

CREAZIONE E INSTALLAZIONE DI UN CERTIFICATO USANDO LA CA DI WINDOWS

Creare un certificato SSL

SSL permette di eseguire un tunnel di dati criptati tra il server WEB e il client WEB

Nella gestione di SSL esistono due tipi di certificati

1. Certificato SERVER (Rilasciato da una CA riconosciuta dal browser)
2. Certificato Utente

Utilizzando un certificato SERVER riconosciuta dal Browser internet non ho bisogno di installare un certificato sul client.

Utilizzando un certificato creato dalla mia CA (ad esempio l'autorità di certificazione installabile su Windows 2000 Server e 2003 Server) e quindi non riconosciuta dal Web browser occorre installare la chiave pubblica di tale certificato sul Browser.

Per questo motivo nei siti di e-commerce sarebbe impossibile dire a tutti gli utenti di installare il certificato contenente la chiave pubblica. Occorre pertanto comperare un certificato da una CA commerciale nota e pubblica in quanto riconosciuta automaticamente dai browser come attendibile.

Occorre fare delle considerazioni sulla CA che si vuole utilizzare anche in base a questo problema.

L'ente per eccellenza che certifica i server è VERISIGN.

Per chiedere un certificato SERVER a VERISIGN o ad un'altra CA Pubblica occorre preparare la richiesta cliccando sulla maschera qui sotto di IIS.

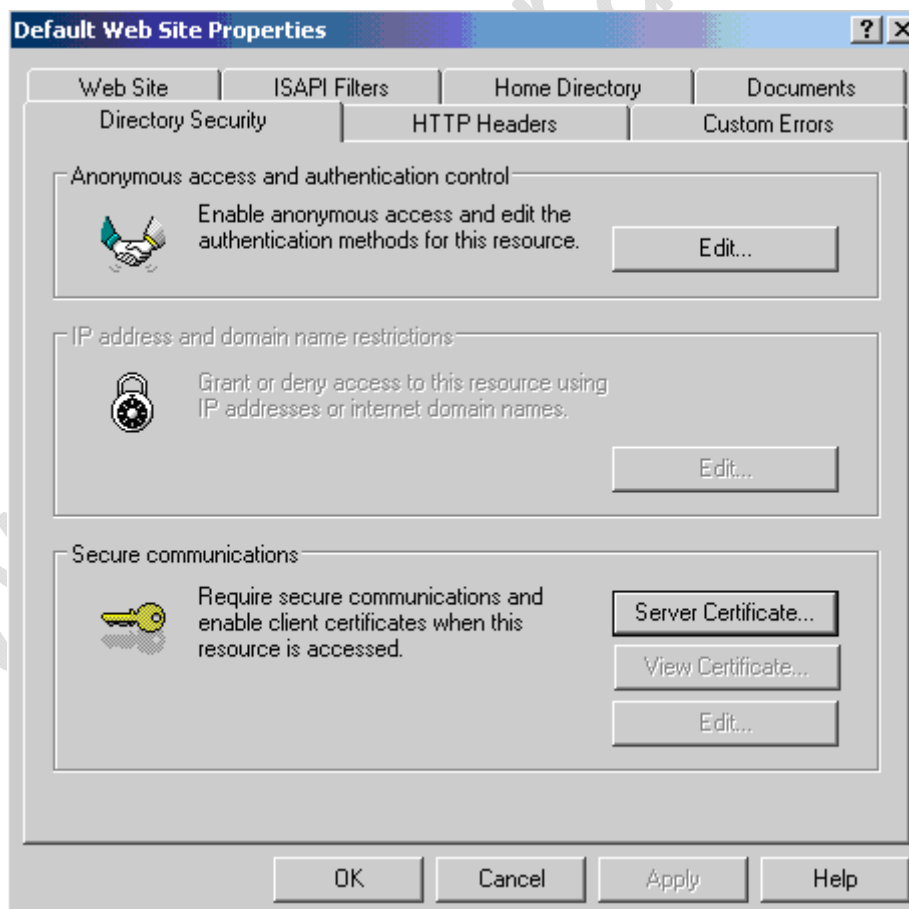


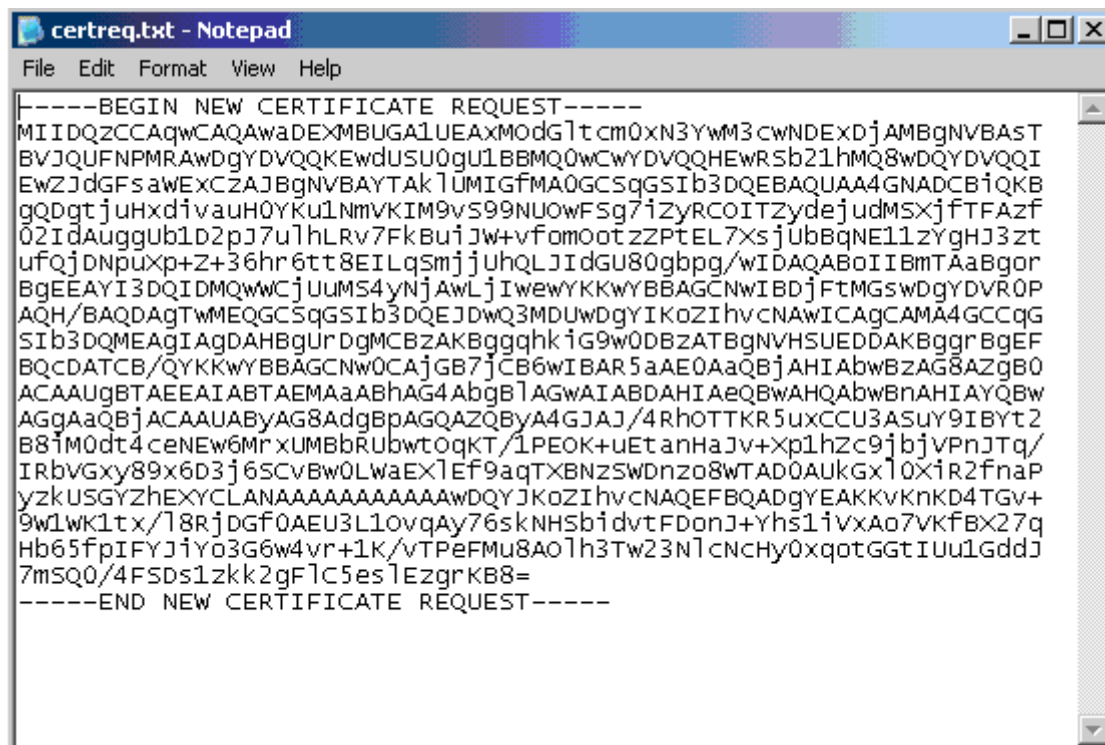
Fig.1

Cliccando su Server Certificate creremo la richiesta per l'invio ad una CA Pubblica.

