Grid y Computación de Altas Prestaciones

GRyCAP

Tema 2. Seguridad en un Entorno Grid

Conceptos Básicos de la Computación en Grid y Cloud

Objetivos

Grid y Computación de Altas Prestaciones
GRyCAP

- Definir los conceptos básicos de seguridad en el Grid (Autenticación, Autorización, Confidencialidad, Integridad, Confiabilidad, Trazabilidad, no Repudio y Delegación).
- Describir las tecnologías básicas que dan soporte a la seguridad en el Grid.
- Describir y aplicar los mecanismos que dan soporte a la seguridad en el Grid.

Contenidos Teóricos

Grid y Computación de Altas Prestaciones
GRyCAP

- La Seguridad en el Grid.
  - Aproximaciones.
  - Los Riesgos de una Aproximación Insegura.
  - Problemas de la Seguridad en el Grid.
- Implementación de la Seguridad en el Grid.
  - Introducción a la Criptografía.
  - Certificados digitales y Autoridades de certificación.
  - Public Key Infrastructure (PKI).
  - Globus Security Infrastructure (GSI).

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.

Contenidos Teóricos

Grid y Computación de Altas Prestaciones
GRyCAP

- **La Seguridad en el Grid.**
  - Aproximaciones.
  - Los Riesgos de una Aproximación Insegura.
  - Problemas de la Seguridad en el Grid.
- Implementación de la Seguridad en el Grid.
  - Introducción a la Criptografía.
  - Certificados digitales y Autoridades de certificación.
  - Public Key Infrastructure (PKI).
  - Globus Security Infrastructure (GSI).

La Seguridad en el Grid

Grid y Computación de Altas Prestaciones
GRyCAP

- El Concepto de Grid Implica el **Acceso a Recursos de Forma Distribuida** en Diferentes Dominios Administrativos.

- Interconectar Dominios Diferentes Requiere Aumentar los Niveles de Seguridad, ya que **la Seguridad Global Viene Limitada por la Seguridad del Servicio o Recurso Más Débil**.

La Seguridad en el Grid
Aproximaciones (1)

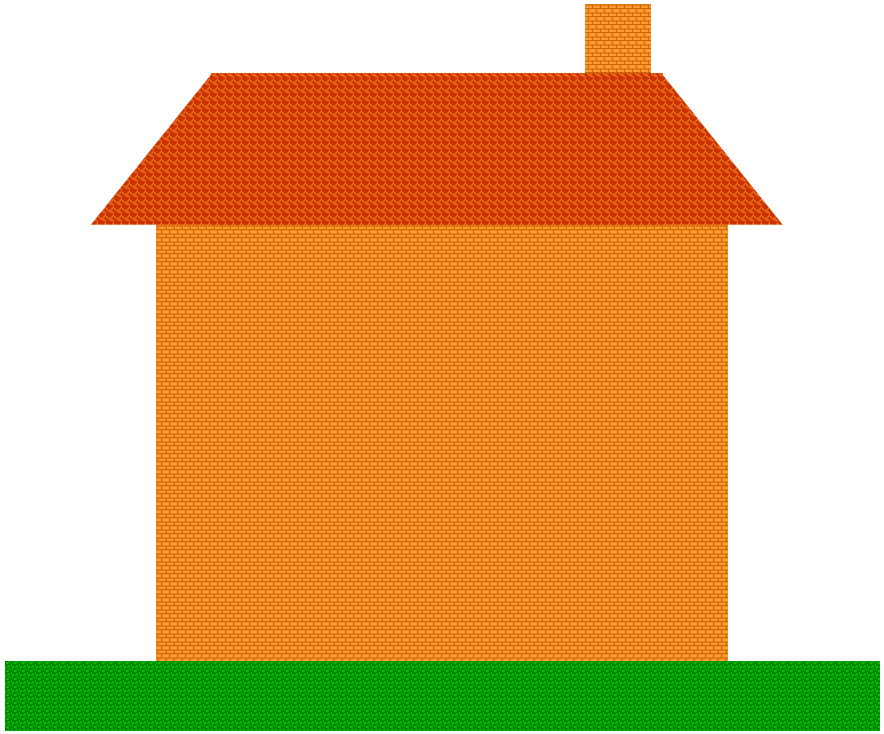
- El Usuario Confiado:
  - Usa Comunicaciones Descifradas.
  - Medios Identificación Débiles (Fácilmente Deducibles) o Inexistentes.
  - Identificación Privada en un Acceso Público. (Ej. El usuario y password en un Posix en el monitor)

La Seguridad en el Grid
Aproximaciones (1) - Riesgos

Grid y Computación de Altas Prestaciones
GRyCAP

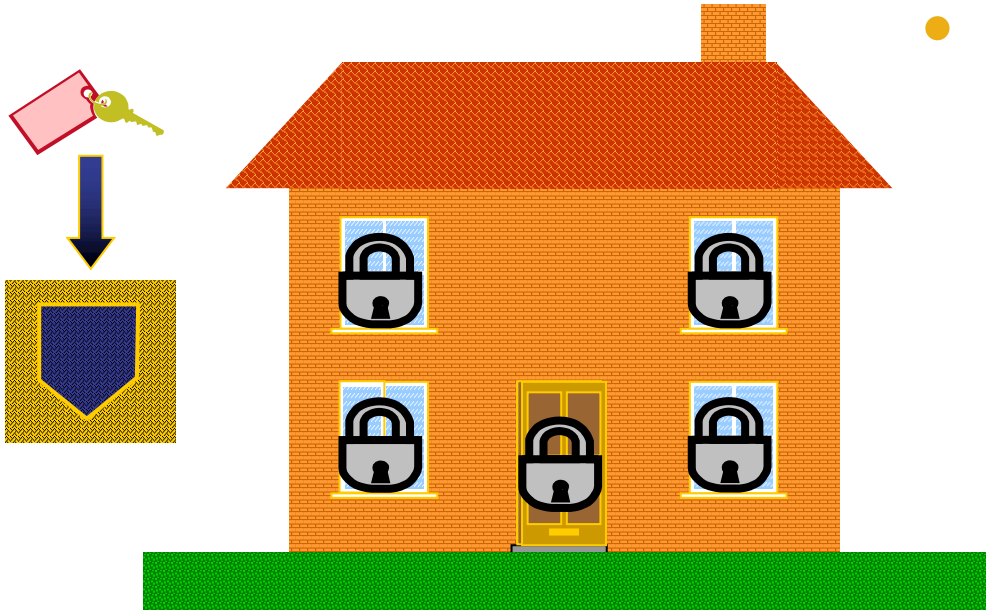
- Permitiría Lanzar Ataques a Múltiples Sitios
  - Las Granjas de Procesadores Distribuidos Son Muy Atractivas Para Lanzar Ataques de Denegación de Servicio (DoS). (Ej. Colapso del Index Information Service Central de sistema MDS).
- Distribución Ilegal o Inapropiada de Datos y Acceso a Información Sensible.
  - Además del Riesgo de Acceso a Datos Confidenciales, Estos Entornos Pueden Utilizarse de Forma Malintencionada para Almacenar Información Voluminosa Ideal (Como Copias Ilegales de Películas).
- Daños Causados por Virus y Gusanos.
  - En Infraestructuras Altamente Conectadas, Los Gusanos y Virus Se pueden Propagar Más Rápidamente.

La Seguridad en el Grid
Aproximaciones (2)



- El Usuario Paranoico:
  - No Usa Ningún Tipo de Comunicaciones.
  - Nunca Deja el Computador Desatendido.

La Seguridad en el Grid
Aproximaciones (3)



- El Usuario Realista:
  - Cifra Todas las Comunicaciones Sensibles.
  - Utiliza Medios de Identificación Fuertes y Difíciles de Violentar.
  - Mantiene la Identificación Segura en Todo Momento.
  - Sólo Permite el Acceso a Usuarios Autorizados.

Seguridad en el Grid
Problemas de la Seguridad en el Grid

Grid y Computación de Altas Prestaciones GRyCAP

- Los Problemas que se Enfrenta la Arquitectura de Seguridad de un Entorno Grid son:
  - **Autenticación y Autorización** de usuarios.
  - **Confidencialidad** e **Integridad** de datos.
  - **Confiabilidad** de los servicios.
  - **Trazabilidad** y **no Repudio**.
  - La **delegación.**
  - **Coordinar** las Políticas de Acceso a Recursos Locales.
  - Facilitar el **Acceso** a los Recursos de Forma **General**.

