01-2025

code
URJC

Desarrollo Web

Tema 3.1
Seguridad Web

Universidad Rey Juan Carlos

Micael Gallego, Francisco Gortázar, Michel Maes, Óscar Soto e Iván Chicano

code
URJC

Micael Gallego, Francisco Gortázar, Michel Maes, Óscar Soto, Iván Chicano

Seguridad Web

code URJC

- **Servicios de seguridad**
  - Un **servicio de seguridad** protege las comunicaciones de los usuarios ante determinados ataques. Los principales son:
    - **Autenticación (authentication)**
    - **Autorización (authorization)**
    - **Integridad (data integrity)**
    - **Confidencialidad (data confidentiality)**

Seguridad Web

code URJC

- **Servicios de seguridad**
  - **Autenticación (authentication):** sirve para garantizar que una entidad (persona o máquina) es quien dice ser
  - **Autorización (authorization):** sirve para discernir si una entidad tiene acceso a un recurso determinado

Seguridad Web

code URJC

- **Servicios de seguridad**
  - **Integridad (data integrity):** garantiza al receptor del mensaje que los datos recibidos coinciden exactamente con los enviados por el emisor
  - **Confidencialidad (data confidentiality)** proporciona protección para evitar que los datos sean revelados a un usuario no autorizado

Seguridad Web

code URJC

- **Autenticación**
  - La autenticación se consigue mediante:
    - **Algo que sabes.** Por ejemplo, unas credenciales login-password
    - **Algo que tienes.** Por ejemplo, una tarjeta de acceso
    - **Algo que eres.** Por ejemplo, cualidades biométricas (huella digital…)

Seguridad Web

code URJC

- **Autorización**
  - La autorización determina si un **usuario puede acceder** a un recurso determinado en base a permisos (*grants*), lista de control de acceso (*Access Control List*, ACL), políticas (*policies*), roles, tokens, …
  - Normalmente requiere **autenticación** previa (es decir, confirmar la **identidad** del usuario)

Seguridad Web

code URJC

- **Integridad**
  - La integridad se consigue típicamente con funciones **Hash criptográficas** (**resumen**)
  - Son funciones que convierten un **texto plano** en una **secuencia alfanumérica**
  - Partiendo de la secuencia alfanumérica **no se puede generar de nuevo el texto plano** de entrada
  - Es muy difícil que **dos textos** planos tengan la **misma** cadena alfanumérica de salida

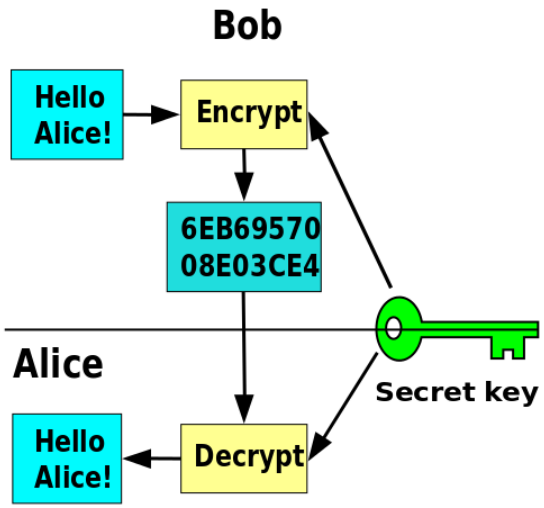
Seguridad Web

code URJC

- **Confidencialidad**
  - La confidencialidad se consigue típicamente usando técnicas criptográficas de **cifrado de mensajes**
  - Tipos de sistemas criptográficos:
    - **Clave secreta** (simétricos)
    - **Clave pública** (asimétricos)

