Utilizzo di Certificati SSL e relative implicazioni

Affinché possano essere correttamente stabilite delle connessioni cifrate tramite i protocolli SSL/TLS ai servizi di IceWarp, è necessario che sul server sia installato un certificato.
Per dotare il server di un certificato si può procedere in due modalità:

- Generare autonomamente un proprio certificato senza alcun costo
- Acquistare un certificato rilasciato da una delle autorità di certificazione riconosciute (es: GeoTrust, VeriSign, GlobalSign, Thawte, ecc.)

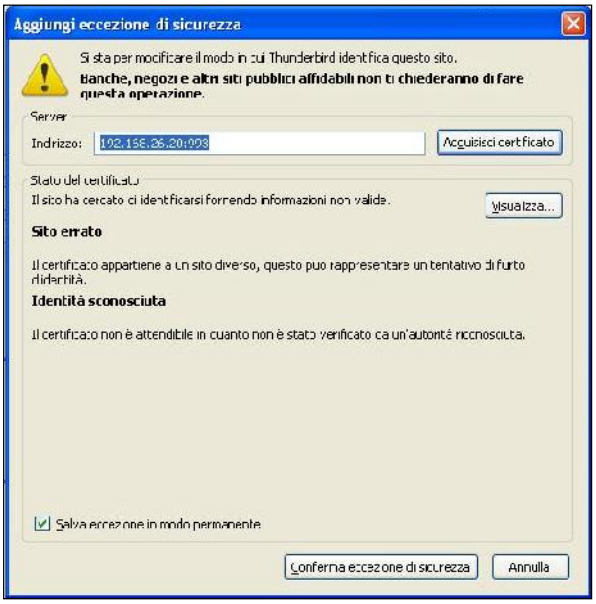
Certificati auto-generati

La differenza pratica nell'utilizzo di un certificato auto-generato, invece di uno rilasciato da un'autorità di certificazione, risulta chiara ad esempio quando si tenta di accedere in HTTPS alla pagina di un qualsiasi sito Web definito su IceWarp Server, richiedendo quindi che il trasferimento dei contenuti avvenga in modalità cifrata tramite SSL. Il browser utilizzato per visualizzare la pagina avviserà l'utente della presenza, sul server che ospita il sito, di un certificato che non è possibile ricondurre a nessuna delle autorità note (ovvero a nessuna delle autorità presenti nella lista di certificati in dotazione al browser).

L'utente dovrà perciò a questo punto scegliere fra abbandonare il sito oppure proseguire nella navigazione, ritenuta potenzialmente non sicura. Alcuni browser (ad esempio IE) propongono solo la possibilità di proseguire nella navigazione in quel determinato momento mentre altri browser (ad esempio Mozilla Firefox) consentono di proseguire solo previa generazione di un'eccezione di sicurezza aggiungendo la possibilità di far acquisire il certificato al browser così che il potenziale rischio non venga mai più notificato.

FAST*flow* S.r.l. – IceWarp Italia
Via A. Manzoni, 25 – 22040 Lurago d'Erba (CO)
Tel. 031-697457, Fax: 031-2280459
e-mail: info@icewarp.it - web: www.icewarp.it

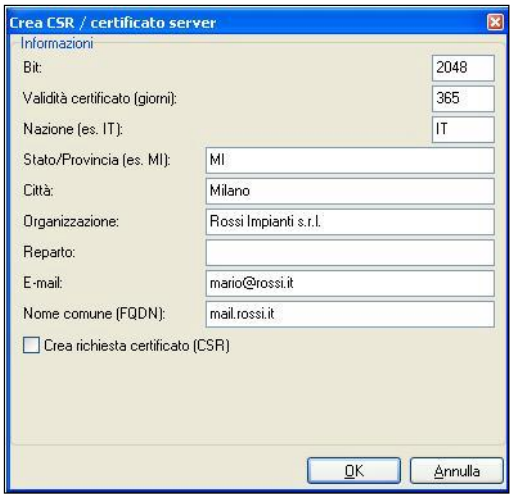
La stessa situazione viene notificata anche da un qualsiasi client di posta elettronica qualora si tenti di configurare un account in modo da stabilire connessioni ai servizi in SSL o TLS.



FAST*flow* S.r.l. – IceWarp Italia
Via A. Manzoni, 25 – 22040 Lurago d'Erba (CO)
Tel. 031-697457, Fax: 031-2280459
e-mail: info@icewarp.it - web: www.icewarp.it

Definizione di un proprio certificato (auto-certificazione)

Per definire un proprio certificato è sufficiente accedere alla sezione certificati, fare clic su "Crea CSR / certificato server" e immettere i dati nella maschera che viene presentata, senza selezionare la casella "Crea richiesta certificato".



Dopo aver definito il certificato verrà proposta la possibilità di impostarlo come predefinito e pertanto renderlo ineliminabile.

In caso la scelta sia negativa il certificato verrà comunque salvato nella cartella *<IceWarp_root>\config_certs\private* e sarà poi possibile aggiungerlo associandolo ad uno specifico indirizzo IP.