Seguridad en el Grid
Problemas de la Seguridad en el Grid (Autenticación y Autorización)

Grid y Computación de Altas Prestaciones
GRyCAP

- Autenticación
  - Garantía de la Veracidad de la **Identidad** del Actor de un Proceso o de unos Datos.
  - La Identidad Generalmente se Acredita Mediante unas Credenciales en Cuya Veracidad se Puede Confiar por Algún Mecanismo.
- Autorización
  - Verificación de que un Actor Debidamente Autenticado Tiene Derecho a **Realizar una Acción Determinada**.
  - La Autorización Final para la Realización de una Determinada Acción Debe Ser **Controlada por el Propietario** de los Recursos.

Seguridad en el Grid
Problemas de la Seguridad en el Grid (Confidencialidad e Integridad)

Grid y Computación de Altas Prestaciones
GRyCAP

- Confidencialidad
  - Garantía de que los **Datos** Transmitidos o Almacenados **Sólo Pueden Ser Visibles para los Usuarios Autorizados y** debidamente **Autenticados**.
  - La Confidencialidad Implica Generalmente el **Cifrado de los Datos** de Forma que Sólo los Usuarios Autorizados puedan Descifrarlos.
- Integridad
  - Garantía de que los **Datos que se Acceden No han Sido Modificados** por Otro Actor sin que Quede Constancia de Éste Hecho.

Seguridad en el Grid
Problemas de la Seguridad en el Grid (Confiabilidad)

Grid y Computación de Altas Prestaciones
GRyCAP

- Confiabilidad
  - Capacidad de un Recurso o Servicio de **realizar su Función de la Manera Prevista.**
  - También se Puede definir como la probabilidad en que se Realizará su Función Prevista sin Incidentes por un Período de Tiempo Especificado y Bajo Condiciones Indicadas.

Seguridad en el Grid
Problemas de la Seguridad en el Grid (Trazabilidad y No Repudio)

Grid y Computación de Altas Prestaciones
GRyCAP

- Trazabilidad
  - Capacidad de garantizar el **Registro de Todas las Acciones** y Recursos y de quienes son sus ejecutores.

- No Repudio
  - **Garantiza la Identidad del Ejecutor de una Cierta Acción.**
  - Ofrece Protección a un Usuario Frente a que Otro Usuario Niegue Posteriormente que en Realidad se Realizó Cierta Comunicación.
  - Esta Protección se Efectúa por Medio de una Colección de Evidencias Irrefutables que Permitirán la Resolución de Cualquier Disputa.
  - El **No Repudio de Origen** Protege al Receptor de que el Emisor Niegue Haber Enviado el Mensaje, Mientras que el **No Repudio de Recepción** Protege al Emisor de que el Receptor Niegue Haber Recibido el Mensaje.

Seguridad en el Grid
Problemas de la Seguridad en el Grid (Delegación)

Grid y Computación de Altas Prestaciones
GRyCAP

- Delegación
  - Consiste en la **Cesión del Derecho de Actuar en Nuestro Nombre** (y por Tanto de los Permisos) a Otro Actor (Organización, Persona o Servicio) para que Realice una Determinada Tarea.
  - La Delegación es Fundamental para Preservar los Permisos y para Poder Realizar Operaciones No Interactivas.
  - La Delegación Debe ser Temporal y Realizarse con las Mismas Garantías de Cualquier Otro Proceso.

Seguridad en el Grid
Problemas de la Seguridad en el Grid
(Coordinar las Políticas de Acceso a Recursos Locales)

Grid y Computación de Altas Prestaciones
GRyCAP

- Coordinación de las políticas de acceso
  - Generalmente se realiza de forma centralizada (Ej. VOMS Service).
  - Se necesita **organizar la VO** en usuarios, grupos de usuarios y roles, para permitir el acceso a los recursos locales.

Seguridad en el Grid
Problemas de la Seguridad en el Grid
(Acceso a los Recursos de forma General)

Grid y Computación de Altas Prestaciones
GRyCAP

- Acceso a los recursos de forma general
  - El interfaz de **acceso permitirá el acceso** a los recursos a cualquier usuario **de forma homogénea**.
  - Será el que ofrezca el middleware Grid que se utilice (Ej. Globus Toolkit 6, UMD.

Seguridad en el Grid
Problemas de la Seguridad en el Grid (Resumen)

Grid y Computación de Altas Prestaciones
GRyCAP

- **Autenticación y Autorización** de usuarios.
- **Confidencialidad** e **Integridad** de datos.
- **Confiabilidad** de los servicios.
- **Trazabilidad** y **no Repudio**.
- La **delegación.**
- **Coordinar** las Políticas de Acceso a Recursos Locales.
- Facilitar el **Acceso** a los Recursos de Forma **General**.

Contenidos Teóricos

Grid y Computación de Altas Prestaciones
GRyCAP

- La Seguridad en el Grid.
  - Aproximaciones.
  - Los Riesgos de una Aproximación Insegura.
  - Problemas de la Seguridad en el Grid.
- **Implementación de la Seguridad en el Grid.**
  - **Introducción a la Criptografía.**
  - Certificados digitales y Autoridades de certificación.
  - Public Key Infrastructure (PKI).
  - Globus Security Infrastructure (GSI).

Implementación de la Seguridad en el Grid
Introducción a la Criptografía

Grid y Computación de Altas Prestaciones
GRyCAP

- Estudio de los Mecanismos que Permiten **Convertir** la Información **de su Forma Normal y Comprensiva a un Formato Incomprensivo**, Haciéndola Ilegible sin el Conocimiento de una Clave.

- En la Terminología Básica de la Criptografía:
  - **Texto plano.** La Información Original que será Protegida.
  - **Clave.** Fragmento de Información Secreto que Caracteriza la Forma en que se Produce el Cifrado.
  - **Cifrado.** Es el Proceso de Convertir el Texto Plano en una Forma Ilegible.
  - **Descifrado.** El Proceso Reverso al Cifrado, que Consiste en Recuperar el Texto Plano de un Cifrado.
  - **Cipher.** Algoritmo para el Cifrado y Descifrado, Generalmente Controlado por una Clave y Definido por un Protocolo y una Serie de Parámetros.
  - **Sistema Criptográfico.** Conjunto de Protocolos, Ciphers, Manejadores de Claves y Acciones Prescritas por el Usuario Implementados en Conjunto como un Sistema.

- Se pueden Definir dos Tipos Fundamentales de Algoritmos Criptográficos en Función del Tipo de Claves a Utilizar por los Ciphers.
  - Criptografía **de Clave Simétrica**
    - La Clave Para el Descifrado de un Mensaje es Directamente la Clave de Cifrado o Puede Obtenerse de Forma Sencilla.
  - Criptografía de **Clave Asimétrica o Clave Publica**
    - La Clave que se Requiere para el Descifrado es Diferente y No puede Obtenerse de Manera Sencilla a Partir de la Clave de Cifrado.

Grid y Computación de Altas Prestaciones
GRyCAP

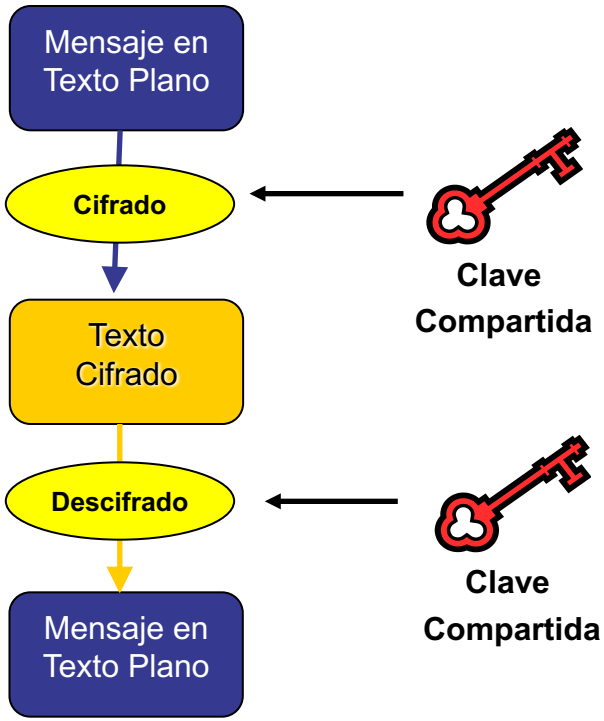
- Criptografía de Clave Simétrica
  - Implica que la Clave debe de ser Conocida por los Dos Interlocutores, con lo que el Problema Pasa a Cómo Compartir la Clave.
  - Utilizado por el protocolo de autenticación de redes (**Kerberos**), y algoritmos de cifrado como **DES / 3DES** o el International Data Encryption (**IDEA**)