Questa richiesta sarà un file TXT in BASE64 contenente i dati da inviare alla CA come nell'immagine successiva.

Attenzione a specificare esattamente il nome del dominio ad esempio `www.agensportregionelazio.it` altrimenti verrà mostrato il Warning che il certificato non corrisponde al nome del dominio.

Il nome del dominio deve essere inserito tutto incluso il suffisso `www` e `.it`



```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIDQZCCAqWCAQAwaDEXMBUGA1UEAxMOdGltcm0xN3YwM3cwNDExdjAMBgNVBAST
BVJQUFNPMRAwDgYDVQQKEwdUSU0gU1BBMQ0wCwYDVQQHEwRSb21hMQ8wDQYDVQQI
EwZJdGFiawEXCzAJBgNVBAYTAk1UMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKB
gQDgtjUHxdivauH0YKu1NmVKIM9vS99NUowFsg7iZyRCOITzydejudMSXjftFAzf
02IdAuggUb1D2pJ7u1hLRv7FkBuIjW+vfomootzzPtEL7XsjUbBqNE11zYgHJ3zt
ufQjDNpuxp+Z+36hr6tt8EILqsmj jUHLJIdGU80gbpg/wIDAQABoII BmTAA Bgor
BgEEAYI3DQIDMQwWCjUUMS4yNjAwLjIwewYKKwYBBAGCNwIBDjFtMGswDgYDVR0P
AQH/BAQDAgTWMEQGCsQGSiB3DQEJdWQ3MDUwDgYIKoZIHvCNAwICAgCAMA4GCCqG
SIb3DQMEAgIAgDAHBgUrDgMCBZAKBggqhkiG9w0DBzATBgNVHSUEDDAKBggrBgEF
BQCDATCB/QYKKwYBBAGCNw0CAjGB7jCB6wIBAR5aAE0AaQBJAHIAbwBzAG8AZgB0
ACAAUGBTAEEAIABTAEMAaABHAG4AbgBlAGWAIABDAHIAeQBWAHQAbwBnAHIAyQBw
AGgAaQBJACAAUABYAG8AdgBpAGQAZQByA4GJAJ/4RhOTTKR5uxCCU3ASUY9IBYt2
B8iM0dt4ceNEw6MrxUMBbRUBwtOgKT/1PEOK+uETanHaJv+xp1hzC9jbjvPnJTq/
IRbvGxy89x6D3j6ScvBw0LwaEX1Ef9aqTxBNZsWdNzo8WTAD0AukGx10xiR2fnaP
yzkUSGYzhEXYCLANAAAAAAAAAAAAawDQYJKoZIhvcNAQEFBQADgYEAKKvKND4TGV+
9w1wk1tx/l8RjDGF0AEU3L10vqay76skNHSbidvtFDonJ+Yhs1ivxAo7VKfBX27q
Hb65fpIFYJjiYo3G6w4vr+1K/vTpeFMu8A0lh3Tw23NlCNChy0xqotGGtIUu1Gddj
7mSQ0/4FSDs1zkk2gf7C5es7EzgrKB8=
-----END NEW CERTIFICATE REQUEST-----
```

Fig.2

Nel caso che volessi utilizzare il tool Certification Authority presente sui sistemi Server quali Windows 2000 Server e Windows 2003 Server occorrerà per prima installarlo.

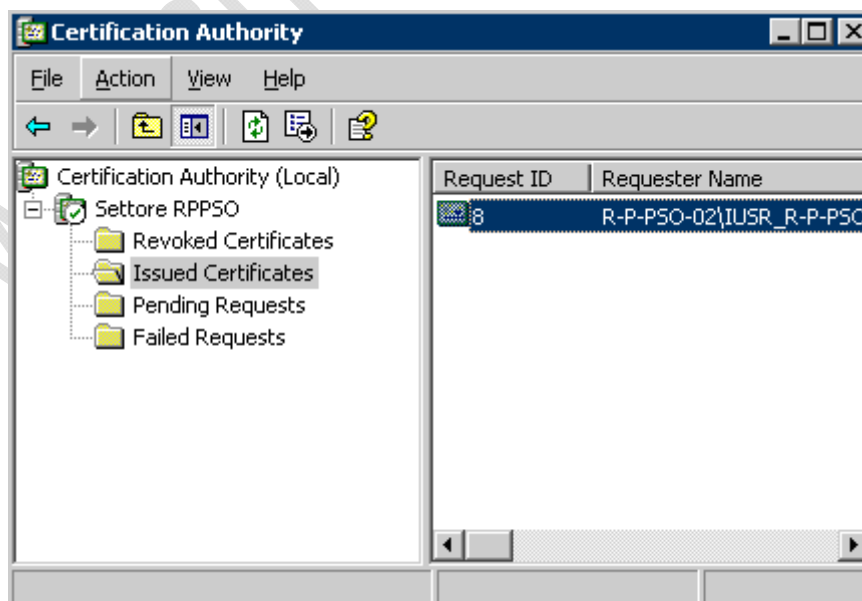


Fig.3

E poi accedere al tool internet installato al momento dell'installazione della Certification Authority privata presente sul server stesso.

Al momento dell'installazione verrà creata un'applicazione WEB presente nella root inetpub/wwwroot/certsrv. Come nell'immagine successiva.

