# Servicios Web Seguros

## Sesión 5: Almacén de certificados

# Puntos a tratar

- Servicios web seguros
- Almacén de certificados
- Par de claves
- Autoridad certificadora
- Importación de certificados

# Servicios web seguros

- Necesidad de encriptar la información
  - Nivel de transporte
    - Conexión SSL
    - Encripta contenido y cabeceras
    - Para ver las cabeceras hay que desencriptarlo entero
  - Nivel de mensaje
    - Encripta partes del mensaje
    - Útil si hay nodos intermedios
- Necesidad de garantizar la autenticidad del mensaje
  - Integridad (Nadie lo ha modificado)
  - Emisor (No hay suplantación de identidad)

# Mecanismos de seguridad

- Encriptación simétrica (única clave)
- Clave pública / Clave privada
  - Una encripta y la otra desencripta (y viceversa)
  - La pública la conoce todo el mundo
  - La privada la utiliza sólo el propietario, para firmar los mensajes y para desencriptar los mensajes que le envían los demás
  - La pública la utilizan los demás para encriptar, y sólo el propietario de la privada es capaz de desencriptarlos

# Difundir las claves públicas

- Cada entidad podría colgar sus claves públicas
  - Podrían ser suplantadas
- Para garantizar la autenticidad de las claves públicas, otra entidad puede firmarlas
  - Hay que fiarse de esa entidad certificadora
    - Ejemplo: VerySign
- Certificado digital: el conjunto de
  - clave pública
  - información de la entidad
  - firma que certifica dicha información

# Almacén de certificados

- Para comprobar la autenticidad de un nuevo certificado, necesitamos el certificado de la autoridad certificadora que lo certifica.
- Los certificados raíz van firmados por la misma entidad que los emite, y debemos aceptarlos explícitamente, fiándonos de su autenticidad.
- Truststore: almacén de certificados raíz
- Keystore: almacén con el resto de certificados que vamos a utilizar en nuestras comunicaciones
- Truststore y keystore pueden ir juntos en uno.

# Almacén de certificados

| Clave privada | Certificado | Firmado por... | Uso |
|---|---|---|---|
| c1-privada | CN=Boyan, DC=jtech, ... Cl.Pública=c1-publica | cCA-privada | Para mí, y para enviar el certificado a otros |
| (no disponible) | CN=Certificate Authority, DC=verysign, ... Cl.Pública=cCA-publica | cCA-privada | Para comunicar con la CA (y así obtener los certificados de los amigos) |
| (no disponible) | CN=Amigo1,DC=domini ... Cl.Pública=c2-publica | cCA-privada | Para cifrar cuando envío a Amigo1 |
| (no disponible) | CN=Amigo2,DC=domini ... Cl.Pública=c3-publica | cCA-privada | Para cifrar cuando envío a Amigo2 |

