Cómo asegurar Sistemas Web con SSL/TLS fácil y sin costo!

Paul F. Bernal B.
paul.bernal@cedia.org.ec

csirt.cedia.org.ec

Agenda

HTTP y HTTPS

Certificados Digitales

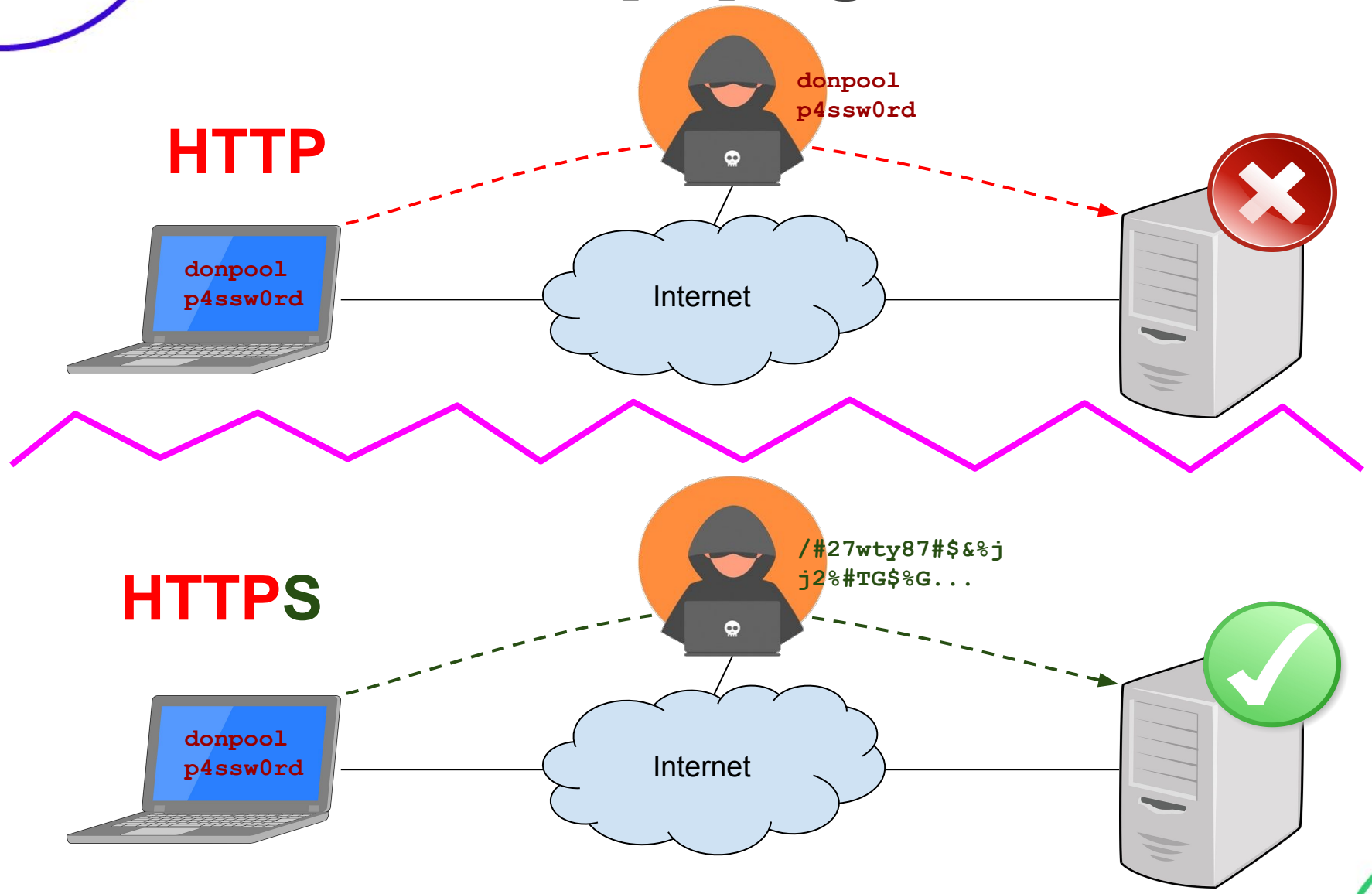
Let’s Encrypt

Manos a la obra

HTTP y HTTPS

csirt.cedia.org.ec

Sitios Web [in]seguros

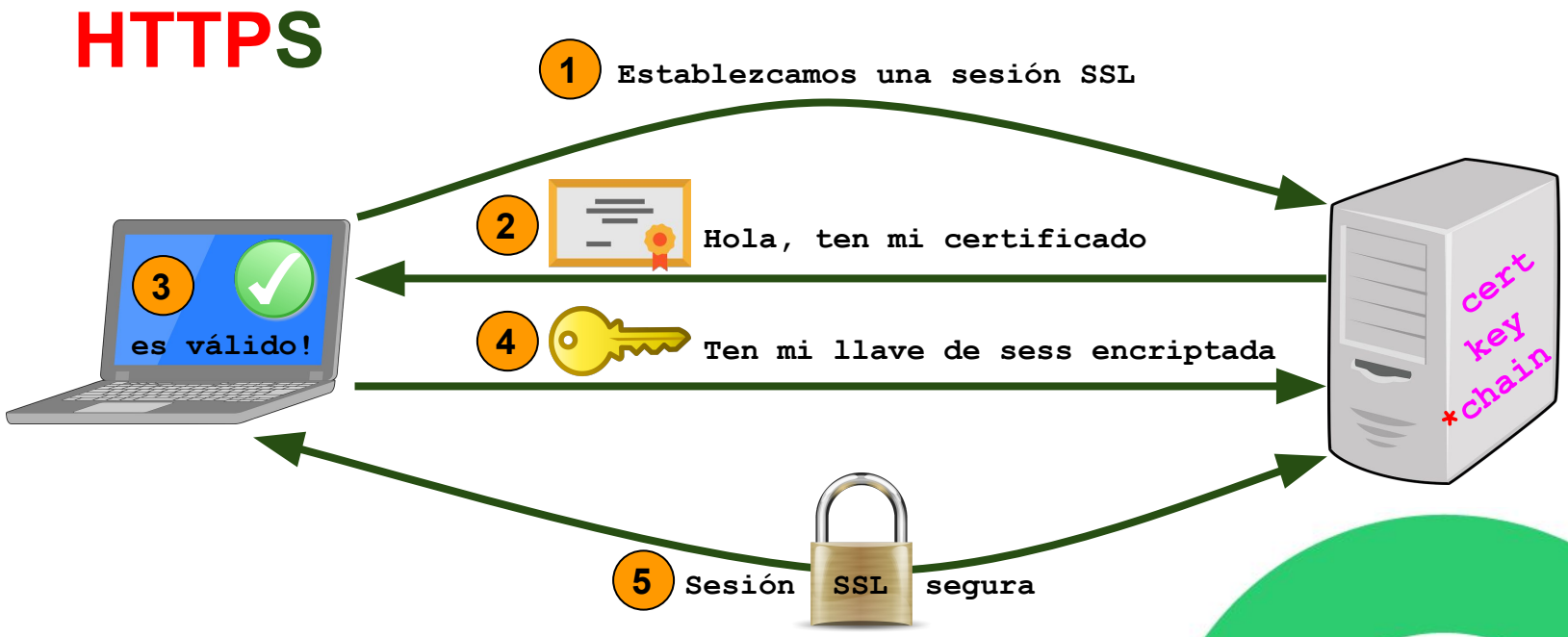


Certificados Digitales

csirt.cedia.org.ec

Certificados Digitales

- Los Certificados Digitales son básicamente un grupo de archivos:
  - Certificado (**cert**)
  - Llave Privada (**key**)
  - Cert. Intermedio (**chain**) *



Porqué necesito SSL/TLS

Los Certificados Digitales logran principalmente 2 cosas:

1. Encriptar las comunicaciones C/S (ya lo vimos)
2. Validar que el sitio que abrí es el sitio que quería abrir

`https://www.cedia.org.ec/correo/login.php`

`https://cedia.org.ec-correo.site/login.php`

¿ Con SSL/TLS, no necesito más ?

¡ FALSO !

- La seguridad se concibe e implementa **por capas**.
- En web, SSL/TLS es sólo una de esas capas
- No impide otros tipos de ataque:
  - Fuerza bruta
  - Clickjacking
  - Cross Site Scripting (XSS)
  - Falsificación de solicitudes entre sitios / CSRF
  - Ejecución remota de código
  - Inclusión de archivos locales (LFI) y remotos (RFI)
  - Inyección SQL
  - Redirección de URL

Programación Segura

csirt cedia

Let's Encrypt

cedia

csirt.cedia.org.ec

Autoridades de Certificación

- Entidades autorizadas a emitir Certificados Digitales
- Usan un certificado para ser identificadas/validadas
- Los navegadores tienen/usan estos certs
- Emisión de Certificados:
  - Existe un costo asociado a la emisión
  - Los costos varían por CA y por tipo de Certificado
  - Se emiten normalmente por un año o más

