v3 Alternate Names

È possibile richiedere certificati con più CN (per più nomi FQDN).

Ad esempio, se un server web risponde ai seguenti nomi:

pippo.units.it

gino.units.it

web.pippo.units.it

è possibile usare un singolo certificato per tutti e 3 i nomi.

Per quanto riguarda i domini, l'Università di Trieste ha attualmente in uso i seguenti domini (con indicazione dell'uso): units.it (consigliato) univ.trieste.it (sconsigliato) univ.ts.it (DEPRECATO)

Si consiglia pertanto di far puntare i vostri siti web e soprattutto quelli in https SOLO con link all'indirizzo canonico <server>.units.it .

In alcuni casi (vedi vecchi indirizzi di posta elettronica) è necessario mantenere la retrocompatibilità con la forma univ.trieste.it .

 Nota di compatibilità per **Apache 2 web server**: Il virtualhost di default deve avere la terzina SSLCertificateFile SSLCertificateKeyFile SSLCertificateChainFile configurata e funzionante per evitare problemi di compatibilità con sistemi che non supportano lo SNI (vedi sotto) o che non abbiano i certificati delle CA intermedie.

Note sulla compatibilità

Most mobile devices support Subject Alternative Names, and most support Wildcard certificates, but all of them support exact Common Name matching.

 Internet Explorer, Firefox, Opera, Safari, and Netscape have all supported Subject Alternative Names since 2003. Internet Explorer has actually supported them since Windows 98.

 Windows Mobile 6 supports Subject Alternative Names and wildcard matching.

 Newer smart phones running Symbian OS Symbian OS supports Subject Alternate Names from version 9.2 and later.

Windows Mobile 5 supports Subject Alternative Names, but it does not support wildcard matching (*.example.com). However, DigiCert wildcard certificates allow you to include SANs in your certificate as a workaround.

Newer Palm Treo devices use WM5, but the older ones run PalmOS and use VersaMail for ActiveSync. The older Treos do not support SAN name matching.

Older smart phones running Symbian OS (Symbian OS 9.1 and earlier) do not support Subject Alternative Name matching. This seems to be resolved in Symbian OS 9.2 (S60 3rd Edition, Feature Pack 1).

Older Palm Treo devices run PalmOS and use VersaMail for ActiveSync. These older Treos do not support SAN name matching.

Because not all mobile devices support the Subject Alternative Name field, it's safest to set your common name to the name that most mobile devices will be using.

TLS Server Name Indication (SNI)

Un indirizzo IP, più certificati

Quando si intende installare più di un server virtuale che risponda sulla porta 443 SSL, è necessario valutarne la compatibilità sia lato client che lato server.

A tal proposito si invita caldamente alla lettura dell'articolo:

http://en.wikipedia.org/wiki/Server_Name_Indication#Support

Aggiunta di nomi a un certificato

Non è possibile aggiungere nomi (AltNames) ad un certificato già emesso.

Bisogna alternativamente:

- crearne uno nuovo con i nomi vecchi e i nuovi
- creare un nuovo VirtualHost (istanza) del server web che utilizzi un nuovo certificato solo per le richieste al proprio nome a dominio. Ciò si ottiene sfruttando di Server Name Indication (solo per server web).
  In questo caso si può usare il nome FQDN come CN del certificato e ripeterlo insieme al nome che si vuole aggiungere nei subjectAltName (oppure valorizzare solo il CN con il nome che si vuole aggiungere).

Non è necessario revocare un certificato dismesso (è necessario invece in caso di compromissione

della chiave privata e consigliato in caso di esternalizzazione del servizio).

Come sicurezza aggiunta, è possibile cambiare la chiave privata per la nuova richiesta di certificato e, una volta sostituito il nuovo certificato a quello vecchio, **distruggerne la chiave privata** corrispondente al vecchio.

Su macchine che fanno da hosting per molti siti web si può anche adottare la politica di usare certificati di validità di **1 anno per i nuovi nomi** e, quando scade quello principale della durata di 3 anni, includere nel nuovo certificato tutti i nomi aggiunti nel frattempo.

Una via alternativa prevede l'utilizzo di **un certificato per ogni VirtualHost** (chiamato anche virtual server o sito web).

Un certificato che contiene tantissimi nomi rallenta la comunicazione con il server in quanto passa più dati in ogni handshake del protocollo TLS.