GlobalTrust®
Securing the Globe

User Guide

Guida tecnica ai certificati SSL

User Guide

SU COSA SI BASANO I CERTIFICATI DIGITALI

I certificati sono basati su un sistema di **crittografia a chiave asimmetrica o pubblica.**

Che cos' è la Crittografia? E come viene applicata?

La crittografia è la *scienza che si occupa di sviluppare metodi crittografici, ossia metodi finalizzati a nascondere il contenuto di un messaggio tramite l' uso di un "algoritmo" e di una "chiave". La crittografia moderna si divide in due branche fondamentali: la* **crittografia a chiave simmetrica** *e la* **crittografia a chiave asimmetrica**.

Crittografia a chiave simmetrica o segreta.....

Nella crittografia a chiave segreta (o comunemente chiamata "crittografia simmetrica") sono due i componenti fondamentali:

- ***Algoritmo/funzione di cifratura:*** *procedura che* trasforma *il messaggio originale (messaggio in chiaro) in messaggio cifrato.*
- ***Chiave segreta (password o parola segreta):*** *è nota soltanto al mittente ed al destinatario del messaggio*

È importante sottolineare il fatto che algoritmo e chiave sono imprescindibili in quanto la trasformazione da messaggio in chiaro a messaggio cifrato (cifratura) è soltanto un procedimento che, per essere attuato, ha bisogno di un'informazione ulteriore (la chiave), da cui dipende fortemente il risultato.

Per decifrare il messaggio (decifratura), quindi, non basta conoscere l'algoritmo di cifratura utilizzato, ma è necessario conoscere anche la chiave (*vedi figura 1).*

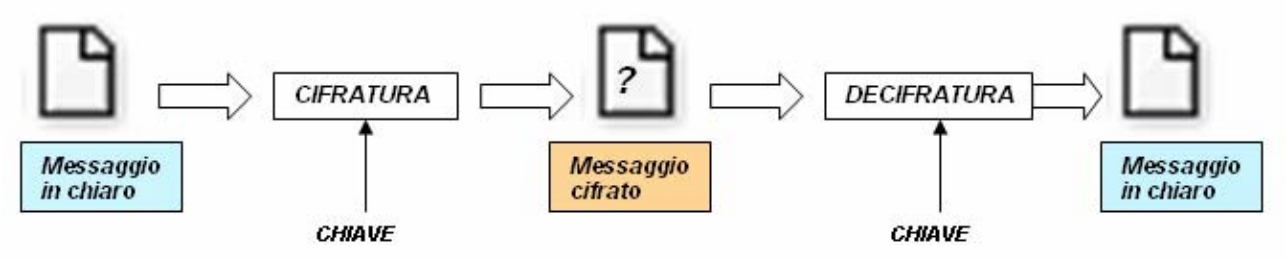
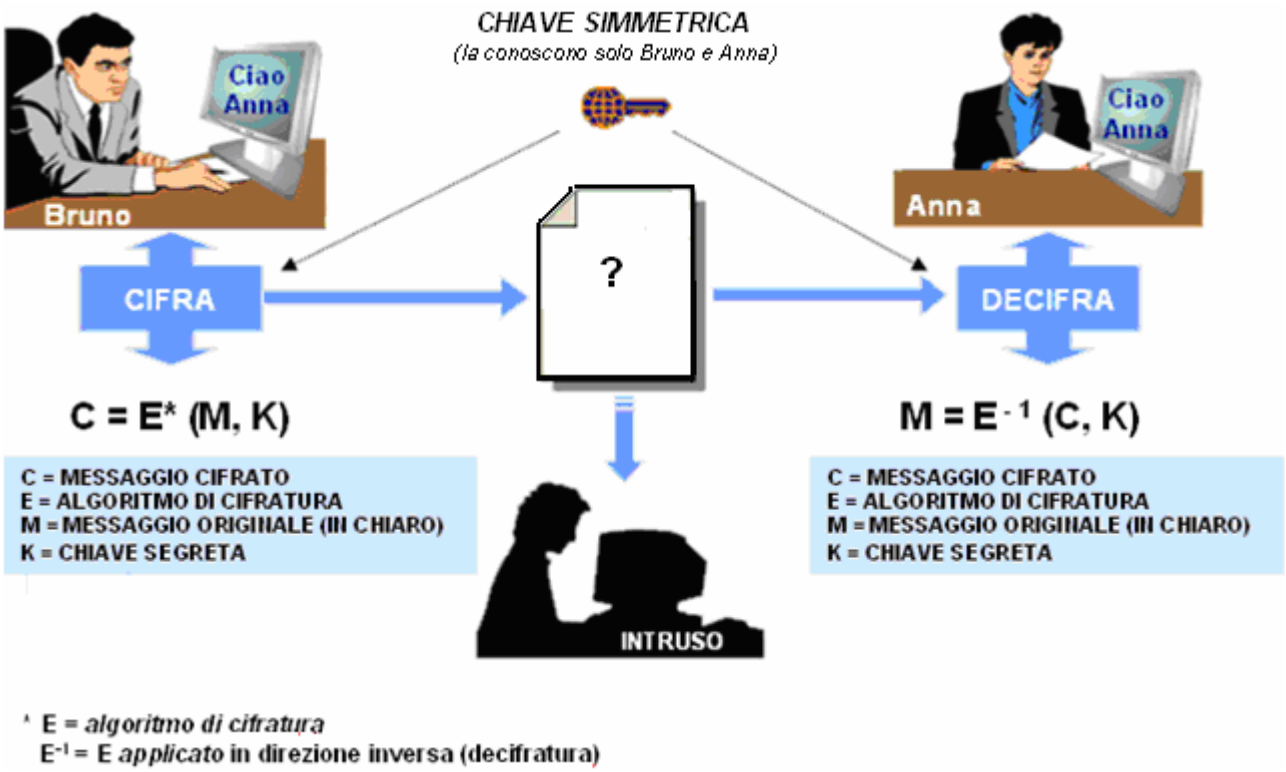


FIGURA 1. Crittografia simmetrica

GlobalTrust Italia S.p.A.
Piazza San Pietro, 2 – 05100 Terni Phone: +39.0744. 441214 Fax: +39.0744. 460269
E-mail: info@globaltrust.it - http://www.globaltrust.it Cap. Soc. € 2.750.000 i.v. REA 89371 P.I .01339760553



Il grosso problema di questo approccio è però la **distribuzione delle chiavi***: se due interlocutori vogliono usare un algoritmo di questo tipo per comunicare in modo sicuro devono prima accordarsi in qualche modo sulla chiave, per esempio vedendosi di persona. Dato che il canale che usano per la trasmissione dei messaggi non è sicuro (altrimenti non avrebbero bisogno di cifrarli), non possono infatti utilizzarlo per trasmettere la chiave. Alcuni algoritmi di questo tipo utilizzati ancora oggi sono:DES e 3-DES.*

Crittografia a chiave asimmetrica o pubblica.....

Il problema della distribuzione delle chiavi è stato risolto in tempi relativamente recenti (anni Settanta) con l'invenzione della crittografia a chiave pubblica*. Con algoritmi di questo tipo ognuno ha due chiavi:*

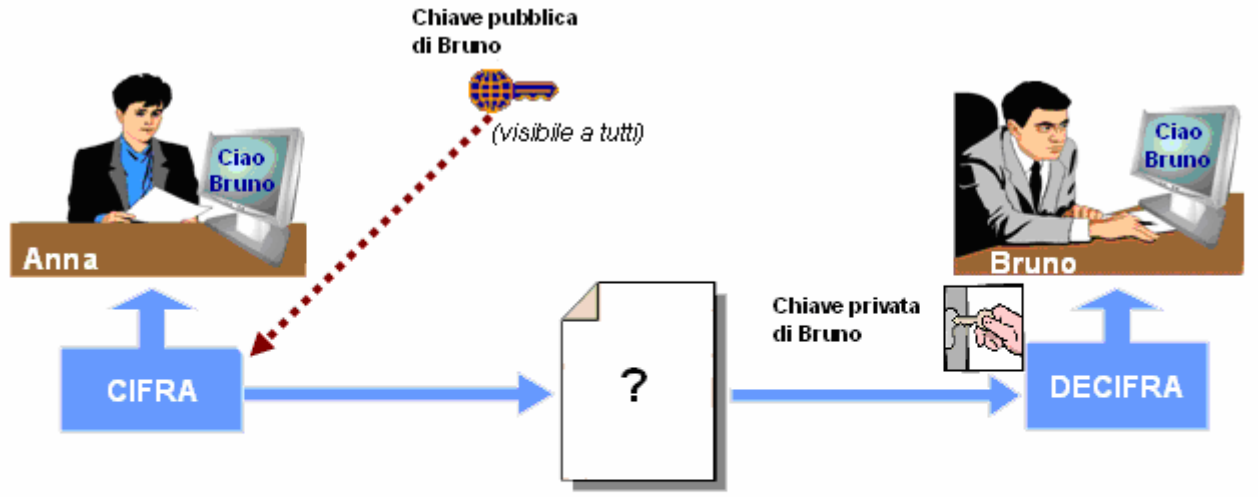
- **Una pubblica** da distribuire a tutti quelli con cui vuole comunicare
- **Una privata** da tenere segreta.