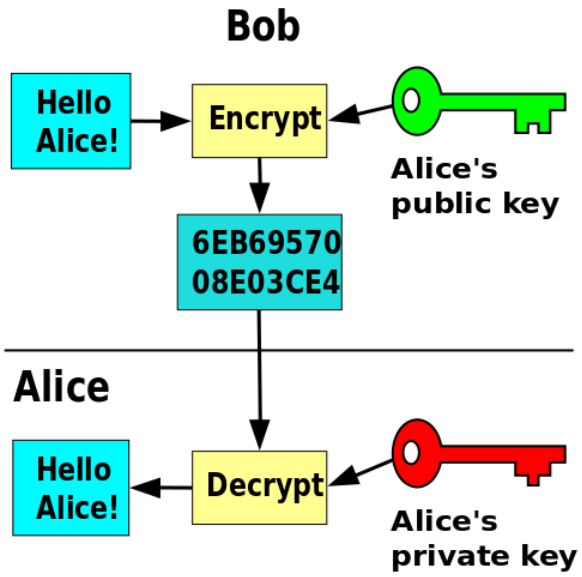
Seguridad Web

- **Clave secreta**
  - En ellos, la **clave** de **cifrado** y de **descifrado** es la **misma**: es una clave secreta que comparten el emisor y el receptor del mensaje.
  - Debido a esta característica son denominados también criptosistemas **simétricos**



Seguridad Web

- **Clave pública**
  - Se distinguen porque cada usuario dispone de dos claves: una **privada**, que debe mantener secreta, y una **pública**, que debe ser conocida por todas las restantes entidades que van a comunicar con ella.
  - Se los conoce también como criptosistemas **asimétricos**



Seguridad Web

code URJC

- **Certificados digitales**
  - En los sistemas de **clave pública**, un **certificado** digital es un fichero que asocia el **nombre de una entidad** con su **clave pública**
  - El certificado digital es emitido por una **Autoridad de Certificación (CA)**, es decir, una entidad reconocida de confianza o "Tercera Parte de Confianza" (TTP, Trusted Third Party)

Seguridad Web

code URJC

- **Diferentes algoritmos de cada tipo**

Criptosistemas asimétricos

- RSA (Rivest, Shamir y Adleman)
- Diffie-Hellman
- ElGamal
- Criptografía de curva elíptica

Funciones hash

- SHA (*Secure Hash Algorithm*)
- MD5 (*Message-Digest Algorithm 5*)
- DSA (*Digital Signature Algorithm*)

Criptosistemas simétricos

- AES (*Advanced Encryption Standard*)
- ES (*Data Encryption Standard*)
- IDEA (*International Data Encryption Algorithm*)
- 3DES
- RC2, RC4, RC5
- Blowfish

