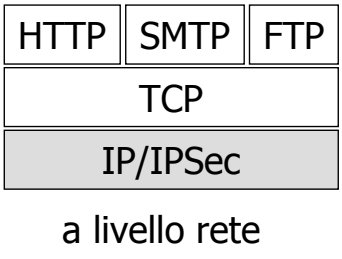
Network Security

Elements of Security Protocols

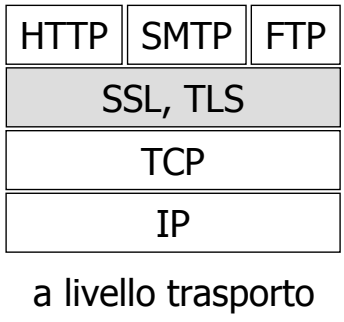
Secure Socket Layer (SSL)

- Architettura
- Il protocollo Record
- Il protocollo Handshake
- Utilizzo di SSL nei pagamenti elettronici
- Limiti di SSL

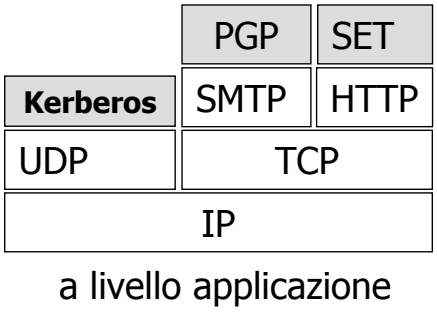
Sicurezza nella pila TCP/IP



a livello rete

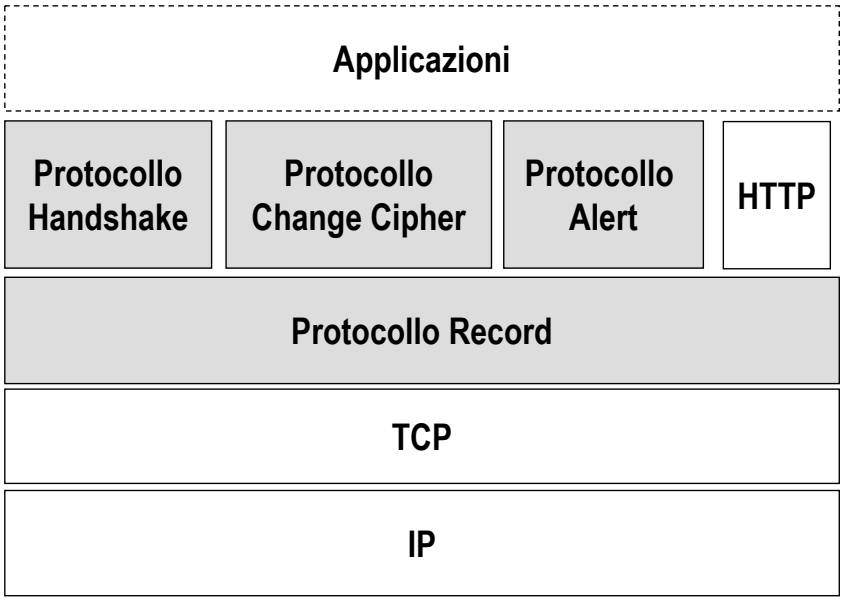


a livello trasporto



a livello applicazione

La suite di protocolli SSL



Riferimenti

- **Secure Socket Layer (SSL)**
  - Progettato da Netscape
  - http://wp.netscape.com/eng/ssl3/
- **Transport Layer Security (TLS)**
  - basato su SSL v3.0
  - RFC 2246
  - ftp://ftp.rfc-editor.org/in-notes/rfc2246.txt

Sessione e connessione

- La sessione è un'associazione logica tra Cliente e Server.
- Una sessione viene creata dal protocollo di Handshake e definisce un insieme di parametri crittografici che possono essere condivisi fra molteplici connessioni.
- La sessione evita la costosa rinegoziazione dei parametri di sicurezza per ciascuna connessione