Ciò che viene cifrato con la chiave pubblica (operazione che può essere fatta da chiunque) può essere decifrato solo con la chiave privata corrispondente (operazione che può essere fatta solo dal proprietario della chiave): in questo modo non c'è più il problema di comunicare segretamente la chiave, perché questa è nota a tutti; per comunicare in modo sicuro con una persona basta cifrare il messaggio con la sua chiave pubblica, come illustrato in figura

GlobalTrust Italia S.p.A.
Piazza San Pietro, 2 – 05100 Terni Phone: +39.0744. 441214 Fax: +39.0744. 460269
E-mail: info@globaltrust.it - http://www.globaltrust.it Cap. Soc. € 2.750.000 i.v. REA 89371 P.I .01339760553

2. Gli algoritmi di questo tipo sono detti a chiave asimmetrica*, e il più noto tra essi è probabilmente RSA.*

FIGURA 2. Crittografia Asimmetrica



- **Anna** deve inviare dei dati riservati a Bruno
- **Anna** cifra i dati utilizzando la chiave pubblica di Bruno (visibile a tutti)

- **Bruno** decodifica il messaggio cifrato da Anna, utilizzando la sua chiave privata (chiave segreta, unica chiave in grado di decifrare il messaggio)

GlobalTrust Italia S.p.A.
Piazza San Pietro, 2 – 05100 Terni Phone: +39.0744. 441214 Fax: +39.0744. 460269
E-mail: info@globaltrust.it - http://www.globaltrust.it Cap. Soc. € 2.750.000 i.v. REA 89371 P.I .01339760553

Come fa il mittente a trovare la chiave pubblica del destinatario?

Mittente e destinatario possono inviarsi le loro chiavi pubbliche tramite e-mail, telefono, fax, posta, possono incontrarsi di persona, ecc.

Che cosa succede se qualcun altro vede la chiave pubblica?

Nessun problema; è pubblica!

Problemi di questo metodo

La cifratura e la decifratura a chiavi pubbliche sono molto dispendiose in termini computazionali. La cifratura di messaggi lunghi, infatti, è molto lenta.

La soluzione a questo problema è stata:

Combinare la cifratura a chiave simmetrica e la cifratura a chiave pubblica.

La chiave "simmetrica" è veloce e robusta (se la chiave è lunga)

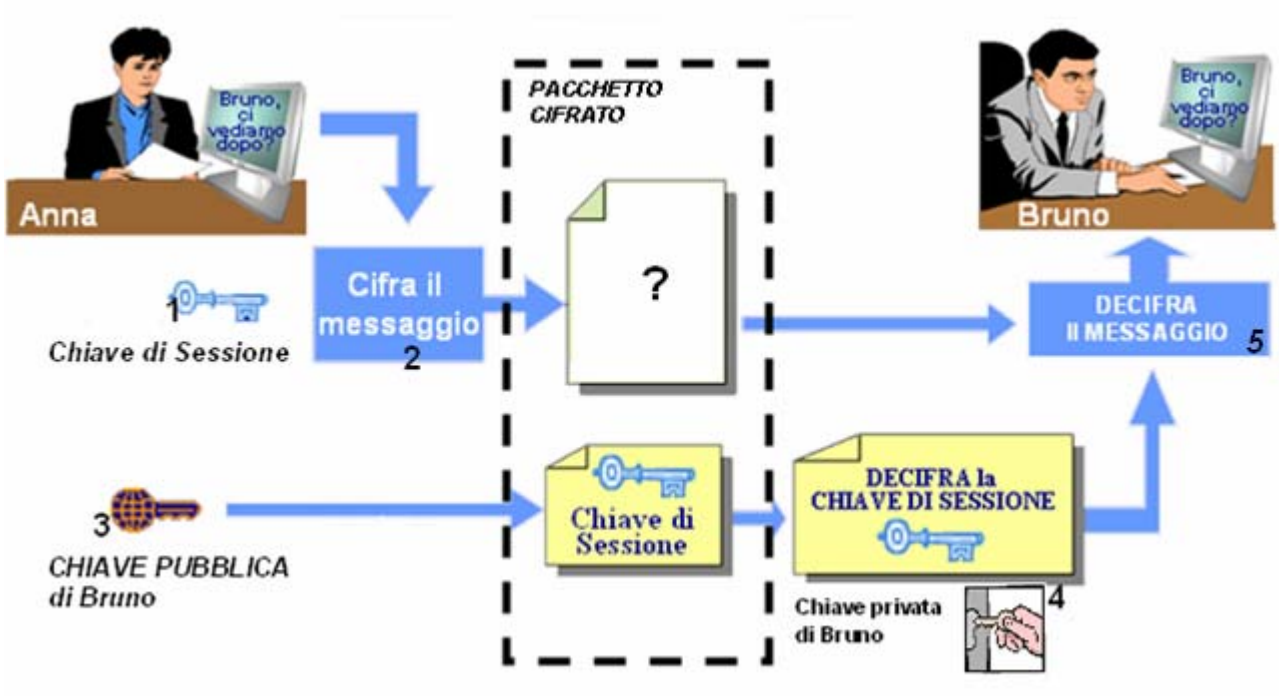
La chiave "pubblica" è valida per lo scambio delle chiavi.

Vediamo come vengono combinate....

- Generiamo una chiave simmetrica, utilizzabile una sola volta (**chiave di sessione**)
- Cifriamo il messaggio con la chiave di sessione
- Cifriamo la chiave di sessione con la chiave pubblica del destinatario

GlobalTrust Italia S.p.A.
Piazza San Pietro, 2 – 05100 Terni Phone: +39.0744. 441214 Fax: +39.0744. 460269
E-mail: info@globaltrust.it - http://www.globaltrust.it Cap. Soc. € 2.750.000 i.v. REA 89371 P.I .01339760553

Dimostrazione:



1. *Viene generata in maniera randomica una chiave di sessione.*
2. *Anna utilizza la suddetta chiave per cifrare il messaggio che deve inviare a Bruno*
3. *Bruno non è in grado di decifrare il messaggio senza conoscere la chiave di sessione utilizzata da Anna. Per questo motivo Anna invia sia il messaggio cifrato, sia la chiave di sessione. Quest' ultima viene cifrata usando la chiave pubblica di Bruno.*
4. *Bruno utilizza la sua chiave privata per conoscere la chiave di sessione.*
5. *Bruno decifra il messaggio utilizzando la chiave di sessione.*