Let's Encrypt.org

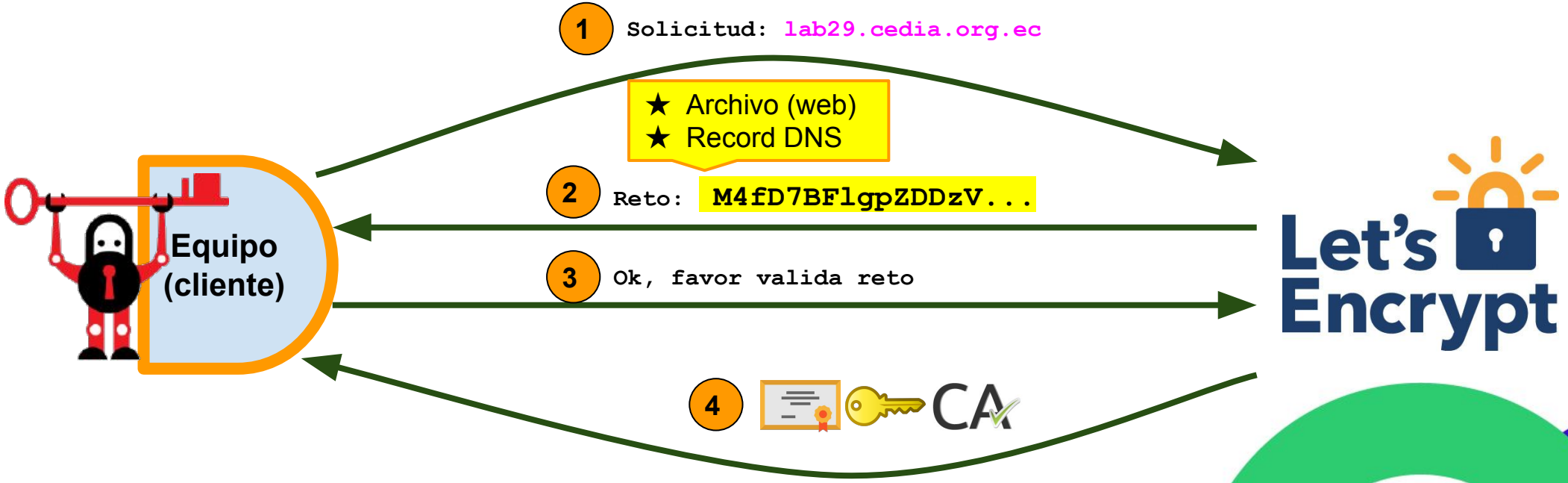
- Autoridad de Certificación (CA)
- Desde abril/2016
- Certificados X.509 **gratuitos**
- Proceso simplificado
- Emisión
- Renovación
- Revocación
- 90 días de vigencia
- "Wildcards" desde marzo/2018

Cómo Funciona Let's Encrypt

- Demostrar control sobre el dominio
- Usa el protocolo ACME
- 2 Métodos principales
  - Validar por archivo (file challenge)
  - Validar por DNS (DNS challenge, para wildcards[*])
- Herramientas (clientes)
  - certbot
  - acme.sh

Cómo Funciona Let's Encrypt

- ★ Instalar el cliente de ACME
- ★ Solicitar la emisión del certificado
- ★ Cumplir el Reto



Cómo Funciona Let's Encrypt

★ Archivos obtenidos. Ejemplo (real):

```
[pbernal@t470s ~]$ ll ~/.acme.sh/paulbernal.com/
total 28
-rw-r--r-- 1 pbernal pbernal 1648 mar 29 00:45 ca.cer
-rw-r--r-- 1 pbernal pbernal 3579 mar 29 00:45 fullchain.cer
-rw-r--r-- 1 pbernal pbernal 1931 mar 29 00:45 paulbernal.com.cer
-rw-r--r-- 1 pbernal pbernal  542 mar 29 00:45 paulbernal.com.conf
-rw-r--r-- 1 pbernal pbernal 1001 mar 29 00:38 paulbernal.com.csr
-rw-r--r-- 1 pbernal pbernal  230 mar 29 00:38 paulbernal.com.csr.conf
-rw-r--r-- 1 pbernal pbernal 1675 may 28  2018 paulbernal.com.key
[pbernal@t470s ~]$
```

Cómo Funciona Let's Encrypt

★ Configurar servidor web (NGINX). Ejemplo (real):

```
server {
    charset utf-8;
    client_max_body_size 128M;

    listen 443 ssl;
    listen [::]:443 ssl;

    server_name yii2.paulbernal.com;
    root        /home/fs/var/www/yii2.paulbernal.com/web;
    index       index.php;

    ssl_certificate /etc/pki/tls/certs/fullchain.cer;
    ssl_certificate_key /etc/pki/tls/private/paulbernal.com.key;
```

csirt cedia

Manos a la Obra

cedia

csirt.cedia.org.ec

Manos a la Obra !!!

Sitio: **lab02.cedia.org.ec**

- ❑ Instalar acme.sh
- ❑ Obtener el certificado
- ❑ Instalar el certificado
- ❑ Configurar Servidor web
- ❑ Probar

Querías las Diapositivas ?

https://bit.ly/WebLab29

csirt cedia

cedia

csirt.cedia.org.ec

¡ Gracias !

Paul F. Bernal B.

paul.bernal@cedia.org.ec

593 98 466 9053

csirt.cedia.org.ec