

## 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 riconosciuto dal browser)

2. Certificato Utente

Utilizzando un certificato SERVER riconosciuto 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 ciccando sulla maschera qui sotto di IIS.

| Directory Sec<br>Anonymous acc<br>En<br>au | curity                                     | HTTP Headers                               | ; [         | Custom Errors  |
|--|--|--|-------------|----------------|
| Anonymous acc<br>En<br>au                  | ess and authentic<br>able anonymous a      | ation control                              |             |                |
| En<br>au                                   | able anonymous a                           | 1 12.11                                    |             |                |
|  | unentication metric                        | access and edit th<br>ods for this resourc | ne<br>De    | Edit           |
| IP address and                             | domain name resti                          | ictions                                    |             |                |
| Gr P                                       | ant or deny acces<br>addresses or inter    | s to this resource<br>net domain name      | using<br>s. |                |
|  |  |  |             | Edit           |
| Secure commun                              | nications                                  |  |             |                |
| Re<br>Re                                   | equire secure com<br>able client certifica | munications and ates when this             | Serve       | er Certificate |
| res  | source is accessed                         | d.   | Viev        | v Certificate  |
|  |  |  |             | Edit           |
|  |  |  |             |                |

Fig.1



Ciccando 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



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.

| Request ID | Requester Name          |
|------------|-------------------------|
| 8          | R-P-PSO-02\IUSR_R-P-PSO |
|            |                         |
|            | Request ID              |



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.





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

| 🚰 Microsoft Certificate Services - Microsoft Internet Explorer 📃 🗖   | ×        |              |
|--|----------|--------------|
| File Edit View Favorites Tools Help  | 1        |              |
| 🌀 Back 👻 🌍 🖌 📓 🐔 🔎 Search 🤺 Favorites 🚳 Media  | »        |              |
| Address 🕘 http://r-p-pso-02/certsrv/certrqad.asp   | inks     |              |
| Microsoft Certificate Services Settore RPPSO Home  | <u></u>  |              |
| Advanced Certificate Request   |          | $\mathbb{N}$ |
| The policy of the CA determines the types of certificates you can request. Click one of the following options to:  |          |              |
| Create and submit a request to this CA.  |          |              |
| Submit a certificate request by using a base-64-encoded<br>CMC or PKCS #10 file, or submit a renewal request by using<br>a base-64-encoded PKCS #7 file. |          |              |
|  |          |              |
| 🙆 🛛 😽 Local intranet   | <b>.</b> |              |
| 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.

## WWW.CHIATTORAFFAELE.IT

| Microsoft Certific  | ate Services - Microsoft Internet Explorer   |       |
|---|--|-------|
| File Edit View F  | avorites Tools Help  | 2     |
| 😋 Back 🝷 💮 👻  | 💌 👔 🏠 🔎 Search 🤺 Favorites 🔮 Media 🧭   | »>    |
| Address 🙆 http://r-p  | -pso-02/certsrv/certrqxt.asp 💽 Go  | Links |
|   |  |       |
| Microsoft Certific  | ate Services Settore RPPSO <u>Hom</u>  | e     |
| Submit a Cert   | ficate Request or Renewal Request  |       |
| To submit a sav<br>or PKCS #10 c<br>generated by a<br>Request box.            | ved request to the CA, paste a base-64-encoded CMC<br>ertificate request or PKCS #7 renewal request<br>n external source (such as a Web server) in the Saved   |       |
| Saved Request:  |  |       |
| Base-64-encoded<br>certificate request<br>(CMC or<br>PKCS #10 or<br>PKCS #7): | yzkUSGYZhEXYCLANAAAAAAAAAAAAWDQYJKoZIhvcN<br>9W1WK1tx/18RjDGfOAEU3L1OvqAy76skNHSbidvt<br>Hb65fpIFYJiYo3G6w4vr+1K/vTPeFMu8AO1h3Tw2<br>7mSQO/4FSDs1zkk2gF1C5es1EzgrKB8=<br>END NEW CERTIFICATE REQUEST |       |
|   | Browse for a file to insert.   |       |
| Additional Attrib   | utes:  |       |
| Attributes:   |  | •     |
| ê   | 🔰 🛛 😼 Local intranet   | ///   |
|   | 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.