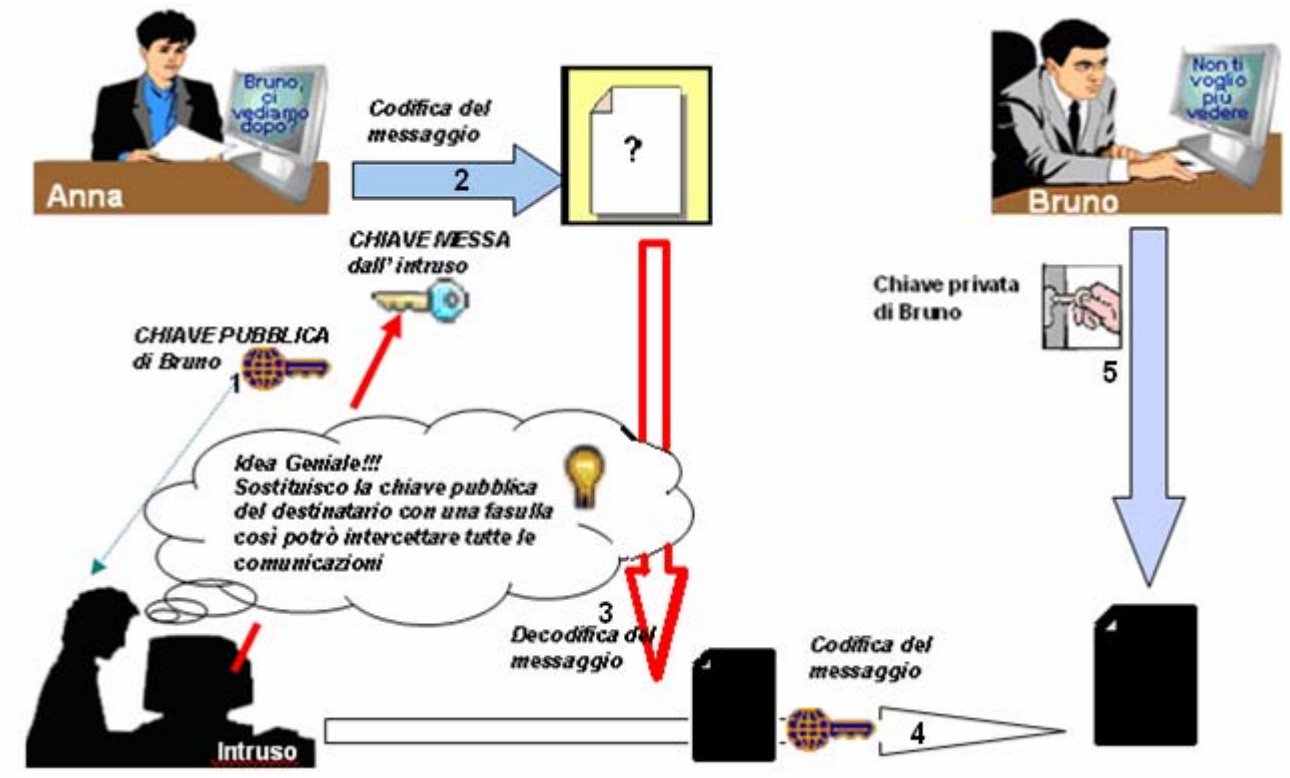
LE SOLUZIONI OFFERTE DAI CERTIFICATI DIGITALI

Un intruso può manomettere una chiave pubblica?

Purtroppo si...

GlobalTrust Italia S.p.A.
Piazza San Pietro, 2 – 05100 Terni Phone: +39.0744. 441214 Fax: +39.0744. 460269
E-mail: info@globaltrust.it - http://www.globaltrust.it Cap. Soc. € 2.750.000 i.v. REA 89371 P.I .01339760553

Vediamo in pratica cosa può accadere...



1. *Un intruso sostituisce la chiave pubblica di Bruno con la sua.*
2. *Anna cifra il messaggio utilizzando la chiave pubblica di Bruno (in realtà è la chiave dell' intruso)*
3. *L' intruso è in grado, quindi, di decifrare il messaggio. Prepara quindi un nuovo messaggio (messaggio alterato) da inviare.*
4. *L' intruso invia il nuovo messaggio a Bruno, cifrandolo utilizzando la "vera" chiave pubblica di Bruno.*
5. *Bruno decodifica il messaggio utilizzando la sua chiave privata*

<u>Né Bruno né Anna scopriranno mai niente di quanto è successo</u>

Il problema della sicurezza riguarda tutte le informazioni (e-mail, pagine web) che viaggiano su Internet, comprese tutte quelle riguardanti il commercio elettronico o strettamente collegate ad applicazioni economiche. ***Internet****, infatti,* ***è totalmente anonima*** *e non si può mai sapere con certezza con chi si sta parlando, a chi si stanno inviando informazioni, ecc...*

GlobalTrust Italia S.p.A.
Piazza San Pietro, 2 – 05100 Terni Phone: +39.0744. 441214 Fax: +39.0744. 460269
E-mail: info@globaltrust.it - http://www.globaltrust.it Cap. Soc. € 2.750.000 i.v. REA 89371 P.I .01339760553

Come è possibile risolvere questo problema?

Per risolvere questo problema è necessario trovare un modo per LEGARE una chiave pubblica al suo proprietario. In particolare:

- **la chiave deve essere registrata da un' autorità che gode della fiducia di entrambe le parti**
- **la terza parte "certifica" che la chiave appartiene al proprietario**

la terza parte in questione viene denominata CA (Certification Authority).

Le varie chiavi pubbliche vengono fornite dalla CA sottoforma di **certificati digitali***, i quali vengono firmati e autenticati dalla stessa.*

E' possibile perciò presentare un certificato al proprio interlocutore e questi, fidandosi dell'autorità di certificazione che lo ha emesso, controlla che sia effettivamente valido e così può essere sicuro dell'identità della persona con cui sta dialogando o scambiando informazioni.

Solitamente i certificati digitali vengono emessi per identificare:

- **L' autorità di certificazione:** a tal fine, i certificati dovrebbero essere prevaricati nei browser, cosicché sia possibile riconoscere, come validi, tutti i certificati emessi da quella CA. È consigliabile controllare la lista dei certificati delle CA presenti sul vostro browser, sia esso Microsoft Internet Explorer, Netscape Navigator o altro:
- **Un sito:** in questo caso si parla di **certificati SSL Web Server.** Essi garantiscono che il server che sta rispondendo corrisponde al dominio certificato. Questo tipo di certificati viene usato in genere per effettuare:
  - ✓ Login sicuri per le Intranet
  - ✓ Login sicuri per siti Web
  - ✓ Form di registrazione sicuri
  - ✓ Invio di informazioni dei clienti
  - ✓ Invio di informazioni di pagamento
  - ✓ Prova dell' identità di un business on-line

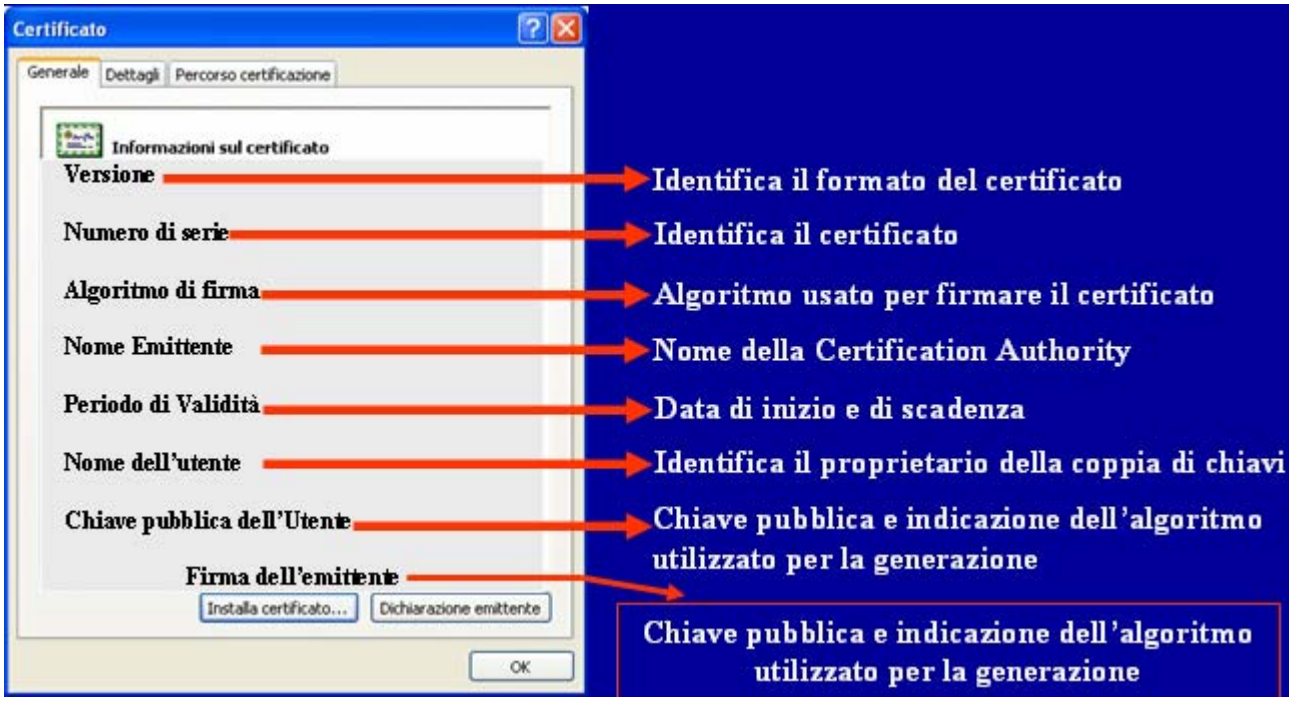
- **Un soggetto:** il certificato contiene informazioni quali nome, cognome, indirizzo, e-mail, ecc.; esso può essere utilizzato per garantire la provenienza di una e-mai, per usufruire di servizi personali, ecc.
- **Un software:** il certificato garantisce la provenienza del software. Questo utilizzo è importante specialmente se il prodotto viene distribuito in Rete.