Implementación de la Seguridad en el Grid
Introducción a la Criptografía (Clave Simétrica)

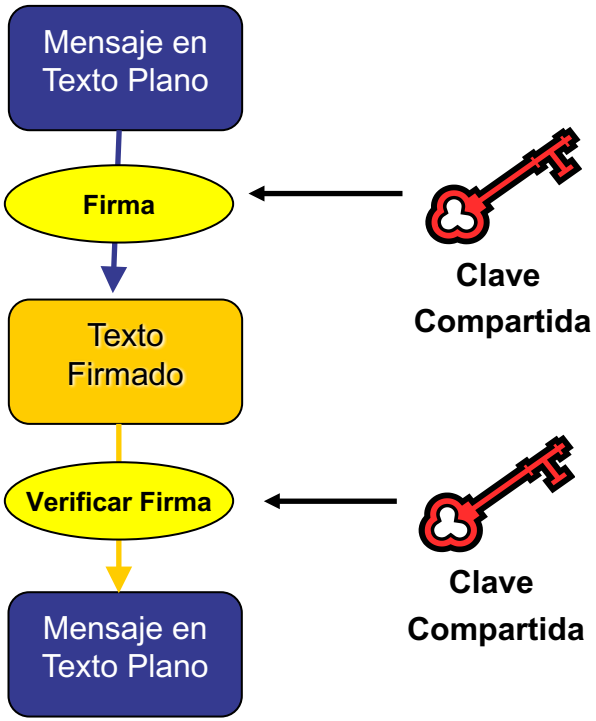
Grid y Computación de Altas Prestaciones
GRyCAP

- La criptografía simétrica se puede emplear para:

Cifrar mensajes



Firmar mensajes



Implementación de la Seguridad en el Grid
Introducción a la Criptografía
(Clave Asimétrica)

Grid y Computación de Altas Prestaciones
GRyCAP

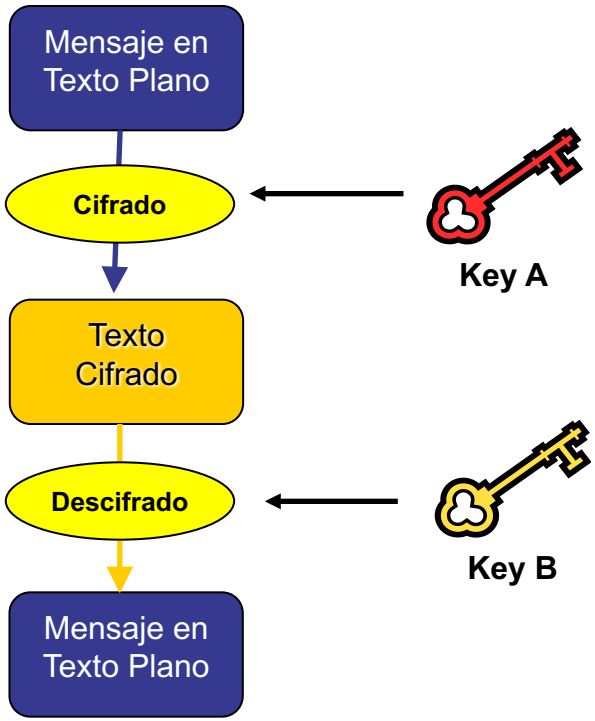
- Criptografía de Clave Asimétrica o Clave Pública
  - Se utilizan generan dos claves, una **Clave Pública (CPub)** que puede ser conocida por todo el mundo y otra **Clave Privada (CPr)** que solo es conocida por el propietario.
  - La Clave que se Utiliza para el Cifrado de los Datos (Clave Privada o Clave Publica) es Diferente y No Puede Deducirse Fácilmente a Partir de la Clave de Descifrado (Clave Pública o Clave Privada).
  - Utilizado en el algoritmo de cifrado **RSA y DSA.**

Implementación de la Seguridad en el Grid
Introducción a la Criptografía (Clave Asimétrica)

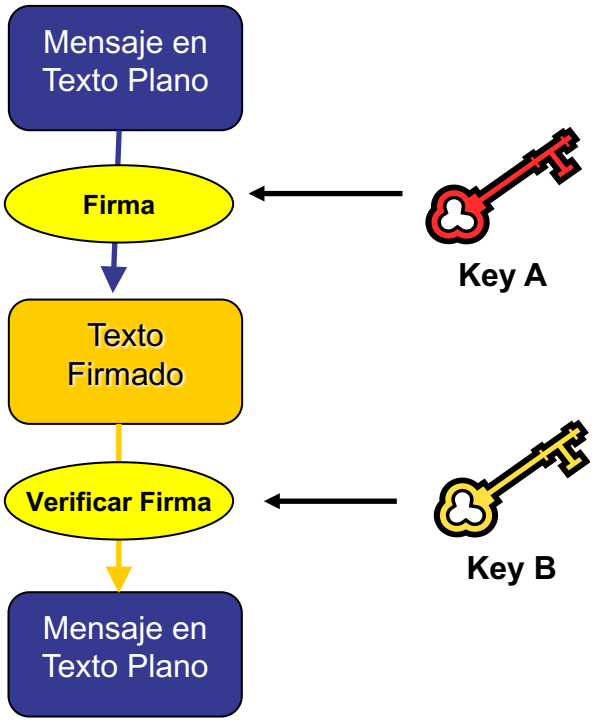
Grid y Computación de Altas Prestaciones
GRyCAP

- La criptografía asimétrica se puede emplear para:

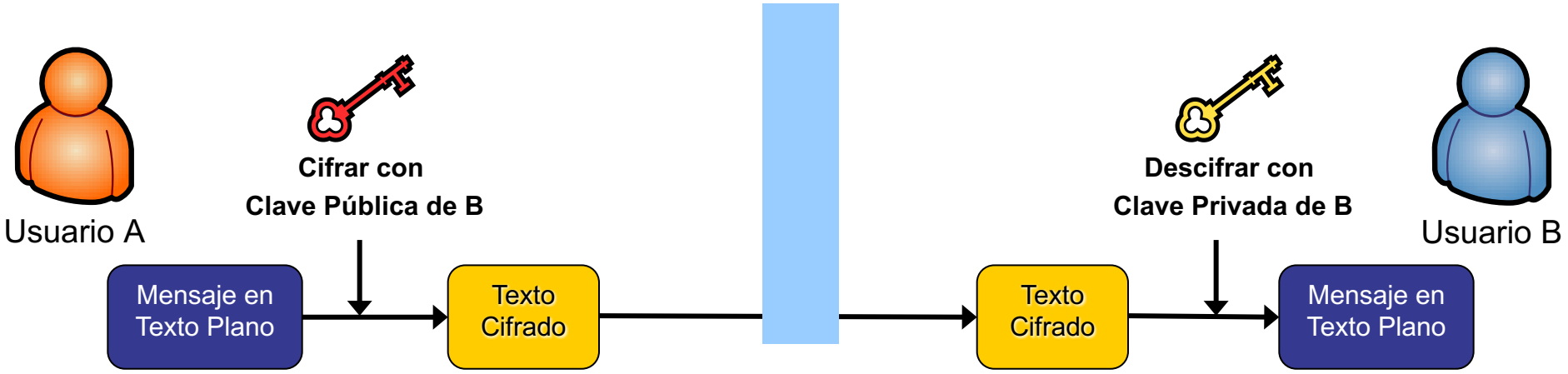
Cifrar mensajes



Firmar mensajes



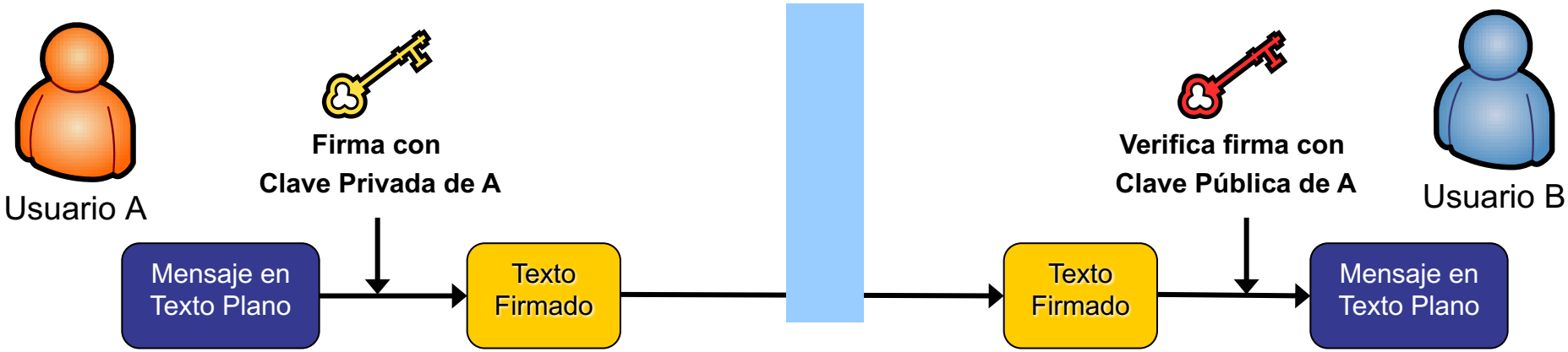
Implementación de la Seguridad en el Grid
Introducción a la Criptografía
(Criptografía Asimétrica – Escenario I Comunicación)



- **Autenticación del Receptor:**
- **Autenticación del Emisor:**
- **Integridad de Datos:**
- **Confidencialidad de Datos:**

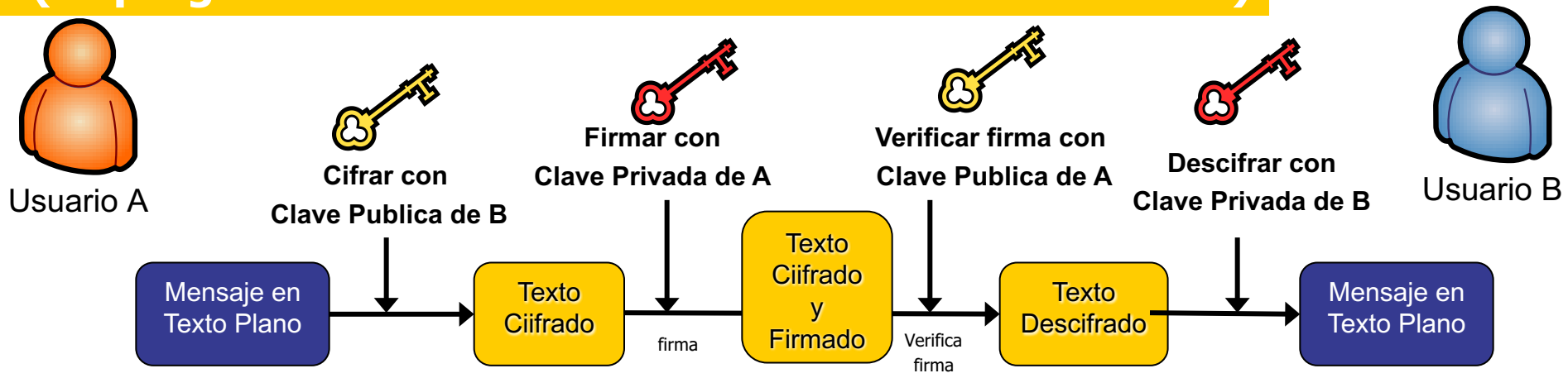
Implementación de la Seguridad en el Grid
Introducción a la Criptografía
(Criptografía Asimétrica – Escenario II Comunicación)

Grid y Computación de Altas Prestaciones
GRyCAP



- **Autenticación del Receptor:**
- **Autenticación del Emisor:**
- **Integridad de Datos:**
- **Confidencialidad de Datos:**

Implementación de la Seguridad en el Grid
Introducción a la Criptografía
(Criptografía Asimétrica – Escenario III Comunicación)



- **Autenticación del Receptor:**
- **Autenticación del Emisor:**
- **Integridad de Datos:**
- **Confidencialidad de Datos:**

Implementación de la Seguridad en el Grid
Introducción a la Criptografía

Grid y Computación de Altas Prestaciones
GRyCAP

- Para la implementación de un Grid se emplea Criptografía Asimétrica.
- **A cada usuario, servicio y recurso** se le provee de una clave privada y una clave pública mediante el soporte de **certificados digitales.**
- Para las comunicaciones se implementan variaciones del **escenario III**, garantizando:
  - Autenticación emisor y receptor
  - Integridad, confidencialidad
  - Trazabilidad y no repudio

¿Delegación?¿confiabilidad ?¿Acceso Homogéneo?

¿Coordinar las Políticas de Acceso a Recursos Locales?

Contenidos Teóricos

Grid y Computación de Altas Prestaciones
GRyCAP

- La Seguridad en el Grid.
  - Aproximaciones.
  - Los Riesgos de una Aproximación Insegura.
  - Problemas de la Seguridad en el Grid.
- **Implementación de la Seguridad en el Grid.**
  - Introducción a la Criptografía.
  - **Certificados digitales y Autoridades de certificación.**
  - Public Key Infrastructure (PKI).
  - Globus Security Infrastructure (GSI).

Implementación de la Seguridad en el Grid
Certificados Digitales

Grid y Computación de Altas Prestaciones
GRyCAP

- Se basan en **Criptografía Asimétrica.**
- Los Certificados Digitales Facilitan:
  - Autentificación (como un Documento de Identidad)
  - Firma Digital
  - Cifrado de Información.
  - Comunicación Segura.
- Soportado por el Software OpenSSL
  - openssl <ca> <req> <x509> <crl> <verify> …
- Acceso Seguro a la Web, LDAP, …

Implementación de la Seguridad en el Grid
Certificados Digitales (Clave privada)

Grid y Computación de Altas Prestaciones
GRyCAP

-----BEGIN RSA PRIVATE KEY-----

Proc-Type: 4,ENCRYPTED

DEK-Info: DES-EDE3-CBC,$DD2341DC31223DD3

FAS452345Dfa23jfhahfjashufy348723j4hsjdfya987sdfyjq23hrjk1h23r876f8asf1hkhr
j12rc·432R”CFj43ft4k3jhHUHu678YJyuYUI6876UHJKHEJTG87652345yGjhJHJKH
JHRJGHJHjhJgvgskJHJgJKHGsd23hxcd878687hj234nf8c12387461723827 4ewvh
2h95872348f47wsde23234754cvsd23ñ3cvmT”$%JBV&CF”)$·235tgnu(CV”$·RX
$”·;FU”·$UJG%”·$bfsCerfUV14q3$N(5423523F(CF$U”·5234F”·L$fasdfarthreysK
HVB%IH$”·CVI·$)C/”·$)CVf”·J$CV$KCVfeqwvwqhar3asdfasdfa24Jwca”$·V%)”·
UJ·LfaXCFJ”·KHRK”·$_C”·dgdsfcv523fX”·$HF”JK·H$XCF·$XC·$”4uijjHvrsFI”·fsda
fXrC”·H”·$XCYCFKSDUFWNEVT(%C(V”·$”hjhdfjkasdh fqu4wceayjhsdfas=

-----END RSA PRIVATE KEY-----

Implementación de la Seguridad en el Grid
Certificados Digitales (Clave pública)

Grid y Computación de Altas Prestaciones
GRyCAP

-----BEGIN RSA PUBLIC KEY-----

MIIB9TCCAV4CAQAwgYIxDTALBgNVBAoTBEdyaWQxEzARBgNVBAsTCkdsb2J1c1Rl
c3QxJDAiBgNVBAsTG3NpbXBsZUNBLXJhbXNlcy5kc2ljLnVwdi5lczEUMBIGA1UE
CxMLZHNpYy51cHYuZXMxIDAeBgNVBAMTF0lnbmFjaW8gQmxhbnF1ZXIgRXNwZXJ0
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDqR3Iu+G3/eftnuv+fyGMADwkD
L8DBOSl/7s44RP3t7t5RPKT33HqREF/vZ8wLYhZYOlS1kuc4o01Q5F5Q4Tu9VzOU
3ofRW7KGnHto27QdUJitohe9rYyko8eGQvvN77hFxj8BzrySjkhE9VoG+pG1TM6Q
LUizzndNdzUcwRofnQIDAQABoDIwMAYJKoZIhvcNAQkOMSMwITARBglghkgBhvhC
AQEEBAMCBPAwDAYDVR0TAQH/BAIwADANBgkqhkiG9w0BAQQFAAOBgQCY5AcTudO
a
lFCawZlep4rJuddDDJMJw0F2vjTgTWwAHnq3Mynbze5HnS3qM/mBWaSkzBCneHC2
7LylV/54fnQpogrWT+J7KcPULec/RdOzZweEBz7eTckruM7+6zAcIebrD2msPBH6
/Sf9ab5Ll/M5Y7+5Z7HufVJ2nMlMZLPc2g==
-----END RSA PUBLIC KEY-----

Implementación de la Seguridad en el Grid
Certificados Digitales (Certificados x509 en el Grid)

Grid y Computación de Altas Prestaciones
GRyCAP

- Los Certificados x509 Digitales son Documentos Electrónicos que **Asocian un Usuario o Recurso Grid con su Clave Pública Específica**.

