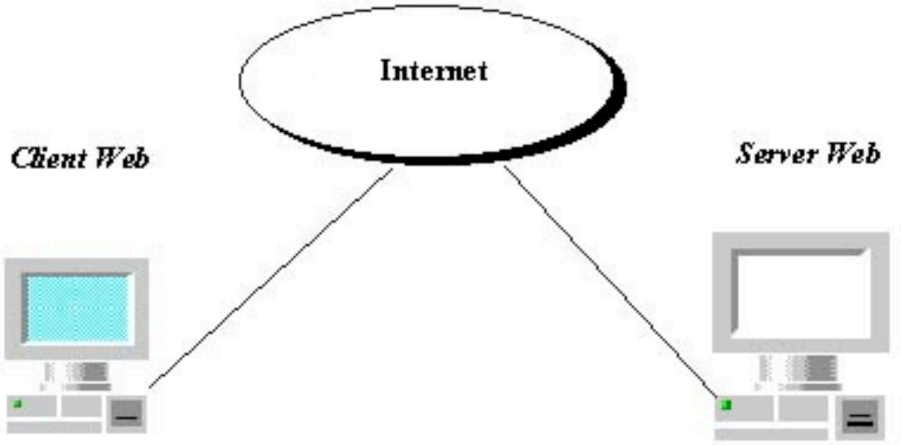
Comunicazioni sicure su Internet: https e SSL

Fisica dell'Informazione

Comunicazione sicure via web

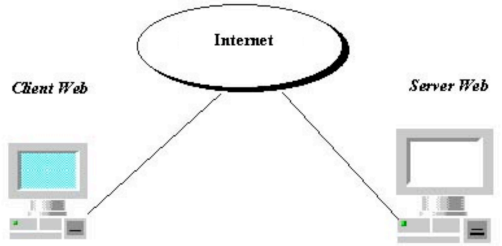
Il servizio World Wide Web (WWW)



Come funziona nel dettaglio il Web?
tre insiemi di regole:

- Uniform Resource Locator (URL)
- Hyper Text Transfer Protocol (HTTP)
- Hyper Text Markup Language (HTML)

Comunicazione sicure via web

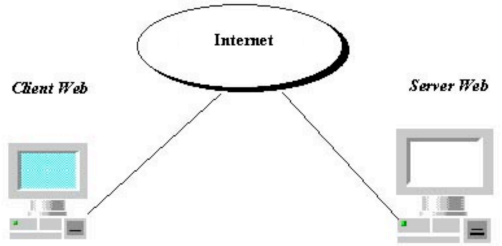


Hyper Text Transfer Protocol (HTTP) -------> HTTPS

L' HTTPS è un **URI** (Uniform Resource Identifier) sintatticamente identico allo schema http:// ma con la differenza che gli accessi vengono effettuati sulla porta 443
e
tra il protocollo TCP e HTTP si interpone un livello di crittografia/autenticazione.

Cfr http://it.wikipedia.org/wiki/HTTPS

Comunicazione sicure via web



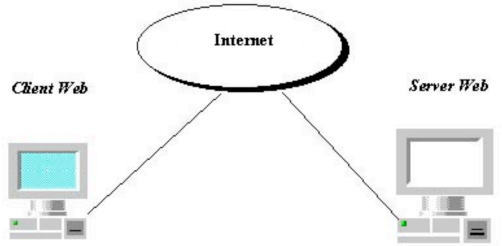
Hyper Text Transfer Protocol (HTTPS)

In pratica viene creato un canale di comunicazione criptato tra il **client** e il **server** attraverso lo scambio di certificati;

una volta stabilito questo canale al suo interno viene utilizzato il protocollo HTTP per la comunicazione.

Questo tipo di comunicazione garantisce che solamente il client e il server siano in grado di conoscere il contenuto della comunicazione.

Comunicazione sicure via web

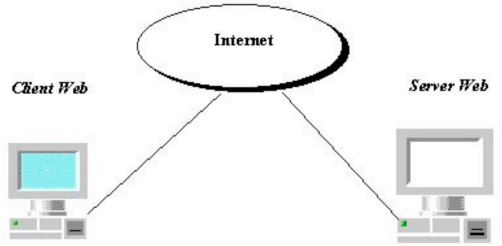


Hyper Text Transfer Protocol (HTTPS)

Questo sistema, inizialmente denominato SSL, fu progettato dalla Netscape Communications Corporation per essere utilizzato nel World Wide Web per situazioni che richiedono particolari esigenze in ambito di sicurezza come per esempio il pagamento di transazioni online.

