Come creare un certificato SSL per IIS utilizzando la CA Privata di Windows 2003 Server

Di Massimiliano Brolli, Roma 24/10/2004

SSL permette di eseguire una connessione criptata tra un Server WEB ed un client utilizzando le porte 443 e 80.

Generalmente per siti internet si tende ad acquistare un certificato dagli enti di certificazione Standard quali **VeriSign, SecureNet, CA** ecc.. già conosciuti dai sistemi operativi Microsoft Unix OS ed altri che ci evitano il compito di far conoscere (Come vedremo in seguito) al sistema operativo client l'ente certificatore.

In altri casi, per applicazioni più limitate o per intranet aziendali è possibile generare certificati SSL in casa tramite l'ausilio di tool di certificazione come viene mostrato in questo Tutorial adottando come ente certificatore l'Authority integrata di Windows 2003 Server.

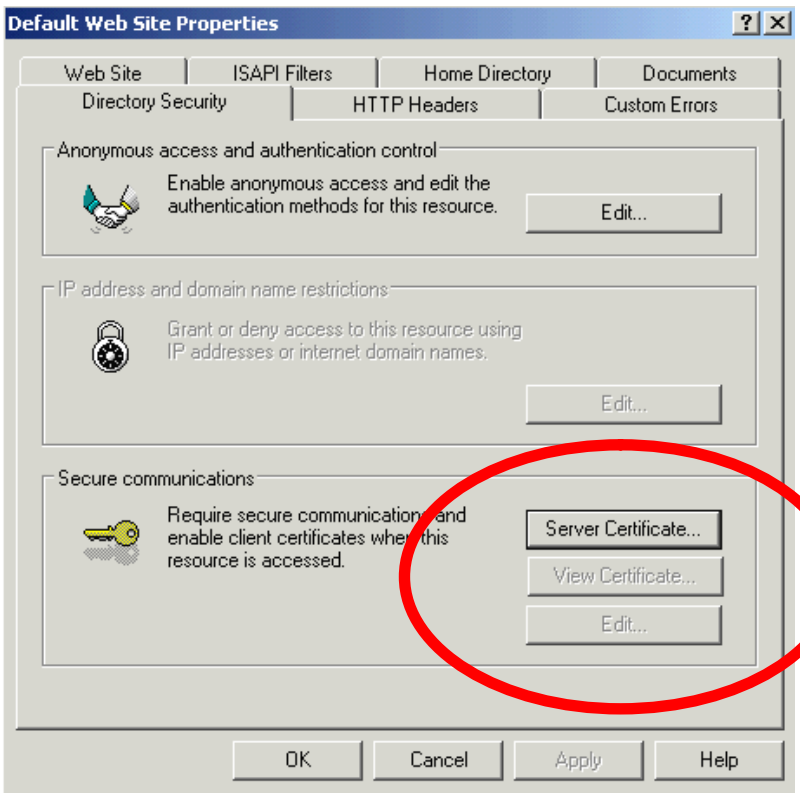
Un'altra ottima alternativa seppur limitata per la generazione di certificati SSL è **OpenSSL** derivante dal Mondo OpenSource.

I certificati che entrano in gioco in questo tutorial sono di due tipi:

1. **Certificato dell'Authority**
2. **Certificato del Server**

Creiamo una richiesta per un certificato SSL

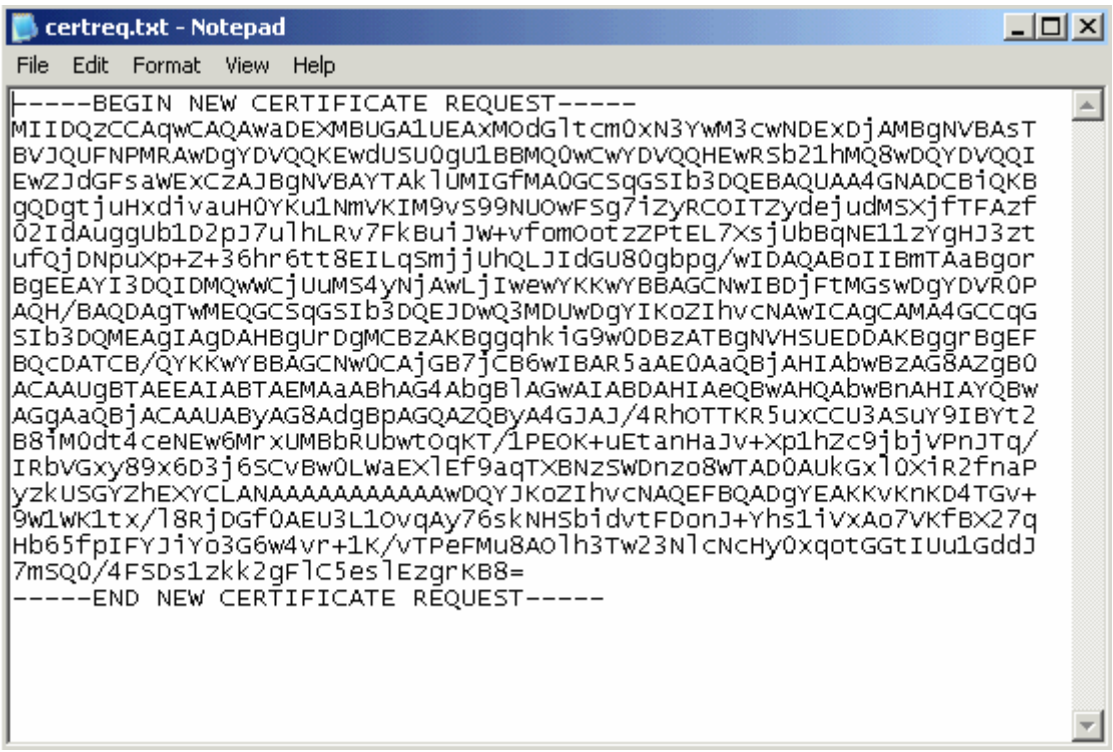
Per chiedere un certificato di tipo Server per SSL ad un ente certificatore occorre preparare una richiesta contenente i dati che dovranno essere certificati.



Ciccando su ***Server Certificate*** verrà creata la richiesta per l'invio ad una CA Pubblica. Questa richiesta sarà un file TXT in encoding BASE64 contenente i dati da inviare all'ente certificatore come viene mostrato nell'immagine successiva.