GlobalTrust Italia S.p.A.
Piazza San Pietro, 2 – 05100 Terni Phone: +39.0744. 441214 Fax: +39.0744. 460269
E-mail: info@globaltrust.it - http://www.globaltrust.it Cap. Soc. € 2.750.000 i.v. REA 89371 P.I .01339760553

Come è composto il certificato

Un certificato digitale, emesso da una CA, contiene le seguenti informazioni:

- il **nome** del possessore, se il possessore è una persona fisica si tratterà di nome e cognome, data di nascita ecc... se invece è un server web sarà presente l'indirizzo web e il nome della compagnia titolare del dominio;
- la **data di scadenza** della chiave pubblica;
- il **nome della CA** che ha emesso il certificato;
- la **firma digitale della CA** che ha emesso il certificato (previene la manomissione del contenuto del certificato).



Esistono vari standard per la creazione di certificati, attualmente il più affermato è quello definito dallo standard internazionale X.509.

GlobalTrust Italia S.p.A.
Piazza San Pietro, 2 – 05100 Terni Phone: +39.0744. 441214 Fax: +39.0744. 460269
E-mail: info@globaltrust.it - http://www.globaltrust.it Cap. Soc. € 2.750.000 i.v. REA 89371 P.I .01339760553

ESEMPIO DI UN CERTIFICATO UTENTE

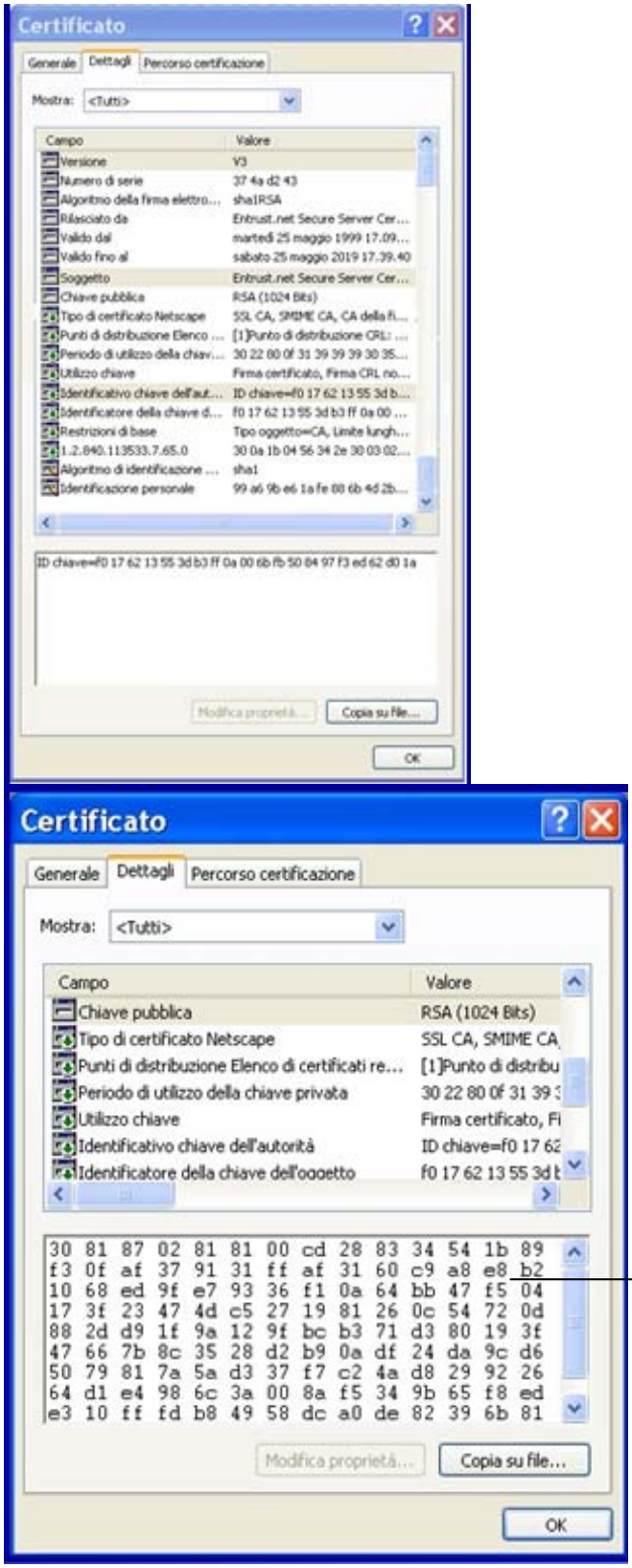
Di chi è il certificato

CA che ha rilasciato il certificato

Periodo di validità del certificato.
Per motivi di sicurezza la validità di un certificato non può essere superiore a 3 anni.

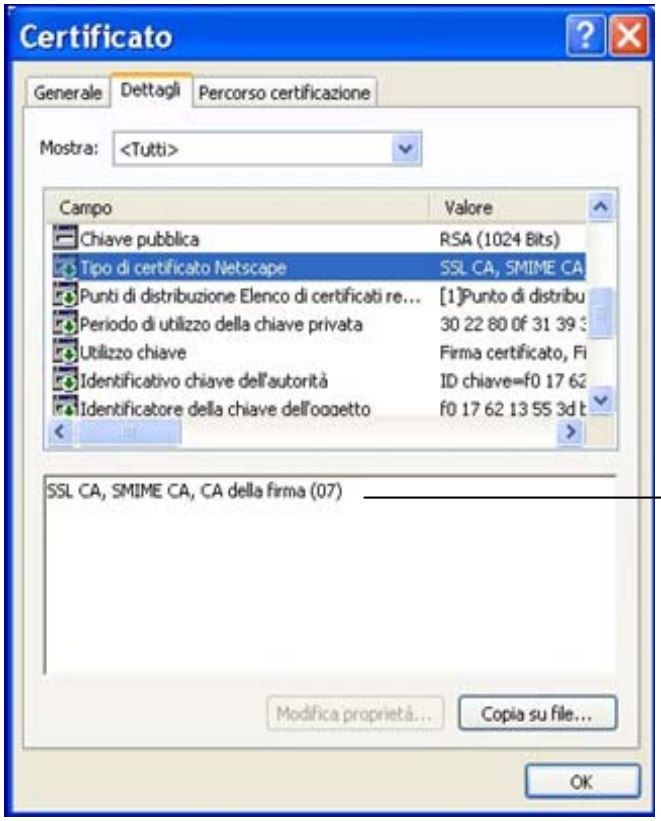
Attributi del certificato X.509 v.3

GlobalTrust Italia S.p.A.
Piazza San Pietro, 2 – 05100 Terni Phone: +39.0744. 441214 Fax: +39.0744. 460269
E-mail: info@globaltrust.it - http://www.globaltrust.it Cap. Soc. € 2.750.000 i.v. REA 89371 P.I .01339760553

