



SSL Secure Socket layer

Di Massimiliano Brolli

Nome documento	Versione documento	Ultima revisione	Note eventuali	Autore
SSL Secure Socket layer	01.00	10/10/2003	nd	Brolli Massimiliano

Modalità di instanziamiento di una connessione

In questo documento viene riassunto la modalità di messaggi 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.

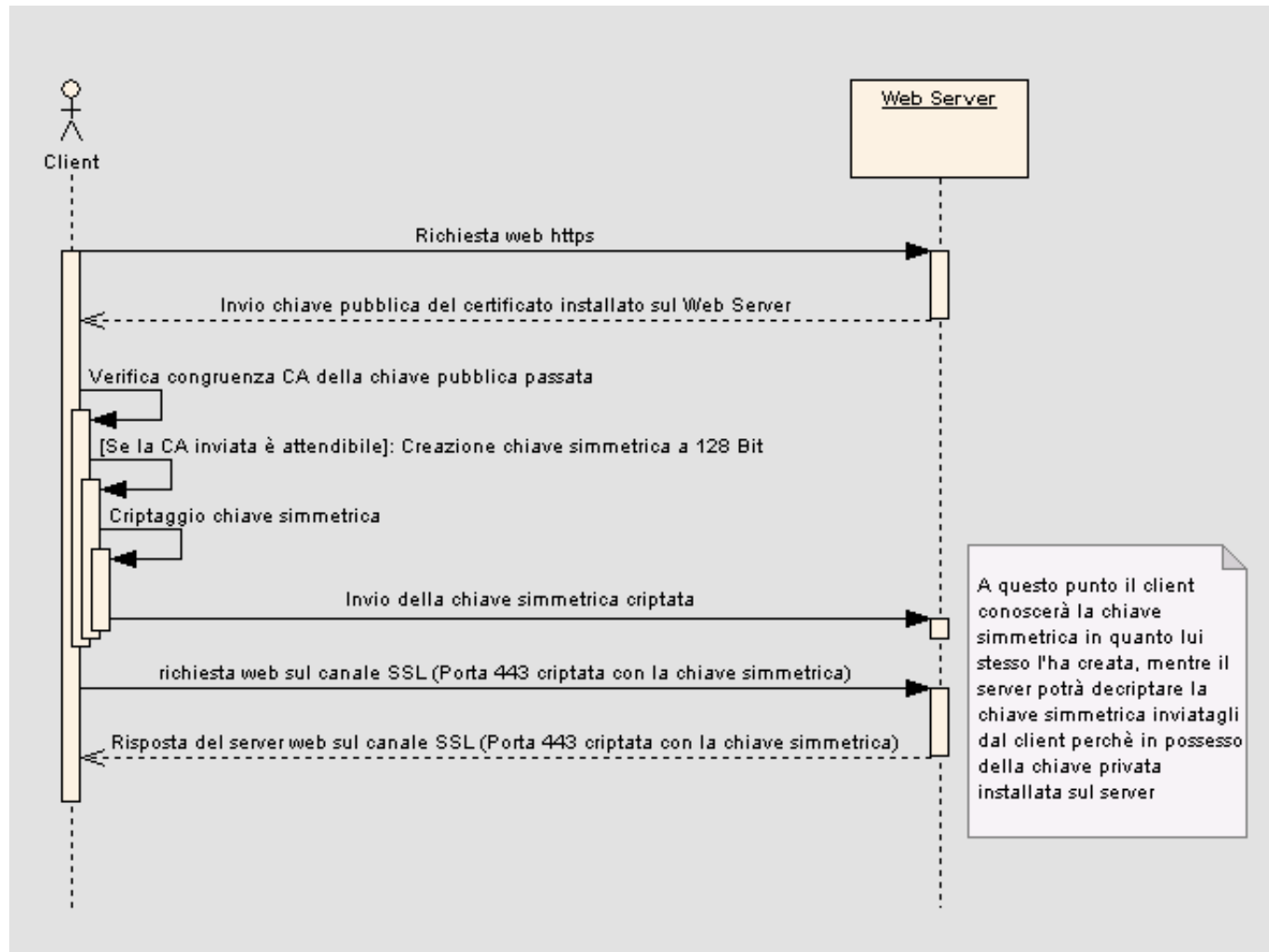
Nome documento	Versione documento	Ultima revisione	Note eventuali	Autore
SSL Secure Socket layer	01.00	10/10/2003	nd	Brolli Massimiliano