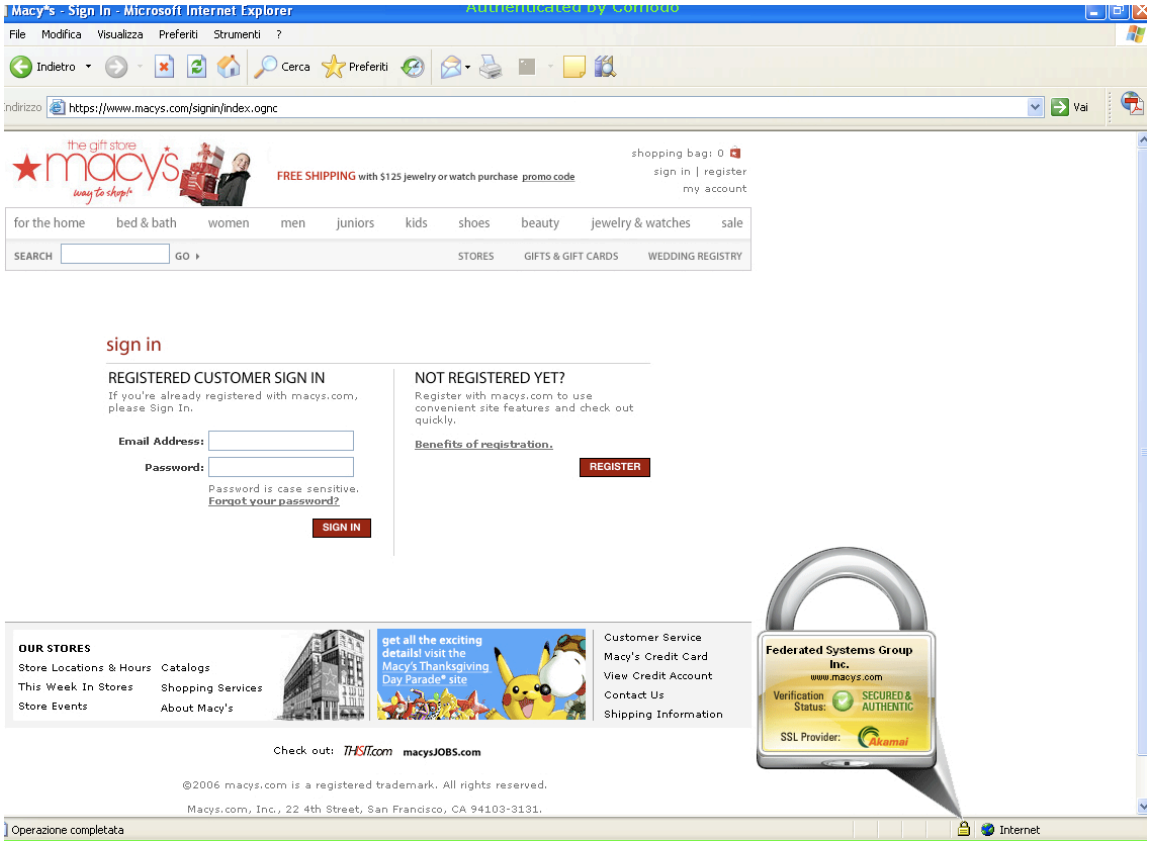
In questo caso SSL garantisce la cifratura dei dati trasmessi e ricevuti su internet.

Comunicazione sicure via web

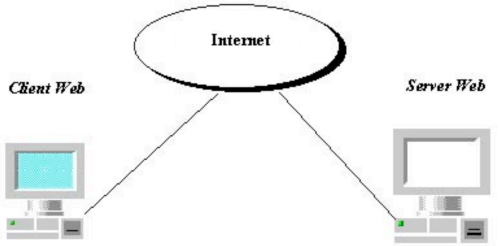


Hyper Text Transfer Protocol (HTTPS)

L'impiego di SSL è evidenziato in modo apposito dal browser web.



Comunicazione sicure via web

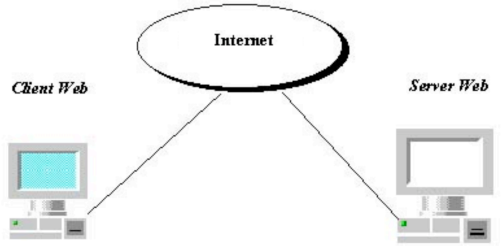


Hyper Text Transfer Protocol (HTTPS)

HTTPS usa la crittografia fornita da SSL

HTTPS non è un protocollo a parte ma si occupa di combinare l'interazione del protocollo HTTP attraverso un meccanismo di crittografia di tipo Secure Sockets Layer (SSL)
o, più recentemente denominato
Transport Layer Security (TLS).

