# Il nuovo servizio TCS e il protocollo ACME

Barbara Monticini
GARR

WORKSHOP GARR 2020

NET MAKERS

Consortium GARR

Codice menti.com: 82 35 02 9

# Il servizio TCS: un po' di storia

Offerto da GARR **gratuitamente** alla propria comunità dal 2007 (Terena SCS)

**Quarta** edizione (Globalsign, Comodo, Digicert, Sectigo)

A partire da **Maggio 2020** Sectigo Limited subentrata a Digicert

**Adesione**:

- Modulo sul sito web
- Firma del rappresentante legale
- Nomina Admin (RAO)

# Il servizio TCS: quali certificati?

L’offerta di certificati x.509:

- SSL OV/EV e IGTF


- Personali e IGTF (personal e robot)

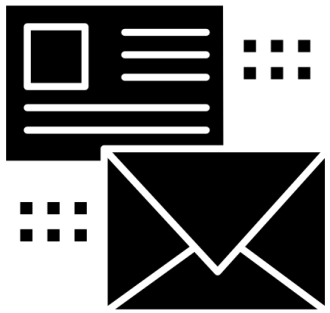

- Code signing


- Document signing (*)

# Il servizio TCS: tutte le novità

**Sito web**

**Wiki TCS**



**Mailing list**
(per RAO e DRAO)

**Adesione**
Firma digitale + trasmissione elettronica

# Il servizio TCS: tutte le novità

La **durata dei certificati ssl** è stata *ulteriormente* ridotta a partire da *Agosto 2020*

**Protocollo ACME** come strumento per l'**automazione** della richiesta / emissione / installazione

# Il servizio TCS: verso il protocollo ACME

- Definizione
  - **Automated Certificate Management Environment**, è uno standard IETF (RFC 8555) per la gestione automatizzata dei certificati X.509
  - Il protocollo ACME è stato implementato per la prima volta da **Let's Encrypt**, la Certification Authority libera e gratuita gestita dal Internet Security Research Group (ISRG).
- Riferimenti
  - **RFC 8555**: https://tools.ietf.org/html/rfc8555
  - Certbot, il client ACME raccomandato: **https://certbot.eff.org**
  - Supporto ACME in Sectigo: vedi il capitolo "Using the Sectigo ACME Service" della guida SCM - Administrator's Guide

# Il servizio TCS: ACME, perché?

- ✓ an **open standard** with a full set of commands and robust error handling, making it easy to adopt both by the enterprise and CAs
- ✓ ongoing enhancements and support by a **community**, not controlled by any one single vendor or organization
- ✓ **low cost**, being free to use

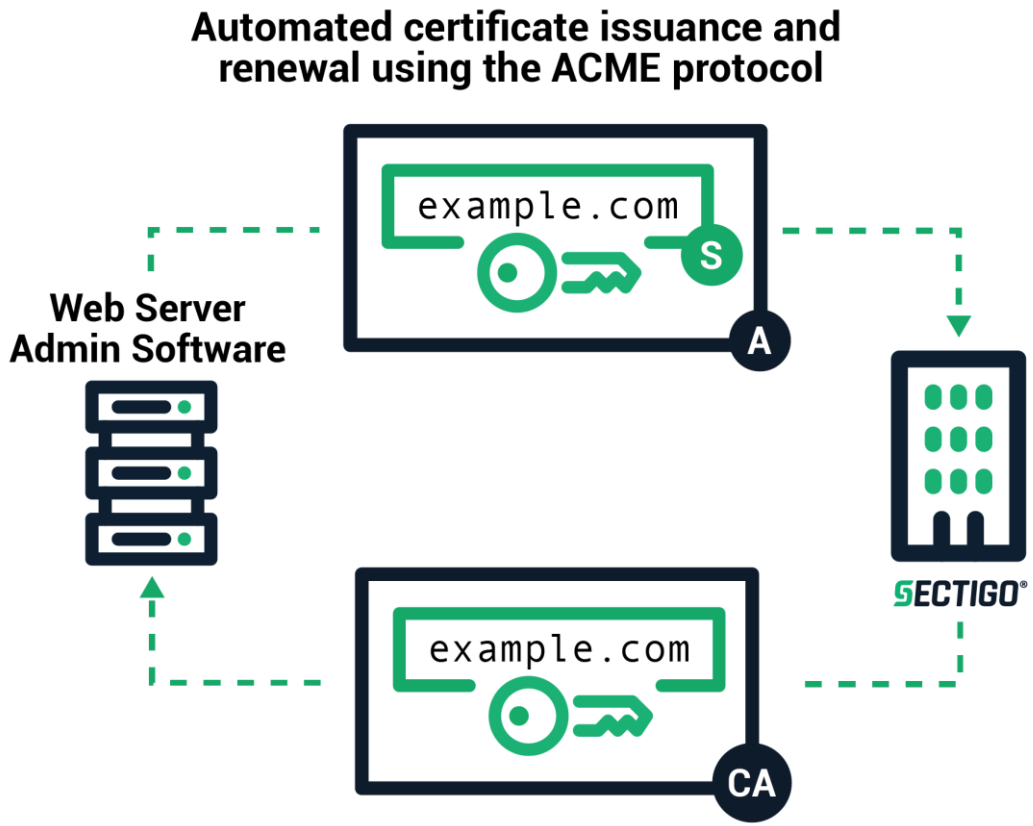
- ✓ https://sectigo.com/resource-library/what-is-acme-protocol

# Il servizio TCS: ACME, how to?

- Con ACME è possibile richiedere OV e EV (*non IGTF* )
- Istruzioni passo-passo nel wiki TCS:
  - **la prima volta**:
    - Installazione di certbot (server)
    - Creazione account ACME (su SCM)
    - Registrazione account ACME via certbot
  - **uso a regime**:
    - richiesta dei certificati (con o senza installazione)
    - rinnovo dei certificati (automatico e manuale)
    - revoca dei certificati
    - Utilizzo su più server

# Il servizio TCS: ACME, come funziona?

1. Il client ACME crea una CSR per richiedere il certificato alla CA per un dato dominio
2. La CSR include una signature fatta con la chiave privata corrispondente alla chiave pubblica parte della stessa CSR
3. ACME client firma l'interna CSR con la chiave dell'account autorizzato così che la CA possa verificarne l'autorizzazione
4. La CA verifica entrambe le firme e se valide emette il certificate basandosi sulla CSR
5. La CA invia il certificato al client ACME



# Il servizio TCS: per saperne di più…

- Codice https://www.menti.com per le domande: **82 35 02 9**

- Sito web: https://servizi.garr.it/cs
- Wiki TCS: https://wiki.idem.garr.it/wiki/GARRCS:GARR-TCS-4
- Sectigo Knowledge Base: https://support.sectigo.com/Com_KnowledgeProductPage?c=Sectigo_Certificate_Manager_SCM
- Contattarci via ticket: garr-ca@garr.it