Seguridad Web: HTTPS

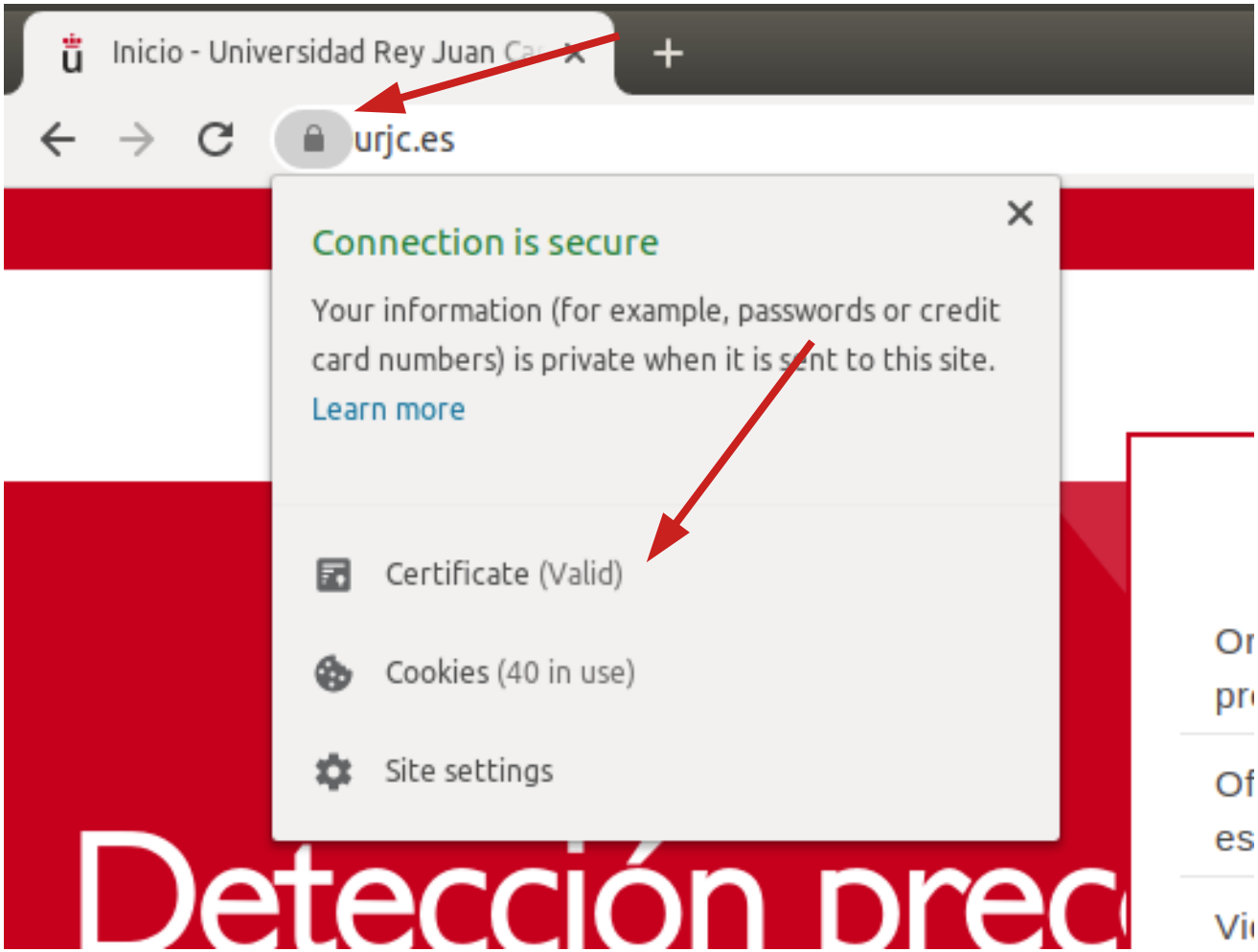
- **Https** *(Hypertext Transfer Protocol Secure)*: Versión segura de HTTP
- Con HTTPS se consigue que toda la información que se intercambie un **navegador** web con un **servidor** web esté **cifrada**
- Es decir, un usuario malicioso no podrá entender la información que viaja por la red
- HTTPS utiliza criptografía de **clave pública** y se apoya en el estándar **TLS**

