Certificados digitales - Indicadores

- TCS-g4
  - 200 instituciones usuarias
  + 650 RAOs, + 200 DRAOs
- Cerficados válidos actualmente
  + 21.000 certificados válidos
  + 11.000 con un solo dominio
  + 9.000 multidominio
  + 1.000 wildcards (+ 500 *.dominio.tld)
  + 3.500 mediante ACME
- Histórico (desde mayo de 2020)
  - + 60.000 certificados emitidos para + 100.000 FQDNs/identidades certificadas
  - Según las tarifas públicas (https://www.rediris.es/tcs/caracteristicas/tarifas) ahorro “estimado” a las instituciones españolas superior a 20.000.000€

Perfil	Nº Certificados emitidos + CNs adicionales				Precio (€)
	1 año	2 años	3 años	Total	
GÉANT OV SSL	29866	1925	0	31791	5.217.504
GÉANT EV SSL	935	60	0	995	224.511
GÉANT OV Multi-Domain	21715 +39844	692 +2343	0 +0	22407 *+42187*	14.072.968
GÉANT EV Multi-Domain	231 +1227	47 +766	0 +0	278 *+1993*	615.449
GÉANT IGTF Multi Domain	797	0	0	797	0
GÉANT Wildcard SSL	2792	112	0	2904	2.246.194
GÉANT Unified Communications Certificate	164	2	0	166	0
Client Certificate	1815	1851	82	3748	89.366
TOTAL				**63220**	**22.465.992**

Certificados digitales - Futuro

- Google y CA/B Forum
  - Planes de reducción de la validez máxima de certificados TLS de los 398 días actuales a 90 días (Moving Forward, Together) (https://www.chromium.org/Home/chromium-security/root-ca-policy/moving-forward-together/)
  - La validez del certificado de 90 días no parece ser el principal objetivo, pero se utiliza para fomentar la automatización y permitir una sustitución más rápida de los certificados.
- Automatización - ACME
  - ¿Necesidad de formación a las instituciones?
  - RedIRIS se ofrece a hacer un taller sobre ACME
    - ¿Alguna institución ofrece un aula?

The Chromium Projects

Moving Forward, Together

2022

2013

Automatizar o morir

The Chromium Projects

Moving Forward, Together

a maximum “term limit” for root CAs whose certificates are included in the Chrome Root Store. Currently, our proposed term duration is seven (7) years, measured from the initial date of certificate inclusion

Add Spanish FNMT root certificate
26/05/2008 – 25/01/2017

`https://bugzilla.mozilla.org/show_bug.cgi?id=435736`

ACME

¿todo resuelto?

ACME

La CA fallará

¿margen de maniobra?

ACME

La renovación fallará

¿monitorizo correctamente?

unServicio.es

04/05/2021 – 02/08/2021

02/08/2021 – 31/10/2021

20/10/2021 – 18/01/2022

18/01/2022 – 18/04/2022

12/02/2024 – 12/05/2024

15/05/2024 – 13/08/2024

ACME

La clave privada…

¿la gestiono correctamente?

unServicio.es

Clave privada

2021

2022

2023

2024

…

ACME

La instalación…

¿algún dispositivo “difícil”?

ACME

La instalación…

¿algún dispositivo “difícil”?

RPA

automatización robótica de procesos