Esempio di dialogo tra un client ed un 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 pocanzi ha inviato al client e disponendo della sua specifica **chiave privata** la decripta.
7. 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.
8. Inizia la connessione in SSL

Nome documento	Versione documento	Ultima revisione	Note eventuali	Autore
SSL Secure Socket layer	01.00	10/10/2003	nd	Brolli Massimiliano

Diagramma delle iterazione sulla connessione SSL

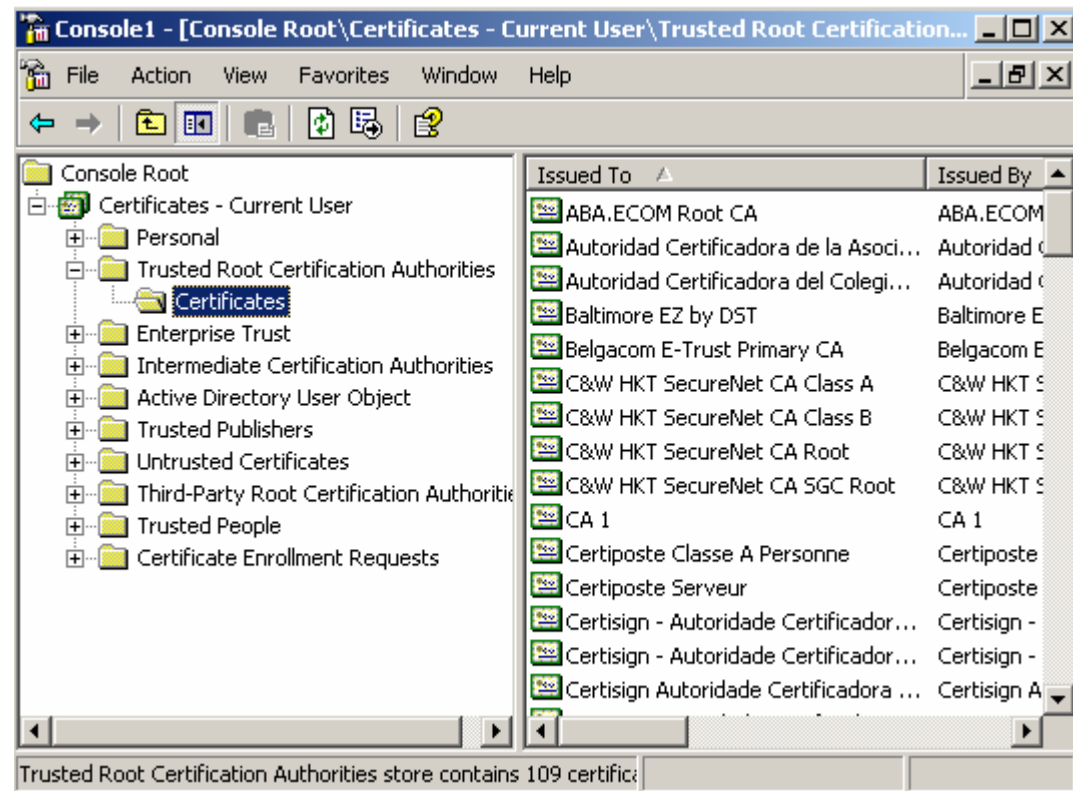


Nome documento	Versione documento	Ultima revisione	Note eventuali	Autore
SSL Secure Socket layer	01.00	10/10/2003	nd	Brolli Massimiliano

Breve analisi del punto 3

Al punto 3 abbiamo visto che il client effettua una verifica del certificato inviato dal server web verificando che colui che l'ha rilasciato sia una CA 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.