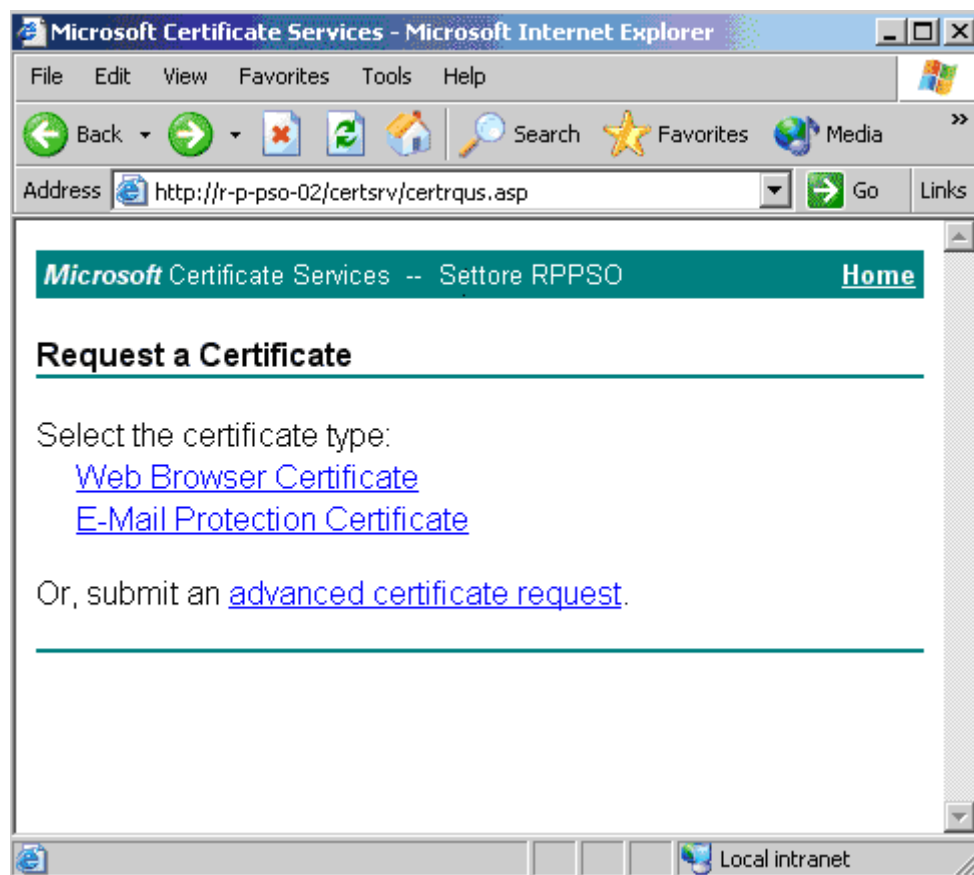


Fig.4

Per richiedere un certificato all'authority privata come in questo caso occorre selezionare. A questo punto possiamo scegliere la tipologia di creazione:

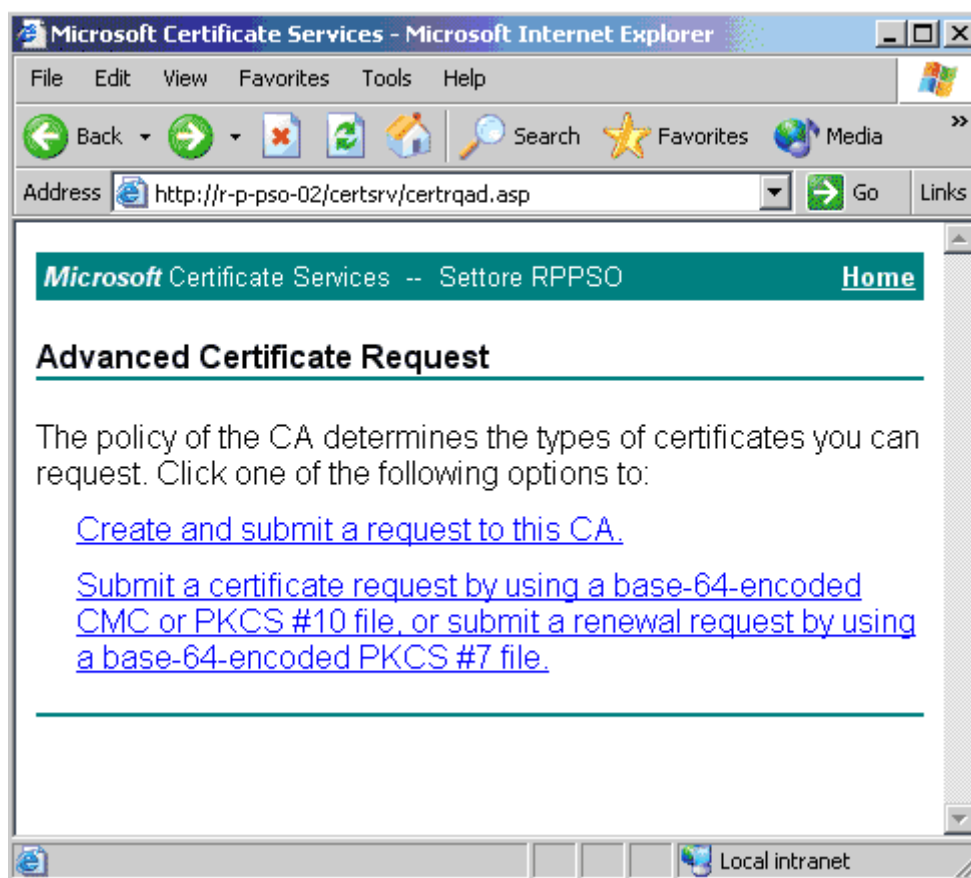


Fig.5

Create and submit a request to this CA. Serve 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 generata dalla richiesta precedente.