Attenzione a specificare esattamente tutto il nome del dominio ad esempio www.agensportregionelazio.it altrimenti verrà mostrato un allarme in fase di accesso SSL corrisponde ad una errata imputazione del nome a dominio.
Il nome del dominio deve essere inserito comprensivo di suffisso **www** e **.it**

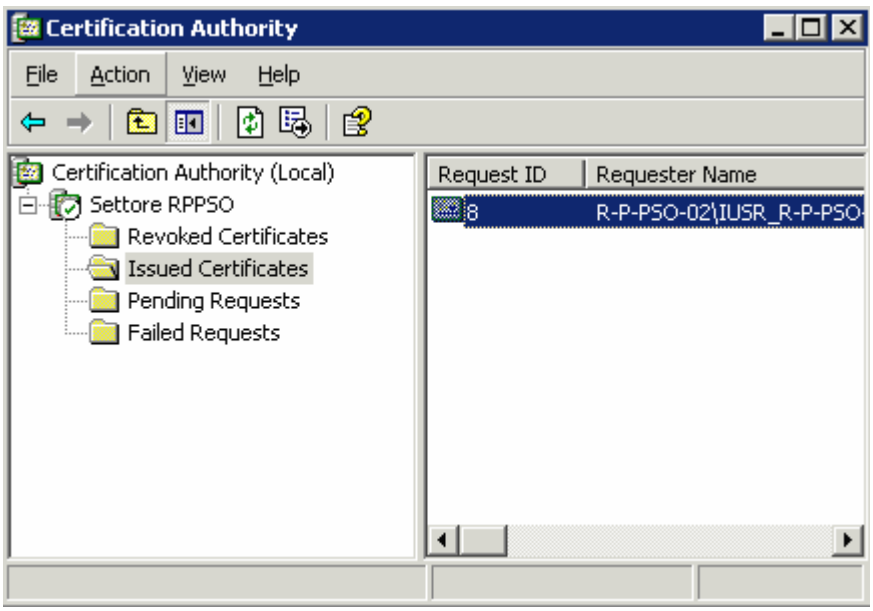
Aprendo il file generato troveremo un insieme di caratteri contenenti la richiesta da inviare all'ente certificatore.



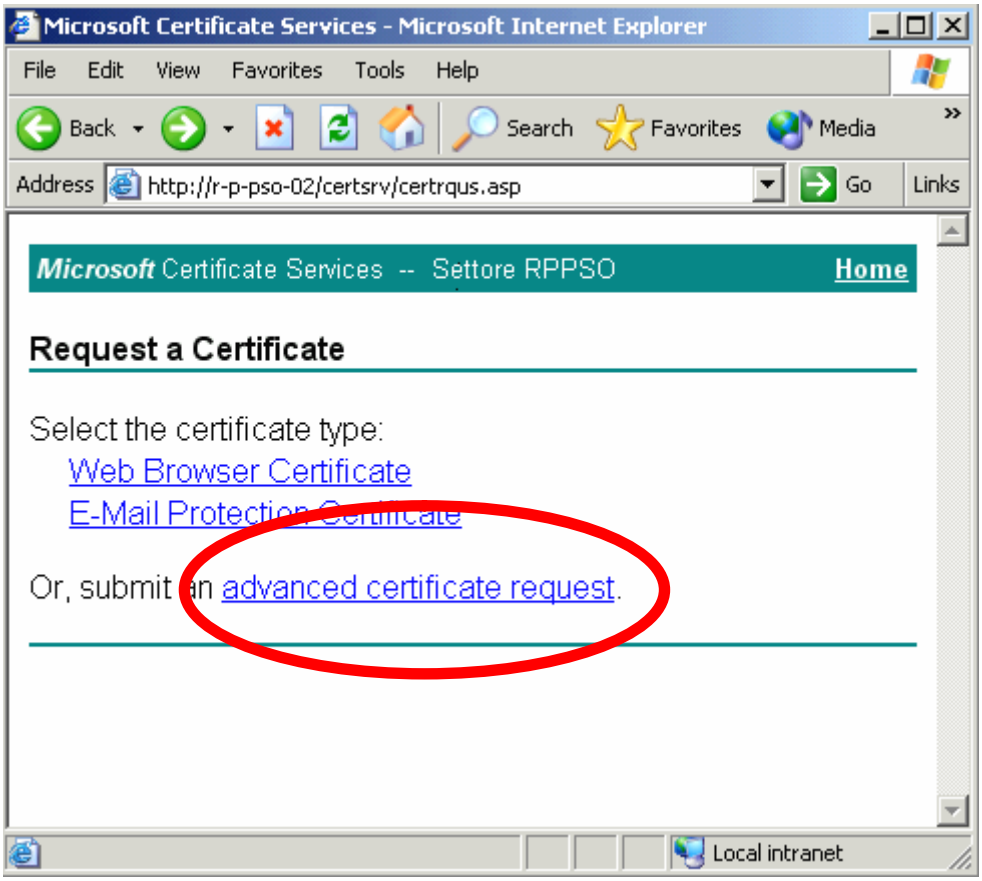
Se non presente installiamo dal pannello di controllo l'ente certificatore presente nei componenti aggiuntivi di Windows. Il Wizard ci chiederà di inserire un nome della CA e un percorso di una directory condivisa che conterrà l'applicazione ASP **CertSrv** che ci permetterà di creare certificati tramite un'interfaccia Web.

Nel caso in cui tale applicazione non venga creata sarò possibile aggiungere ad IIS una directory virtuale di nome **certsrv** e mapparla nella directory
c:\ windows\ system32\ certsrv

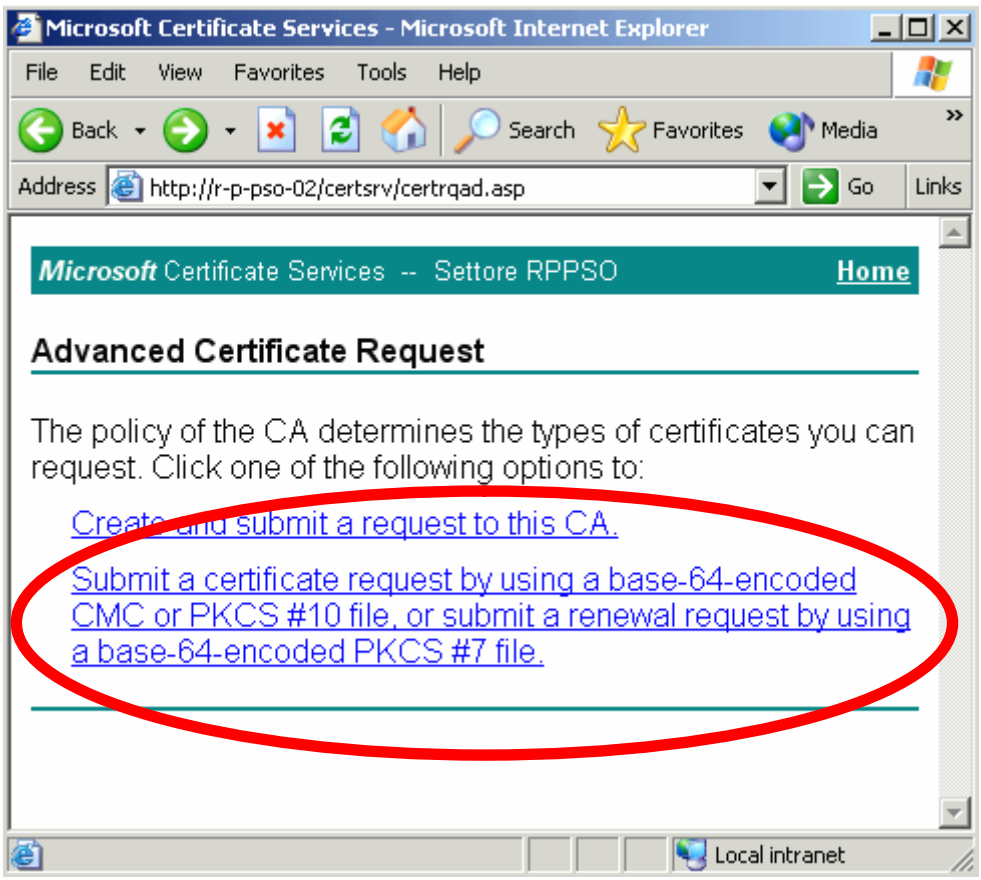
Di seguito viene mostrata una schermata dell'applicativo **Certification Authority** presente in Administration Tools che ci permetterà di rilasciare e di revocare i certificati.