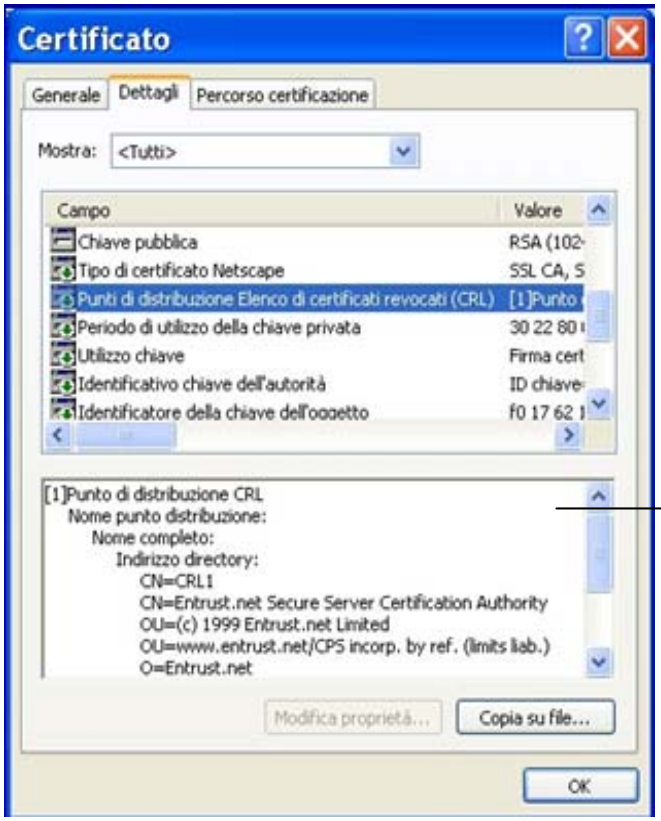


Chiave pubblica

GlobalTrust Italia S.p.A.
Piazza San Pietro, 2 – 05100 Terni Phone: +39.0744. 441214 Fax: +39.0744. 460269
E-mail: info@globaltrust.it - http://www.globaltrust.it Cap. Soc. € 2.750.000 i.v. REA 89371 P.I .01339760553

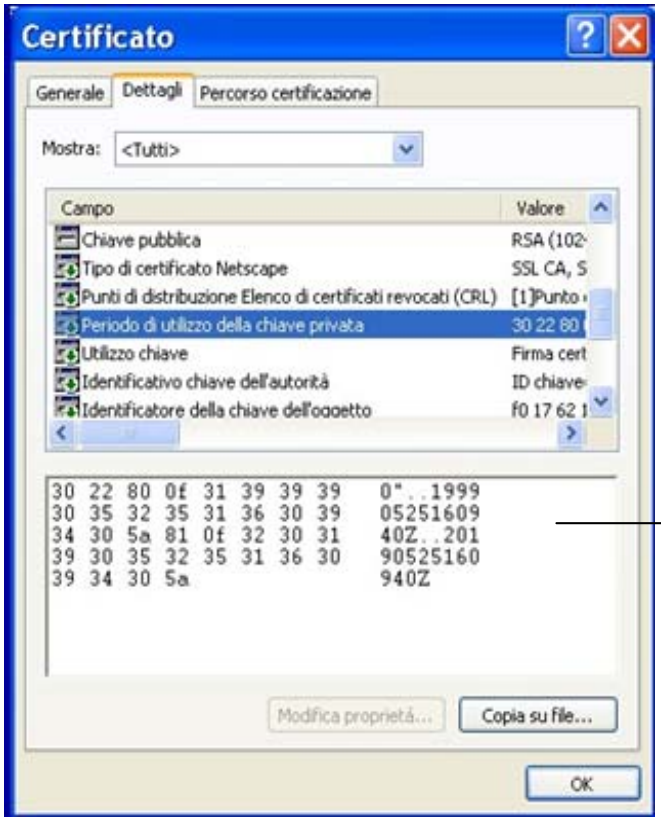


Tipo di certificato

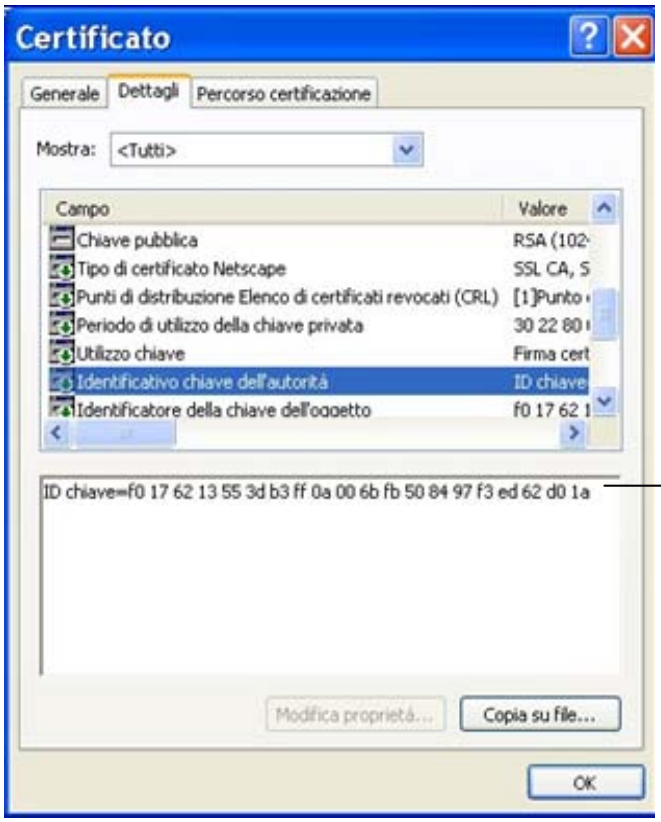


Punti di distribuzione Elenco dei certificati revocati (CRL)

GlobalTrust Italia S.p.A.
Piazza San Pietro, 2 – 05100 Terni Phone: +39.0744. 441214 Fax: +39.0744. 460269
E-mail: info@globaltrust.it - http://www.globaltrust.it Cap. Soc. € 2.750.000 i.v. REA 89371 P.I .01339760553



Periodo di utilizzo della chiave privata



Identificativo della chiave della CA

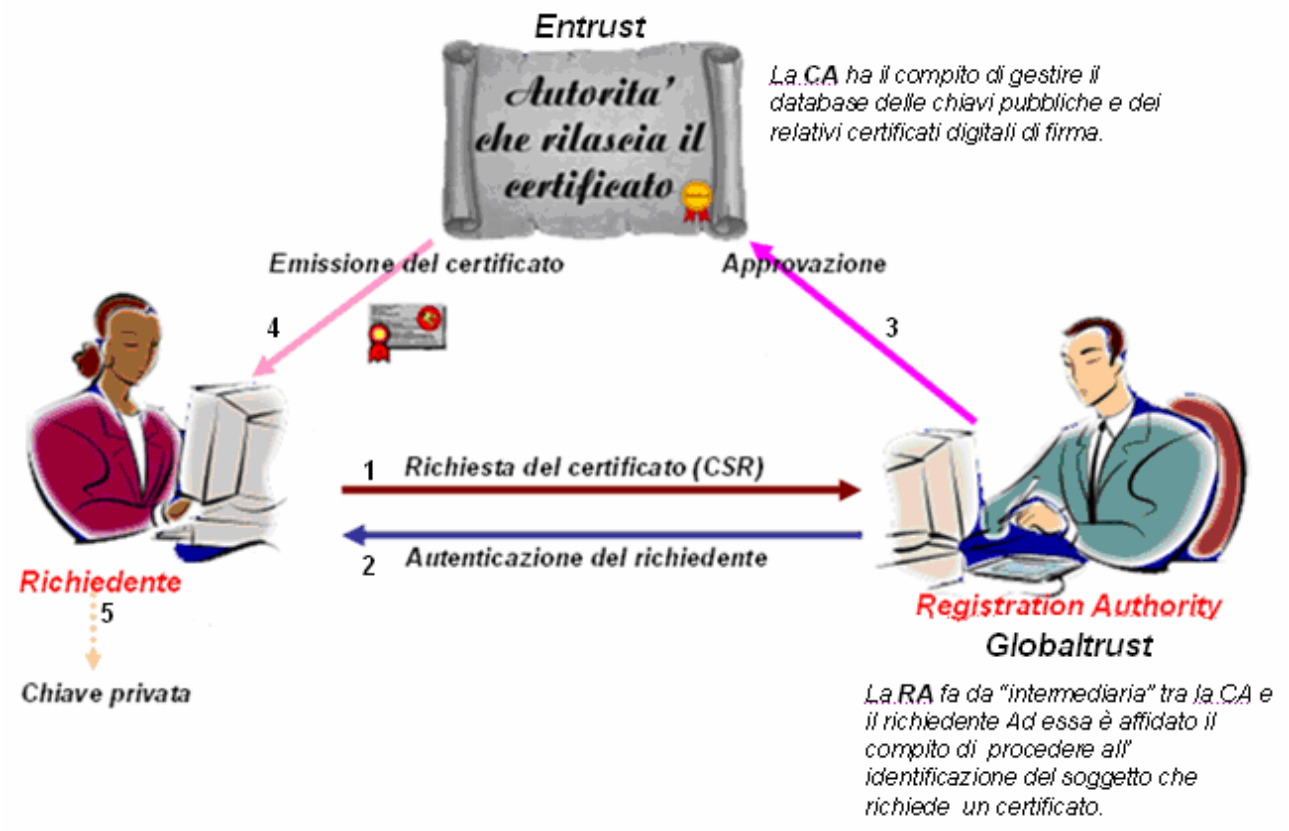
GlobalTrust Italia S.p.A.
Piazza San Pietro, 2 – 05100 Terni Phone: +39.0744. 441214 Fax: +39.0744. 460269
E-mail: info@globaltrust.it - http://www.globaltrust.it Cap. Soc. € 2.750.000 i.v. REA 89371 P.I .01339760553

