Automatizzare la gestione dei certificati con ACME

La gestione tradizionale dei certificati SSL

In moltissime aziende, anche in quelle organizzate nel modo più moderno per quanto riguarda altri aspetti dell'IT, la gestione dei certificati SSL si svolge ancora con procedure "vecchio stile", essenzialmente **manuali**. Quando i certificati da gestire sono numerosi, come nel caso delle grandi aziende private e degli enti pubblici di livello nazionale e regionale, la gestione manuale comporta un **forte dispendio di tempo** (e quindi di denaro) ed altri svantaggi, tra cui una **maggiore probabilità di errori** e **l'incapacità di rinnovare i certificati in modo rapido** quando è necessario. In definitiva, la gestione manuale dei certificati SSL comporta spreco di risorse, inefficienza e rischi anche severi di sicurezza, come dimostrano anche recenti studi [1] [2].

Consideriamo infatti che l'installazione di *ciascun* certificato SSL (che sia la prima emissione oppure un rinnovo) richiede normalmente diverse operazioni tra cui:

- accesso al server;
- generazione di una coppia di chiavi;
- generazione della corrispondente CSR;
- invio della CSR alla propria CA, eventualmente attraverso il team aziendale di gestione PKI (ove esistente);
- predisposizione della risposta ai "challenge" della CA per la validazione dei domini (*);
- risposta alla verifica di autenticità richiesta dalla CA (*);
- scarico e installazione del certificato sul server;
- backup della chiave privata e del relativo certificato;
- tracciamento dell'operazione svolta.

(*) Quando l'azienda è abilitata ad operare come "Enterprise RA", questi passi possono essere eseguiti una tantum e in seguito saltati per un certo periodo di tempo (es. 12 mesi).

Alcune di queste operazioni richiedono la corretta esecuzione di comandi relativamente "esotici" ed usati raramente, pertanto devono essere svolte da sistemisti preparati, ed è comunque abbastanza frequente commettere errori. Inoltre, queste operazioni si svolgono in modo diverso secondo il software di web server (es. Apache, Nginx, Microsoft IIS, ecc.) o l'apparato utilizzato (es. firewall, load balancer, ecc.). E per svolgere con la necessaria attenzione queste operazioni **occorrono molte ore-uomo, quando il numero di certificati da gestire è rilevante**. L'onerosità della gestione manuale dipende anche dal fatto che i vari certificati usati in azienda hanno spesso date di scadenza differenti l'uno dall'altro.

Automatizzare il processo con ACME

È chiaro che per superare gli svantaggi della gestione manuale dei certificati bisogna realizzare un'automazione più o meno spinta del processo, in linea peraltro con una gestione dell'IT sempre più improntata alla metodologia "DevOps".

Diverse CA, tra cui Actalis, offrono ai clienti la possibilità di richiedere i certificati attraverso l'invocazione di API proprietarie. Questa possibilità già consente una significativa automazione del processo, seppure con qualche limitazione legata alla specificità del protocollo, ma per una maggiore interoperabilità e facilità di integrazione è più conveniente adottare un'interfaccia "aperta". Sono stati ideati e standardizzati diversi protocolli per automatizzare la gestione dei certificati, ma uno in particolare ha ottenuto negli ultimi anni un grande successo grazie alla sua particolare efficienza nel caso dei certificati SSL e alla disponibilità di numerose implementazioni open source: parliamo del protocollo ACME.

ACME

ACME (Automated Certificate Management Environment) è un protocollo standard, descritto nella specifica pubblica **RFC8555** [3], che consente di richiedere e gestire i certificati SSL in modo molto più rapido e semplice rispetto a come avviene con la tradizionale gestione manuale affidata ad un sistemista. Di fatto, il protocollo ACME consente ai server di ottenere certificati in modo completamente automatico. Non solo: nella maggior parte dei casi è possibile automatizzare anche l'installazione e il rinnovo dei certificati.

Il protocollo ACME funziona tipicamente nel modo seguente (descrizione semplificata):

1. *una tantum*, si installa sul web server un appropriato agente software (un "**client ACME**") e lo si configura nel modo desiderato (specificando, per es., l'URL della CA da usare e altre opzioni);
2. il client ACME si "registra" presso la CA (crea un nuovo "**account**"); in questa fase viene creata una coppia di chiavi che sarà usata per firmare ogni successiva richiesta verso la CA;
3. il client ACME trasmette alla CA un "**ordine**" di certificato, passando l'elenco dei domini da validare e il metodo di validazione preferito;
4. la CA risponde al client ACME con uno o più "**challenge**" (secondo che vi siano uno o più domini da validare) del tipo richiesto;
5. il client ACME **pubblica automaticamente** le risposte ai challenge con il metodo del caso (es. sul server web oppure sul dominio);
6. la CA interroga il web server e/o il dominio per verificare che la risposta ai challenge sia quella attesa;
7. il client ACME **genera** una coppia di **chiavi** per il web server ed una corrispondente **CSR** e trasmette quest'ultima alla CA;
8. la CA **genera il certificato** e lo restituisce al il client ACME, insieme con la catena di certificazione;
9. (tipicamente) il client ACME **installa il certificato** automaticamente sul web server, rendendolo immediatamente operativo;
10. (tipicamente) il client ACME prepara il **rinnovo automatico** del certificato, schedulando un apposito task.

