VNIVERSITAT DE VALÈNCIA

ACMEBOT: Gestión automatizada de certificados SSL en la UV

Autores: Héctor M. Rulot Segovia y M. Carmen Mifsut Herrera
Ponente: M. Carmen Mifsut Herrera

JT 2026 Red IRIS
A CORUÑA 22-25 JUNIO Universidade da Coruña
red.es | Red IRIS | IGTS | UNIVERSIDADE DA CORUÑA

Introducción

Origen y necesidad de una solución soberana

- Reducción progresiva de vigencia en los certificados TLS
- Inviabilidad de la gestión manual para cientos de dominios
- Primera solución ACME: certi + daemon + certideploy
- La migración anticipada: detonante para automatización total

Magnitud de la infraestructura gestionada

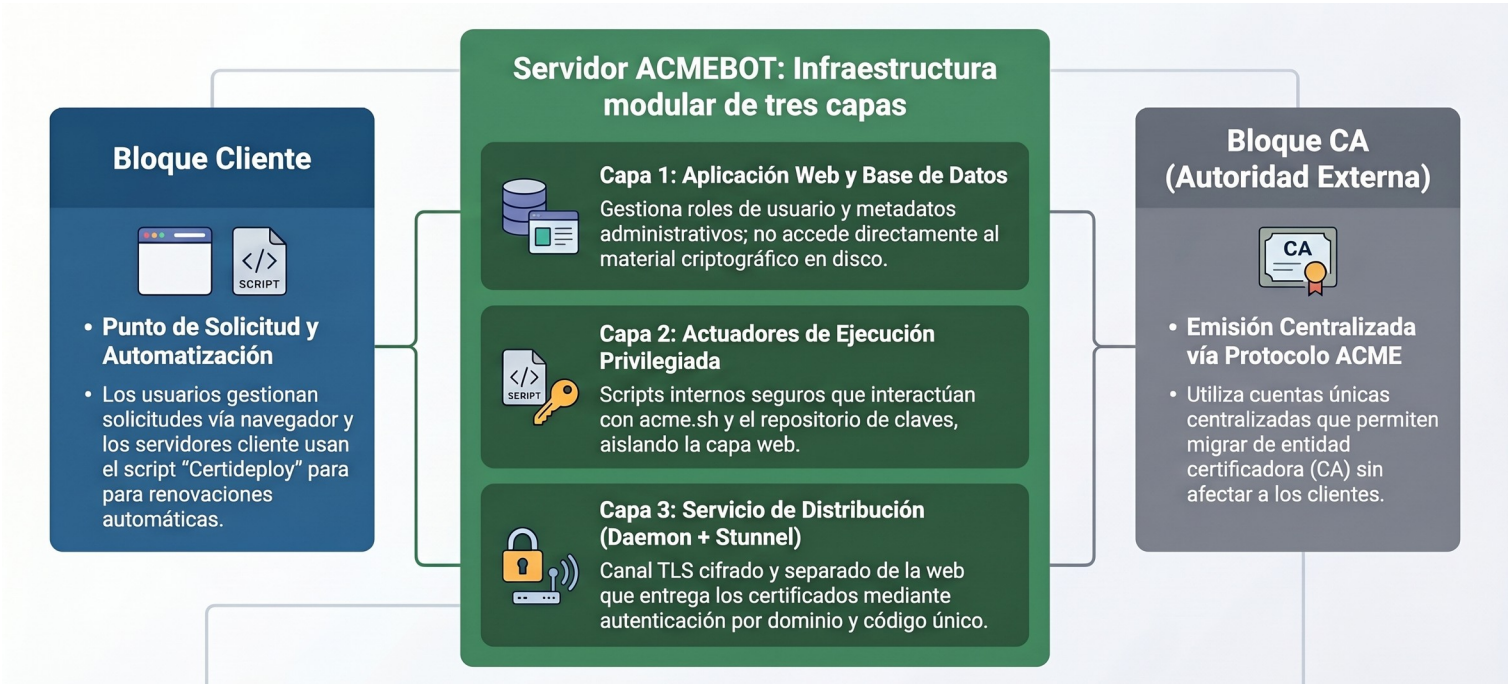
- Gestión centralizada de 354 dominios institucionales
- Servicio prestado a 26 entes universitarios diferentes
- Convivencia de modelos: 176 dominios automatizados y 152 manuales, automatización progresiva

Centralización y Soberanía Tecnológica

- Cuenta ACME únicamente para el servidor ACMEBOT
- Gestión orientada a Dominios: facilita nuevas migraciones
- Independencia de Clientes

Arquitectura

Arquitectura Centralizada



El modelo de despliegue autónomo (certideploy)

- Script modular de ejemplo configurado una sola vez por el administrador del cliente
- Ejecución programada vía cron con lógica de descarga inteligente por fecha
- Independencia de herramientas externas adicionales en el cliente (uso de openssl)

Seguridad por Diseño

Seguridad por diseño

Control de Acceso e Identidad

Restricción de Red y Validación DNS

Acceso limitado por firewall perimetral y validación previa obligatoría contra el DNS institucional.

Vinculación de Personal en Activo

La titularidad de los certificados está estrictamente ligada a personal institucional con vinculación contractual vigente.