CICLO DI VITA DEI CERTIFICATI

Fino ad ora si è parlato dei certificati digitali, dei vantaggi del loro utilizzo e del loro contenuto. Ma:

- **In che modo si ottiene un certificato?**
- **Se perdo la mia chiave privata (associata al certificato), posso in qualche modo recuperarla o il certificato diventa inutilizzabile?**
- **Cosa succede quando scade il periodo di validità del mio certificato?**

Come viene emesso un certificato.....



GlobalTrust Italia S.p.A.
Piazza San Pietro, 2 – 05100 Terni Phone: +39.0744. 441214 Fax: +39.0744. 460269
E-mail: info@globaltrust.it - http://www.globaltrust.it Cap. Soc. € 2.750.000 i.v. REA 89371 P.I .01339760553

PROBLEMATICHE DEL WEB

Vari sono gli aspetti di sicurezza da considerare quando si utilizza l' ambiente Internet. Va infatti subito precisato che se, da un lato, Internet garantisce un' ampia connettività grazie all' utilizzo di un protocollo aperto come il TCP/IP, dall' altro il fatto che si utilizzi quest ultimo è di per sé la principale causa di insicurezza, trattandosi di un protocollo intrinsecamente insicuro.

In particolare sul web, il protocollo **HTTP** è estremamente insicuro in quanto trasmette i dati "in chiaro". Tale protocollo rappresenta, sostanzialmente, il linguaggio comune di due sistemi informatici distinti:

- i **server web**, computer che pubblicano le pagine sulla rete Internet e che, quindi, mettono a disposizione contenuti e raccolgono dati;
- i **sistemi client**, vale a dire quelli utilizzati da un qualsiasi browser. I dati così trasmessi sono, però, facilmente intercettabili.

È per questo motivo che introdurre, ad esempio, i dati della propria carta di credito attraverso moduli o formulari proposti dalle pagine HTML può essere rischioso.

Per quanto concerne confidenzialità e integrità dei dati, aspetti di sicurezza particolarmente sentiti quando si utilizza il Web per effettuare transazioni, due sono i protocolli di sicurezza di maggiore impiego:

- **SSL (Secure Socket Layer)** : messo a punto da Netscape nel 1994, si pone come strato intermedio tra il transport layer (TCP/UDP) e l' application layer (FTP, Telnet, HTTP, SMTP) del protocollo TCP/IP garantendo un canale di comunicazione sicuro.
- **S-HTTP (Secure HTTP)**: lavora a livello applicativo e in particolare estende il protocollo HTTP mediante la definizione di attributi di sicurezza.

Entrambi i protocolli, pur lavorando in modo diverso, realizzano un filtro che crittografa tutto ciò che passa sulla Rete.

Il protocollo S-HTTP è più flessibile dell' SSL poiché, mantenendo una piena compatibilità con l' HTTP, permette di definire alcuni tag su una pagina che, al momento dello scaricamento, si attivano elaborando i dati che vanno sulla Rete. In dipendenza dei valori che vengono attribuiti a questi tag, si può ottenere la crittografia dei dati, l' autenticazione del server e del client Web, oppure apporre una firma elettronica al documento.

Entrambi i protocolli sono impiegati nelle transazioni elettroniche su Internet (i servizi Web migliori li adottano entrambi). Nonostante tutto, in definitiva si preferisce SSL che, fornendo una crittografia di canale, può essere abbinato ad altri specifici protocolli per il pagamento elettronico, come ad esempio il protocollo SET (Secure Electronic Transaction).

GlobalTrust Italia S.p.A.
Piazza San Pietro, 2 – 05100 Terni Phone: +39.0744. 441214 Fax: +39.0744. 460269
E-mail: info@globaltrust.it - http://www.globaltrust.it Cap. Soc. € 2.750.000 i.v. REA 89371 P.I .01339760553

SSL (SECURE SOCKET LAYER) PROTOCOL

Il protocollo SSL è uno standard, prodotto dalla Netscape Communications Corp., per autenticare l' accesso ai server tramite un meccanismo a chiave pubblica (RSA) e per scambiare in modo sicuro una chiave di crittografia tra client e server.

Esso rappresenta al momento la soluzione più sicura ed efficace per criptare le informazioni che transitano dal browser al sito e renderle quindi illeggibili nel caso venissero intercettate.

Nello schema ISO-OSI, si posiziona al di sopra del livello di trasporto, in modo da rendersi indipendente dall' applicazione che lo utilizza.

Le caratteristiche che lo rendono di sicuro interesse sono:

- Possibilità di essere utilizzato senza alcuna modifica preventiva per qualunque applicativo client-server che utilizzi TCP/IP,
- Piena compatibilità con altri tipi di autenticazione: l' SSL è un protocollo di basso livello per la realizzazione di un canale di trasmissione sicuro che non coinvolge i dati scambiati;
- Alta diffusione, sia attraverso gli a applicativi Netscape sia attraverso i prodotti di numerosi licenziatari.

In breve, il protocollo SSL permette una connessione TCP/IP sicura sulla base di tre proprietà:

- ✓ Le entità in comunicazione possono autenticarsi a vicenda utilizzando la crittografia a chiave pubblica;
- ✓ La confidenzialità dei dati trasmessi è garantita dall' utilizzo di una chiave di sessione generata durante l' interazione tra le parti nella prima fase del protocollo;
- ✓ L' integrità dei dati è garantita dall' utilizzo del Message Authetication Code (MAC).

È importante notare come il protocollo SSL non protegga dall' analisi del traffico. Ad esempio, esaminando gli indirizzi IP, che viaggiano in chiaro, o analizzando il volume del flusso del traffico in Rete, un crittoanalista può eventualmente determinare quali parti sono in comunicazione e che tipo di servizi stanno utilizzando.

Per poter essere impiegato, il protocollo SSL richiede che sia il client sia il server abbiano la consapevolezza che la rispettiva controparte la sta utilizzando. Per questo motivo, lo IANA ha riservato un numero di porta separato (**Tabella 1**) per alcune delle applicazioni che supportano l' SSL.

GlobalTrust Italia S.p.A.
Piazza San Pietro, 2 – 05100 Terni Phone: +39.0744. 441214 Fax: +39.0744. 460269
E-mail: info@globaltrust.it - http://www.globaltrust.it Cap. Soc. € 2.750.000 i.v. REA 89371 P.I .01339760553

TABELLA 1 – Numeri di porta utilizzati per applicazioni con supporto SSL

KeyWord	Porta	Descrizione
https	443	http con supporto SSL
Ssmtp	465	SMTP con supporto SSL
Snntp	563	NNTP con supporto SSL
Sldap	636	LDAP con supporto SSL
Spop3	995	POP3 con supporto SSL
ftp-data	889	FTP data con supporto SSL
Ftps	990	FTP con supporto SSL
Imaps	991	IMAP4 con supporto SSL
Telnets	992	TELNET con supporto SSL
Ircs	993	IRC con supporto SSL

L' instaurazione di una connessione sicura mediante SSL comporta una procedura di scambio di messaggi fra client e server (handshaking) che si articola nei seguenti nove passi nella versione 3.0 del protocollo (la versione 2.0, che non effettua l' autenticazione del client, non prevede i passi 6 e 7).