2

## WWW.CHIATTORAFFAELE.IT

| 🚰 Microsoft Certificate Services - Microsoft Internet Explorer 📃 🔲 🗙  | 1 |
|---|---|
| File Edit View Favorites Tools Help   |   |
| 🔇 Back 👻 💮 - 💌 😰 🏠 🔎 Search 🤸 Favorites 🔮 Media 🧭 🔗 - 👋   |   |
| Address 🙆 http://r-p-pso-02/certsrv/certfnsh.asp  |   |
|   | 1 |
| Microsoft Certificate Services Settore RPPSO Home   |   |
|   | 1 |
| Certificate Pending   |   |
| Your certificate request has been received. However, you must wait for an administrator to issue the certificate you requested. | ŀ |
| Your Request ld is 10.  |   |
| Please return to this web site in a day or two to retrieve your certificate.  |   |
| Note: You must return with this web browser within 10 days to retrieve your certificate   |   |
| <b>_</b>  |   |
| 🕘 Done 📃 📃 😽 Local intranet   |   |
| Fig.7   |   |

-2)

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

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 cookies. Accedendo al server si troverà tale certificato come PENDING.

| 🔯 Certification Authority  |                       |  |   |   |
|--|-----------------------|--|---|---|
| <u>File Action View H</u> elp  |                       |  |   |   |
| ← → 🗈 🖬 😰 🗟 🔮  |                       |  |   |   |
| Certification Authority (Local)  Certification Repose Revoked Certificates Certificates Pending Requests Failed Requests | R Binary<br>9B<br>10B | Request Stat<br>The operation<br>The operation | Request Dispo<br>Taken Under<br>Taken Under | Request Submission Date<br>29/07/2004 15.01<br>30/07/2004 12.37 |
|  |                       |  |   | <u>•</u>  |

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.





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:

| Microsoft Certificate Services - Microsoft Internet Explorer    |           |
|---|-----------|
| File Edit View Favorites Tools Help                             | A         |
| 🔇 Back 🔹 🐑 👻 😰 🏠 🔎 Search 🔶 Favorites 😻 Media                   | 🥝 »       |
| Address 🙆 http://r-p-pso-02/certsrv/                            | o Links   |
| For more information about Cartificate Services, see Cartificat |           |
| Services Documentation.   | Ē         |
| Select a task:  |           |
| Request a certificate   |           |
| View the status of a pending certificate request                |           |
| Download a CA certificate, certificate chain, or CRL            |           |
|   |           |
| 🕘 🛛 😼 Local intranet  |           |
| Fig.10  |           |
|   |           |
| Microsoft Certificate Services - Microsoft Internet Explorer    |           |
| File Edit View Favorites Tools Help                             |           |
| 🔇 Back 🔹 💮 🖌 😰 😭 🔎 Search 👷 Favorites 🔮 Media 🧭                 | 🙈 - 볼 👋   |
| Address 🕘 http://r-p-pso-02/certsrv/certcarc.asp                | Go Links  |
|   |           |
| CA certificate:   |           |
| Current [Settore RPPSO]   |           |
|   |           |
|   |           |
| Encoding method:  |           |
|   |           |
| O Base 64   |           |
| Download CA certificate chain                                   |           |
| Download latest base CRL  |           |
|   |           |
|   | ▼         |
| Fig.11  | tranet // |



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

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

| 🛅 Console1 - [Console Root\Certificates - Curre   | nt User\Trusted Root Certification A   | uthorities\Certific 💶 💌   |
|---|--|---|
| 📸 File Action View Favorites Window Hel   | p  | _ <b>B</b> ×  |
| ← → 🗈 📧 💼 🔂 💀 😫   |  |   |
| Console Root Certificates - Current User Personal Certificates Certificate Enrollment Requests Certificates Certificates (Local Computer) | Issued To<br>NO LIABILITY ACCEPTED, (c)97 V<br>PTT Post Root CA<br>Saunalahden Serveri CA<br>Saunalahden Serveri CA<br>Secure Server Certification Authority<br>SecureNet CA Class A<br>SecureNet CA Class B<br>SecureNet CA Class B<br>SecureNet CA Root<br>SecureSign RootCA1<br>SecureSign RootCA2<br>SecureSign RootCA3<br>SecureSign RootCA3<br>SERVICIOS DE CERTIFICACION<br>Settore RPPSO<br>SIA Secure Client CA<br>Sia Secure Server CA<br>Swisskey Root CA | Issued By NO LIABILITY ACCEPTED, (c)9 PTT Post Root CA Saunalahden Serveri CA Saunalahden Serveri CA Saunalahden Serveri CA Secure Server Certification Au SecureNet CA Class A SecureNet CA Class B SecureNet CA Class B SecureNet CA SGC Root SecureSign RootCA1 SecureSign RootCA2 SecureSign RootCA3 SERVICIOS DE CERTIFICACIO Settore RPPSO SIA Secure Client CA SIA Secure Server CA Swisskey Root CA |
| Trusted Root Certification Authorities store contains 110   | certificates.  |   |