Accedendo tramite Internet Explorer a **http://127.0.0.1/Certsrv** verrà mostrata la Home Page del tool Web per la richiesta dei certificati.

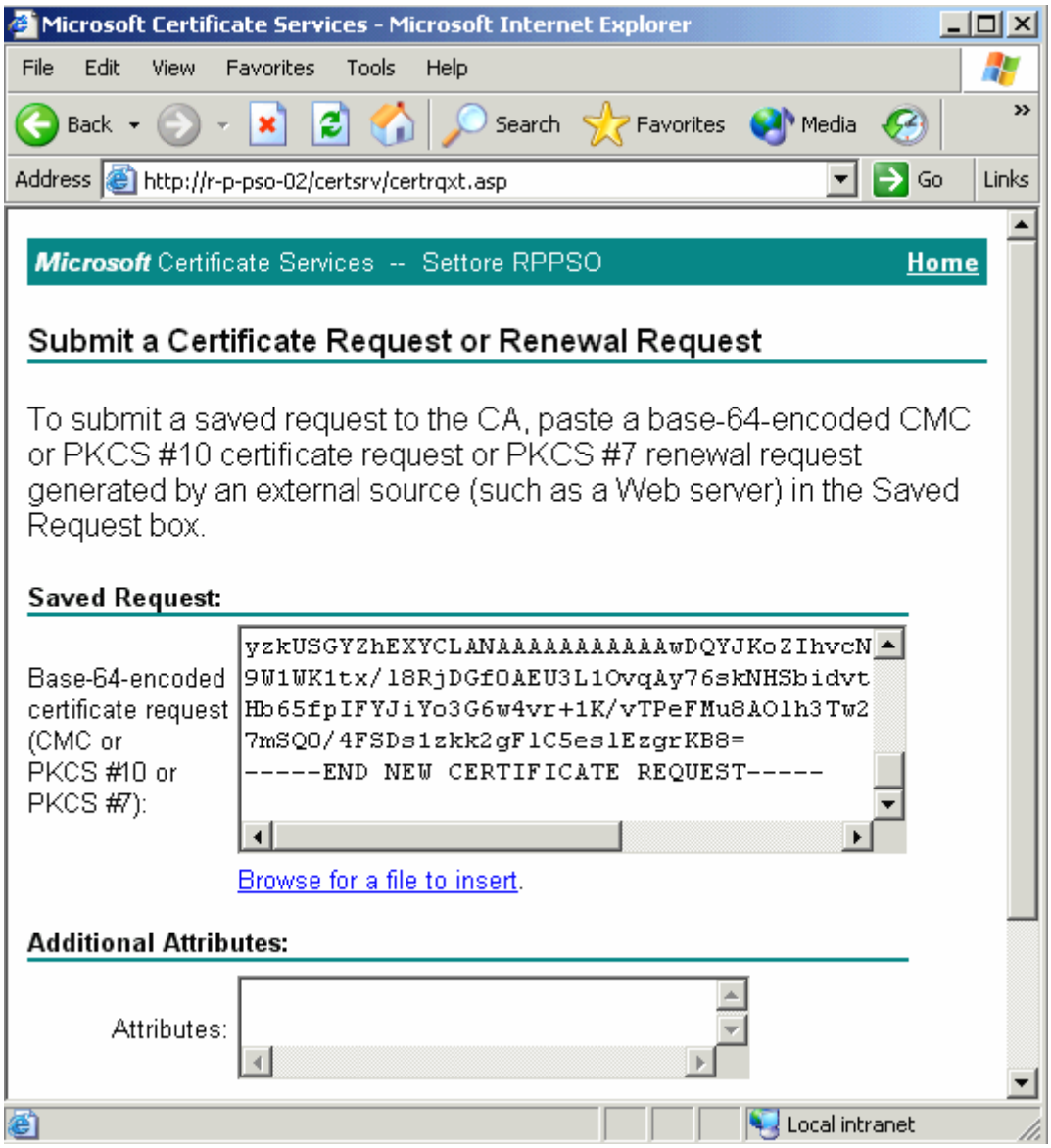


Per richiedere un certificato occorre selezionare Il link sotto riportato.

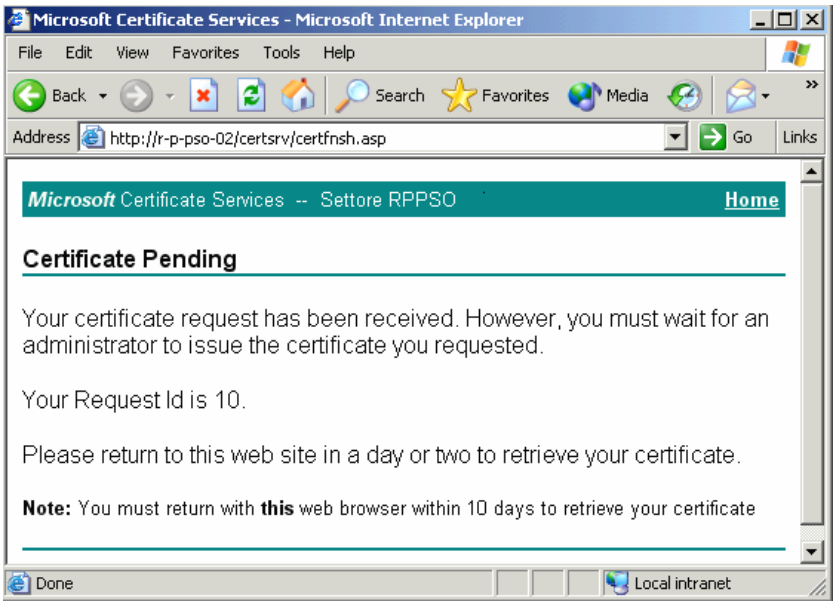


Create and submit a request to this CA. server per creare un nuovo certificate da zero.
Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file. Serve per creare un certificato inserendo la stringa BASE64.

Clicchiamo su questo link per procedere nella richiesta del certificato.