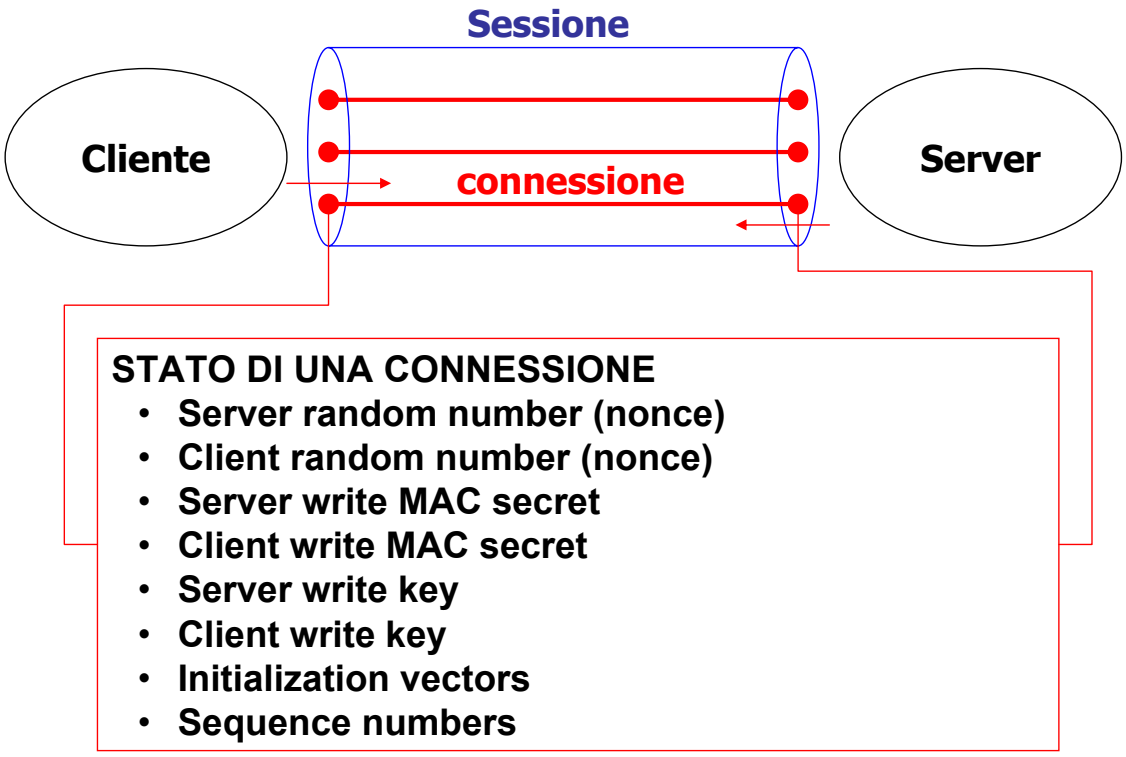
Sessione e connessione

STATO DI UNA SESSIONE

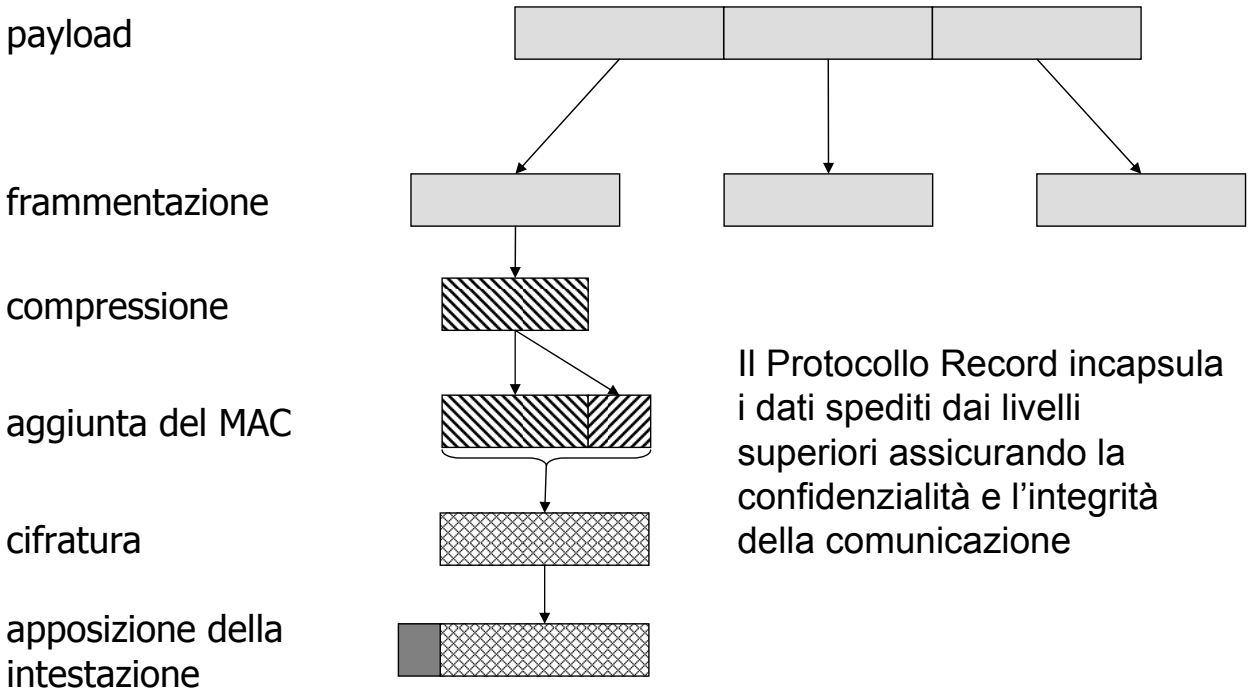
- **Identificatore di sessione** (session identifier)
- **Certificato del peer (X.509v3)**
- **Metodo di compressione** (**compression method**)
- **Cifrario ed algoritmo hash** (**cipher spec**)
- **Segreto principale** (**master secret**) [48 bit]

Questi valori definiscono lo stato di ciascun **endpoint** della sessione

Sessione e connessione



Il Protocollo Record



Il Protocollo Record incapsula i dati spediti dai livelli superiori assicurando la confidenzialità e l'integrità della comunicazione

