credenciales

respuestas.txt →Texto con las respuestas planteadas en el ejercicio.