Seguridad Web: HTTPS

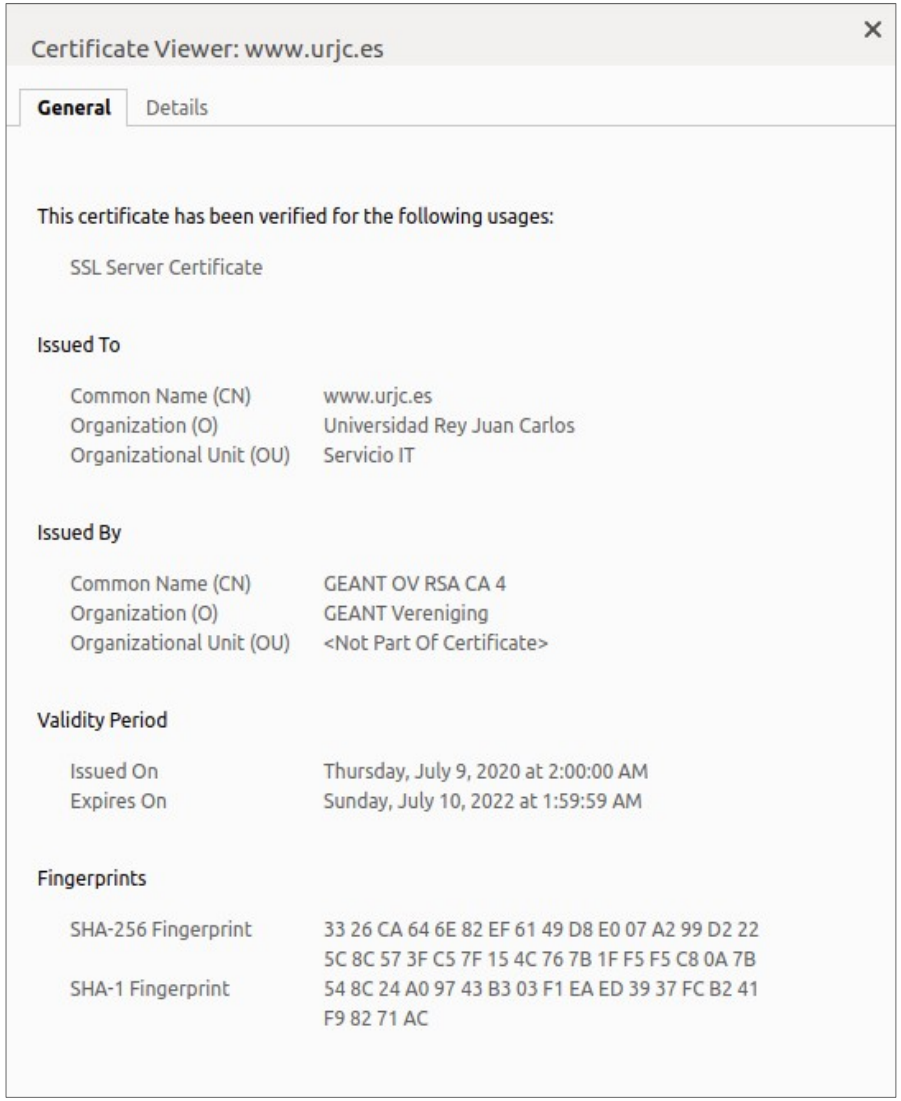
code URJC

- Los navegadores tienen una **lista de Autoridades de Certificación (CA)** en las que confían
- Cuando un usuario accede a una página web mediante https, el servidor web presenta un **certificado firmado por una CA**

