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.

	ite Properties			? ×
Web Site Director	ISAPI Fi y Security	lters Aome Dire HTTP Headers	ectory Documents	
Anonymou	s access and auth	entication control		
\$	Enable anonymo authentication m	ous access and edit the nethods for this resource.	Edit	
- IP address	and domain name	restrictions		
	Grant or deny ar IP addresses or	ccess to this resource usir internet domain names	ng	
S.		n norres, section in realized.	Edit	
Secure co	mmunications			
~0	 Require secure enable client ce 	communication and rtificates when this	Server Certificate	
	resource is acce	essed.	View Certificate	
			Edit	
			Edit	
			Edit	

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 <u>www.agensportregionelazio.it</u> 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.

📙 certreq.txt - Notepad	
File Edit Format View Help	
HBEGIN NEW CERTIFICATE REQUEST MIIDQZCCAqwCAQAwaDEXMBUGALUEAXMOdGltcm0XN3YwM3cwNDEXDjAMBgNVBA BVJQUFNPMRAwDgYDVQQKEwdUSU0gU1BBMQ0wcwyDVQQHEwRSb21hMQ8wDQYDVQ EwZJdGFsaWExCZAJBgNVBAYTAklUMIGFMA0GCSqGSIb3DQEBAQUAA4GNADCBiC gQDgtjuHxdivauH0YKu1NmVKIM9vS99NU0wFsg7iZyRCOITZydejudMSXjfTFA 02IdAuggUb1D2pJ7ulhLRv7FkBuiJW+vfomOotZZPtEL7xsjUbBqNE11zygHJ3 ufQjDNpuXp+Z+36hr6tt8EILqSmjjUhQLJIdGU80gbpg/wIDAQABoIIBmTAaBo BgEEAYI3DQIDMQWCjUUMS4yNjAwLjIwewYKKWYBBAGCNWIBDjFtMGSwDgYDVF AQH/BAQDAgTWMEQGCSqGSIb3DQEJDwQ3MDUWDgYIKOZINvCNAWICAgCAMA4GCC SIb3DQMEAgIAgDAHBgUrDgMCBZAKBggqhkiG9w0DBZATBgNVHSUEDDAKBggrBo BQCDATCB/QYKKWYBBAGCNW0CAjGB7jCB6wIBAR5aAE0AaQBjAHIAbWBZA68A20 ACAAUgBTAEEAIABTAEMAAABhAG4AbgBlAGWAIABDAHIAeQBwAHQAbwBnAHIAYO AGgAaQBjACAAUABYAG8AdgBpAGQAZQBYA4GJAJ/4RhOTTKR5uxCCU3ASUY9IBY B81M0dt4ceNEw6MrxUMBbRUbwtoqKT/IPEOK+uEtanHaJv+xp1hZc9jbjVPNJT IRbVGxy89x6D3j6ScVBw0LwaEXlEf9aqTXBNZSWDnzo8WTAD0AUKGx10XiR2fr yzkUSGYZhEXYCLANAAAAAAAAAAAWDQYJKOZINvCNAQEFBQADGYEAKKVKNKD4TG 9W1Wk1tx/18RjDgf0AEU3L10vqAy76skNHSbidvtFDonJ+YhS1iVXA07VKfBX2 Hb65fpIFYJiY03G6w4vr+1K/vTPeFMu8A01h3Tw23NlcNcHy0xqotGGtIUU1G0 7mSQ0/4FSDS1zkk2gFlC5eslEzgrKB8= END NEW CERTIFICATE REQUEST	AST QQI QXB AZF 3Zt 3GOP CQG GEF GB0 QBW (t2 Cq/ TaP SV+ 27q ddJ

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.

📴 Certification Authority	
<u>File</u> <u>Action</u> <u>View</u> <u>H</u> elp	
← → 🗈 🖪 🗗 🕄	
Certification Authority (Local)	Request ID Requester Name
E 😨 Settore RPPSO	8 R-P-P5O-02\IUSR_R-P-P5O
Revoked Certificates	
Pending Requests	
Failed Requests	
I	

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 II link sotto riportato.



<u>Create and submit a request to this CA.</u> server per creare un nuovo certificate da zero. <u>Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a</u> <u>renewal request by using a base-64-encoded PKCS #7 file.</u> Serve per creare un certificato inserendo la stringa BASE64. Clicchiamo su questo link per procedere nella richiesta del certificato.

🖉 Microsoft Certifica	ate Services - Microsoft Internet Explorer	<u>- 🗆 ×</u>
File Edit View F	avorites Tools Help	-
🕞 Back 🔹 🕥 🗸	💌 💈 🏠 🔎 Search 🤺 Favorites 🔇 Media 🥝	»
Address 🕘 http://r-p	-pso-02/certsrv/certrqxt.asp 🗾 🕞 Go	Links
		_
Microsoft Certific	ate Services Settore RPPSO <u>Ho</u>	me
Submit a Certi	ficate Request or Renewal Request	-
To submit a sav or PKCS #10 c generated by ar Request box.	red request to the CA, paste a base-64-encoded CM ertificate request or PKCS #7 renewal request n external source (such as a Web server) in the Save	IC d
Saved Request:		
Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):	yzkUSGYZhEXYCLANAAAAAAAAAAAAAAAAAAAAAA 9W1WK1tx/18RjDGfOAEU3L1OvqAy76skNHSbidvt Hb65fpIFYJiYo3G6w4vr+1K/vTPeFMu8AO1h3Tw2 7mSQ0/4FSDs1zkk2gF1C5es1EzgrKB8= END NEW CERTIFICATE REQUEST	
Additional Attribu	ites:	
Attributes:		_
٢	📃 🛛 😽 Local intranet	