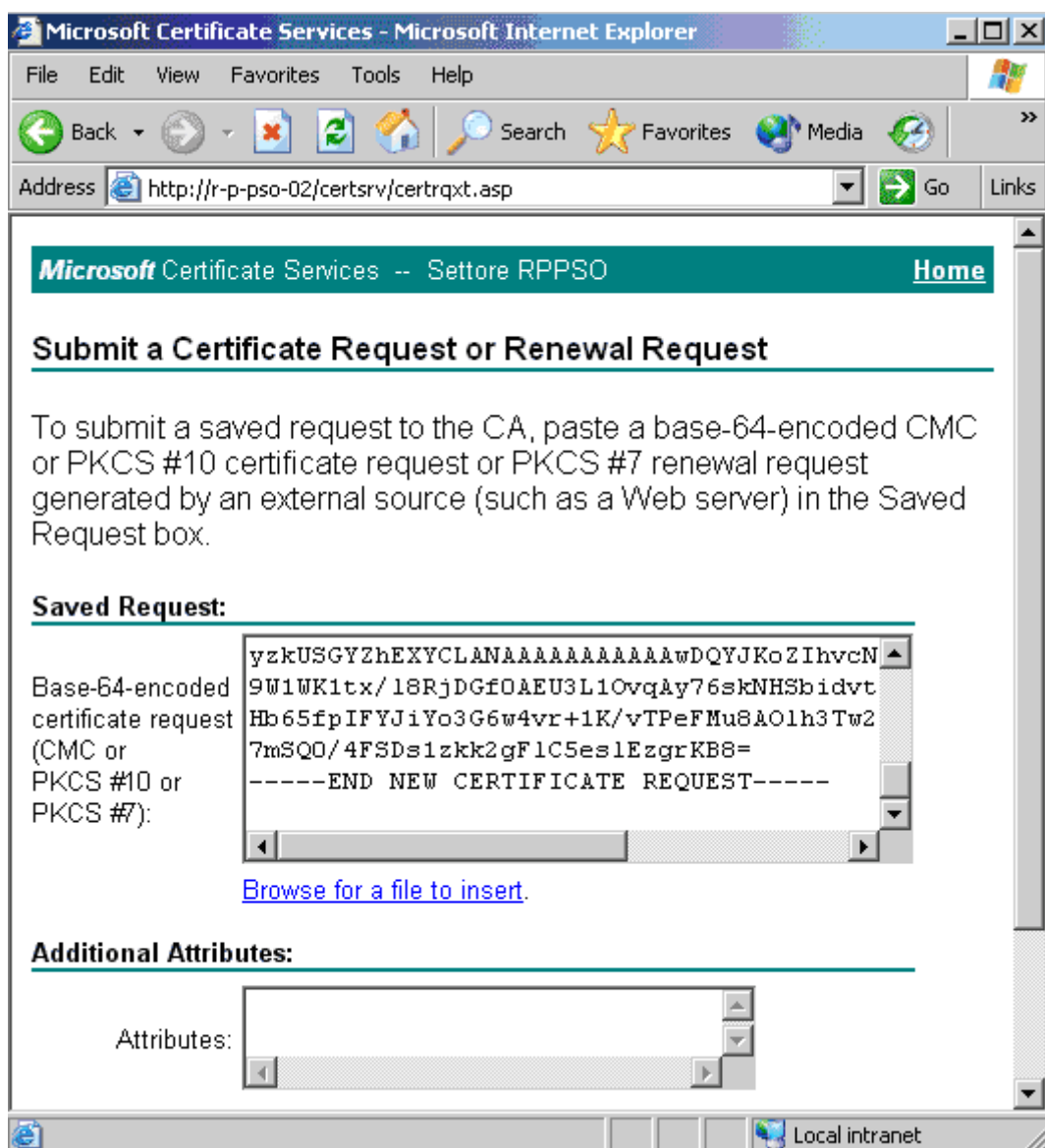


Fig.6

In questo caso Ho selezionato tutto il contenuto presente nel file contenente la richiesta del certificato e lo ho incollato nella textarea BASE64.

Occorre inserire tutto anche:

-----BEGIN NEW CERTIFICATE REQUEST-----

-----END NEW CERTIFICATE REQUEST-----.

Sottomettere la richiesta.

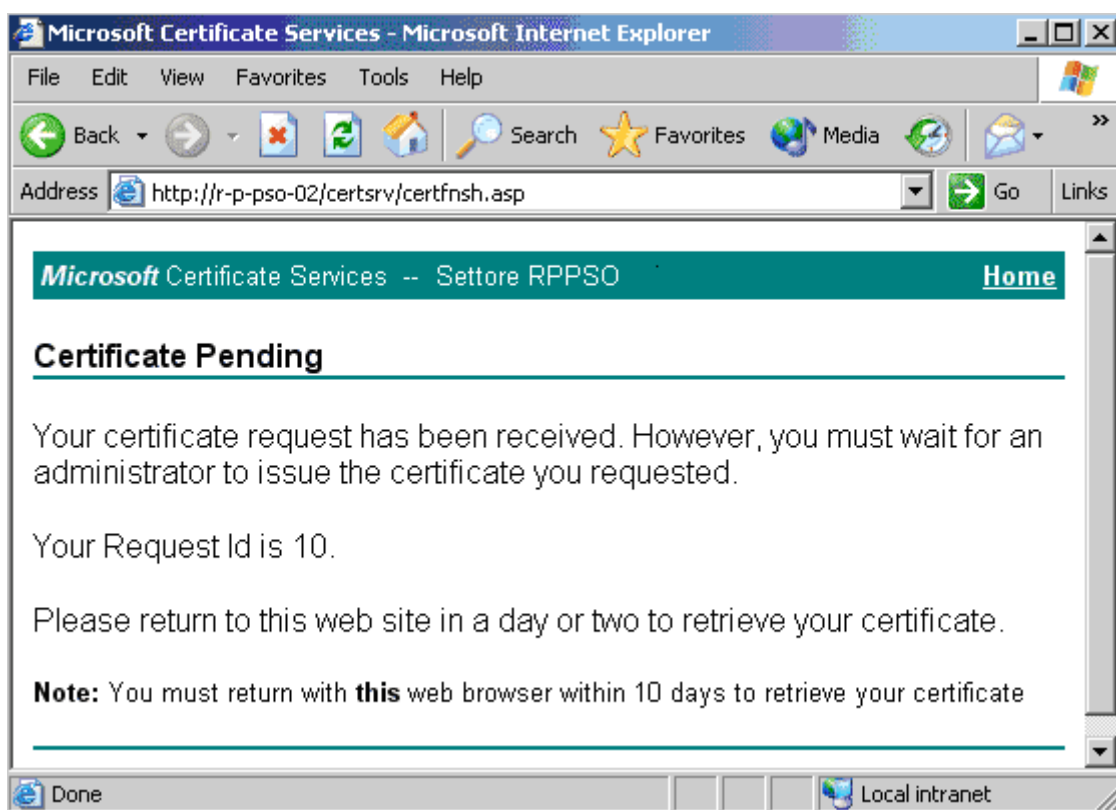


Fig.7

A questo punto la CA installata su Windows 2000/2003 Server dovrà rilasciare il certificato che sarà scaricabile dallo stesso indirizzo della richiesta pendente.