Comunicazione sicure via web



A cosa serve SSL

Scopo primario di SSL è fornire sistemi di crittografia per comunicazioni affidabili e riservate sulla rete sfruttabili in applicazioni quali, ad esempio, posta elettronica e sistemi di autenticazione.
Il protocollo SSL provvede alla sicurezza del collegamento garantendo:

Authentication:

sicurezza dell'identita dei soggetti che comunicano

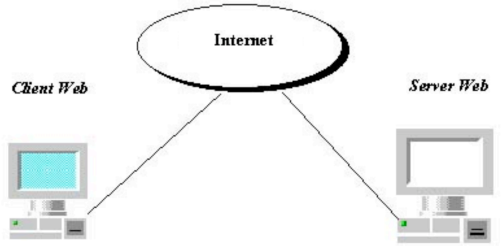
Data Confidentiality:

protezione dei dati da osservatori non autorizzati

Data Integrity:

sicurezza che il dato ricevuto è uguale al dato inviato

Comunicazione sicure via web



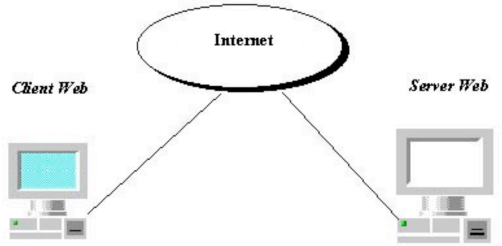
A cosa serve SSL

Authentication:

l'identità nelle connessioni può essere autenticata usando la crittografia asimmetrica, ovvero a chiave pubblica (RSA, DSS, EL-Gamal).

Così ogni client comunica in sicurezza con il corretto server, prevenendo ogni interposizione.
È prevista la certificazione del server e, opzionalmente, quella del client.

Comunicazione sicure via web



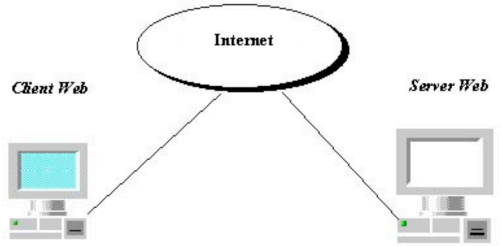
A cosa serve SSL

Data Confidentiality nella trasmissione dei dati:

la crittografia è usata dopo un handshake (accordo) iniziale per definire una chiave segreta di sessione.

In seguito, per crittografare i dati è usata la crittografia simmetrica (AES,3DES, RC4, ecc.).

Comunicazione sicure via web



A cosa serve SSL

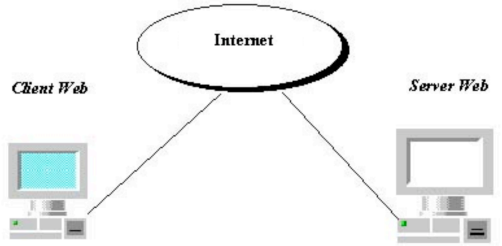
Data Integrity :

il livello di trasporto include un controllo dell'integrità del messaggio basato su un apposito
MAC (Message Authentication Code)
che utilizza funzioni hash sicure (MD5, SHA, RIPEMP-160, ecc).

In tal modo si verifica che i dati spediti tra client e server non siano stati alterati durante la trasmissione.

http://it.wikipedia.org/wiki/Secure_Sockets_Layer

Comunicazione sicure via web



A cosa serve SSL

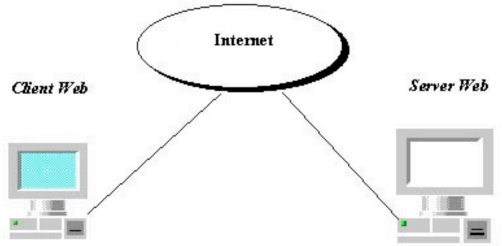
Data Integrity : il ruolo delle funzioni di HASH

Nel linguaggio scientifico, l'hash è una funzione non invertibile, atta alla trasformazione di un testo di lunghezza arbitraria in una stringa di lunghezza fissa, relativamente limitata.