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

Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
😋 Back 🔹 🕥 🖌 📓 🐔 🔎 Search 👷 Favorites 📢 Media 🚱 🔗 💌
Address 🕘 http://r-p-pso-02/certsrv/certfnsh.asp
Microsoft Certificate Services Settore RPPSO Home
Certificate Pending
Your certificate request has been received. However, you must wait for an administrator to issue the certificate you requested.
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
ど Done

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.

📴 Certification Authority				
Eile Action View Help				
Certification Authority (Local)	R Binar	y Request Stat.	Request Dispo	Request Submission Date
E Settore RPPSO	📴 9 I	3 The operation	Taken Under	29/07/2004 15.01
Issued Certificates	10	3 The operation	Taken Under	30/07/2004 12.37
Pending Requests				
	•			Þ

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.

🚰 Microsoft Certificate Services - Microsoft Internet Explorer 📃	
File Edit View Favorites Tools Help	2
🌀 Back 👻 🌍 🔹 👔 🌈 Search 🤸 Favorites 🔇 Media 🍕) »
Address 🙆 http://r-p-pso-02/certsrv/	Links
For more information about Certificate Services, see <u>Certificate</u> <u>Services Documentation</u> . Select a task:	_
Request a certificate	
View me status of a pending certificate request	
Download a CA certificate, certificate chain, or CRL	
🦉 🛛 😽 Local intranet	

Microsoft Cer	rtificate Services - Microsoft Internet Explorer	
File Edit Vie	w Favorites Tools Help	2
G Back 👻 🕘	📎 - 💌 😰 🏠 🔎 Search 🤺 Favorites 📢 Media 🧭 😒 🎍	»
Address 🙆 http	p://r-p-pso-02/certsrv/certcarc.asp	Links
CA certificat	e:	
	Current [Settore RPPSO]	
Encoding me	ethod:	
	© DFR	
	O Base 64	
Download (CA certificate	
Download	OA contificate chain	
Download I	latest base CRL	
		-
Ē	Second	

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**.

Certificate	? ×
General Details Certification Path	
Certification path	
	View Certificate
Certificate status:	
This certificate is OK.	
	ОК

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.

Secure Communications
Require secure channel (SSL)
Require 128-bit encryption
Client certificates
Ignore client certificates
C Accept client certificates
C Require client certificates
Enable client certificate mapping
Client certificates can be mapped to Windows user accounts. This allows access control to resources using client certificates.
Enable certificate trust list
Current CTL:
New Edit
OK Cancel Help

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.

🚰 The page must be viewed over a secure channel - Microsoft Internet Explorer	
File Edit View Favorites Tools Help	2
🕞 Back 🔹 📀 - 💌 😰 🏠 🔎 Search travorites 🔇 Media 🤗 🔗	• »
Address 🙆 http://r-p-pso-backup 🔽 🄁 Go	Links
	-
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: Type https:// at the beginning of the address you are attempting to reach and press ENTER. 	
HTTP Error 403.4 - Forbidden: SSL is required to view this resource. Internet Information Services (IIS)	
Technical Information (for support personnel)	
 Go to <u>Microsoft Product Support Services</u> and perform a title search for the words HTTP and 403. 	
 Open IIS Help, which is accessible in IIS Manager (inetmgr), and search for topics titled About Security, Secure Sockets Layer (SSL), and About Custom Error Messages. 	
	-
🕘 Done 📃 📃 📢 Local intranet	//.

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.

🚡 Console1 - [Console Root\Certificates - Current User\Trusted Root Certification 💶 🗖 🗙				
📸 File Action View Favorites Window	Help	_ 8 ×		
← → 🗈 📧 💼 🗗 🛱 😫				
Console Root Certificates - Current User Certificates - Current User Certificates - Current User Certificates Certificate Enrollment Requests	Issued To A ABA.ECOM Root CA Autoridad Certificadora de la Asoci Autoridad Certificadora del Colegi Baltimore EZ by DST Belgacom E-Trust Primary CA CAW HKT SecureNet CA Class A CAW HKT SecureNet CA Class B CAW HKT SecureNet CA Class B CAW HKT SecureNet CA SGC Root CA 1 Certiposte Classe A Personne Certiposte Classe A Personne Certiposte Serveur Certipicade Certificador	Issued By ABA.ECOM ABA.ECOM Autoridad (Baltimore E Belgacom E C&W HKT 5 C&W HKT 5 C&W HKT 5 C&W HKT 5 C&W HKT 5 CA 1 Certiposte Certiposte Certiposte Certisign -		
	Certisign Autoridade Certificadora	Certisign A 🚽		
Trusted Root Certification Authorities store contains 109 certifica				



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	Р	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.