Rilascio di certificati per SERVER

Trusted Certificate Service (TCS) - Terena - I miei Certificati.

Prima della richiesta

Il servizio permette di ottenere **gratuitamente** certificati per i server pubblici dell'Università.

Alcuni dei possibili usi possono essere:

- Certificati server per servizi istituzionali quali web (HTTPS), email (IMAPS), l'autenticazione di server e di qualsiasi numero di servizi basati su SSL o TLS che richiedono l'uso di certificati.
- Certificati per l'autenticazione di server Wireless, compresi i server che partecipano al progetto eduroam.
- Certificati per l'autenticazione di server IdP e SP, compresi i server che partecipano alla federazione IDEM.

Requisiti della CA:

- Il server su cui viene installato il certificato non deve essere ubicato in uno dei Paesi interdetti.

Requisiti obbligatori:

1. Il fully qualified domain name (FQDN) del server corrispondente al campo X.509 DN (Distinguished Name), deve essere registrato nell'albero del dominio *.units.it (o eventualmente *.univ.trieste.it per supportare vecchi nomi in disuso)
2. Gli altri campi X.509 (diversi da CN e C) non vanno valorizzati altrimenti fallisce la firma.
3. I certificati non vengano utilizzati per la sicurezza delle transazioni di carte di credito, pagamenti online, o transazioni monetarie.
4. La lunghezza minima delle chiavi è di 2048 bit.

Requisiti di massima:

1. Non si rilascia il certificato wildcard *.units.it
2. Nomi alternativi: è possibile richiedere certificati server con nomi multipli.
   Per non impattare negativamente sulla latenza delle connessioni, si consiglia di limitare il numero di nomi alternativi in quanto aumentano la dimensione del certificato scambiato ad ogni nuova connessione.
3. Le richieste devono essere in formato UNICODE.
4. La durata dei certificati rilasciati è attualmente di 1 anno (in realtà di solito sono circa 11 mesi).

L'amministratore di sistema:

1. Si impegna a tenere segreto il materiale crittografico di cifratura.
2. Si impegna a cifrare in maniera forte (la passphrase non basta) qualsiasi eventuale trasmissione della chiave privata, che in ogni caso rimane fortemente sconsigliata.
3. Dà immediata ed esaustiva comunicazione in caso di compromissione anche sospetta del certificato a rete@units.it o al telefono 040 558 3331.

Procedura di firma

1. Generare la CSR (Certificate Signing Request) in formato PEM (testo base64 encoded) seguendo le istruzioni in COMODO CSR Generation instructions.
    1. Procedura per: openssl.
    2. Procedura per: IIS 8 or IIS 8.5 on Windows Server 2012.
2. Inserire la richiesta nella pagina web https://tcscerts.units.it/ nella sezione *“Le mie richieste”*.
3. Attendere **qualche giorno** per il rilascio del certificato.

Una volta ottenuto il certificato

1. Il richiedente si impegna a:
    1. Prevenire la compromissione, la perdita, la diffusione, la modifica o qualsiasi altra azione non consentita sulla chiave privata associata alla chiave pubblica relativa al certificato emesso.
    2. Far pervenire con la massima sollecitudine alla Sezione Infrastrutture Informatiche e Telematiche le richieste di revoca dei certificati sospettati di essere stati compromessi o non più in regola con le politiche del CPS (ad esempio perché il titolare non è più membro dell'Organizzazione).
    3. Far cessare l'utilizzo di certificati scaduti o revocati.
2. A seconda della suite server utilizzata, verificare nella documentazione come deve essere installato il certificato e la CA Chain. Alcuni vogliono due file separati, alcuni un file unico con certificato e CA chain in un ordine preciso, alcuni ancora un solo file pkcs12. Per l'installazione è possibile consultare alcuni suggerimenti su COMODO Certificate Installation instructions.
    -  Nota bene: il certificato della CA intermedia tra il certificato rilasciato e la root CA normalmente non è preinstallato e contrassegnato affidabile dai diversi client (ad esempio browser). Per evitare quindi segnalazioni all'utente da parte del client (ad esempio messaggi di errore “connessione non sicura” da parte del browser), sarà quindi necessario che il server comunichi al client tale certificato intermedio.
        - Link alla CAchain per certificati rilasciati dopo il 5.5.2020.
        - ~~Link alla CAchain per certificati rilasciati dopo il 1.7.2015.~~
        - ~~Link alla CAchain per certificati rilasciati dopo il 8.10.2014.~~
        - ~~Link alla CAchain per certificati rilasciati prima del 8.10.2014.~~
        - Si prega in caso di dubbi/problemi di contattare i gestori del servizio all'indirizzo tcscerts@units.it.
3. È possibile trasformare il certificato PEM encoded in formato P12, che va bene ad esempio per IIS, con openssl:

```
$ cn=cert_name
$ cat $cn.crt GEANT-OV-RSA-CA4.crt > $cn-chain.crt
$ openssl pkcs12 -in $cn-chain.crt -inkey $cn.nokey -export -out $cn.p12
```

1. **Verificare** che l'installazione e il chaining del certificato siano corrette. Se il server è un server web pubblico è possibile usare il tool di Digicert.
2. **Verificare** con SSL Labs che il grado sicurezza ottenuto sia soddisfacente. In caso contrario modificare o aggiornare la configurazione in modo da mantenere il server in sicurezza. Si segnala che nei test di SSL Labs la segnalazione come caratteristica negativa di “Chain issues:Contains anchor” è controversa.

Rinnovi

Il rinnovo del certificato va richiesto **almeno una settimana** prima della scadenza.

Il rinnovo è di fatto una nuova richiesta di firma.

A discrezione dei requisiti dell'utente si può pertanto (dalla procedura più facile alla più complessa):

- Usare la stessa richiesta di firma certificato (CSR) usata per il vecchio certificato (se si è ancora in possesso di questa).
- Generare una nuova richiesta di firma usando la stessa chiave privata del vecchio certificato.
- Generare una nuova chiave privata e una nuova richiesta.

Risorse

- CAchain per certificati rilasciati dopo il 5.5.2020.
- CAchain ~~per certificati UC rilasciati dopo il 1.7.2015.~~
- CAchain ~~per certificati EV rilasciati dopo il 1.7.2015.~~
- CAchain ~~per certificati rilasciati dopo il 8.10.2014.~~
- CAchain ~~per certificati rilasciati prima del 8.10.2014.~~
- Si prega in caso di dubbi/problemi di contattare i gestori del servizio all'indirizzo tcscerts@units.it.

Alcuni suggerimenti per il troubleshooting con openssl.