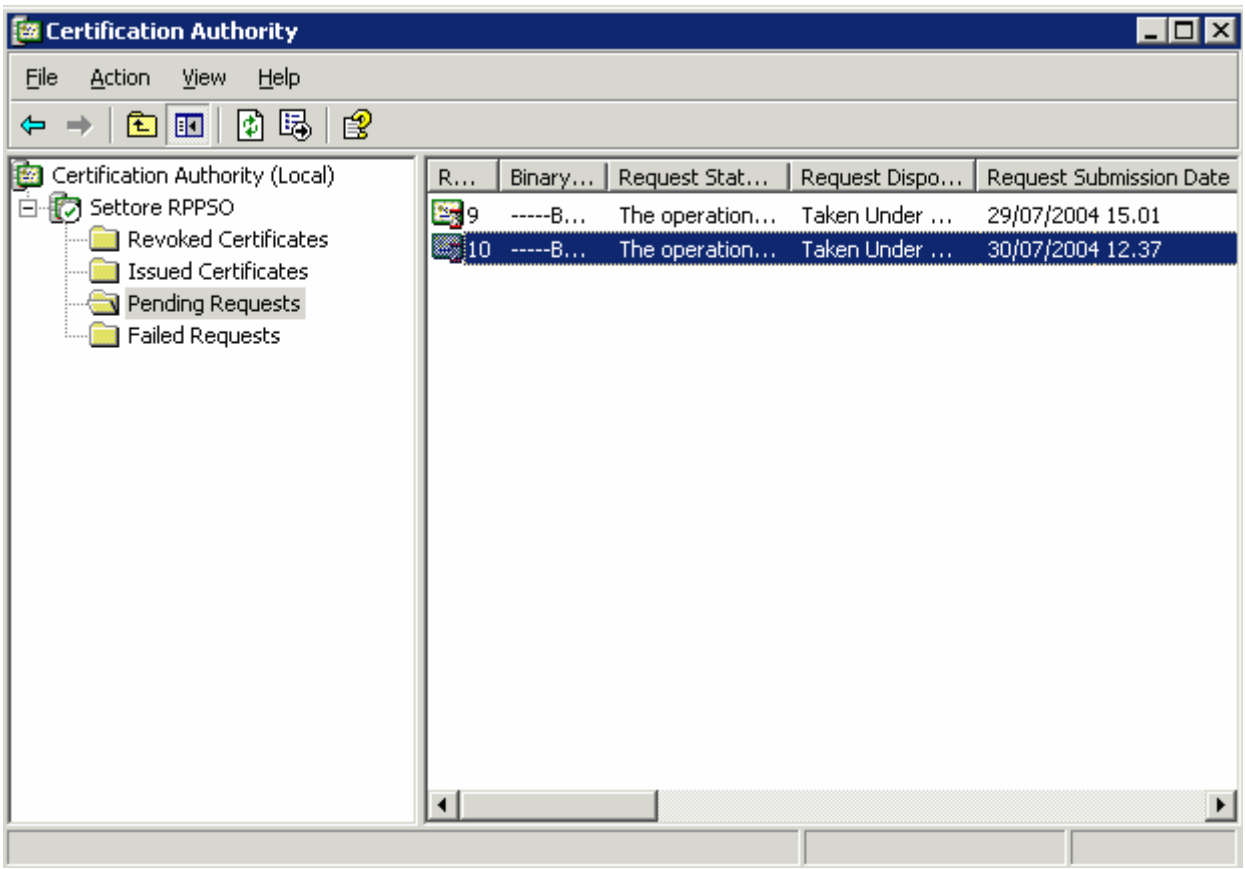


In questo selezioniamo tutto il contenuto presente nel file contenente la richiesta del certificato e incolliamolo nel box BASE64.
Occorre inserire tutto anche **-----BEGIN NEW CERTIFICATE REQUEST-----** e **-----END NEW CERTIFICATE REQUEST-----**.
Ciccare su invio



A questo punto la CA installata su Windows 2000/2003 Server dovrà rilasciare il certificato che sarà scaricabile dal tool Web **Certsrv**.

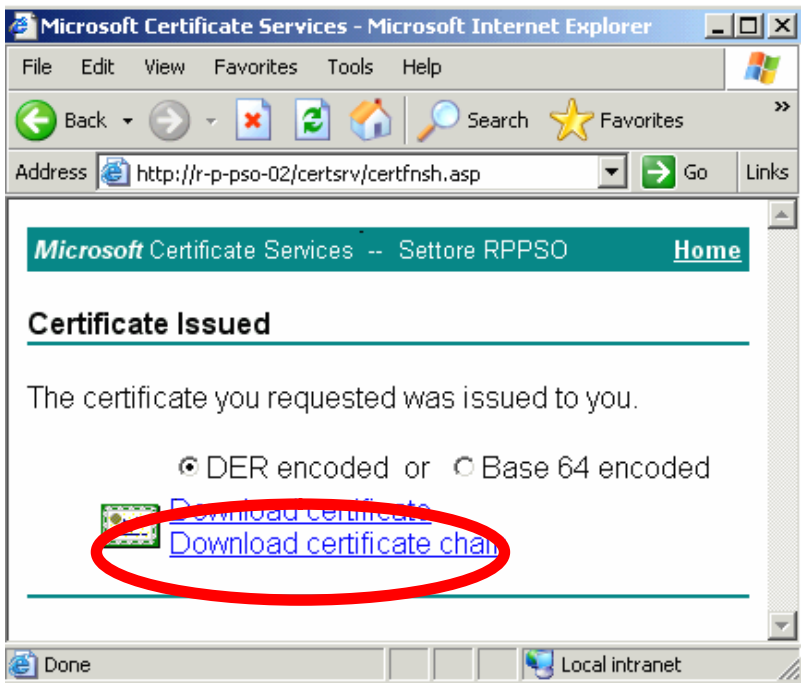
Attenzione che solo questo browser potrà accedere a questo certificato in quanto il web server ha salvato un cokies che identificherà tale richiesta.
Quindi non cancellare i cokies.
Accedendo al server si troverà tale certificato nella directory **Pending Request**.



A questo punto la CA chiamerà la persona che ha richiesto il certificato indagando sulla corretta identità del soggetto chiedendo di inviare documenti tramite fax ecc..

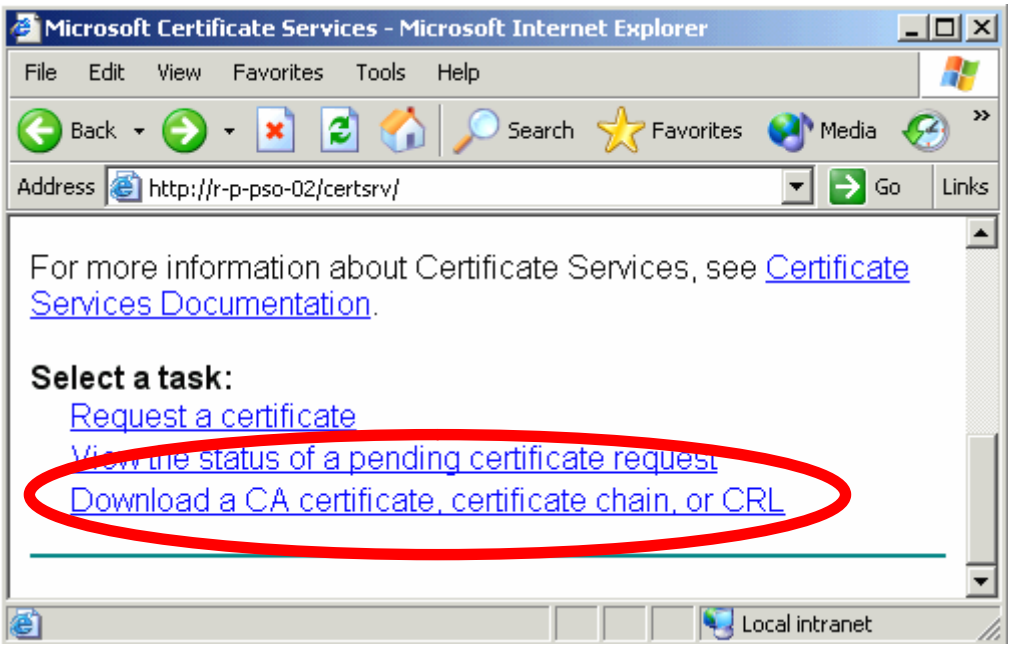
Ma non è il nostro caso.