Doble Factor de Descarga

Autorización obligatoria por Nombre Canónico del host y código de acceso único por dominio.

Blindaje Arquitectónico y Criptográfico

Canal de Distribución Cifrado (Stunnel)

Distribución autenticada de certificados a través de un canal TLS dedicado e independiente de la web.

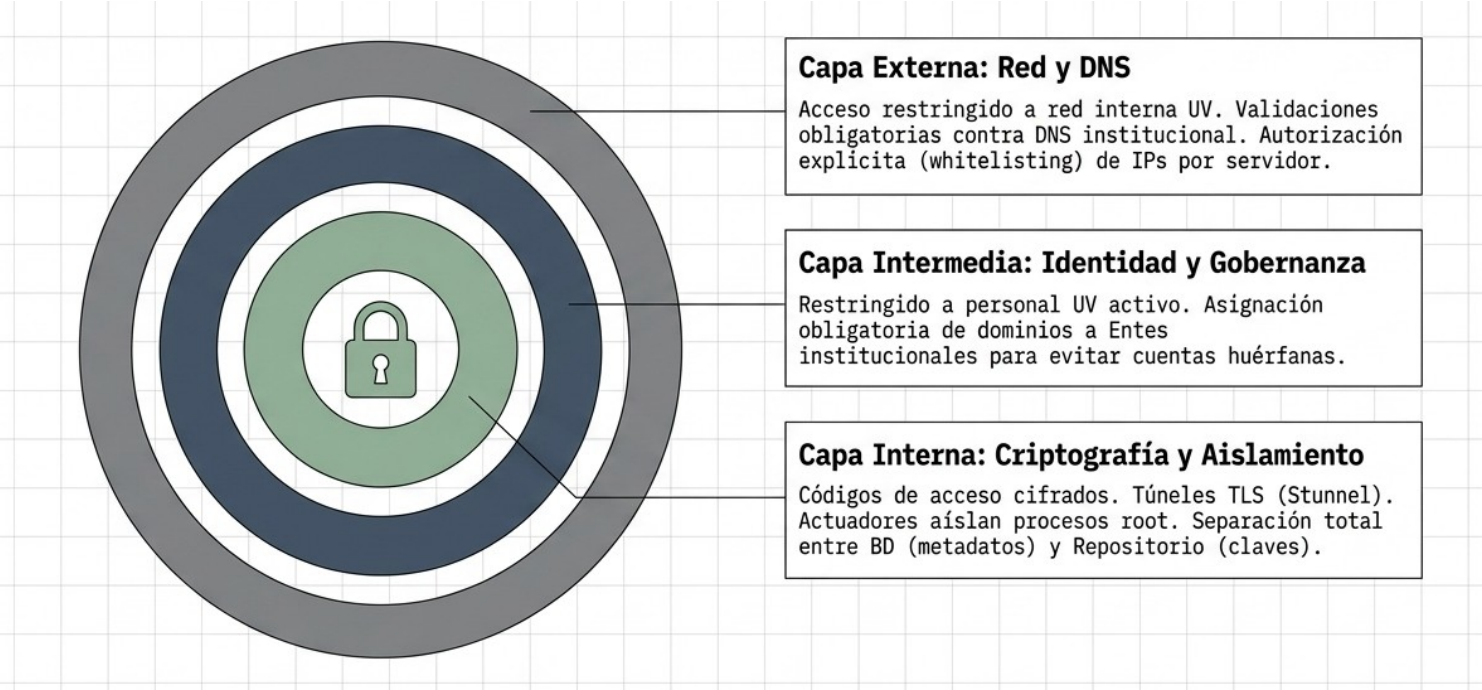
Arquitectura de "Actuadores" Privilegiados

Separación física que impide que la aplicación web acceda directamente al disco o al repositorio.

Higiene Criptográfica Automática

Rotación automática de claves privadas en cada ciclo de renovación del certificado.