1. Client Hello: il client invia una challenge phrase al server e comunica la scelta di un algoritmo a chiave privata per lo scambio dei messaggi (DES, RC2 o RC4), di un algoritmo a chiave pubblica per lo scambio delle chiavi di sessione (RSA, Diffie-hellman, Fortezza-KEA) e di un algoritmo di hashing (MD5).
2. Server Hello: il server invia al client il proprio server certificate (ottenuto da una CA), fornisce il proprio acknowledgment ai protocolli scelti dal client e genera un connection identifier da usarsi nella successiva fase di comunicazione client-server.
3. Client master Key: il client verifica il server certificate inviatogli dal server (i certificati sono memorizzati nel browser per connessioni successive), genera una master session key usata come chiave generatrice di una coppia di chiavi simmetriche (una per le comunicazioni in uscita e l' altra per le comunicazioni in entrata) e la crittografa con la server public key contenuta nel public server certificate; il tutto è inviato al server.
4. Client finished: il client, dopo aver inviato il messaggio cifrato, termina la propria sessione crittografando con la propria client-read key (server-write key) il connection identifier inviatogli dal server e si pone in attesa del messaggio server finished.
5. Server verifier: il server decrittografa la master session key inviatagli con la propria server private key, genera la coppia di chiavi simmetriche di sessione (lato server) e invia al client la challenge phrase iniziale crittografata con la server-write (client-read) key; a questo punto il server è autenticato.
6. Request certificate: il server chiede che il client presenti un valido client certificate e invia al client una nuova challenge phrase crittografata con la server-write (client-read) key.
7. Client certificate: il client invia al server una response phrase costruita crittografando, con la client-write key, la client public key unita all' hash (crittografato come firma elettronica, con la client private key) della challenge phrase unita alla server public key; il server ricalcala l' hash e lo confronta con quello ricavato decrittografando con la client public key la firma elettronica contenuta nella response phrase (il client è ora autenticato).

GlobalTrust Italia S.p.A.
Piazza San Pietro, 2 – 05100 Terni Phone: +39.0744. 441214 Fax: +39.0744. 460269
E-mail: info@globaltrust.it - http://www.globaltrust.it Cap. Soc. € 2.750.000 i.v. REA 89371 P.I .01339760553

8. Server finished: il server termina la propria sessione inviando al client un session identifier (un numero univoco generato in modo casuale), utilizzabile in ogni altra sessione per evitare ulteriori handshaking che rallenterebbe la performance sul sistema.
9. Start communication sessions: ogni altra sessione clien-server si instaurerà utilizzando le chiavi di sessione e i relativi algoritmi di crittografia simmetrici (più veloci di quelli asimmetrici) precedentemente definiti.

Al termine della procedura di autenticazione si è formato un canale sicuro in cui tutti i dati in transito vengono criptati secondo la chiave di sessione e non utilizzando la coppia di chiavi in possesso dalle due parti. Questo modo di operare porta a una comunicazione più veloce, visto che la dimensione della chiave di sessione è nettamente inferiore a quella delle chiavi segrete. Nonostante il keyspace sia in tal modo diminuito, la sicurezza della comunicazione non viene meno, perché l' utilizzo di una chiave di sessione è limitata appunto a quel particolare scambio di informazioni e il numero di tentativi necessari per la scoperta della chiave occuperebbero un tempo troppo elevato rispetto al tempo in cui tale chiave viene utilizzata.

Una considerazione importante da fare è che **tanto più è lunga la chiave di sessione, tanto più è valido il grado di cifratura.**

Una chiave di cifratura a 40 bit è considerata "standard" mentre una chiave a 128 bit (utilizzata dall'ultima versione di SSL, la 3) è conosciuta come **strong encryption** ed è supportata dalle versioni più recenti dei browser (Microsoft Explorer e Netscape Navigator dalle versioni 4).

La scelta del tipo di cifratura da utilizzare (e la conseguente sicurezza che essa garantisce) dipende essenzialmente dal tipo di attività che si intende svolgere attraverso il sito e, più in particolare, dal tipo di dati che si raccolgono e trattano (gestione di carte di credito, transazioni economiche in generale, dati riservati o sensibili di altra natura ovvero transazioni nelle quali vengano, invece, inseriti dati riservati ma non dati sensibili o delicati).
L'affidabilità delle informazioni è, invece, garantita da speciali controlli sull'integrità dei dati realizzati con l'utilizzo di algoritmi di hashing quali SHA (Secure Hash Algorithm) o MD5 (Message Digest Algorithm 5). Tutti coloro che sono interessati alla transazione sanno che ciò che stanno vedendo corrisponde esattamente a ciò che è stato inoltrato dall'altro lato della comunicazione.

CERTIFICATI PER SERVER WEB (SSL)

I certificati digitali per Server Web (SSL) vengono utilizzati per garantire sicurezza e privacy a qualsiasi utente che usa un sito di e-commerce o simile, (cioè usufruisce del web per accedere a servizi, acquistare merce e/o trasmettere proprie informazioni personali).
In particolare, vedere la presenza di un certificato SSL per Server Web su un sito, rende l' utente sicuro del fatto che tutte le informazioni da lui inserite nel modulo di registrazione presente nel sito a cui si collega sono:

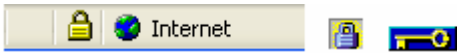
GlobalTrust Italia S.p.A.
Piazza San Pietro, 2 – 05100 Terni Phone: +39.0744. 441214 Fax: +39.0744. 460269
E-mail: info@globaltrust.it - http://www.globaltrust.it Cap. Soc. € 2.750.000 i.v. REA 89371 P.I .01339760553

- trasmesse e ricevute in assoluta privacy
- non sono soggette ad intercettazione da parte di nessuno
- l' ordine, la richiesta di servizi od altro non possono essere soggette a ripudio
- attraverso il certificato che autentica il sito, è possibile verificare online le credenziali e l' intestatario per eventuali rivalse e l' identità del certificatore.

COME SI PUÒ VERIFICARE LA SICUREZZA DI UN SITO

Quando un utente si collega ad un sito per inserire delle informazioni o accedere a servizi che richiedono la compilazione di form online, può rendersi immediatamente conto se le informazioni vengono raccolte in una sessione SSL (e quindi sicura) oppure no.

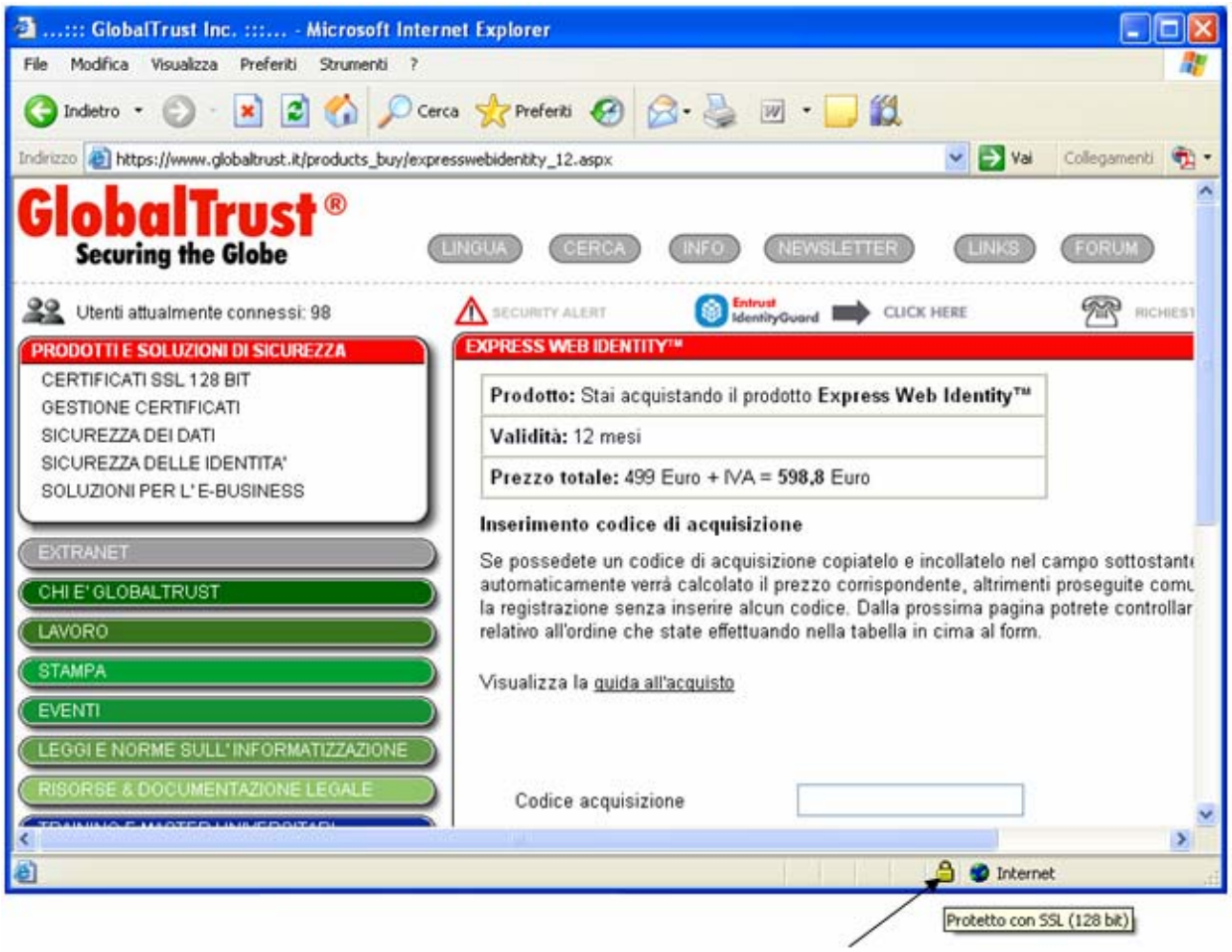
La cosa è semplice da verificare in quanto l' URL del sito cambia da **http** in **https** (es. https://www.sito.it) ed in basso a destra appare un lucchettino (vedi immagini).