Tale stringa rappresenta una sorta di "impronta digitale" del testo in chiaro, e viene detta **valore di hash**, **checksum crittografico** o **message digest**.

http://it.wikipedia.org/wiki/Hash

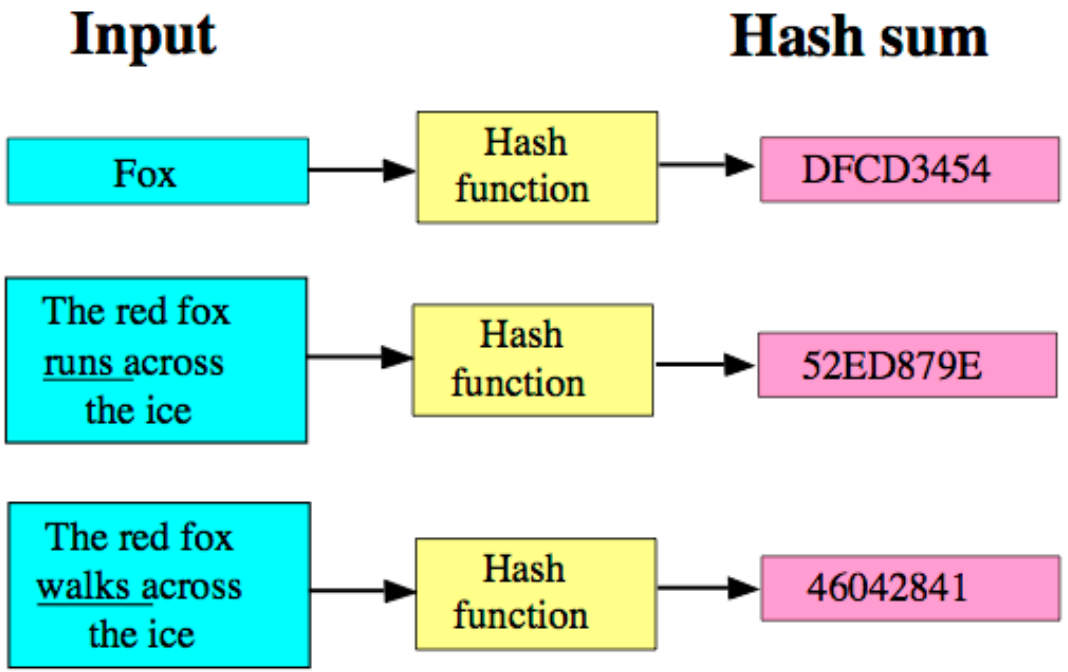
Comunicazione sicure via web



A cosa serve SSL

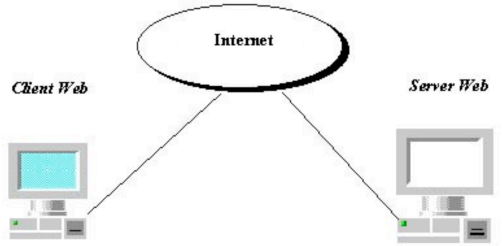
Data Integrity : il ruolo delle funzioni di HASH

Esempio:



http://it.wikipedia.org/wiki/Hash

Comunicazione sicure via web



Hash functions

L'algoritmo di hash elabora una stringa di bit in ingresso (di lunghezza arbitraria) e restituisce una stringa di bit di lunghezza definita (es. 256). Deve soddisfare i seguenti requisiti:

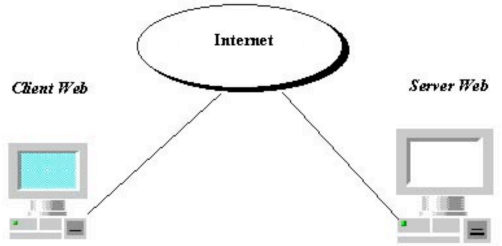
1. L'algoritmo restituisce una stringa di numeri e lettere a partire da un qualsiasi flusso di bit di qualsiasi dimensione (può essere un file ma anche una stringa). L'output è detto digest.

2. La stringa di output è univoca per ogni documento e ne è un identificatore. Perciò, l'algoritmo è utilizzabile per la firma digitale.

3. L'algoritmo non è invertibile, ossia non è possibile ricostruire il documento originale a partire dalla stringa che viene restituita in output.

http://it.wikipedia.org/wiki/Hash

Comunicazione sicure via web



Hash functions

Il problema delle collisioni

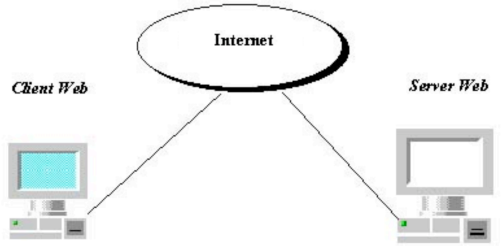
2. La stringa di output è univoca per ogni documento e ne è un identificatore. Perciò, l'algoritmo è utilizzabile per la firma digitale.