Capas de protección y perímetros de seguridad

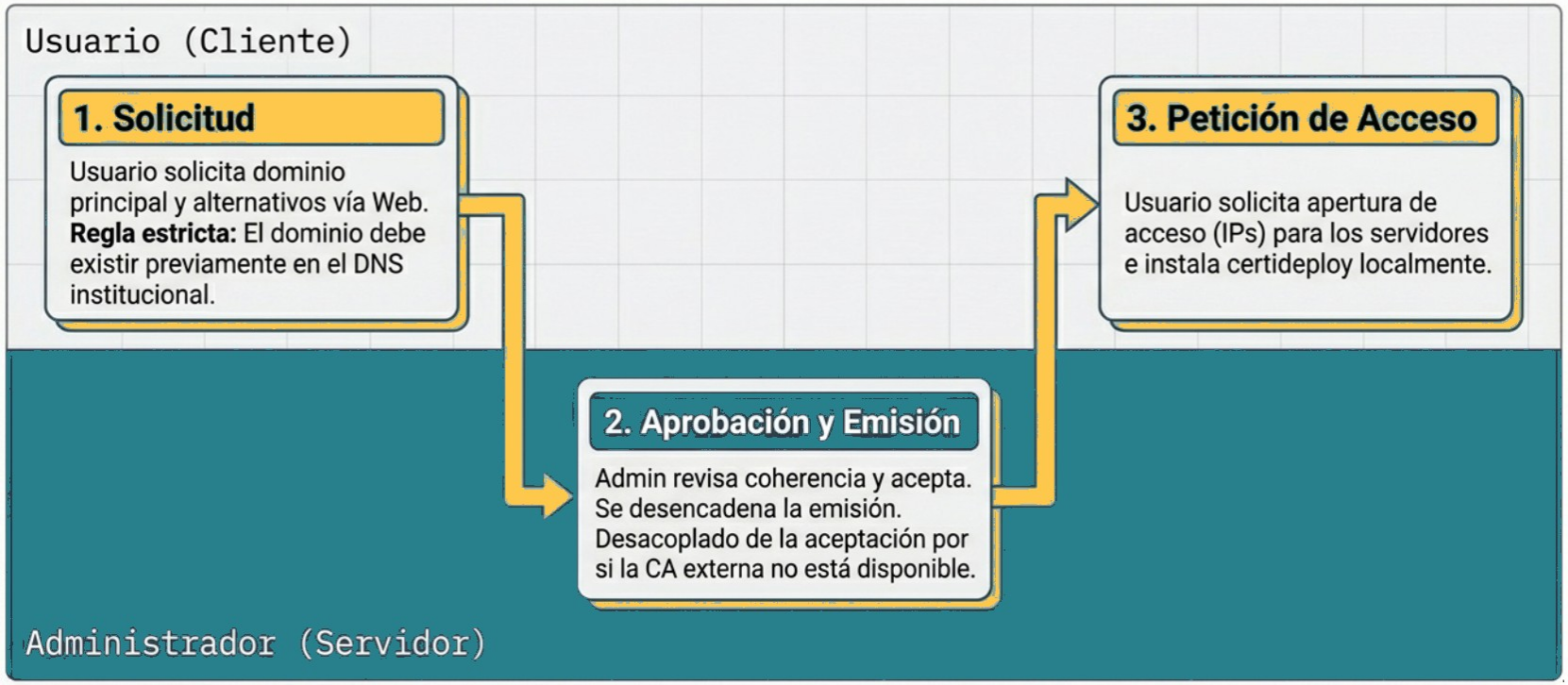


Garantías en la entrega de material criptográfico

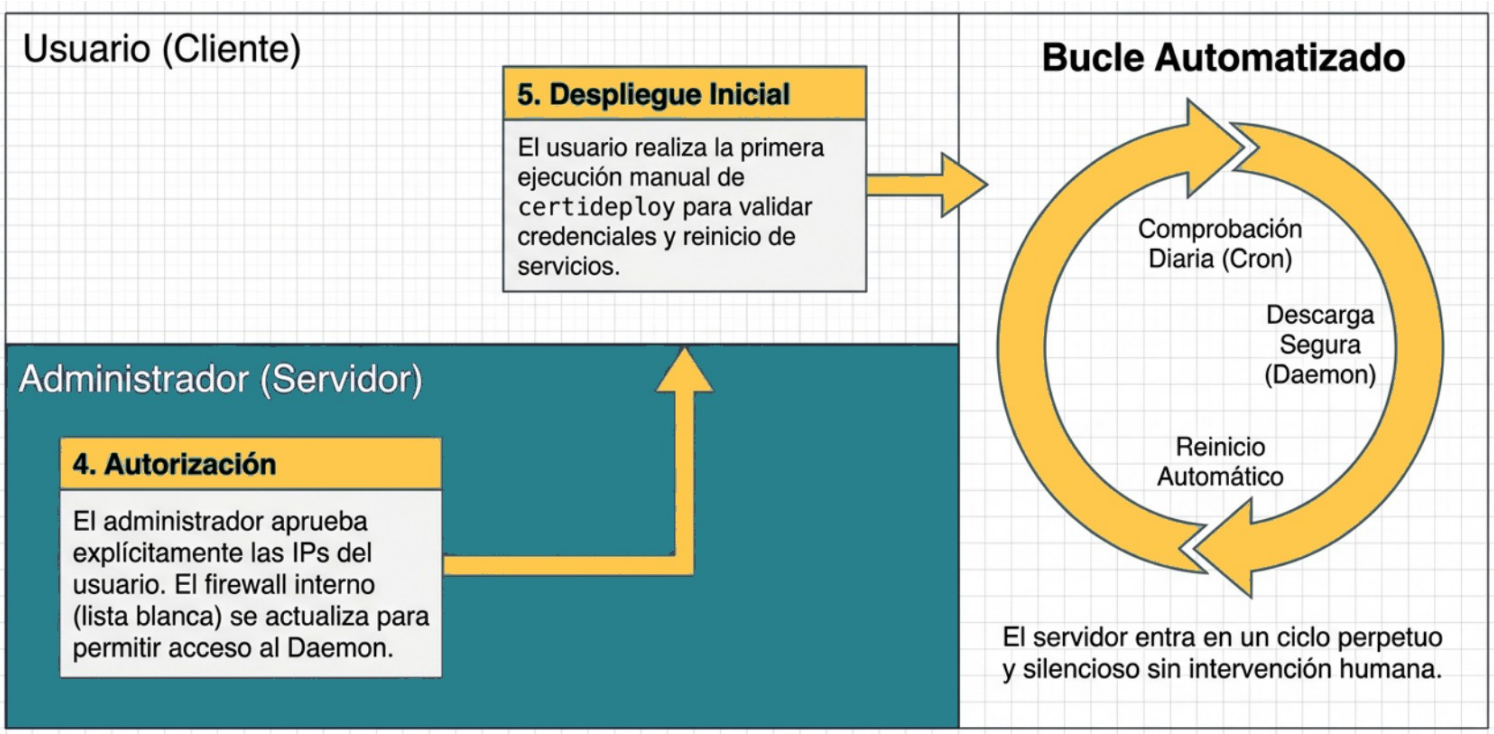
- **Lista blanca de servidores autorizados por nombre canónico (evita riesgos por reutilización de IP)**
- **Doble factor de descarga: Validación de Host + Código de acceso encriptado único por dominio**
- **Uso de túnel TLS dedicado (stunnel) para el transporte seguro**