- Un Certificado x509 es una Estructura de Datos que Contiene la Clave Pública y los Detalles Relevantes de la Identidad de un Usuario o Recurso como las fechas de validez del certificado o el **Nombre Distintivo (DN)**.

- **Nombre Distintivo (DN)**

  - Define una Identidad Dentro de un Contexto, por Ejemplo una Organización. Los Nombres Distintivos Están Definidos en el Estándar X.509. Típicamente:
    - Nombre Común (CN), el Nombre a ser Certificado.
    - Organización o Compañía (O), el Nombre Asociado con la Organización.
    - Unidad (OU), Sección o Área de la Organización.
    - Ciudad/Localidad (L) Ciudad donde está Localizado el CN.
    - Estado/Provincia (SP) Provincia donde está Localizado el CN.
    - País (C) , el país donde está Localizado CN.

Implementación de la Seguridad en el Grid
Certificados Digitales (Certificados x509 en el Grid)

Grid y Computación de Altas Prestaciones GRyCAP

- Los Certificados x509 **no Contienen Información Confidencial** y su Distribución no Implica una Pérdida de Seguridad.
- En entornos en los que existan muchos recursos y usuarios (ej. En un entono Grid):

¿podemos garantizar que cuando un usuario/recurso presente un dato cifrado con su cPriv, la cPub (Certificado x509) utilizada para descifrar pertenece al recurso o persona listada en el certificado?

¿y si es así, es viable su aplicación en estos ámbitos?

Implementación de la Seguridad en el Grid
Certificados Digitales (Certificados x509 en el Grid)

Grid y Computación de Altas Prestaciones
GRyCAP

- En los Certificados Firmados, la Entidad Certificadora (CA) Prueba que la Clave Pública Contenida Pertenece a la Entidad (recurso o persona (subject) Listada en el Certificado.

- La Firma de un Certificado Consiste en Cifrar con la Clave Privada de una CA, una Cadena (Hash) con la identificación del Usuario, su Clave Pública y el Nombre de la CA.
  - Prueba que el Certificado Viene de la CA.
  - Prueba la Identificación del Usuario.
  - Prueba la Conexión entre la Clave Pública y la Identificación.

- Técnicamente, un Certificado No Puede Alterarse de Forma Indetectable y Constituye una Comprobación de la Integridad del Propio Certificado → no se puede descrifrar la cadena, cambiarla y volver a cifrar ya que no se puede conoce la clave privada de la CA.

Implementación de la Seguridad en el Grid
Certificados Digitales (Certificados x509 en el Grid)