Attenzione che solo questo browser potrà accedere a questo certificato in quanto il web server ha salvato un cookie che identificherà tale richiesta, quindi non cancellare i cookies.

Accedendo al server si troverà tale certificato come PENDING.

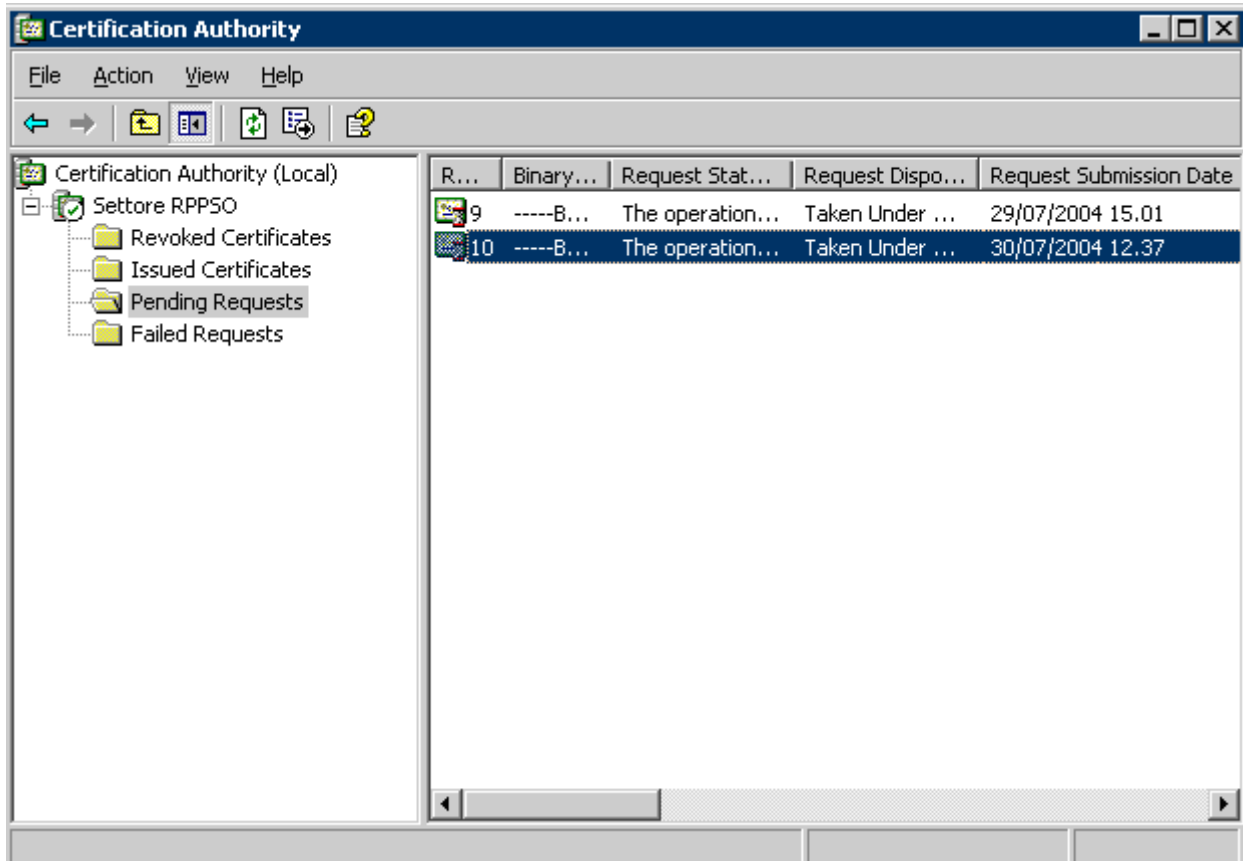


Fig.8

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

A questo punto tasto destro sul certificato -> All Task -> Issue

Andando a visualizzare la richiesta di prima troveremo il certificato presente per essere scaricato e installato sulla macchina.

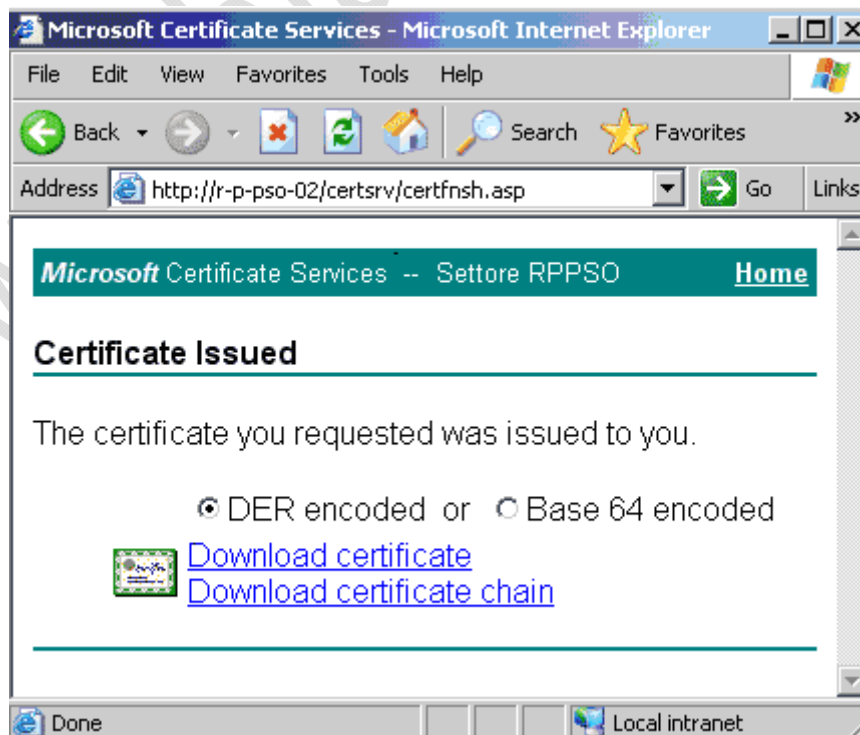


Fig.9

Quindi scarico il certificato e lo salvo sul disco.

Se lo vado ad aprire non ci sarà il TRUST con la macchina server che ha rilasciato e quindi occorrerà il certificato del SERVER della CA altrimenti il certificato rilasciato non sarà valido.