Ciclo Completo

Procedimiento operativo de gestión



Automatización del Ciclo de Vida

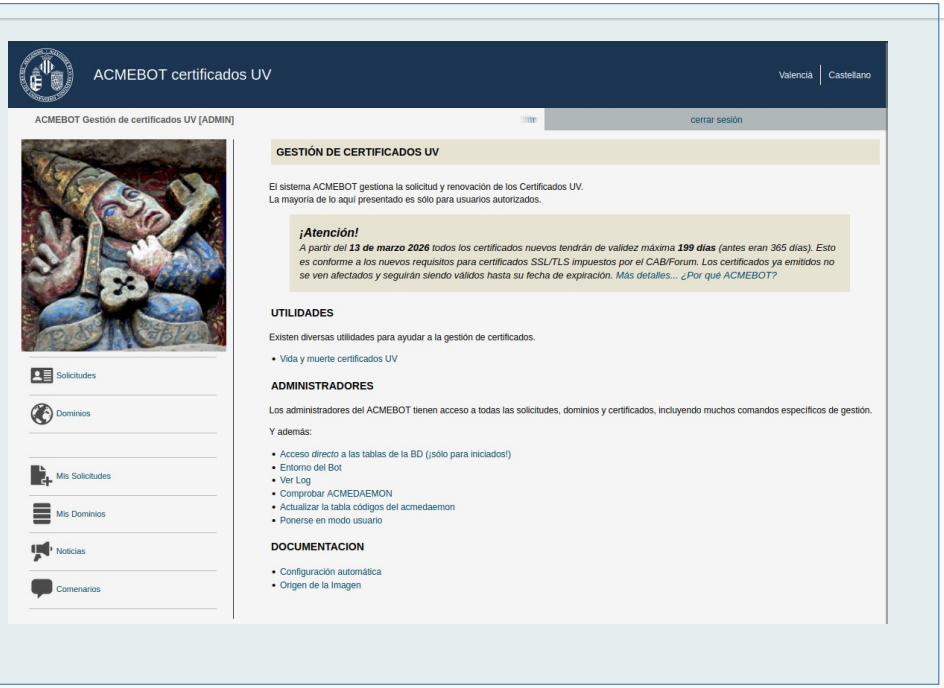


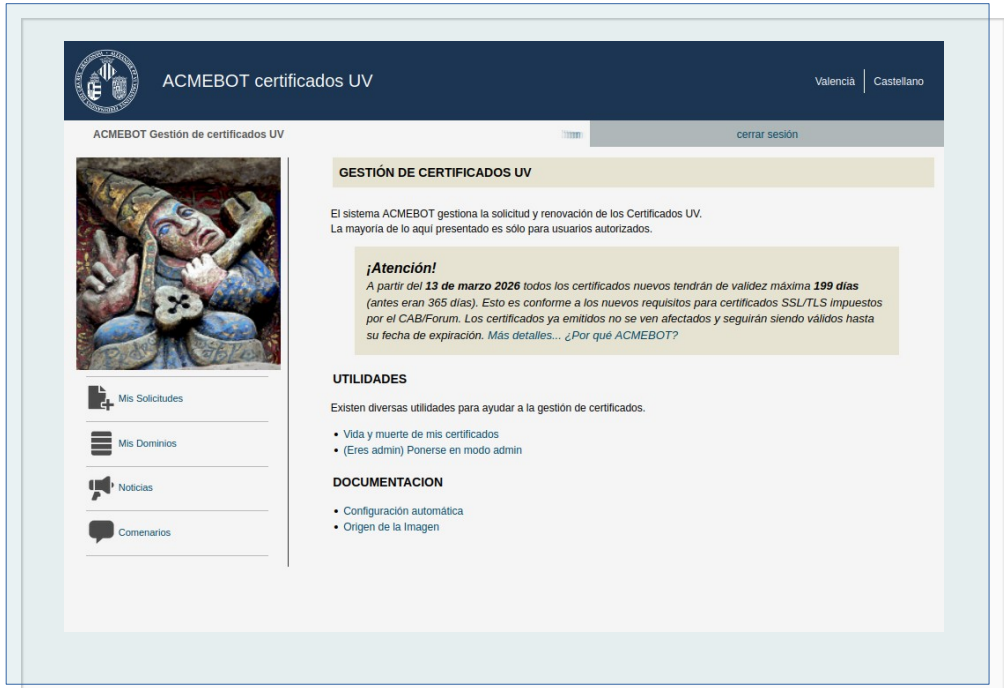
Estado Actual y Roadmap

Balance de situación y evolución del proyecto

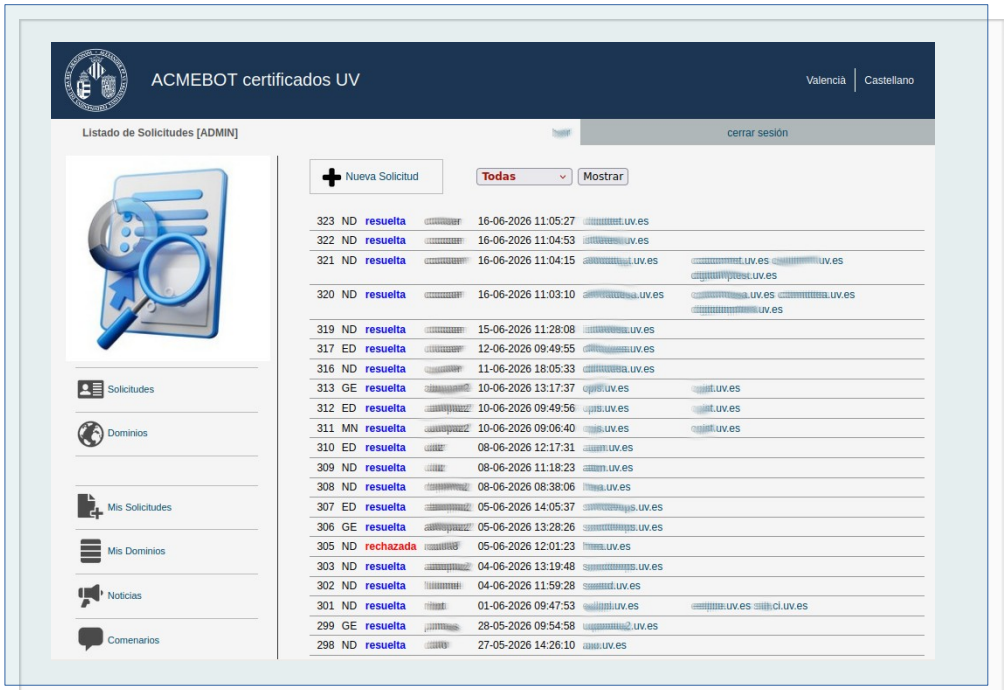
- **Eliminación de caducidades no detectadas y auditoría completa de actividad**
- **Gobierno de toda la infraestructura desde la aplicación**
- **Evolución activa, próximos pasos**
  - **Adaptación para clientes Windows (PowerShell)**
  - **Viabilidad de Proxy ACME local**