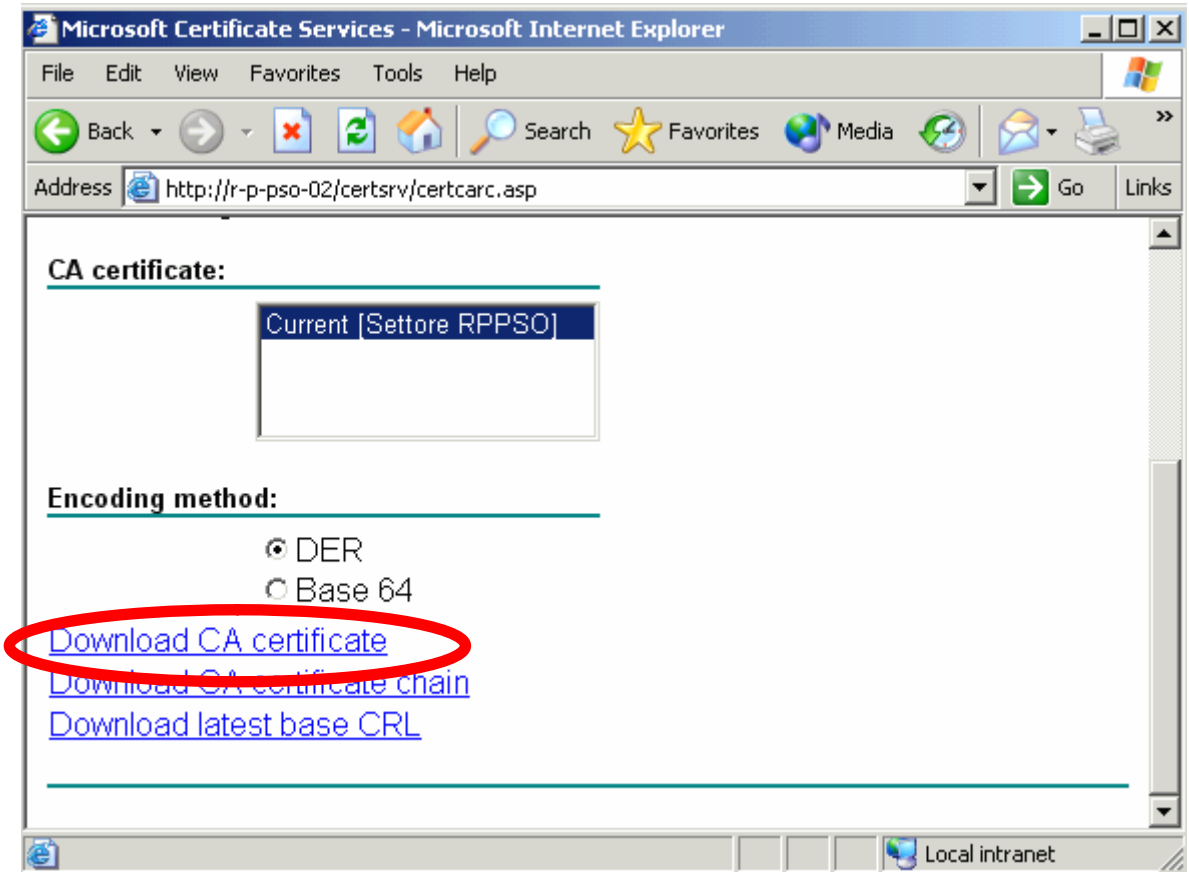
A questo punto ciccare con il tasto destro sul **certificato -> All Task -> Issue**
Accedendo nuovamente al Tool CertSrv verrà visualizzato il certificato rilasciato dall'Authority certificatrice.



Scarichiamo il certificato e salviamolo sul disco.

Scarico infine il certificato dell'Authority che lo ha rilasciato.