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!

| ertificate              |                 |      |             | ? × |    |
|-------------------------|-----------------|------|-------------|-----|----|
| General Details Cer     | tification Path |      |             |     |    |
| Certification path      |                 |      |             |     |    |
| Settore RPPSC           | )<br>3w041      |      |             |     | ·X |
|                         |                 | Vier | w Certifica | te  | C. |
| Certificate status:     |                 |      |             |     |    |
| This certificate is OK. |                 |      |             |     |    |
|                         |                 |      |             | ОК  |    |
|                         | 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 encription a 128 bit:

•

0

| <br>- |   |
|-------|---|
| - )   | ١ |
| <br>4 | l |
|       |   |

Facciamo

| s                | ecure Communications   | ×             |
|------------------|--|---------------|
|                  | Require secure channel (SSL)   | 1             |
|                  | Require 128-bit encryption   |               |
|                  | Client certificates  | 1             |
|                  | <ul> <li>Ignore client certificates</li> </ul>   |               |
|                  | C Accept client certificates   |               |
|                  |  |               |
|                  | Enable client certificate mapping  |               |
|                  | Client certificates can be mapped to Windows user<br>accounts. This allows access control to resources using<br>client certificates. | $\mathcal{N}$ |
|                  | Enable certificate trust list  |               |
|                  | Current CTL:   |               |
|                  | New Edit   |               |
|                  | OK Cancel Help   | 1             |
|                  | Fig.14   | _             |
| iamo delle prove | $O_{x}$  |               |
|                  |  |               |
|                  |  |               |
| 0                |  |               |
|                  |  |               |
| N.               |  |               |



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

| The page must be viewed over a secure channel - Microsoft Internet Explorer   | . 🗆 🗙    |
|---|----------|
| File Edit View Favorites Tools Help   | 2        |
| 🌍 Back 🔻 🕥 🖌 📓 🐔 🔎 Search   👷 Favorites 🔇 Media 🥝 🔗   | - »      |
| ddress 🙆 http://r-p-pso-backup 💿 💽 Go   | Links    |
|   | <b>_</b> |
| The page must be viewed over a secure channel   |          |
| The page you are trying to access is secured with Secure Sockets Layer (SSL).   |          |
| Please try the following:   |          |
| <ul> <li>Type https:// at the beginning of the address you are attempting to reach<br/>and press ENTER.</li> </ul>  |          |
| HTTP Error 403.4 - Forbidden: SSL is required to view this resource.<br>Internet Information Services (IIS)   |          |
| Technical Information (for support personnel)   |          |
| <ul> <li>Go to <u>Microsoft Product Support Services</u> and perform a title search for the<br/>words HTTP and 403.</li> </ul>                                    |          |
| <ul> <li>Open IIS Help, which is accessible in IIS Manager (inetmor), and search<br/>for topics titled About Security, Secure Seckets Layer (SSL), and</li> </ul> |          |
| About Custom Error Messages.  |          |
| Done  |          |
| 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:



| Security | Aler   |   |   |                          | ×               |
|----------|--|---|---|--------------------------|-----------------|
| ß        | Information you exchange with this site cannot be viewed or<br>changed by others. However, there is a problem with the site's<br>security certificate. |   |   |                          | r<br>e's        |
|          | ⚠  | The security certificate was issue<br>not chosen to trust. View the cert<br>you want to trust the certifying au | ed by a cor<br>tificate to c<br>uthority. | npany you<br>letermine v | have<br>whether |
|          | 0  | The security certificate date is va   | alid.                                     |                          |                 |
|          | 0  | The security certificate has a vali<br>of the page you are trying to view                                       | id name ma<br>v.                          | atching the              | name            |
|          | Doy  | ou want to proceed?   |   |                          |                 |
|          |  | Yes No  | View Ce                                   | ertificate               |                 |
|          |  | Fig.16  |   |                          | $\sim$          |

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, pocihe' una CA Enterprise richiede l'utilizzo di utenti registrati in AD.