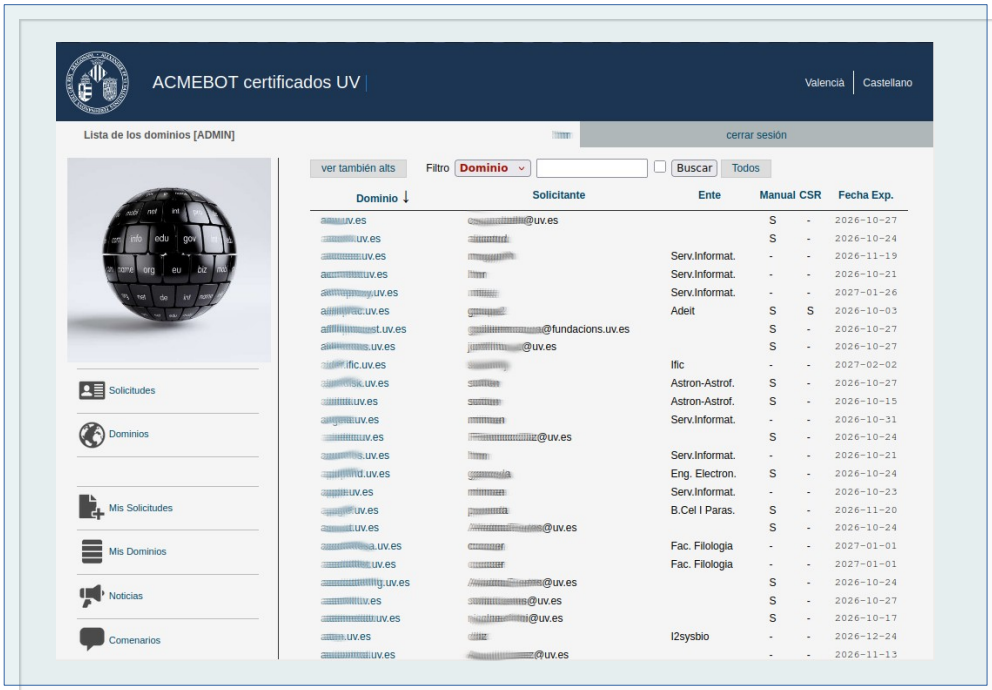
Aplicación ACMEBOT - Inicio



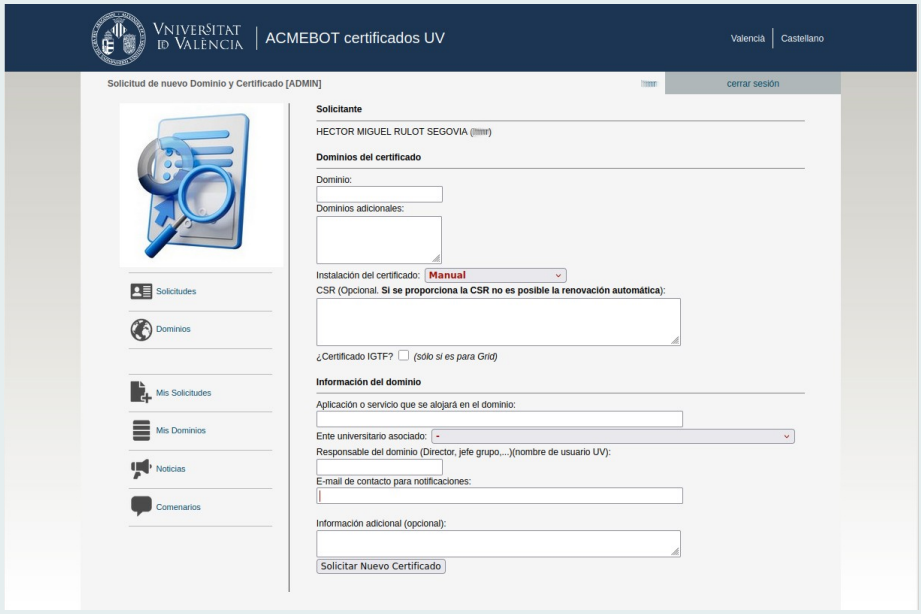


Aplicación ACMEBOT - Admin

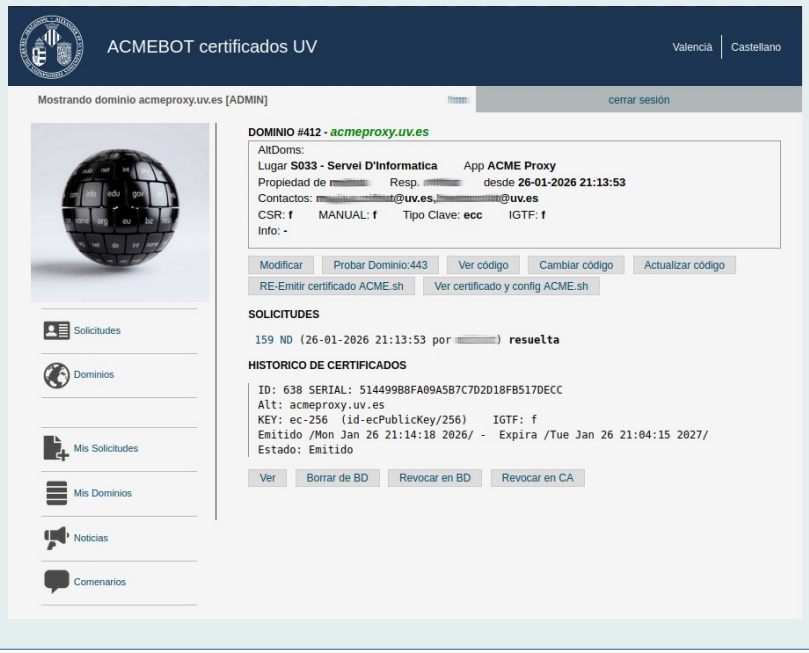


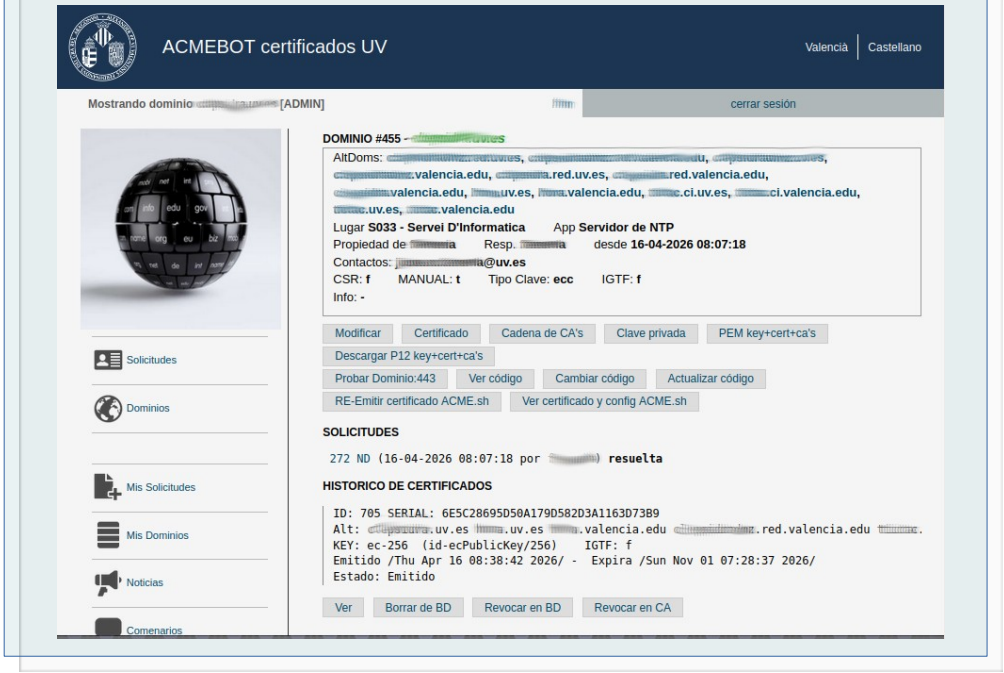


Aplicación ACMEBOT - Solicitud



Aplicación ACMEBOT - Dominio





Conclusiones

¿Qué nos aporta ACMEBOT?

Eficiencia y Gestión Centralizada

Gestión Integral del Ciclo de Vida

Control total automatizado: desde la solicitud inicial y emisión hasta la renovación y baja.

Centralización Estratégica