Per scaricare il certificato del server:

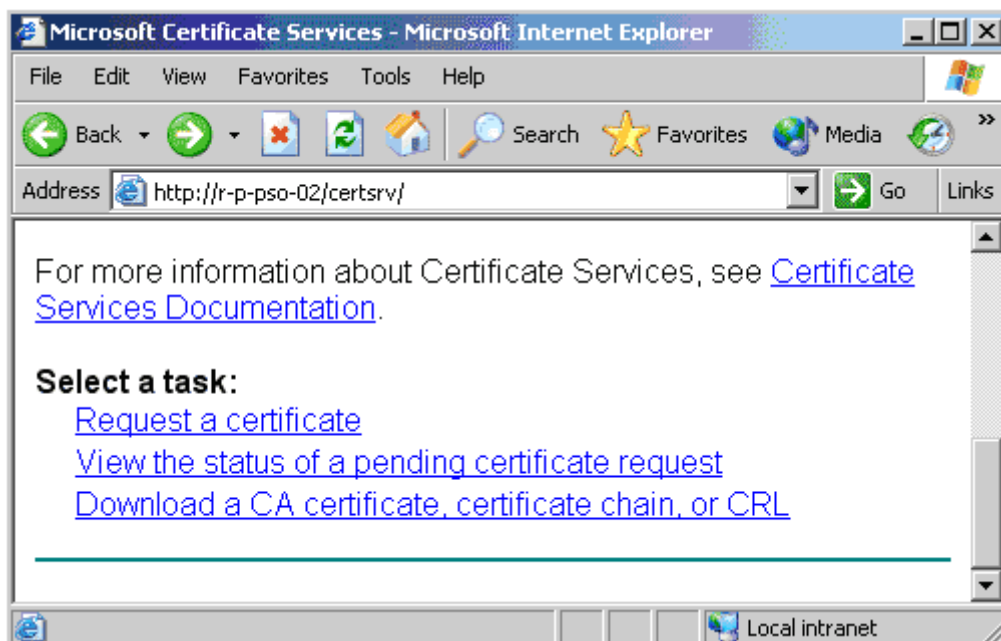


Fig.10

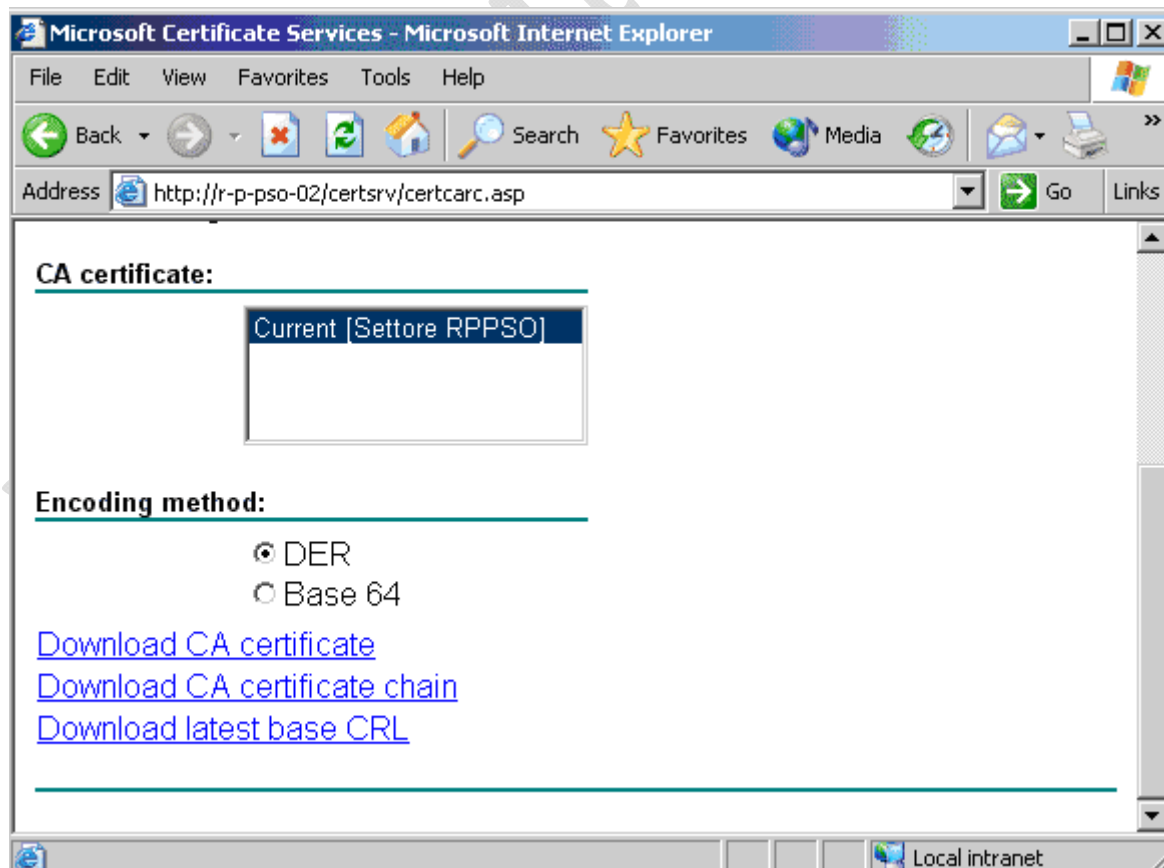


Fig.11

Una volta installato il certificato dovrà essere presente nella macchina alla voce delle authority il rilascio dei certificati come nel caso seguente.

Logicamente in tale certificato sarà presente solamente la chiave pubblica del certificato.