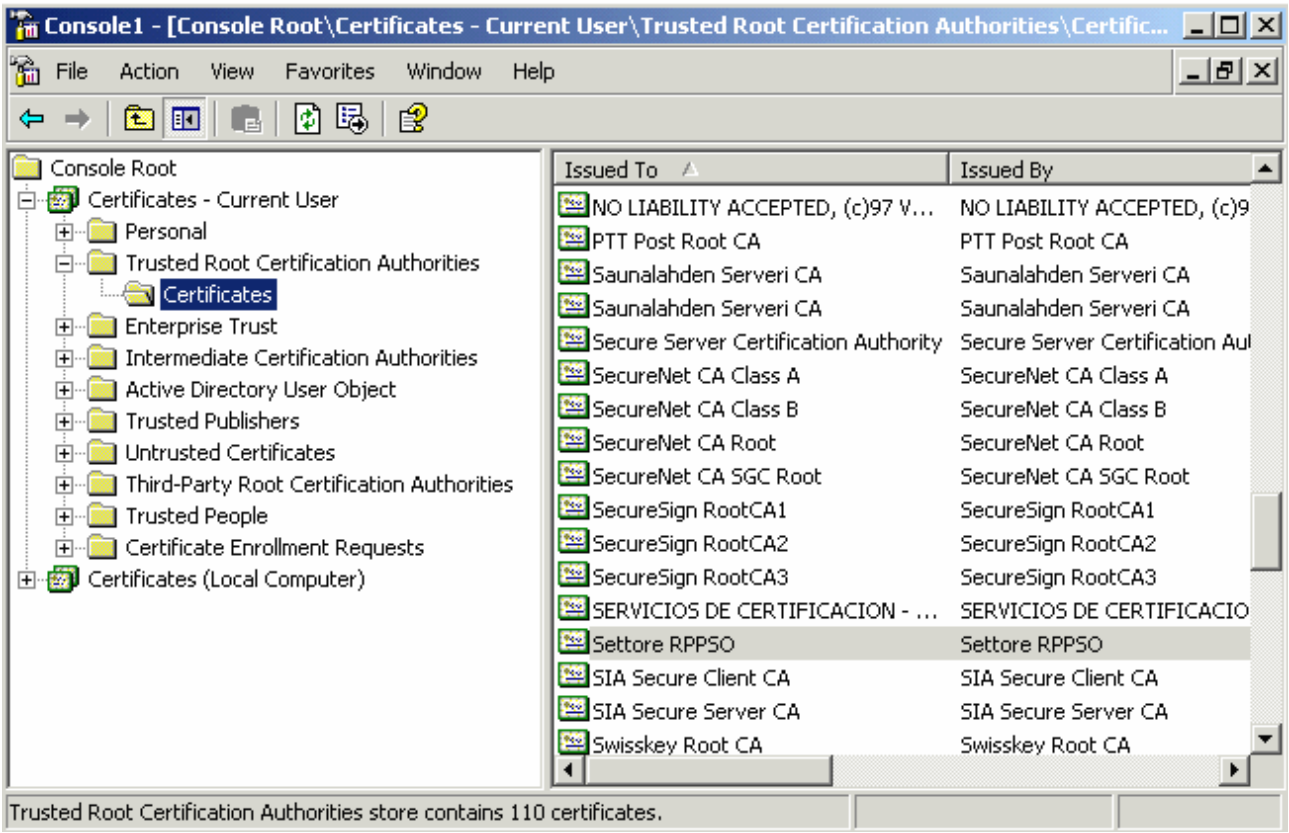




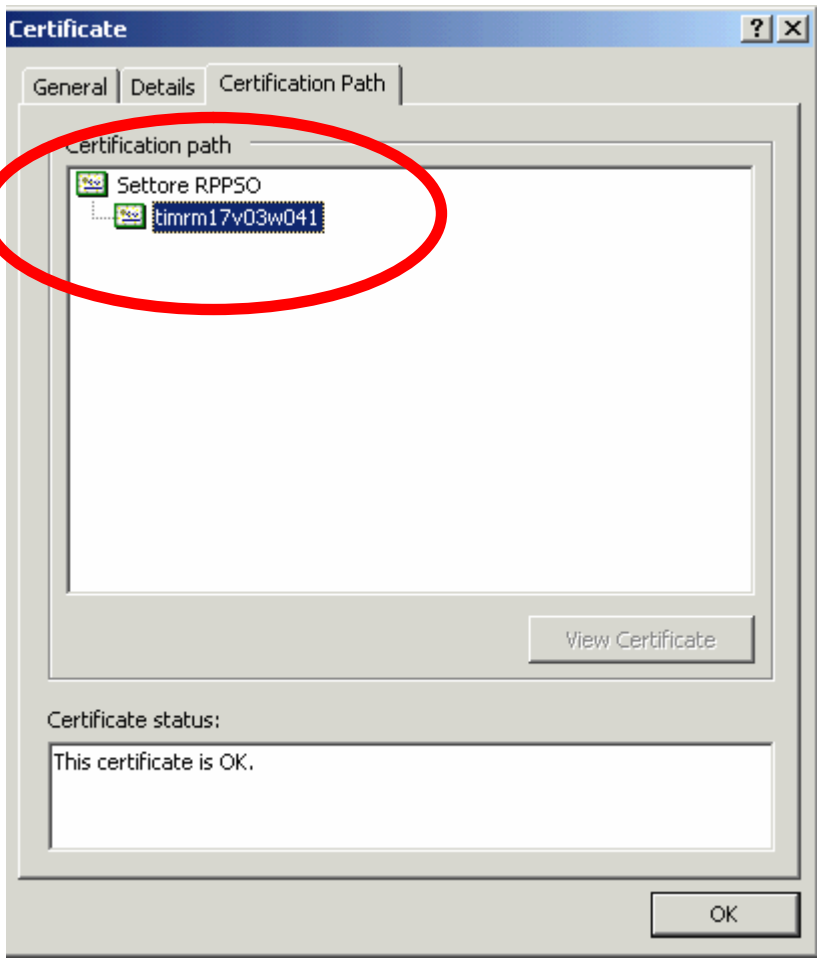
Nel nostro caso, la macchina stessa fa da Cliente e da Fornitore in quanto essa provvederà a richiedere e a rilasciare i certificati..

Al momento dell'installazione della **Certification Authority** il Wizard in automatico installa nella macchina il certificato CA nelle **Trusted Root Certification Authority**, cioè le autorità che rilasciano certificati come si può verificare accedendo allo snapin dei certificati di Windows.

Logicamente il certificato conterrà solo la chiave pubblica. In quanto la chiave privata sarà di proprietà dell'ente certificatore e non verrà distribuita in giro.



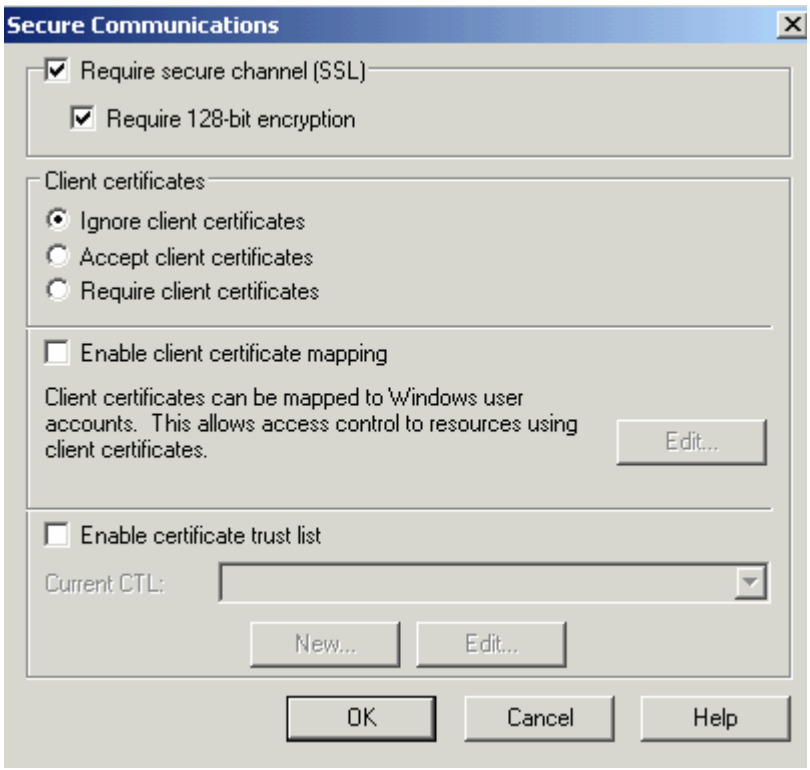
Quindi se apriamo il certificato rilasciato per il nostro Server Web troveremo nel tab ***Certification Path*** l'ente certificatore **Settore RPPSO** (Certificato dell'Authority installato dal Wizard) padre del certificato **timrm17v03w41.**



A questo punto installeremo il certificato su IIS nella stessa maschera dalla quale avevamo generato il certificato in precedenza.

Ovviamente occorre selezionare il certificato che abbiamo generato per primo e non il secondo appartenente alla CA privata.

