Linee guida per la produzione di un file di richiesta (CSR) per certificati riconosciuti su Internet

DOCUMENTO PUBBLICO

VERSIONI DEL DOCUMENTO		
Revisione	Descrizione delle modifiche	Emissione
01	Aggiornamento link	18/02/2016
02	Aggiornamento link	18/05/2016

Indice degli argomenti

1 Cosa inserire nel certificato..... 4

1.1 Subject DN.....4

1.2 Fully Qualified Domain Name (FQDN) 4

1.3 Subject Alternative Names (SAN) 4

2 Gestione dei file di richiesta e certificati ricevuti..... 5

2.1 Generazione di un file di richiesta 5

2.2 Lavorazione del certificato ricevuto, produzione del .pfx o .p12 6

IMPORTANTE

È importante usare una nuova chiave privata per ogni richiesta di certificato, il nostro servizio è impostato per funzionare esclusivamente con chiavi non utilizzate in precedenza.

Non possono essere prodotti quindi Certificati da file di request già utilizzati in precedenti richieste. I file di request prodotti con chiavi private usate per precedenti verranno scartati applicativamente.

Vi invitiamo a controllare accuratamente tutte le informazioni che verranno sottoposte alla nostra Certification Authority per evitare di perdere tempo prezioso per entrambe le parti.

1 Cosa inserire nel certificato

Di seguito le indicazioni per l'inserimento dei contenuti. Queste informazioni identificano il certificato e devono essere compilate correttamente per garantire l'emettibilità dello stesso.

1.1 Subject DN

I campi più comuni, indicati di seguito, devono contenere informazioni coerenti all'ambito in cui vengono richieste:

- **CN** (Common Name) - Url da certificare, deve essere FQDN (vedi sotto) e deve essere riconducibile a colui che richiede il certificato.
- **O** (Organization) - Azienda per la quale si richiede il certificato (es. Telecom Italia SpA)
- **OU** (Organization Unit) - Ramo dell'azienda specificata sopra
- **L** (Locality) - Città in cui risiede l'azienda (es. Pomezia)
- **ST** (State or Province) - Sigla provinciale della città (es. RM)
- **C** (Country) - Stato (es. IT)

Attualmente i campi obbligatori, sono CN, O, ST. Gli altri risultano essere facoltativi ma la loro compilazione è fortemente raccomandata.

1.2 Fully Qualified Domain Name (FQDN)

Un **FQDN** (acronimo di ***F**ully **Q**ualified **D**omain **N**ame*) è un nome di dominio non ambiguo che specifica la posizione assoluta di un nodo all'interno della gerarchia dell'albero DNS. Per distinguere un FQDN da un nome di dominio standard si aggiunge il nome dell'host alla stringa del dominio, in modo da renderla assoluta.

***Esempio di applicazione*:**

Per esempio, dato un host con il nome "miopc" e un dominio "miodomino.it", il FQDN è "miopc.miodominio.it.".

1.3 Subject Alternative Names (SAN)

Dal 1 Gennaio 2014 , i certificati emessi tramite la Global CA, devono obbligatoriamente avere almeno un Subject Alternative Name (SAN), che deve corrispondere alla url specificata nel campo CN.

I SAN possono essere più di uno, si possono certificare più domini nello stesso certificato, ma devono anch'essi essere FQDN.

L'utilizzo del Subject Alternative Name (SAN) permette di certificare una o più url all'interno dello stesso certificato. Le direttive internazionali per l'emissione di un certificato contemplano la necessità della presenza di almeno uno o più SAN.

2 Gestione dei file di richiesta e certificati ricevuti

L'obbligo della presenza di uno o più SAN, può creare difficoltà nella produzione di un file di request (csr) laddove lo strumento utilizzato per la gestione dei certificati non permetta di inserire SAN (es. vecchi apparati).

Lo strumento che utilizziamo e che ci permettiamo di suggerire è OpenSSL, software multipiattaforma Opensource.

Per policy interna, TI Trust Technologies non fornisce alcun supporto per la generazione di un file di request, riteniamo tuttavia che possa essere utile condividere con Voi una possibile soluzione per ovviare ai limiti di cui sopra.

Oltre a questa premessa, teniamo a precisare che non forniremo alcun supporto nè nella personalizzazione nè nella gestione di eventuali errori che l'utente incontrerà nell'uso di questa guida, in quanto questi potranno derivare da un'infinità di fattori che non è possibile prevedere (errori di sintassi, configurazioni pdl errate, ecc..)

2.1 Generazione di un file di richiesta

OpenSSL, per generare una richiesta di certificato ha bisogno di un'opportuna sintassi (riga di comando) che richiami un file di configurazione tramite il quale specificare i SAN da includere nella richiesta.

Le opzioni sono molteplici, qui ne verrà specificata una, questa:

C:\OpenSSL-Win32\bin\openssl req -new -newkey rsa:2048 -batch -keyout c:\chiave_privata.key -nodes -subj "/CN=Prova/O=Prova/OU=Prova/L=Pomezia/ST=RM/C=IT/" –out c:\request.csr -config c:\openssl.cfg

File esterno di configurazione

Il file openss.cfg citato a fine riga di comando è un file esterno (disponibile a questo link), che andrà personalizzato in corrispondenza della "riga 225", nella sezione in cui vengono definiti i Subject Alternative Names.

Qui sotto è riportato un esempio di sintassi per il file di configurazione:

```
[alt_names]

DNS.1= server1.yourdomain.tld
DNS.2= mail.yourdomain.tld
DNS.3= www.yourdomain.tld
```

(eliminate le voci DNS incrementali che non usate, eliminate soprattutto le voci di esempio che trovate all'apertura del file.. se le lasciate il file sarà inquinato, quindi inutilizzabile).

La riga di comando produrrà due file: chiave_privata.key ; request.csr

Il file request.csr servirà alla CA per produrre il certificato e potrà esserci inviato tramite le seguenti modalità:

- **il personale interno** potrà caricarlo sul portale intranet https://ca.telecomitalia.it
- **il cliente** potrà inviarlo alla casella di servizio delivery-ca@telecomitalia.it,

Il file chiave_privata.key andrà conservato, servirà al server per verificare la proprietà del certificato da importare sul proprio server.

2.2 Lavorazione del certificato ricevuto, produzione del .pfx o .p12

Una volta ricevuto il certificato dalla CA, potrà essere necessario utilizzare nuovamente OpenSSL per produrre un file p12, da importare sul server.

Per produrre un file p12, saranno necessari:

- Il file **chiave_privata.key** , prodotto col precedente comando di generazione richiesta.
- Il file **certificato_ricevuto.cer** , ricevuto dalla CA, tramite la mail di delivery.
- Il file **"Root_TTGlobal_base64.cer",** che corrisponde alla versione base64 del certificato di Root, della Global CA, allegato nella mail di delivery.

La sintassi da usare in OpenSSL è la seguente:

C:\OpenSSL-Win32\bin\openssl pkcs12 -export -inkey d:\chiave_privata.key -in d:\certificato_rivecuto.cer -certfile d:\Root_TTGlobal_base64.cer -out d:\certificato.p12

Verrà chiesto di impostare una password di sicurezza, che servirà per installare il file p12 prodotto.