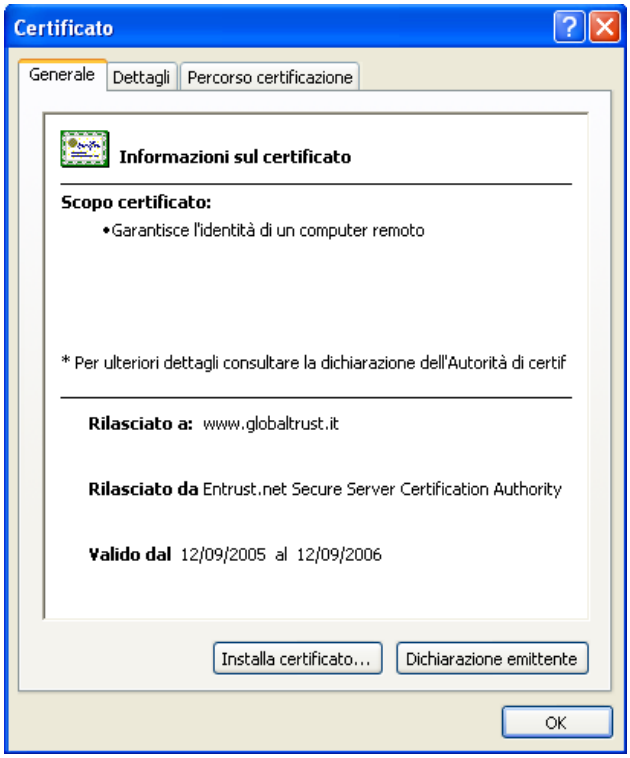


Qualora non fosse così, tutte le informazioni inserite nel modulo di richiesta possono essere intercettate, cambiate, alterate o sostituite con altre, i dati possono essere **usati da altri**. Inoltre chi si è occupato della realizzazione del sito è responsabile dei danni subiti dall' utente ed in alcuni casi tale responsabilità può essere anche di natura penale. Ma la cosa peggiore è che le informazioni dell' utente potrebbero essere catturate ed usate per altri scopi (rubando la sua identità) ed usandola per scopi non leciti.

Per essere sicuri basta cliccare sul lucchetto che appare nella finestra del browser in basso a destra e visualizzare le informazioni circa l' emissione del certificato.

GlobalTrust Italia S.p.A.
Piazza San Pietro, 2 – 05100 Terni Phone: +39.0744. 441214 Fax: +39.0744. 460269
E-mail: info@globaltrust.it - http://www.globaltrust.it Cap. Soc. € 2.750.000 i.v. REA 89371 P.I .01339760553

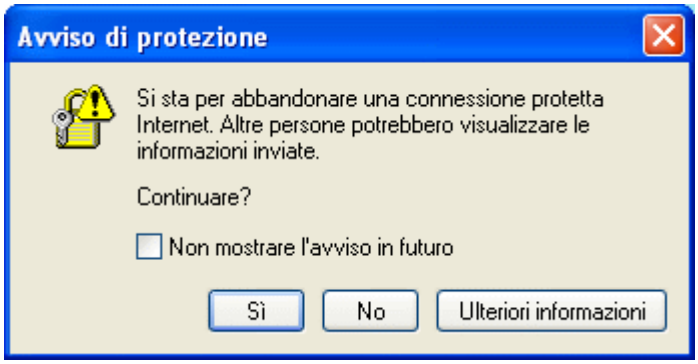




GlobalTrust Italia S.p.A.
Piazza San Pietro, 2 – 05100 Terni Phone: +39.0744. 441214 Fax: +39.0744. 460269
E-mail: info@globaltrust.it - http://www.globaltrust.it Cap. Soc. € 2.750.000 i.v. REA 89371 P.I .01339760553

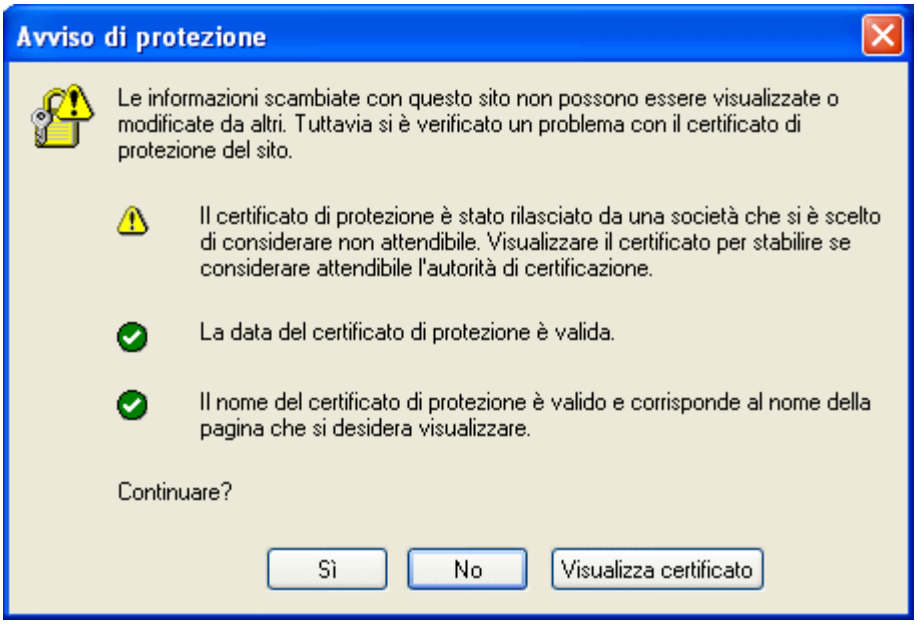
ALCUNE SEMPLICI RACCOMANDAZIONI

Attenzione! Quando si lascia l'area di sicurezza appare la seguente finestra di dialogo:



Da questo momento in poi tutte le informazioni che si inseriscono nel sito sono a rischio.

Le informazioni che fornisce il Browser si spiegano da sole, **basta leggere**. Altra cautela va tenuta quando, pur entrando in un sito di cui si può anche conoscere l'origine, perché nota e pubblicizzata ampiamente, si riceve il seguente avviso andando nella zona protetta (certificato non attendibile):



Attualmente sul mercato sono presenti due categorie principali di certificati SSL per server Web:

- certificati SSL a 128 bit
- certificati SSL a 40 bit

Quest' ultimi però sono ormai obsoleti ed insicuri. Per approfondire l' argomento

GlobalTrust Italia S.p.A.
Piazza San Pietro, 2 – 05100 Terni Phone: +39.0744. 441214 Fax: +39.0744. 460269
E-mail: info@globaltrust.it - http://www.globaltrust.it Cap. Soc. € 2.750.000 i.v. REA 89371 P.I .01339760553