(I dettagli delle varie fasi possono variare secondo il client ACME utilizzato).

Tutte queste operazioni vengono svolte in automatico e in tempo "reale" con la sola eccezione della fase di "setup" (l'installazione del client ACME, la sua configurazione e la prima esecuzione). Anche la schedulazione del client ACME ai fini del rinnovo avviene solitamente in automatico, al termine della prima esecuzione.

Questo elimina quasi tutto il lavoro normalmente necessario per la richiesta e installazione manuale dei certificati SSL, il che può significare un notevole risparmio quando vi sono molti certificati da gestire in azienda.

Che tipi di certificati si possono ottenere?

Attraverso il protocollo ACME è possibile ottenere certificati di ogni tipo: **singolo dominio**, **multi-dominio** ("SAN"), **wildcard**. Le possibilità effettive dipendono dalla particolare CA utilizzata e dal metodo di validazione (ovvero dal tipo di "challenge") che si decide di utilizzare.

Anche per quanto riguarda la classe di certificato (DV, OV, EV) il protocollo ACME in se stesso non pone limitazioni: evidentemente, però, per poter ottenere certificati di classe OV/EV è necessario che la CA possa autenticare la chiamata ACME, così da poterla attribuire ad una specifica organizzazione previamente validata ed autorizzata. I dettagli tecnici relativi alla modalità di autenticazione possono variare secondo la particolare CA utilizzata. La stessa esigenza si applica anche ai certificati di classe DV nel caso di un servizio a pagamento.

Come si usa ACME in pratica

Si deve anzitutto decidere quale client ACME utilizzare. La scelta è ampia: esistono infatti numerosi client ACME, generalmente open source, per ogni ambiente immaginabile. Sono disponibili non solo software client pronti all'uso, ma anche tante librerie che consentono lo sviluppo di un *proprio* client ACME con il linguaggio di programmazione preferito (C/C++, C#, Java, Python, ecc.).

Di solito, in ambiente Linux si raccomanda di usare **Certbot**: è sicuramente il client più potente e più diffuso. Di seguito forniamo un esempio di richiesta di certificato basata su questo client.

Certbot esiste anche per ambiente Windows, ma ad oggi con minori funzionalità della versione Linux. Altre possibili scelte per l'ambiente Windows sono **win-acme**, **AutoACME**, ecc.

Di seguito si mostra come invocare **certbot** per richiedere un certificato SSL per il dominio `example.com` contattando la propria CA all'indirizzo <URL>, supponendo che il web server sia basato su apache:

```
certbot --apache --server <URL> -d example.com
```

Il rinnovo funziona essenzialmente nello stesso modo, semplicemente specificano il comando **renew**, ma senza necessità di fornire nuovamente a **certbot** le informazioni passate per la prima emissione, poiché queste vengono memorizzate:

```
certbot --apache renew
```

Normalmente, però, non c'è bisogno di dare questo comando manualmente, perché dopo l'installazione del primo certificato **certbot** si auto-schedula per il rinnovo, creando automaticamente un "cron job".

Supporto ACME di Actalis

La CA di Actalis supporta il protocollo ACME, per i clienti Enterprise.

Attraverso **l'applicazione web "Enterprise RA"**, i clienti possono in autonomia **creare un end-point ACME configurato secondo le proprie necessità** ed utilizzarlo attraverso il cliente ACME di propria scelta.

In particolare, Actalis supporta:

- chiavi RSA da 2048 a 4096 bit
- chiavi ECDSA P256 e P384
- più URL ACME per ciascun cliente
- challenge di tipo HTTP-01
- challenge di tipo DNS-01

Nota: Non è possibile garantire il supporto di tutti i client ACME esistenti. Actalis svolge test principalmente con i client Certbot e Acme4J.

È disponibile un ambiente di test che consente alle aziende/enti interessate al tema ACME di svolgere delle prove.

Riferimenti

[1] https://info.keyfactor.com/the-impact-of-unsecured-digital-identities-ponemon-report
[2] NIST SPECIAL PUBLICATION 1800-16
[3] https://tools.ietf.org/rfc/rfc8555.txt

Actalis S.p.A.
Via San Clemente 53, Ponte San Pietro 24036 (BG)
VAT Reg. No. 03358520967 | **Tax ID No.** 03358520967
REA [Administrative and Economic Index] 436479 | **Share Capital** € 6,300,000.00 fully paid up |
Certified email: amministrazione@pec.actalis.it | **Website** actalis.it