Account ACME per il rilascio automatico dei certificati server

ACME (nella declinazione UniTS) consente:

1. Richiesta autonoma di nuovi certificati
2. Rinnovo automatizzato dei certificati

La durata dei certificati rilasciati verrà ridotta in futuro fino al massimo di 47 giorni per cui si consiglia vivamente il rinnovo automatico con il sistema ACME.

Servizio in fase di test avanzato

Richiedere uno o più account ACME

E' possibile richiedere uno o più account ACME per il rilascio e rinnovo automatico dei certificati.

- Ad amministratori di sistema o aziende contrattualizzate diverse devono corrispondere account ACME diversi.
- Un singolo amministratore di sistema può richiedere più account ACME qualora desideri dividere amministrativamente più gruppi di server. In tal caso dovrà porre attenzione a fornire una descrizione puntuale della funzione di ogni singolo account e assegnare uno short-name all'atto della creazione dell'account.

Il titolare dell'account ha il dovere di comunicare a sicurezzainformatica@units.it qualsiasi tipo di compromissione dell'account ACME o dei certificati da questo gestiti.

Email per le richieste: **acme@units.it** Dati obbligatori:

- Matricola richiedente
- Brevissima descrizione funzionale dell'account di cui si chiede la creazione e nickname associato

Ti verrà restituito un account composto da:

- Key ID
- HMAC Key
- Server URL

Con i dati qua sopra e con il tuo email registrerai in certbot (dopo averlo installato, vedi più avanti) l'account ACME da usare

```
certbot register --email <EMAIL> --server <Server URL> --eab-kid <Key ID> --
eab-hmac-key <HMAC Key>
```

Con certbot non è possibile registrare due account ACME di Harica sullo stesso client.
E' possibile avere più account ACME registrati sullo stesso client solo a patto che siano di due Certification Autority differenti.
Prima di registrare un nuovo account ACME della stessa CA occorre rimuovere il precedente.

Il risultato sarà la creazione dell'account e della relativa chiave nella directory /etc/letsencrypt/accounts.

Server PUBBLICI

Il client di riferimento per l'uso di Let's Encrypt e del protocollo ACME, adottato anche dalla Certyification Authority corrente è certbot. Scaricalo e installano secondo quanto descritto nella pagina certbot selezionando il tuo server web re sistema operativo.

Avrete bisogno dei seguenti partametri:

- Key ID
- HMAC Key
- Server URL

Key ID e HMAC KEy devono rimanere riservati.

Il comando può configurare automaticamente i server Apache (–apache) e NGINX (–nginx). In tutti gli altri casi e' possibile scaricare solo i certificati (certonly –standalone).

```
certbot run --apache --email <EMAIL> --server <SERVER URL> --domain <FQDN-
certificato> --key-type ecdsa --elliptic-curve secp384r1 --cert-name
<FRIENDLY-NAME>
certbot run --nginx --email <EMAIL> --server <SERVER URL> --domain <FQDN-
certificato> --key-type ecdsa --elliptic-curve secp384r1 --cert-name
<FRIENDLY-NAME>
certbot certonly --standalone --email <EMAIL> --server <SERVER URL> --domain
<FQDN-certificato> --key-type ecdsa --elliptic-curve secp384r1 --cert-name
<FRIENDLY-NAME>
```

```
certbot certonly --standalone --email <EMAIL> --server <SERVER URL> --domain
<FQDN-certificato1>,<FQDN2-certificato>,<FQDN3-certificato> --key-type ecdsa
--elliptic-curve secp384r1 --cert-name <FRIENDLY-NAME>
```

Specificare sempre **-server <SERVER URL>** altrimenti il certificato verrà emesso dalla Certification Authority Let's Encrypt (default di certbot) anziché da quella HARICA per una durata inferiore e con validazione più stretta

Nello specificare piu nomi FQDN assicurarsi che siano registrati a DNS per evitare che la validazione fallisca.

Server PRIVATI (non raggiungibili da Internet)

La procedura per questo genere di server è un po' più complessa e prevede la pubblicazione del nome sul DNS pubblico. E' possibile verificare l'esistenza del nome usando dns pubblici come ad esempio:

- Cloudflare DNS: 1.1.1.1 e 1.0.0.1.
- Google Public DNS: 8.8.8.8 e 8.8.4.4.
- OpenDNS: 208.67.222.222 e 208.67.220.220.

```
Linux:
  host mioserver.zonaprivata.units.it 1.1.1.1
  dig mioserver.zonaprivata.units.it @1.1.1.1

Windows:
  nslookup
    server 1.1.1.1
    mioserver.zonaprivata.units.it
```

- Se il nome non è pubblico, chiederne la pubblicazione a scopo certificato ACME a **acme@units.it**.

Uso del proxy per Linux (pip) e server in rete PRIVATA SENZA NAT

- Installare certbot **come per i server pubblici (vedi sopra)**, ma:
  - Prima di fare sudo `/opt/certbot/bin/pip install certbot certbot-apache`, in */opt/certbot/pip.conf* va aggiunto:

```
[global]
proxy = http://proxy.units.it:8080
```

- Ridare il comando di aggiornamento di pip
- Aggiungere questi due environment per abilitare certbot ad usare il proxy prima di richiedere il certificato

```
echo "export http_proxy=http://proxy.units.it:8080" >>
/opt/certbot/bin/activate
echo "export https_proxy=http://proxy.units.it:8080" >>
/opt/certbot/bin/activate
```

Utilità

Quali account sono registrati in un'istanza di certbot

Scoprire se un'instanza di certbot ha già degli account associati:

```
certbot show_account
```

Verificare i certificati in uso

```
certbot certificates
```

Aggiungere un deploy-hook al rinnovo

E' possibile far eseguire uno script per installazioni custom dei certificati in posizioni specifiche e riavvio conseguente del servizio se necessario.

- Creare il file **/etc/letsencrypt/cli.ini** se non esiste gia
- Aggiungere la riga:

```
deploy-hook = /path/to/custom/certbot_deploy_hook.sh
```

Rinnovo automatico e forzato dei certificati

La semplicità con cui è possibile rinnovare i certificati è molto probabilmente il maggior punto di forza di ACME e certbot.

Il rinnovo avviene con il comando renew e rinnova automaticamente tutti i certificati presenti in /etc/letsencrypt e che stanno per scadere entro 30 giorni:

```
certbot renew
```

Ci sono una serie di opzioni utili per il rinnovo dei certificati che è bene conoscere:

```
    --quiet silenzia il comando, utile per richiamare il rinnovo da cron.
    --force-renewal forza il rinnovo di tutti i certificati
indipendentemente dalla loro data di scadenza.
    --reuse-key rinnova solo il certificato, ma non emette anche una nuova
chiave (default false).
```

Revoca dei certificati

Per revocare i certificati emessi utilizzare il comando revoke(sostituire <SERVER URL> con il corrispondente valore presente nell'account ACME sul CM di Harica):

Nel caso di certificati per più nomi di dominio, basterà specificare uno dei nomi validi. Inoltre tramite

l'opzione –cert-path è possibile utilizzare il percorso del certificato al posto del nome di dominio:

```
certbot revoke --email <EMAIL> --server <SERVER URL> --cert-path
/etc/letsencrypt/live/<FQDN-certificato>/cert.pem
```

Altri client ACME e ulteriori risorse

E' possibile usare altri client ACME come ad esempio acme.sh, lego, win-acme, ma non riusciamo a fornire assistenza su questi.

Guida GARR Certification Service