# JKS

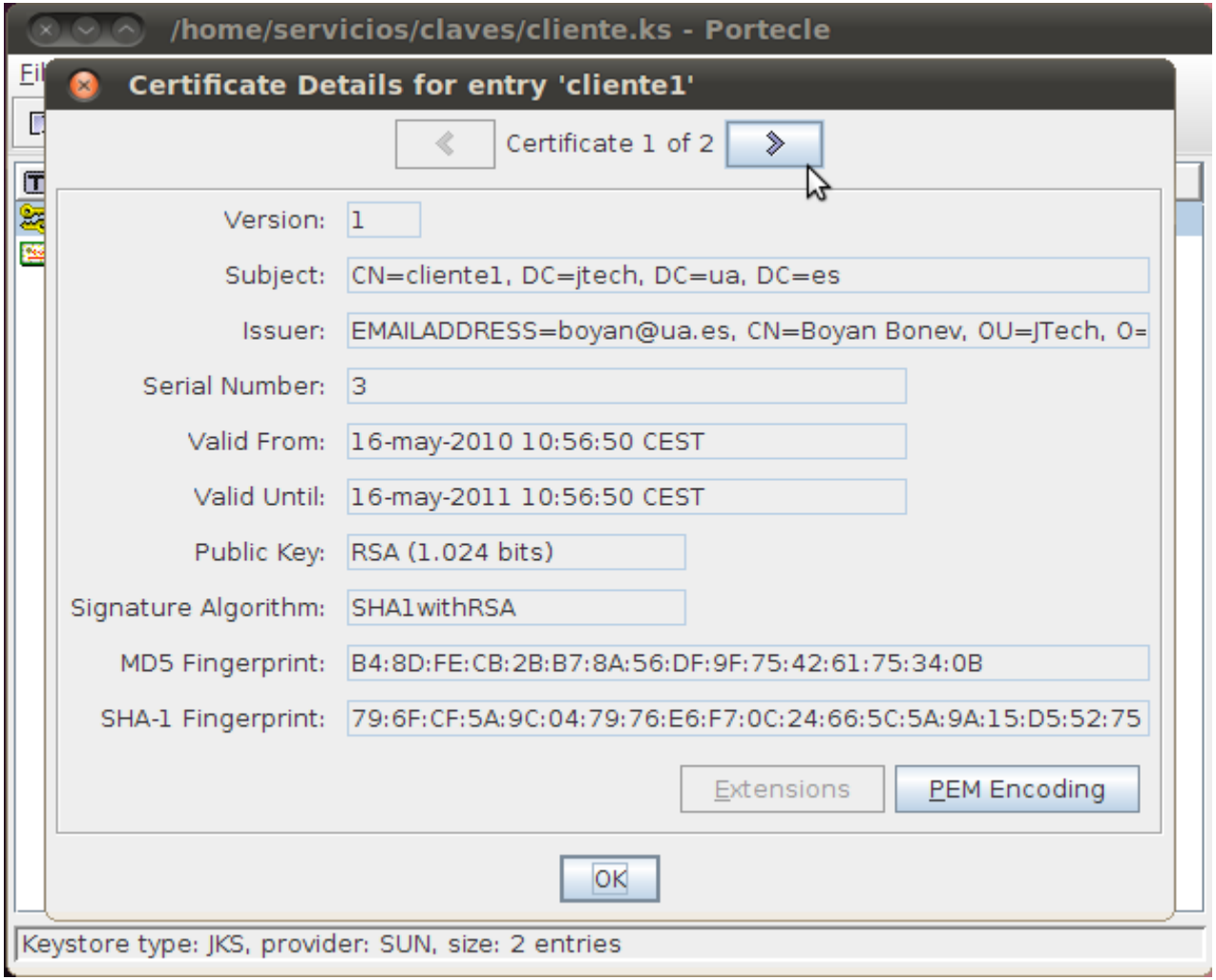
- Formato Java Key Store
- Soportado por Apache Tomcat, Rampart, etc.
- Utilidades:
  - Keytool
  - Interfaces gráficas de Keytool: Portecle