La corrispondenza non puo' in principio essere biunivoca…

Un buon algoritmo ha un basso tasso di collisioni (corrispondenze di due testi diversi con uno stesso digest).

http://it.wikipedia.org/wiki/Hash

Comunicazione sicure via web

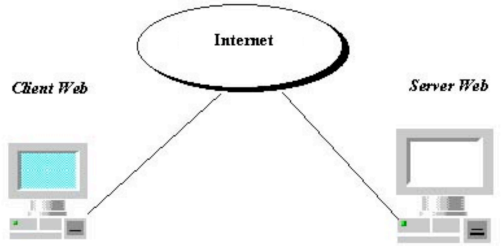


Come funziona SSL

Sia TLS che SSL richiedono sostanzialmente tre fasi:

1. Negoziazione tra le parti dell'algoritmo da utilizzare
2. Scambio di chiave segreta per crittografia simmetrica tramite cifratura a chiave pubblica e identificazione tramite l'utilizzo di certificati
3. Cifratura del traffico tra le parti a chiave (segreta) simmetrica

Comunicazione sicure via web



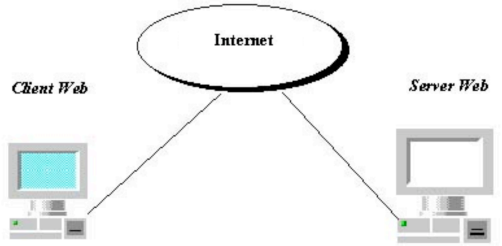
Il certificato digitale

Un certificato digitale è un documento elettronico che associa l'identità di una persona ad una chiave pubblica.

Viene emesso da una autorità di certificazione riconosciuta secondo standard internazionali (X.509) e viene firmato con la chiave privata dell'autorità.

Gli enti che fanno da autorità devono sottostare a regole rigidissime per quanto riguarda la gestione dei dati personali, pertanto si possono considerare sicuri.

Comunicazione sicure via web

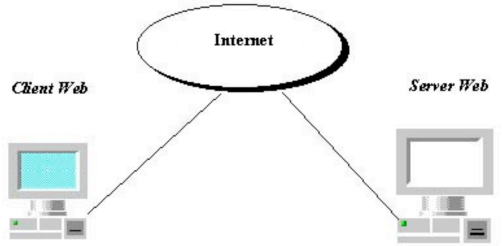


La Certification Authority (CA)

Le Certification Authority sono caratteristiche di una infrastruttura PKI (Private Key Infrastructure), così organizzata:

- una policy di sicurezza che fissa i principi generali;
- un certificate practise statement (CPS), ossia il documento in cui è illustrata la procedura per l'emissione, registrazione, sospensione e revoca del certificato;
- un sistema di certification authority (CA);
- un sistema di registration authority (RA), ovvero il sistema di registrazione e autenticazione degli utenti che domandano il certificato;
- un certificate server.

Comunicazione sicure via web

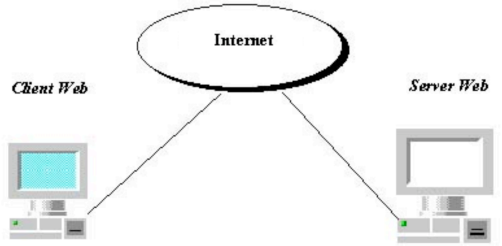


La Certification Authority (CA)

Possono essere certificate persone fisiche, organizzazioni, server, applicazioni, ogni CA precisa nel proprio CPS (certificate practise statement) chi sono le entità finali che essa è disposta a certificare e per quali scopi di utilizzo.

Esempio:
certificati di firma e cifratura dei messaggi di posta elettronica, certificati di autenticazione dei server FTP (SFTP)

Comunicazione sicure via web



La Certification Authority (CA)

Cosa fa una CA

- identificazione certa di chi richiede la cert. della chiave pubblica;
- rilascio e pubblicazione del certificato;
- manutenzione del registro delle chiavi pubbliche;
- revoca o sospensione dei certificati in caso di abuso o richiesta

Il tutto dietro pagamento !

CNIPA
Centro Nazionale per l'Informatica nella Pubblica Amministrazione

In Italia l'autorità che vigila sulle CA è per legge il CNIPA (Centro Nazionale per l'Informatica nella Pubblica Amministrazione).

CA in Italia e nel mondo

Elenco completo delle CA italiane su:

http://www.cnipa.gov.it/site/it-IT/Attività/Certificatori_accreditati/Elenco_certificatori_di_firma_digitale/Certificatori_attivi/