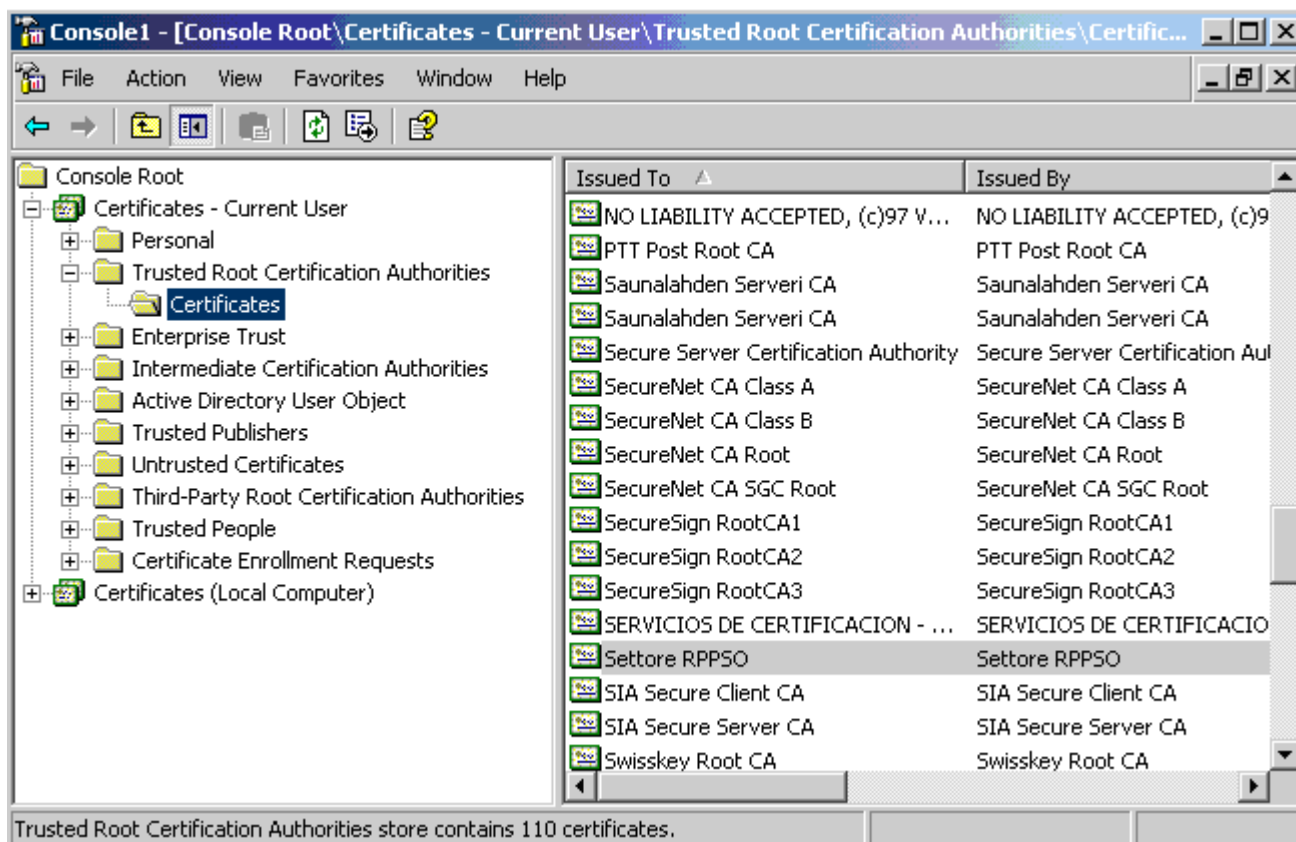
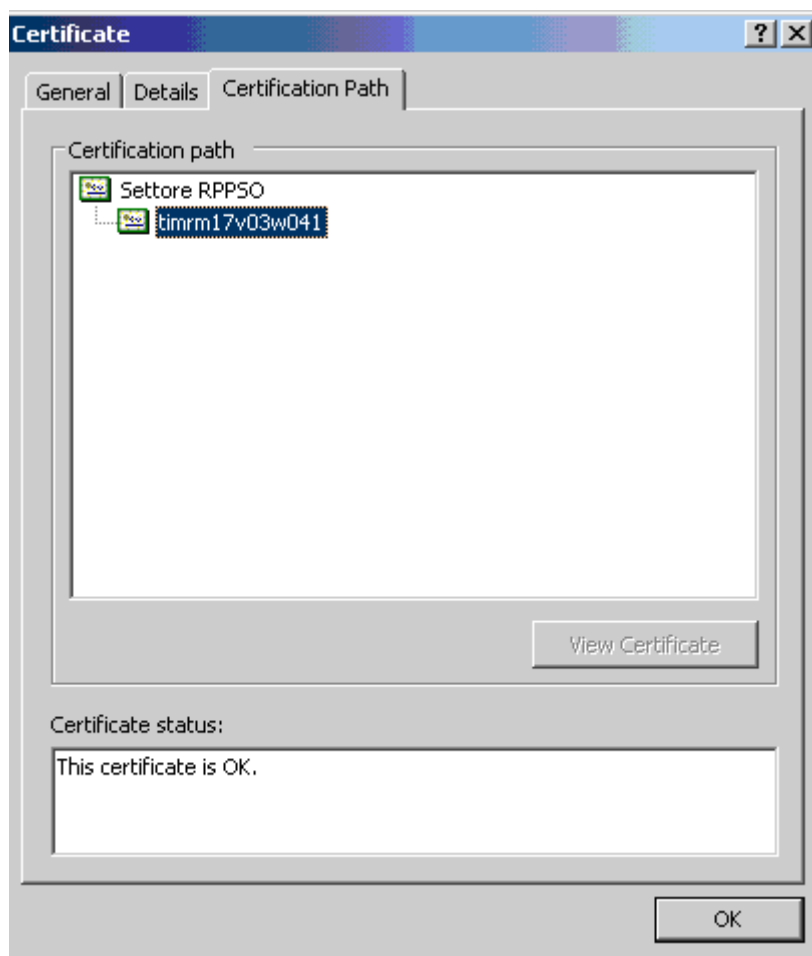


Fig.12

Quindi aprendo il certificato rilasciato troveremo l'ente certificatore Settore RPPSO (Precedentemente installato sotto forma della sola chiave pubblica) che ha rilasciato il certificato timrm17v03w41 che lo riesco ad aprire in quanto ho la chiave pubblica dell'ente certificatore!