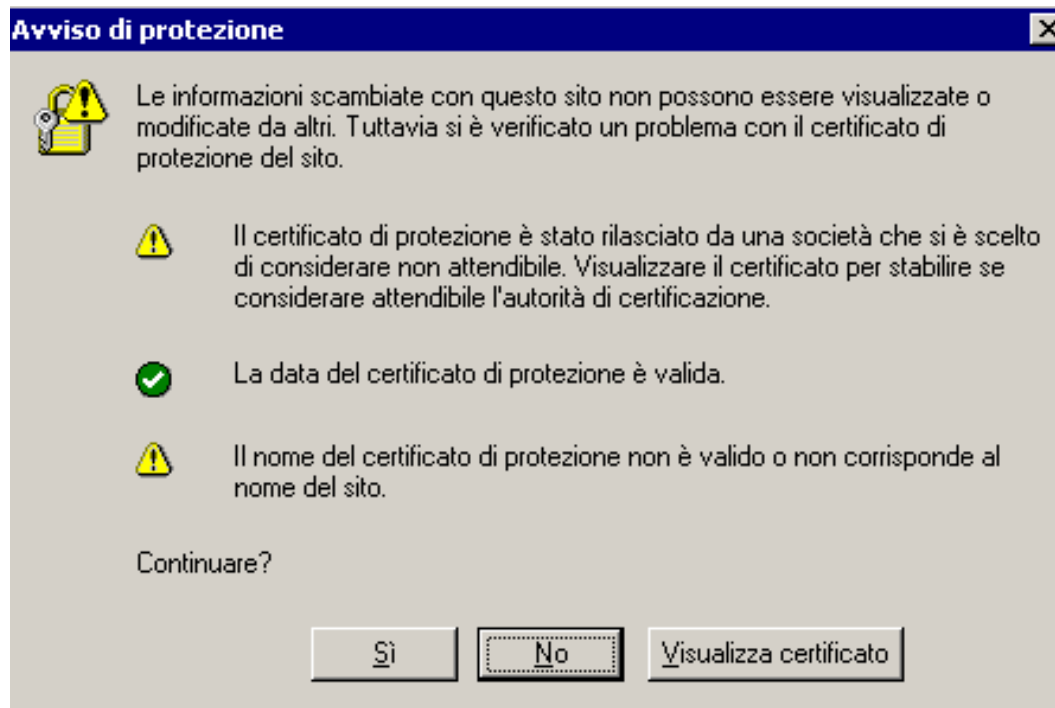
Nome documento	Versione documento	Ultima revisione	Note eventuali	Autore
SSL Secure Socket layer	01.00	10/10/2003	nd	Brolli Massimiliano

Avviso di protezione

Nel caso in cui l'ente certificatore non sia presente verrà mostrata la maschera seguente

che vi 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



Nome documento	Versione documento	Ultima revisione	Note eventuali	Autore
SSL Secure Socket layer	01.00	10/10/2003	nd	Brolli Massimiliano

Sniffing packet SSL

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

SSL (secure Socket Layer) è un protocollo che permette l'invio di pacchetti criptati in Internet ed possibile "abbinarlo" al normale HTTP per avere maggior sicurezza sul traffico prodotto dal server e dal client.

Il sistema come da figura precedente lavora su una porta differente da quella http standard (**Porta 80**) ma di solito sulla porta **443**.

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**.

Nome documento	Versione documento	Ultima revisione	Note eventuali	Autore
SSL Secure Socket layer	01.00	10/10/2003	nd	Brolli Massimiliano