Seguridad Web: HTTPS



Seguridad Web: HTTPS



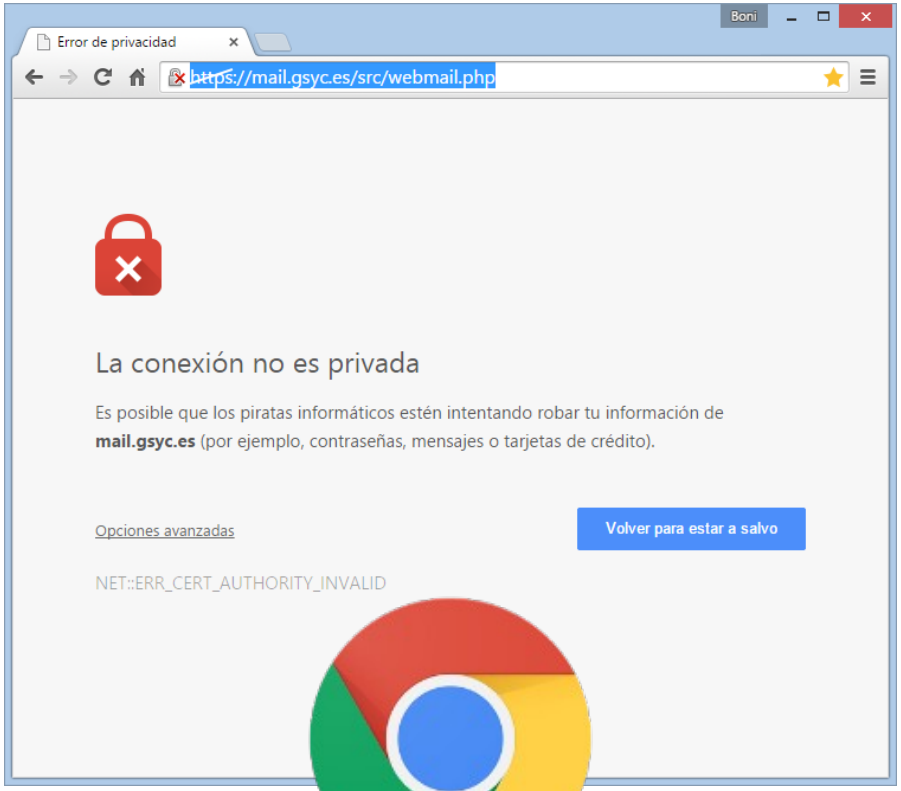
Seguridad Web: HTTPS

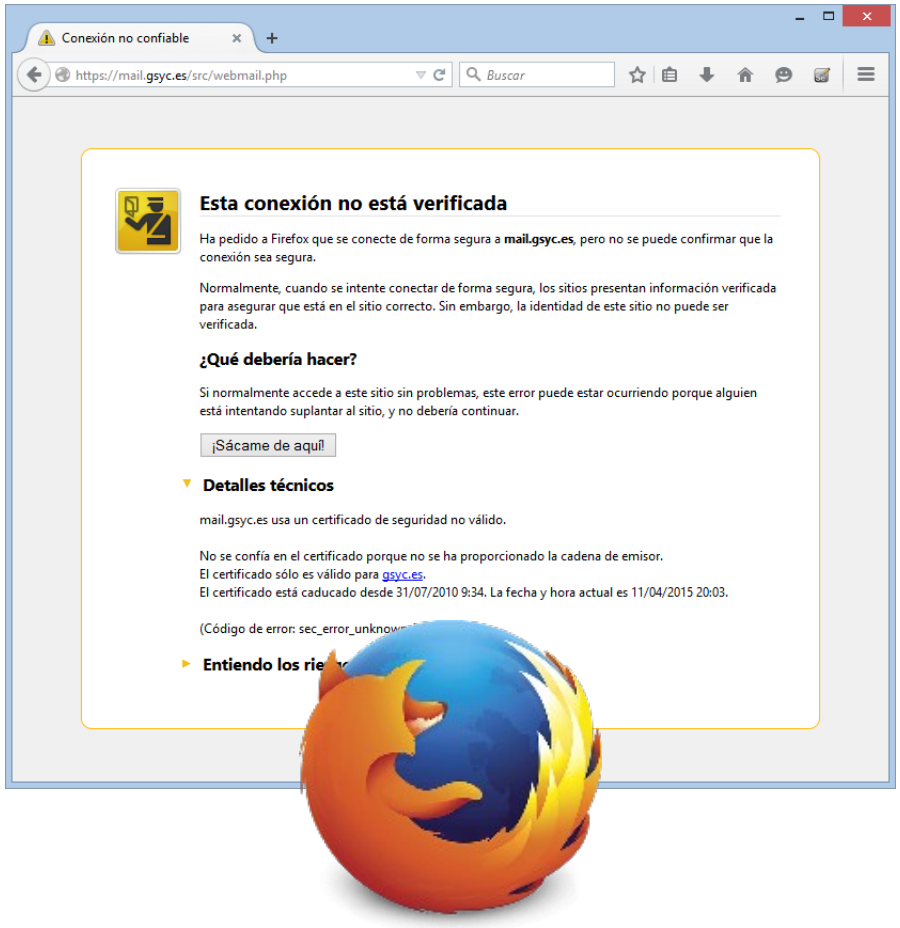
code URJC

- Si el usuario se conecta a una página web que presenta un certificado firmado por una **CA no reconocida** por el navegador web, se muestra un **aviso al usuario de que podría estar sufriendo un ataque**

Seguridad Web: HTTPS

code URJC





Seguridad Web: HTTPS

code URJC

- **¿Cómo conseguir un certificado?**
  - Comprándolo a una **Autoridad de Certificación**
  - Gratis con **Let's Encrypt**
  - Gratis creándolo uno mismo (**inseguro**)

Seguridad Web: HTTPS

code URJC

- **Comprándolo a una Autoridad de Certificación**
  - Se necesita un dominio
  - Puede costar entre **10€ y 1000€** anuales

digicert®

GoDaddy™

IONOS by 1&1

Seguridad Web: HTTPS

code URJC

- **Gratis con Let's Encrypt**
  - Se necesita un dominio
  - Let’s Encrypt es una entidad sin ánimo de lucro que proporciona certificados de confianza
  - Apoyada por la industria

Seguridad Web: HTTPS

code URJC

- **Gratis creándolo uno mismo**
  - No se necesita dominio
  - No ofrece **ninguna seguridad**
  - Los navegadores mostrarán el **aviso** de entidad no reconocida a los usuarios
  - Se usa para pruebas
  - Se suele denominar **self-signed certificate** (certificado autofirmado)