**Fig.13**

A questo punto installare il certificato in IIS in quanto è rimasta pending la richiesta SSL. Ovviamente occorre selezionare il certificato che abbiamo scaricato per primo e non il secondo. Abilitare la richiesta di SSL con encryption a 128 bit:

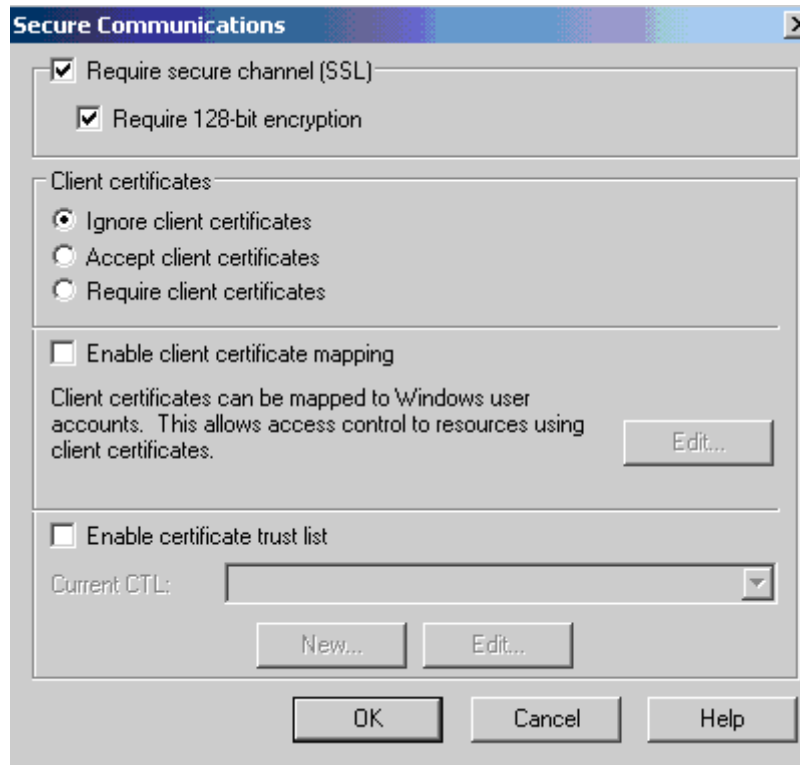


Fig.14

Facciamo delle prove

Se richiediamo una url al server senza http il server rispnderà:

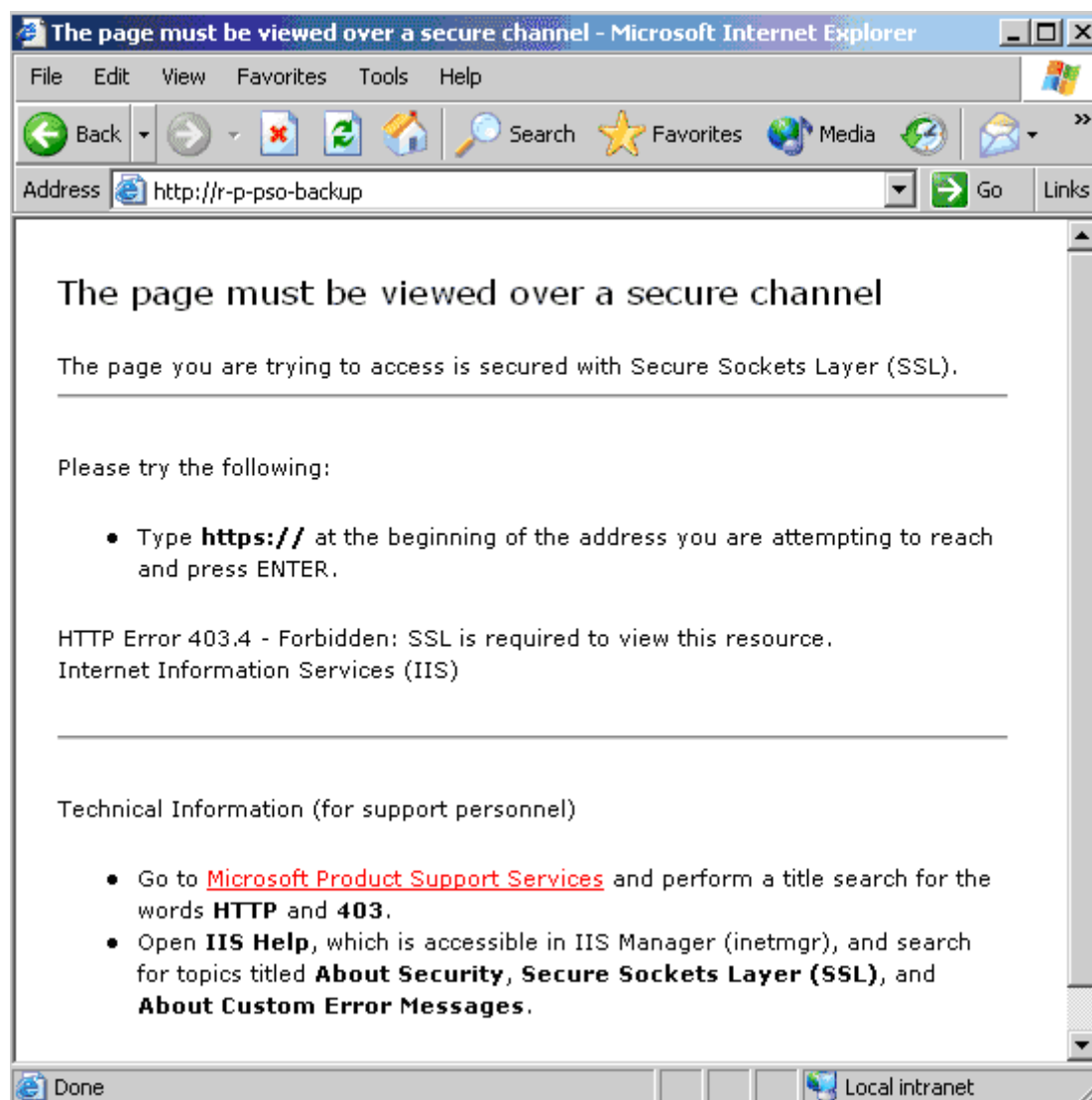


Fig.15

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:



Fig.16

Questa maschera ci dice che il certificato è OK ma non può essere Trustato dalla authority di appartenenza, questo vuol dire che non è presente la relativa chiave pubblica nella root delle certificazioni.

Installiamo quindi il certificato e non verrà più mostrata questa macchina in quanto risulterà possibile effettuare il TRUST.

Nota: durante l'installazione della Certification Authority di Windows, eseguire l'installazione della CA in modalità "Stand-Alone" nel caso in cui si debbano distribuire certificati all'esterno del dominio, poiché una CA Enterprise richiede l'utilizzo di utenti registrati in AD.