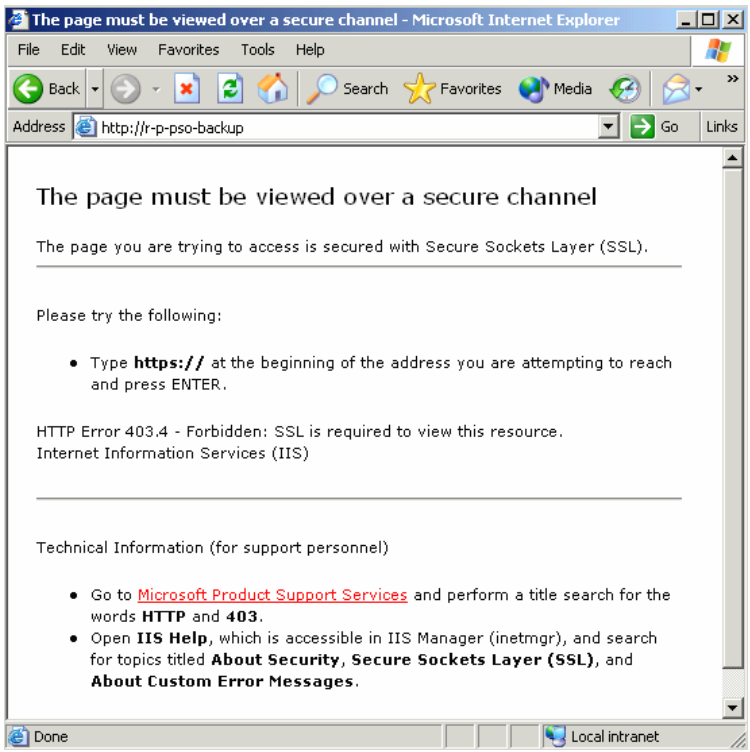
Abilitare la richiesta di SSL con encryption a 128 bit.
Ciò significa che verrà generata dal Web Client (Internet Explorer o Mozilla ecc..) una chiave simmetrica a 128 Bit tramite la quale verranno criptate le informazioni sia in Upload che in Download.



Facciamo delle prove

A questo punto accediamo ad una Virtual Directory con abilitato il supporto SSL.

Se tale URL non disporrà del suffisso **Https://** verrà inviato un messaggio di allarme che ci invita a utilizzare il suffisso **Https://** in quanto stiamo accedendo ad un canale protetto come mostra la figura in seguito.



se invece invocheremo la pagina con il suffisso **Https://** senza però aver installato il certificato rilasciato dall'Authority nella **Trusted Root Certification Authority** verrà visualizzato questo messaggio

Questo messaggio ci avverte che il certificato è Valido e che il nome del sito al suo interno contenuto è lo stesso del sito in questione, ma che Windows non dispone del certificato dell'Authority che lo ha rilasciato.

Se stiamo accedendo dalla macchina stessa sarà impossibile che venga verificata una situazione del genere in quanto come abbiamo precedentemente visto in fase di installazione dell'Authority verrà automaticamente installato il certificato nelle **Trusted Root Certification Authority.**

Quindi in tutte le macchine che non disporrano del certificato Padre dell'Authority che ha rilasciato il certificato Server verrà visualizzato questo tipo di allarme che potrà essere opportunamente rimosso installando nei client stessi il certificato dell'Authority in questione.

SSL, modalità di instanziamento di una connessione

In questo documento viene riassunto la modalità di messagi che vengono scambiati da un client ed un server che espone un servizio in un tunnel SSL (Sicure Socket layer).

Occorre sapere che l'instaurazione di una connessione SSL avviene con due specifiche modalità di cifratura.
In primo luogo in **modalità asimmetrica** e in secondo in **modalità simmetrica**.
La modalità asimmetrica viene utilizzata solo ed esclusivamente per lo scambio di una chiave detta simmetrica che servirà a cifrare i pacchetti che verranno scambiati tra il server web e il client.

Il perché si utilizza una chiave simmetrica al posto di una asimmetrica ha lo scopo unicamente di alleggerire la decifratura dei messaggi dato che gli algoritmi asimmetrici occupano molti cicli di CPU e quindi sono molto più pesanti da utilizzare.

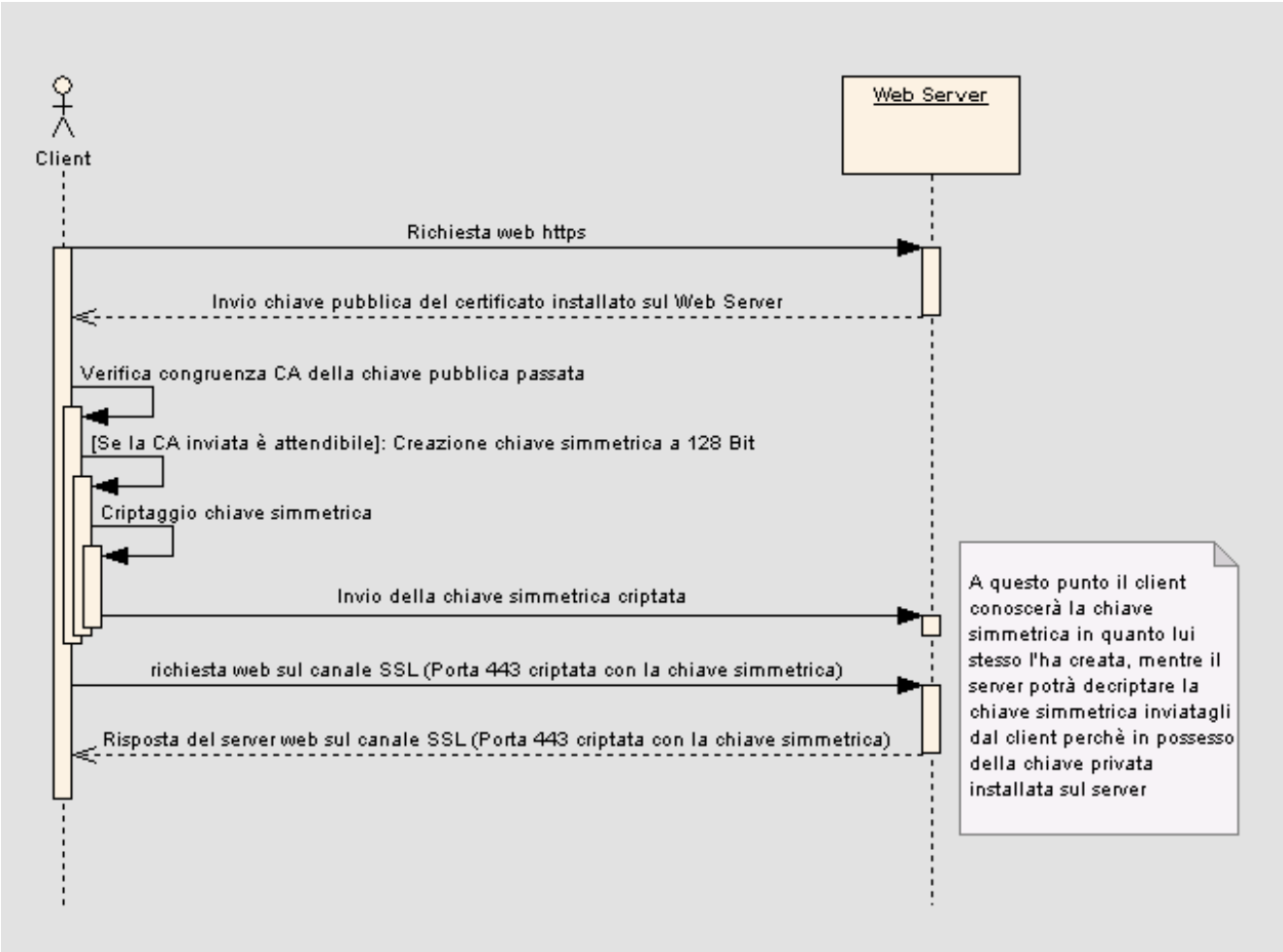
L'utilizzo del certificato installato sul server serve esclusivamente a far passare la chiave asimmetrica in un tunnel cifrato tra client e server.