Uso de cuenta única de CA que simplifica migraciones y la gestión institucional masiva.

Simplicidad Absoluta para el Cliente

Automatización real sin dependencias externas ni necesidad de conocimientos técnicos del protocolo ACME.

Seguridad y Éxito Operativo

Seguridad Robusta por Diseño

Múltiples capas de protección integradas, incluyendo canales cifrados y códigos de acceso únicos.

Éxito Operativo Contrastado

Plataforma estable en evolución activa que gestiona cientos de dominios con éxito rotundo.

Resumen del Alcance y Escala Actual

354	26	122
Dominios gestionados	Entes universitarios	Servidores automatizados

¿Qué podemos aportar?

Si en vuestra institución estáis planteando un reto similar, estamos disponibles para **compartir** nuestra experiencia: **criterios de diseño**, **decisiones** que tomamos por el camino y los **problemas** con los que nos hemos ido encontrando.

No es un camino que haya que recorrer en solitario.

¿Preguntas?

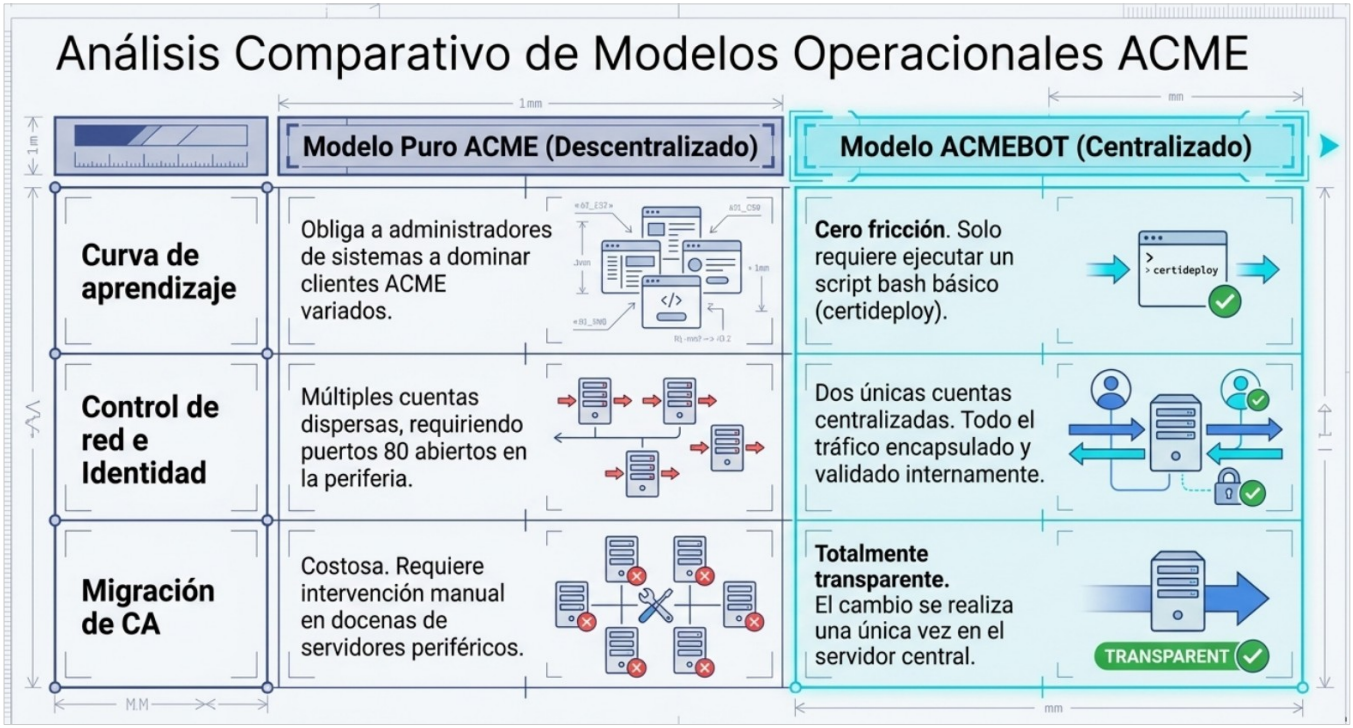
Muchas gracias. ¿Preguntas?