Grid y Computación de Altas Prestaciones GRyCAP

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 4 (0x4)
        Signature Algorithm: md5WithRSAEncryption
        Issuer: O=Grid, OU=GlobusTest, OU=simpleCA-ramses.dsic.upv.es, CN=Globus Simple CA
        Validity
            Not Before: Apr  1 17:43:48 2003 GMT
            Not After : Mar 31 17:43:48 2004 GMT
        Subject: O=Grid, OU=GlobusTest, OU=simpleCA-ramses.dsic.upv.es, OU=dsic.upv.es, CN=Ignacio Blanquer Espert
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    ea:47:72:2e:f8:6d:ff:79:fb:67:ba:ff:9f:c8:63:00:0f:09:03:2f:c0:7f:ee:ce:38:44:fd:ed:ee:de:51:3c:a4:f7:dc:7a:91:
                    cc:0b:62:16:58:3a:54:b5:92:e7:38:a3:4d:50:e4:5e:50:3b:bd:57:33:94:de:87:d1:5b:b2:86:9c:7b:68:db:b4:1d:50:
                    17:bd:8c:a4:a3:c7:86:42:fb:cd:ef:b8:45:c6:3f:01:ce:bc:92:8e:48:44:f5:5a:06:fa:91:b5:4c:ce:90:2d:48:b3:ce:77:4d
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            Netscape Cert Type:
                SSL Client, SSL Server, S/MIME, Object Signing
    Signature Algorithm: md5WithRSAEncryption
        27:66:59:1d:63:31:b3:64:a3:98:7e:52:94:ed:b1:16:42:d8:d4:62:79:90:b5:4c:52:76:f1:77:ca:d5:eb:4c:ff:0a:3a:df:e5:
        1d:b6:a2:34:49:7a:d0:7a:9e:77:5a:ac:c4:47:9f:6d:74:12:c8:a9:d5:ee:dd:a0:ef:92:d2:7b:e8:4d:86:35:2b:d9:88:dc:92:
        0f:c7:79:60:c7:a1:0d:e2:d6:e3:3a:77:ff:df:6c:22:bc:29:16:97:67:1b:bc:86:b3:ce:a2:b6:b7:c7:3b:7f:ad:7e:
        7b:cc:ce:64:73:99:a5:7c:2a:cc:ec:ec:9f:5e:c8:4e:ee:e9:ad:2b
```

DN de la CA

DN del Usuario

CPub del Usuario

Firma (CPub + Data)

Implementación de la Seguridad en el Grid
Autoridades de Certificación (CA)

Grid y Computación de Altas Prestaciones
GRyCAP

- Una Entidad Certificadora (Certification Authority o CA) es una Entidad que Existe Únicamente **Para Firmar Certificados**.
- Los Usuarios se Autentican Con Sus Credenciales Firmadas por las CAs. Los Certificados de la CA son Auto-Firmados.
- Confianza
  - Los Usuarios y Proveedores del Grid Deben Confiar en las CAs Únicamente.
  - Generalmente hay Pocas CAs que Deben Estar Acreditadas por Organismos Transnacionales.
  - Una Infraestructura Grid Puede Reconocer Varias CAs.
- Tareas
  - Verificar la Identidad del Solicitante del Certificado
    - Generalmente son las **Registration Authorities (RAs)** las que Realizan la Verificación Efectiva.
  - Firmar los Certificados de Usuario Acordes con su Política.
  - Gestionar las Listas de Revocación de Certificados (Certificate Revocation Lists o CRLs).

p.e. https://lcg-registrar.cern.ch/pki_certificates.html

Implementación de la Seguridad en el Grid
Autoridades de Certificación (CA)

Grid y Computación de Altas Prestaciones
GRyCAP

- CAs Comerciales y Académicas.

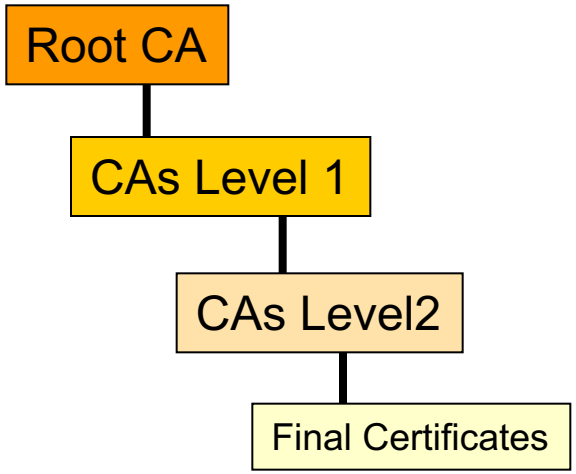
Implementación de la Seguridad en el Grid
Autoridades de Certificación (CA)

Grid y Computación de Altas Prestaciones
GRyCAP

Implementación de la Seguridad en el Grid
Autoridades de Certificación (CA)

Grid y Computación de Altas Prestaciones
GRyCAP

- Jerarquía de Certificación
  - CAs Raíz (Root CAs) (self signed)
  - CAs encadenadas (Chainned CAs)
  - Estructura escalable
  - Problema técnico. Globus.
- Las CAs Delegan en Otras Autoridades (Registration Authorities o RAs) la Tarea de Verificación de la Identidad de los Solicitantes.
- CRL – Lista de certificados revocados
- Creación de una CA
  - Sencillo desde el punto de vista técnico
  - Políticas de Certificación. Seguridad
  - Coordinación para el desarrollo de CAs
- CAs dedicadas a GRID
  - euGridPMA http://www.eugridpma.org
    - 1 CA por país, múltiples RAs
    - Recomendaciones
    - Requerimientos Minimos
  - /C=ES/O=DATAGRID-ES/CN=DATAGRID-ES CA
    - http://grid.ifca.unican.es/ca/datagrid-es



eugridpma

Implementación de la Seguridad en el Grid
Autoridades de Certificación (Revocación)

Grid y Computación de Altas Prestaciones
GRyCAP

- Los Certificados Son Válidos Por Definición Durante el Período de Validez.
- Para Revocar un Certificado, es Necesario Disponer de una Lista Actualizada de los Certificados Anulados.
- Las CA's Publican Listas de Certificados Revocados, Indicando el Número de Serie y la Razón.

Certificate Revocation List (CRL):
Version 2 (0x1)
Signature Algorithm: md5WithRSA
Encryption Issuer: /DC=es/DC=irisgrid/CN=IRISGridCA
Last Update: Aug 9 10:50:15 2006 GMT
Next Update: Sep 8 10:50:15 2006 GMT
CRL extensions: X509v3
Authority Key Identifier:
keyid:9D:42:64:2E:5B:…:F1:B6:43:98:AD:1A
DirName:/DC=es/DC=irisgrid/CN=IRISGridCA
serial:00 X509v3
CRL Number: 30
Revoked Certificates:
Serial Number: 01
Revocation Date: Mar 13 09:12:02 2006 GMT CRL
entry extensions: X509v3
CRL Reason Code: Superseded

Implementación de la Seguridad en el Grid
Certificados Digitales
(Tipos de Certificados en Grid)

Grid y Computación de Altas Prestaciones
GRyCAP

- Tipos de Certificados en Grid
  - Certificados de Usuarios
    - Emitidos para una Persona Física
    - DN= C=E, O=UPV, OU=GRID, CN=Juan García
    - El Único Tipo de Certificado Válido para un Usuario.
  - Certificado de Máquina Grid
