Actualidad servicio SCS

http://www.rediris.es/scs/

Cáceres, 24 de Noviembrede 2014

Índice

SHA-1 en SCS

- SHA-1 no es un algoritmo de firma seguro
  - https://www.schneier.com/blog/archives/2012/10/when_will_we_se.html

Los principales navegadores dejarán de confiar en certificados firmados con SHA-1 a partir del **1 Enero de 2017**

  - http://blogs.technet.com/b/pki/archive/2013/11/12/sha1-deprecation-policy.aspx
  - http://googleonlinesecurity.blogspot.co.uk/2014/09/gradually-sunsetting-sha-1.html
    - http://googlechromereleases.blogspot.nl/2014/11/stable-channel-update_18.html

SHA-1 en SCS

- Reacción de Comodo CA Limited/SCS
  - Octubre/2014
    - Certificados firmados con SHA-256 disponibles vía portal central de COMODO y sólo bajo petición (mail)
    - Modificación fecha de expiración de los certificados (*Valid until* 2016-12-31 23:59:59)
  - Noviembre/2014
    - Nuevas CAS que firman usando SHA-256
      - Actualización cadenas de certificación
        - http://www.rediris.es/scs/capath2.html
        - http://www.terena.org/activities/tcs/repository/

Cambio de proveedor en SCS

- (Julio 2009-Julio 2015) Proveedor actual de certificados SCS Comodo CA Limited
  - http://www.terena.org/news/fullstory.php?news_id=2405

- Continuidad asegurada del Servicio a partir de Junio 2015
  - Call for Proposals – TERENA Certificate Service (Feb 2014)
    - En breve será anunciado el ganador del concurso
    - Interesantes mejoras ofertadas por el adjudicatario
  - Trabajos por parte de RedIRIS para garantizar una transición sin impacto

¡¡Muchas gracias!!

chelo.malagon@rediris.es
javier.masa@rediris.es

Edificio Bronce,
Plaza Manuel Gómez Moreno s/n
28020 Madrid. España
Tel.: 91 212 76 20 / 25, Fax: 91 212 76 35