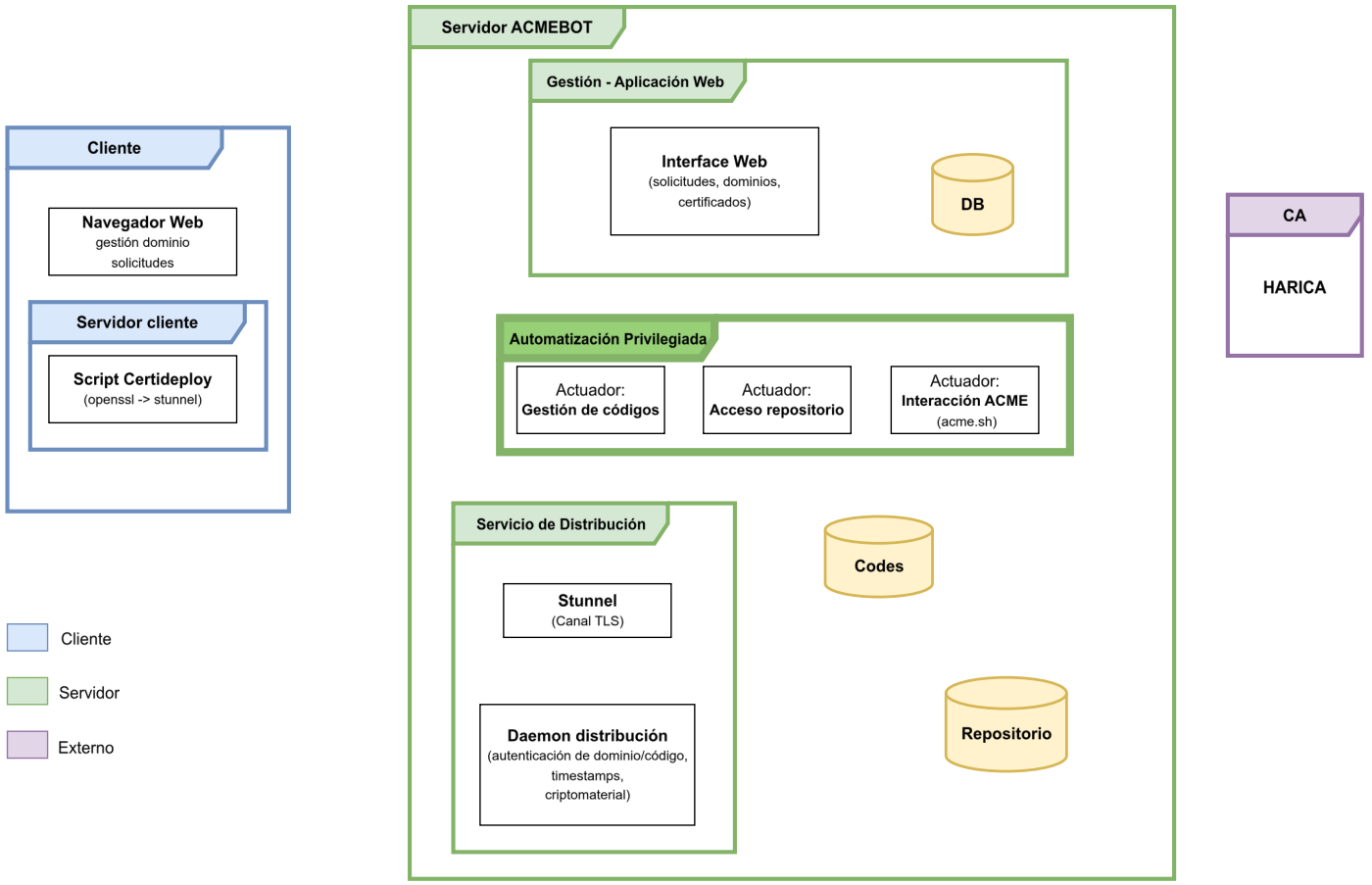
M. Carmen Mifsut Herrera
maria.c.mifsut@uv.es

VNIVERSITAT DE VALÈNCIA

Anexos

Modelo Puro vs Centralizado




Cliente
Navegador Web
gestión dominio
solicitudes
Servidor cliente
Script Certideploy
(openssl -> stunnel)
Servidor ACMEBOT
Gestión - Aplicación Web
Interface Web
(solicitudes, dominios,
certificados)
DB
Automatización Privilegiada
Actuador:
Gestión de códigos
Actuador:
Acceso repositorio
Actuador:
Interacción ACME
(acme.sh)
Servicio de Distribución
Stunnel
(Canal TLS)
Daemon distribución
(autenticación de dominio/código,
timestamps,
criptomaterial)
Codes
Repositorio
CA
HARICA
Cliente
Servidor
Externo