Esempio di dialogo tra un Client e Server tramite SSL.

1. Il client richiede il servizio tramite il suffisso **https://**
2. il web server invia al client la **chiave pubblica** del certificato installato.
3. Il client verifica se il certificato inviato dal web server è garantito da una specifica **Authority** (CA Pubblica o CA Privata) e comunica all'utente tramite interfaccia la possibilità di accettare o di non accettare la connessione.
4. Il client **crea una chiave simmetrica a 128 Bit** che servirà per criptare e decriptare i dati
5. Il client **cripta la chiave simmetrica con la chiave pubblica** inviata dal web server e la invia al server web stesso.
6. Il web server riceve la chiave simmetrica criptata con la chiave pubblica che ha generato precedentemente il client e disponendo della sua specifica **chiave privata** la decripta.

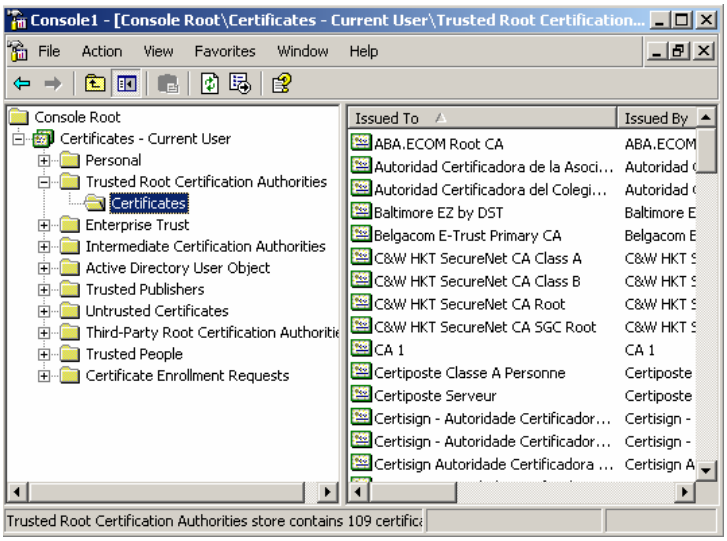
   Nota : A questo punto il client e il server hanno a disposizione la **chiave simmetrica a 128 Bit in chiaro** tramite la quale criptare e decriptare i dati.
7. Inizia la connessione in SSL

Il Sequence Diagram in seguito mostra lo scambio di messaggi tra Client e Server.



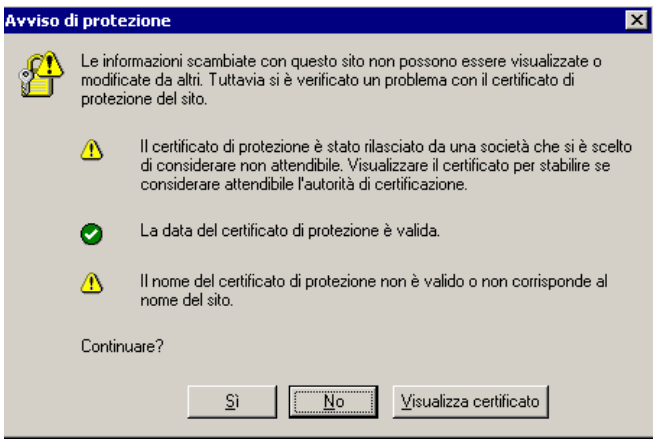
Breve analisi del punto 3

Al punto 3 abbiamo visto che il client effettua una verifica del certificato inviato dal server web verificando che l'Authority che l'ha rilasciato sia una Authority presente nella lista delle **Trusted root certification authority.**



Se il certificato è presente nella lista degli enti certificatori la connessione SSL verrà attivata immediatamente senza chiedere un'ulteriore conferma.

Nel caso in cui l'ente certificatore non sia presente verrà mostrata la maschera di allarme visualizzata in seguito.



che ci chiede di confermare o meno l'attivazione della connessione SSL specificando che **"il certificato di protezione è stato rilasciato da una società che si è scelto di considerare non attendibile."**

Il terzo avviso è una avviso che viene mostrato quando il browser non trova una correlazione tra il nome del dominio e il nome del certificato SSL

SSL (secure Socket Layer) è un protocollo che permette l'invio di pacchetti criptati in connessioni Http per avere maggior sicurezza sul traffico dei dati prodotto.

Il sistema come mostra la figura riportata in seguito utilizza le porte 443 e 80 per avviare una comunicazione protetta.

N	Time	MAC So...	MAC D...	Frame	Protocol	IP Source	IP Destina...	P	P	S...	A...	Size
1	13.54.47....	00:0D:9...	00:10:B...	IP	TCP->H...	10.12.18.61	10.12.18.63	3	443	2...	1...	365
2	13.54.47....	00:10:B...	00:0D:9...	IP	TCP->H...	10.12.18.63	10.12.18.61	4	3...	1...	2...	1514
3	13.54.47....	00:10:B...	00:0D:9...	IP	TCP->H...	10.12.18.63	10.12.18.61	4	3...	1...	2...	1514
4	13.54.47....	00:0D:9...	00:10:B...	IP	TCP->H...	10.12.18.61	10.12.18.63	3	443	2...	1...	54
5	13.54.47....	00:10:B...	00:0D:9...	IP	TCP->H...	10.12.18.63	10.12.18.61	4	3...	1...	2...	876
6	13.54.47....	00:0D:9...	00:10:B...	IP	TCP->H...	10.12.18.61	10.12.18.63	3	443	2...	1...	505
7	13.54.47....	00:10:B...	00:0D:9...	IP	TCP->H...	10.12.18.63	10.12.18.61	4	3...	1...	2...	287
8	13.54.47....	00:0D:9...	00:10:B...	IP	TCP->H...	10.12.18.61	10.12.18.63	3	443	2...	1...	54
9	13.54.55....	00:30:0...	00:0D:9...	IP	TCP->N...	10.12.18.62	10.12.18.61	1	4...	2...	3...	60
10	13.54.55....	00:0D:9...	00:30:0...	IP	TCP->N...	10.12.18.61	10.12.18.62	4	139	3...	2...	54

Quindi è importante ricordare che nei server web in cui sono disponibili servizi SSL occorre abilitare l'accesso del traffico in entrata veicolato sulla porta **443** ad esempio creando un filtro IPSEC di tipo TCPIP sulla porta 443.