    - Emitidos para un Equipo Servidor en el Grid (p.e. un Resource Broker, un Computing Element, etc.).
    - DN= C=E, O=UPV, OU=GRID, CN=host/odin.dsic.upv.es
  - Certificado de Servicio
    - Emitidos para un Programa Ejecutándose en una Máquina Grid
    - DN= C=E, O=UPV, OU=GRID, CN=ldap/odin.dsic.upv.es

P1, P2 y P3

Contenidos Teóricos

Grid y Computación de Altas Prestaciones
GRyCAP

- La Seguridad en el Grid.
  - Aproximaciones.
  - Los Riesgos de una Aproximación Insegura.
  - Problemas de la Seguridad en el Grid.
- **Implementación de la Seguridad en el Grid.**
  - Introducción a la Criptografía.
  - Certificados digitales y Autoridades de certificación.
  - **Public Key Infrastructure (PKI).**
  - Globus Security Infrastructure (GSI).

Implementación de la Seguridad en el Grid
Infraestructuras de Clave Pública (PKI)

Grid y Computación de Altas Prestaciones
GRyCAP

- La PKI es una Colección de Protocolos y Estándares **que Proporciona Autenticación, Integridad, Confidencialidad y No Repudio**.
- Basado en el Cifrado Asimétrico.
  - La Clave Pública es Accesible por todo el Mundo.
  - La Clave Privada Sólo es Accesible por su Propietario.

- La Clave Pública
  - Permite Comprobar que un Mensaje ha sido Cifrado Usando la Clave Privada Asociada, a la Cual Sólo Tiene Acceso su Propietario
  - Si la conocemos de Forma Fiable, Permite Comprobar la Identidad (Autentificación)
  - Esto Funciona Bien Entre Conocidos que Intercambian Claves
  - Pero no Puede Escalar a Miles de Usuarios que Además no se Conocen Personalmente
- PKI se Usa en SSL, PGP, GSI, WS security, S/MIME, etc.

Contenidos Teóricos

Grid y Computación de Altas Prestaciones
GRyCAP

- La Seguridad en el Grid.
  - Aproximaciones.
  - Los Riesgos de una Aproximación Insegura.
  - Problemas de la Seguridad en el Grid.
- **Implementación de la Seguridad en el Grid.**
  - Introducción a la Criptografía.
  - Certificados digitales y Autoridades de certificación.
  - Public Key Infrastructure (PKI).
  - **Globus Security Infrastructure (GSI).**

Implementación de la Seguridad en el Grid
Grid Security Infrastructure (GSI)

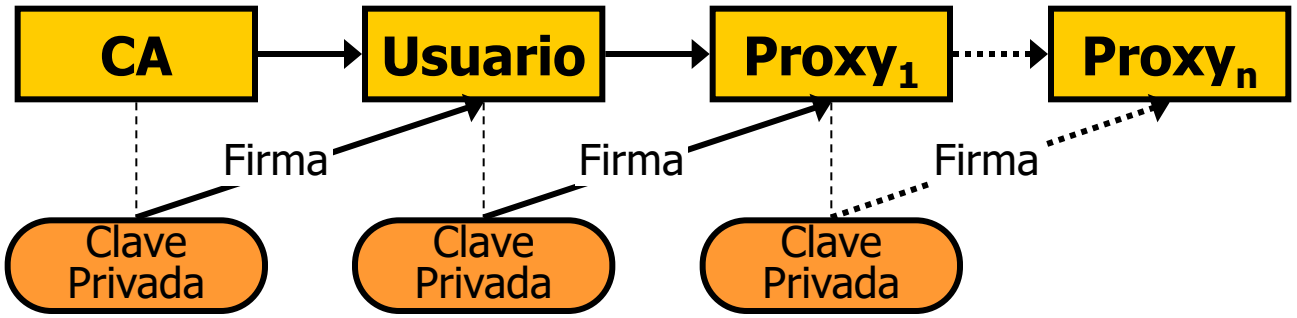
Grid y Computación de Altas Prestaciones
GRyCAP

- Estándar *de facto* para Middlewares Grid.
- Basado en PKI
  - GSI asigna a cada recurso y cliente Grid una serie de credenciales mediante certificados digitales.
- Implementa**:**
  - **Autenticación Única (Single sign-on):** No es Necesario Proporcionar la Clave en Cada Acción.
  - **Delegación**: Un Servicio Puede Actuar en el Nombre de Una Persona.
  - **Autenticación Mútua:** Ambas Partes Deben Autenticarse Entre sí.
  - **Autorización de Acceso a Recursos.** Permite Configurar para cada Recurso una Política de Seguridad Según el Usuario que Accede y las Credenciales que Presente.

Implementación de la Seguridad en el Grid
Grid Security Infrastructure (GSI)
El proxy

Grid y Computación de Altas Prestaciones GRyCAP

- El Proxy
  - Credenciales Temporales que los Crean Clientes a Partir de las que ya Disponen, Válidas para un Tiempo Determinado.
  - Estas Credenciales son También un Certificado Llamado "Proxy".
  - Estos Certificados de Corta Duración Incluyen su Clave Privada y que se Firman con el Certificado del Usuario.
  - Con Estos Certificados se Crean Comunicaciones Seguras entre los Clientes y Recursos, Además de Garantizar la Autenticación de los Usuarios.



Implementación de la Seguridad en el Grid
Grid Security Infrastructure (GSI)
El proxy

Grid y Computación de Altas Prestaciones
GRyCAP

- Los Proxies Limitan el Riesgo de Exposición de las Credenciales.
  - Los Proxies Se Transmiten por la Red Para Evitar que la Clave Privada Viaje o Evitar que Se Reintroduzca en Cada Operación.
- Los Proxies Identifican al Usuario:
  - "Subject" del Usuario: `/C=E/O=UPV/OU=GRID/CN=J. Damian Segrelles`
  - "Subject" del Proxy: `/C=E/O=UPV/OU=GRID/CN=J.Damian Segrelles/CN=id_proxy`
- Tipos de Proxy
  - Proxy Completo
    - Un Proxy Creado a Partir de un Certificado de Usuario o a Partir de Otro Proxy Completo Mediante Delegación Normal.
  - Proxy Limitado
    - Un Proxy Creado a Partir de Otro Proxy Mediante Delegación Limitada o a Partir de Otro Proxy Limitado.

Implementación de la Seguridad en el Grid
Grid Security Infrastructure (GSI)
Autorización

- La **Autorización Grid** Consiste en la Concesión o Denegación de Permisos a un Usuario Grid Perteneciente a una VO Para Llevar a Cabo una Determinada Acción Sobre un Recurso Determinado.
- Conceptos Clave
  - **Organización Virtual (VO).** Entidad Compuesta por un Conjunto de Usuarios, Instituciones y Recursos, en la que Todos Ellos Pertenecen a un Mismo Dominio Administrativo Virtual.
  - **Proveedor de Recursos (RP).** Entidad o Dispositivo que ofrece Recursos (CPUs como Recursos Computacionales, Recursos de Almacenamiento, etc.) a Otros Miembros Pertenecientes a una Misma VO, de Acuerdo con unas Políticas de Colaboración.

Implementación de la Seguridad en el Grid
Grid Security Infrastructure (GSI)
Autorización

Grid y Computación de Altas Prestaciones
GRyCAP