# Keytool

- Generar par de claves
- Generar petición de certificado (.csr)
- Importar certificados en un almacén
- Muchas funciones más

```
-certreq    [-v] [-protected]
            [-alias <alias>] [-sigalg <algoritmo_firma>]
            [-file <archivo_csr>] [-keypass <contraseña_clave>]
            [-keystore <almacén_claves>] [-storepass <contraseña_almacén>]
            [-storetype <storetype>] [-providername <name>]
            [-providerclass <provider_class_name> [-providerarg <arg>]] ...
            [-providerpath <pathlist>]

-changealias [-v] [-protected] -alias <alias> -destalias <destalias>
            [-keypass <contraseña_claves>]
            [-keystore <almacén_claves>] [-storepass <contraseña_almacén>]
            [-storetype <storetype>] [-providername <name>]
            [-providerclass <provider_class_name> [-providerarg <arg>]] ...
            [-providerpath <pathlist>]

-delete     [-v] [-protected] -alias <alias>
            [-keystore <almacén_claves>] [-storepass <contraseña_almacén>]
            [-storetype <storetype>] [-providername <name>]
            [-providerclass <provider_class_name> [-providerarg <arg>]] ...
            [-providerpath <pathlist>]

-exportcert [-v] [-rfc] [-protected]
            [-alias <alias>] [-file <archivo_cert>]
            [-keystore <almacén_claves>] [-storepass <contraseña_almacén>]
            [-storetype <storetype>] [-providername <name>]
            [-providerclass <provider_class_name> [-providerarg <arg>]] ...
            [-providerpath <pathlist>]

-genkeypair [-v] [-protected]
            [-alias <alias>]
            [-keyalg <algoritmo_clave>] [-keysize <tamaño_clave>]
            [-sigalg <algoritmo_firma>] [-dname <nombre_d>]
            [-validity <días_validez>] [-keypass <contraseña_clave>]
            [-keystore <almacén_claves>] [-storepass <contraseña_almacén>]
            [-storetype <storetype>] [-providername <name>]
            [-providerclass <provider_class_name> [-providerarg <arg>]] ...
            [-providerpath <pathlist>]

-genseckey  [-v] [-protected]
            [-alias <alias>] [-keypass <keypass>]
            [-keyalg <algoritmo_clave>] [-keysize <tamaño_clave>]
            [-keystore <almacén_claves>] [-storepass <contraseña_almacén>]
            [-storetype <storetype>] [-providername <name>]
            [-providerclass <provider_class_name> [-providerarg <arg>]] ...
            [-providerpath <pathlist>]

-importcert [-v] [-noprompt] [-trustcacerts] [-protected]
            [-alias <alias>]
            [-file <archivo_cert>] [-keypass <contraseña_clave>]
            [-keystore <almacén_claves>] [-storepass <contraseña_almacén>]
            [-storetype <storetype>] [-providername <name>]
            [-providerclass <provider_class_name> [-providerarg <arg>]] ...
            [-providerpath <pathlist>]

-importkeystore [-v]
            [-srckeystore <srckeystore>] [-destkeystore <destkeystore>]
            [-srcstoretype <srcstoretype>] [-deststoretype <deststoretype>]
            [-srcstorepass <srcstorepass>] [-deststorepass <deststorepass>]
            [-srcprotected] [-destprotected]
            [-srcprovidername <srcprovidername>]
            [-destprovidername <destprovidername>]
            [-srcalias <srcalias> [-destalias <destalias>]
              [-srckeypass <srckeypass>] [-destkeypass <destkeypass>]]
            [-noprompt]
            [-providerclass <provider_class_name> [-providerarg <arg>]] ...
            [-providerpath <pathlist>]

-keypasswd  [-v] [-alias <alias>]
            [-keypass <contraseña_clave_antigua>] [-new <nueva_contraseña_clave>]
            [-keystore <almacén_claves>] [-storepass <contraseña_almacén>]
            [-storetype <storetype>] [-providername <name>]
            [-providerclass <provider_class_name> [-providerarg <arg>]] ...
            [-providerpath <pathlist>]

-list       [-v | -rfc] [-protected]
            [-alias <alias>]
            [-keystore <almacén_claves>] [-storepass <contraseña_almacén>]
            [-storetype <storetype>] [-providername <name>]
            [-providerclass <provider_class_name> [-providerarg <arg>]] ...
            [-providerpath <pathlist>]

-printcert  [-v] [-file <archivo_certif>]

-storepasswd [-v] [-new <nueva_contraseña_almacén>]
            [-keystore <almacén_claves>] [-storepass <contraseña_almacén>]
            [-storetype <storetype>] [-providername <name>]
            [-providerclass <provider_class_name> [-providerarg <arg>]] ...
            [-providerpath <pathlist>]
```

# Portecle



# Autoridad certificadora (CA)

- Configurar una autoridad certificadora propia:
  - OpenSSL
- Generar una petición de certificado (.pem)
- Generar certificado autofirmado
- Finalmente podemos firmar la petición de certificado con la clave privada de la autoridad certificadora que hemos configurado

# Importar certificados

- Hay que importar los certificados en el almacén de certificados
  - Certificado autofirmado de la CA
    - Hay que confiar explícitamente en él
  - Nuestro certificado firmado por la CA
    - Se confía automáticamente en él, ya que se ha confiado en la CA y ésta lo firma.

# ¿Preguntas...?