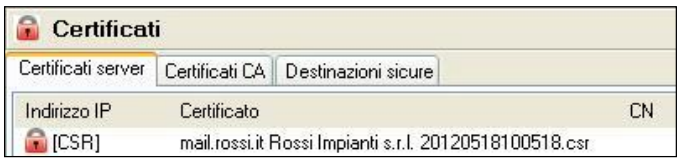
FAST*flow* S.r.l. – IceWarp Italia
Via A. Manzoni, 25 – 22040 Lurago d'Erba (CO)
Tel. 031-697457, Fax: 031-2280459
e-mail: info@icewarp.it - web: www.icewarp.it

Acquisto di un nuovo certificato da un'autorità di certificazione riconosciuta

Il primo passo per l'acquisto di un certificato è la definizione di un file di richiesta CSR procedendo come per la definizione di un proprio certificato ma al contempo selezionando la casella “Crea richiesta certificato (CSR)” la quale consente appunto di creare un file nel formato *CSR* che, opportunamente sottoposto ad un'autorità di certificazione, permetterà di ottenere un certificato SSL.
La richiesta CSR verrà elencata nella sezione Certificati e i rispettivi file .csr e .key verranno salvati nella cartella *<IceWarp_root>\config_certs\csr*.
Il file con suffisso .key è di fondamentale importanza e deve essere conservato con cura per l’utilizzo futuro, in quanto contiene la **chiave privata** sulla base della quale l'autorità di certificazione emetterà il certificato attuale ed eventuali futuri rinnovi dello stesso.

Le procedure per l’ottenimento del certificato variano leggermente a seconda del fornitore, ma generalmente occorre presentare la richiesta CSR e alcuni altre informazioni, finalizzate ad attestare il proprio diritto di chiedere e ottenere un certificato per il nome o dominio indicato.
Il certificato può essere offerto in alcuni formati differenti, a seconda del software su cui verrà installato. IceWarp Server utilizza il formato standard X.509, all’interno di file .crt (o .pem), che potrebbe essere indicato come destinato all’uso con OpenSSL.
Certificati in altri formati possono essere eventualmente convertiti con le utility fornite da OpenSSL o con procedure indicate dalla stessa autorità di certificazione.

Una volta ottenuto il file di certificato .crt, esso andrà importato facendo doppio clic sulla CSR precedentemente creata nella console di amministrazione di IceWarp Server.



La procedura provvederà automaticamente a recuperare la chiave privata utilizzata per la richiesta CSR e la unirà al certificato appena ottenuto, in modo da renderlo operativo.
Molto spesso le autorità di certificazione, oltre al certificato richiesto, forniscono al cliente anche uno o più **certificati intermedi**, necessari per ricostruire l'intera catena di certificazione.

Il proprio certificato e i certificati intermedi indicati, andranno uniti in un unico file .crt utilizzando un semplice editor di testo, prima di importarlo in IceWarp Server con la suddetta procedura. Nel comporre il file si dovrà andare in ordine gerarchico crescente, dall’elemento più specifico (il proprio certificato acquistato) a quello più generale (spesso un certificato principale dell’autorità di certificazione, “*CA Root Certificate*”). Le autorità di certificazione forniscono generalmente indicazioni sulla corretta sequenza dei certificati intermedi e alcune forniscono un unico file che li contiene tutti nell’ordine previsto.

FAST*flow* S.r.l. – IceWarp Italia
Via A. Manzoni, 25 – 22040 Lurago d’Erba (CO)
Tel. 031-697457, Fax: 031-2280459
e-mail: info@icewarp.it - web: www.icewarp.it

Il file risultante da importare in IceWarp Server dovrà pertanto avere una struttura simile alla seguente:

```
-----BEGIN CERTIFICATE-----

Certificato acquistato

-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----

Certificato intermedio 1

-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----

Certificato intermedio 2

-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----

Certificato CA

-----END CERTIFICATE-----
```

Rinnovo di un certificato fornito da un'autorità di certificazione riconosciuta

Alla scadenza del periodo di validità del certificato acquistato, generalmente le autorità di certificazione prevedono procedure semplificate di rinnovo, che richiedono una semplice conferma da parte del titolare. Raramente è necessario presentare una nuova richiesta CSR.
Di norma il nuovo certificato viene quindi rilasciato sulla base delle stesse informazioni utilizzate per la richiesta CSR originale e quindi, cosa fondamentale, sulla base della stessa **chiave privata** utilizzata per il primo certificato, di cui si dovrà disporre per applicare e utilizzare il certificato rinnovato.

L'operazione di inserimento nel Server IceWarp del certificato rinnovato differisce dalla prima attivazione, in quanto nella console di amministrazione non avremo a disposizione la CSR in sospeso alla quale associare il nuovo certificato. Occorrerà procedere manualmente alla composizione di un file .pem completo, in maniera molto simile a quanto visto in precedenza, ma con l'aggiunta in testa al file della chiave privata.

Il file risultante da importare in IceWarp Server in sostituzione di quello scaduto, dovrà pertanto avere una struttura simile alla seguente:

```
-----BEGIN PRIVATE KEY-----

Chiave privata creata in origine

-----END PRIVATE KEY-----
-----BEGIN CERTIFICATE-----

Certificato acquistato

-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----

Certificato intermedio 1

-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----

Certificato intermedio 2

-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----

Certificato CA

-----END CERTIFICATE-----
```

Se si ha difficoltà a reperire la chiave privata o non è stata conservata dopo la richiesta originale, è comunque possibile estrarla facilmente dal file .pem del certificato appena scaduto o da uno ancora precedente. La chiave privata, infatti, non varia e non ha scadenza.
Se proprio la chiave privata non fosse più reperibile in alcun modo, il nuovo certificato sarà inutilizzabile e occorrerà contattare il fornitore per una eventuale procedura di ri-emissione, con le stesse modalità della richiesta originale.
Poiché i certificati vengono generati sulla base della chiave privata utilizzata per firmare la richiesta CSR originale, infatti, non è possibile creare semplicemente una nuova chiave privata, in quanto non troverà corrispondenza con il certificato.

In caso di non corrispondenza o assenza della chiave privata, il motore SSL non potrà essere avviato e i servizi del server IceWarp saranno disponibili soltanto “in chiaro” e non in modalità cifrata SSL/TLS.
Di questo genere di problemi è riportata evidenza nel log degli Errori.