- La Autorización de un Usuario Grid a un Recurso se Define Generalmente a Partir de la VO.
  - Los Permisos son Comunes a Todos los Miembros de la VO.
  - Un Usuario Puede Pertenecer a Varias VOs, Aunque en el Esquema GSI Puede Ocasionar Problemas.
- Los Administradores de las VOs Conceden los Permisos a Nivel de VO a los Usuarios Grid y Además se Encargan de Establecer Acuerdos con los RPs para el Acceso a los Recursos.
  - Generalmente se Establecen Usuarios Locales que Disponen de Permisos Concretos y se Mapean los Usuarios Grid con los Usuarios Locales.
  - No Se Puede Mapear un Usuario desde Dos VOs Diferentes en GSI.
- Los RPs, a su vez, Implantan sus Propias Políticas de Seguridad Local que Aplicarán en Función de las Credenciales que el Usuario Grid Presente y los Acuerdos Establecidos con las VOs Correspondientes.

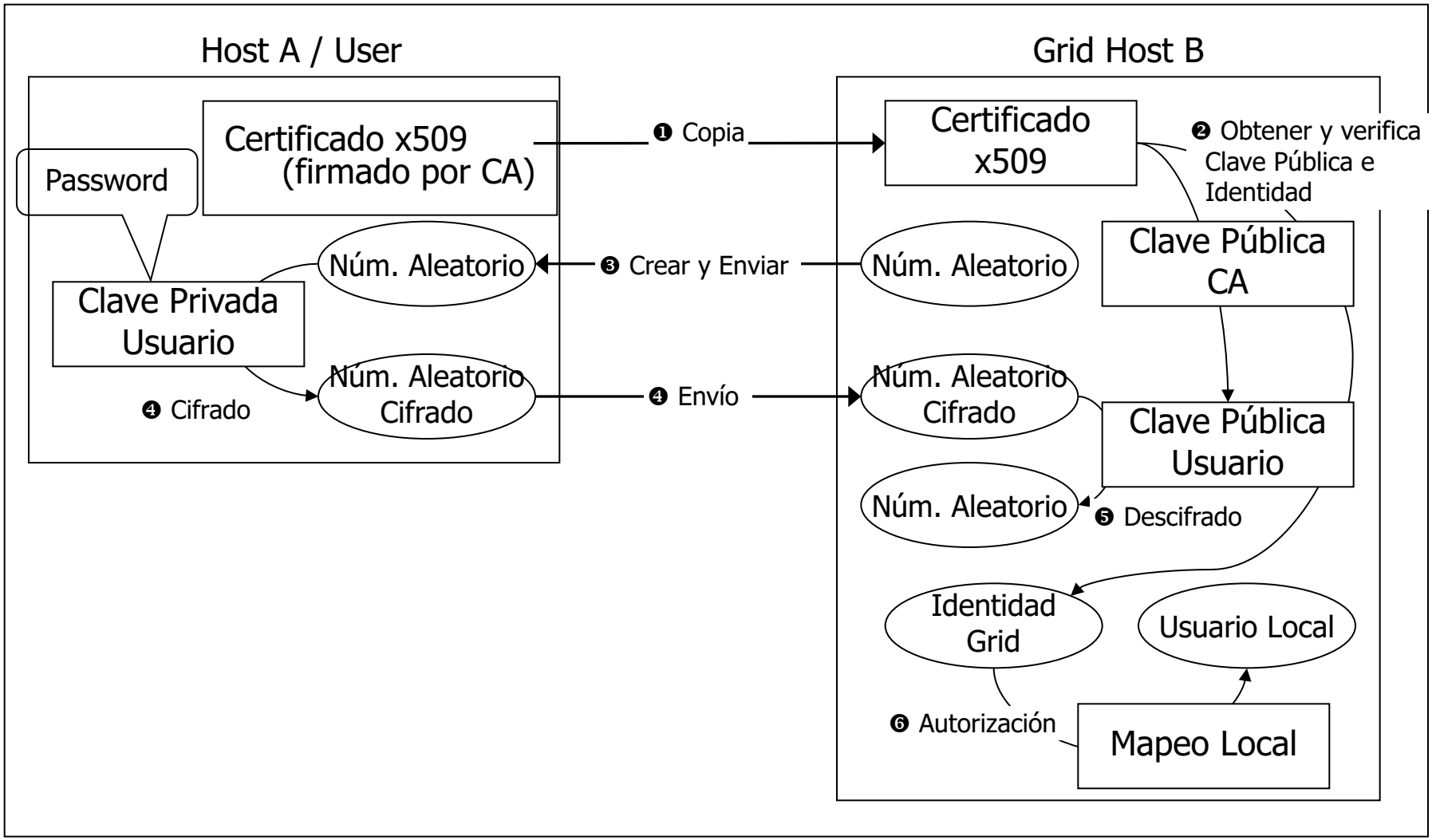
Implementación de la Seguridad en el Grid
Grid Security Infrastructure (GSI)
Autorización

Grid y Computación de Altas Prestaciones
GRyCAP

- Estructura de una VO
  - Listado de DNs Aceptados.
  - Copia de los Directorios Remotos en Ficheros de Configuración Locales.
  - Fichero de Mapeo (grid-mapfile)
    - "/C=ES/O=UPV/CN=José Pérez" grid
    - "/C=ES/O=UPV/CN=Antonio Martínez" grid
    - "/C=ES/O=UPV/CN=Juan García" grid_user
    - "/C=ES/O=UPV/CN=Pedro Ramírez" grid_user
  - Existen Modelos Más Complejos
    - Permiten Definir Grupos y Subgrupos (Ej. VOMS service).
    - Manejan de Forma Efectiva la Pertenencia a Dos VOs.
    - Permiten Definir Roles y Asociar Permisos a Roles.

Implementación de la Seguridad en el Grid
Grid Security Infrastructure (GSI)
(Ej. Escenario Autenticación y Autorización en el Grid)

Grid y Computación de Altas Prestaciones
GRyCAP



Implementación de la Seguridad en el Grid
Grid Security Infrastructure (GSI)
(Ej. Escenario Autenticación y Autorización en el Grid)

Grid y Computación de Altas Prestaciones
GRyCAP

- El Proceso que se Sigue para Garantizar la Confianza Mutua entre dos Hosts A y B que Quieren Comunicar en el Grid es:
  1. Se Envía el Certificado x509 Firmado por la CA al Host Remoto (Host B).
  2. El Host B Obtiene del Certificado la Clave Pública del Certificado y la Identidad del Usuario Mediante la Clave Pública de la CA. De Esta Forma se Garantiza que la Identidad del Usuario está Verificada por la CA.
  3. El Host B Crea un Número Aleatorio y lo Envía al Origen (Host A).
  4. Una Vez Recibido, El host A Cifra el número con la Clave Privada (que Podría Estar Protegida por una Contraseña Adicional) y Envía el Número Cifrado al Host B.
  5. El Host B Descifra el Número con la Clave Pública del Usuario Contenida en el Certificado y Comprueba que es el Número Enviado. De Esta Forma se Verifica que el Usuario Dispone de su Clave Privada.
  6. Una Vez Verificada la Identidad y que esta se encuentra Firmada por la CA, se Verifica que la Identidad (Generalmente en Forma de un Nombre Distintivo (Distinguished Name ó (DN) como "O=Grid/O=Globus/OU=itso.grid.com/CN=your name", se Encuentra en el Directorio de Usuarios Autorizados.

Implementación de la Seguridad en el Grid
Grid Security Infrastructure (GSI)
(Riesgos Potenciales de Seguridad)

Grid y Computación de Altas Prestaciones
GRyCAP

- Aunque un Entorno PKI Proporciona al GSI los Servicios Necesarios Para Desarrollar una Solución Grid Segura, Esto no Garantiza que No Hayan Riesgos.
- Los **Principales Riesgos** se Encuentran en el Almacenamiento de las Claves Privadas y Certificados:
  - **Suplantación de Identidad.** Un Usuario con Suficientes Privilegios Podría Robar un Certificado Proxy y Utilizarlo para Suplantar la Identidad de Otro Usuario de Forma Fraudulenta.
    - Esto Sólo Podría Hacerse Por Tiempo Limitado (Duración de un Proxy).
  - **Robo de la Clave Privada** de un Certificado de Usuario. Un Usuario con Suficientes Privilegios Podría Copiar y Adueñarse de la Clave Privada.
    - Se Necesitaría del Password Para poder Realizar Operaciones.
  - **Robo de la Clave Privada de la CA.** Permitiría Emitir Certificados Fraudulentos o Destruir la Clave Privada.
    - Seguiría Necesitando del Password, pero los Riesgos Son Mucho Mayores.
    - Generalmente las CAs se Encuentran Desconectadas de Toda Red y Alojadas en un Lugar Seguro, Aunque Necesitan Disponer de Dispositivos Removibles para Poder Copiar las Peticiones.

Responsibilidades del Usuario

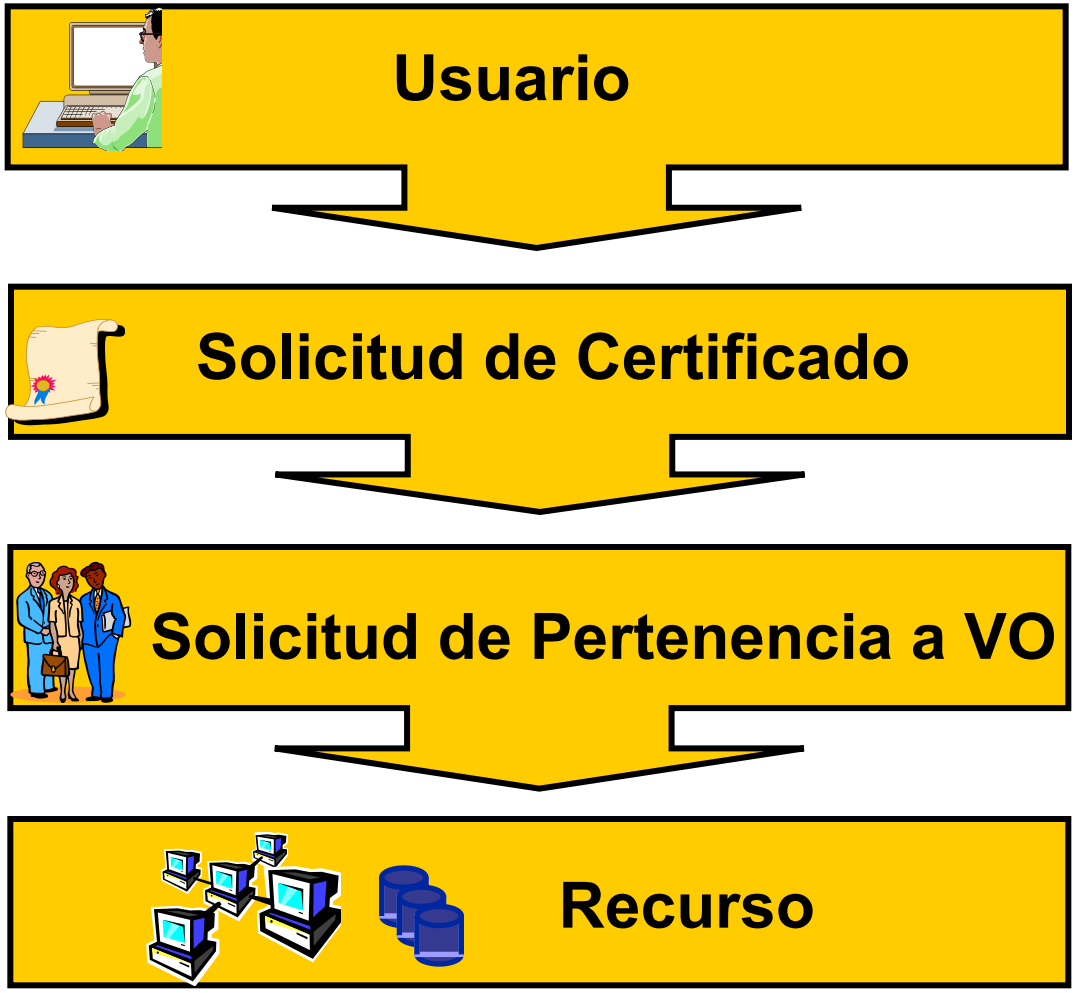
Grid y Computación de Altas Prestaciones GRyCAP

- Mantener la Clave Privada en un Lugar Seguro.
- No Prestar el Certificado (Con la Clave Privada) a Nadie.
- Informar a los Contactos Locales y Regionales si el Certificado ha Sido Comprometido.
- No Lanzar Un Servicio de Delegación Por Más Tiempo Que lo que Necesita la Tarea.

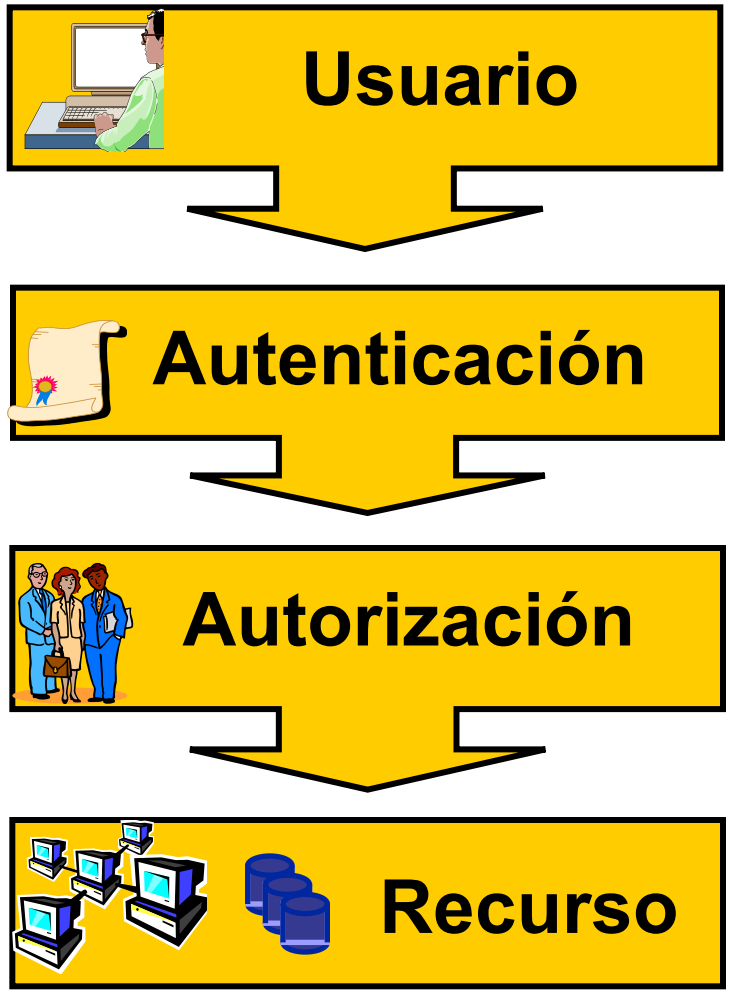
Si una Persona Diferente Utiliza un Certificado o Servicio Delegado No Podrá Probarse que Fuera Otra Persona.

Resumen: Credenciales

Grid y Computación de Altas Prestaciones
GRyCAP



Resumen: Acceso



via Certificados y Servicios Delegados

Vía la VO y las Políticas Locales

P4