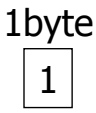
Il Protocollo Record

- La *frammentazione* frammenta i dati applicativi in blocchi di al più 2^{14} byte
- La *compressione* deve essere senza perdita e non deve far aumentare le dimensioni di un blocco di più di 1024 byte (default = null)
- Il *MAC* utilizza il [Server | Client] write MAC secret, il sequence number, il blocco compresso, pad,…
- La *cifratura* utilizza la [Server | Client] write key può essere a blocchi o a caratteri e non deve far aumentare le dimensioni di un blocco di più di 1024 byte

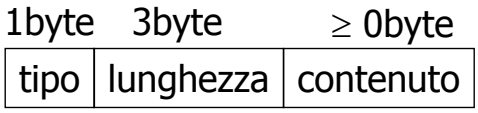
Il Protocollo Record

- Intestazione
  - Tipo di payload (change cipher, alert, handshake, application)
  - Versione principale
  - Versione minore
  - Lunghezza compressa ($\leq 2^{14} + 2048$)

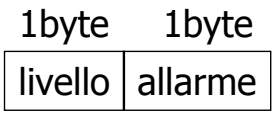
Tipi di payload



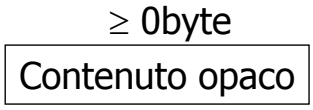
Protocollo Change Cipher



Protocollo Handshake



Protocollo Alert



Protocollo Applicativo (HTTP,...)

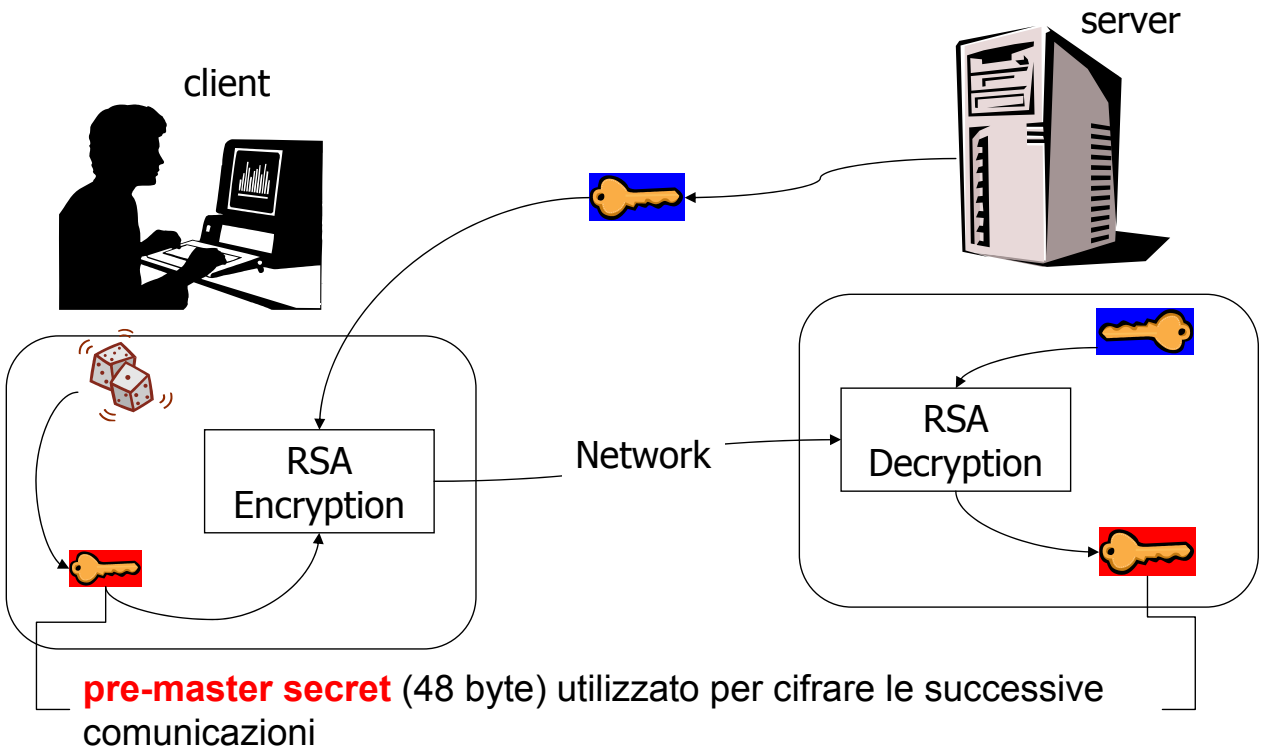
Il Protocollo Handshake

Il protocollo Handshake permette di stabilire una sessione sicura e cioè permette

- al cliente ed al server di autenticarsi a vicenda;
- di negoziare la suite di cifratura (cipher suite)
  - il metodo per lo scambio delle chiavi;
  - l'algoritmo di cifratura (utilizzato nel Protocollo Record)
  - l'algoritmo per il MAC (utilizzato nel Protocollo Record);
- di stabilire un segreto condiviso (master secret)

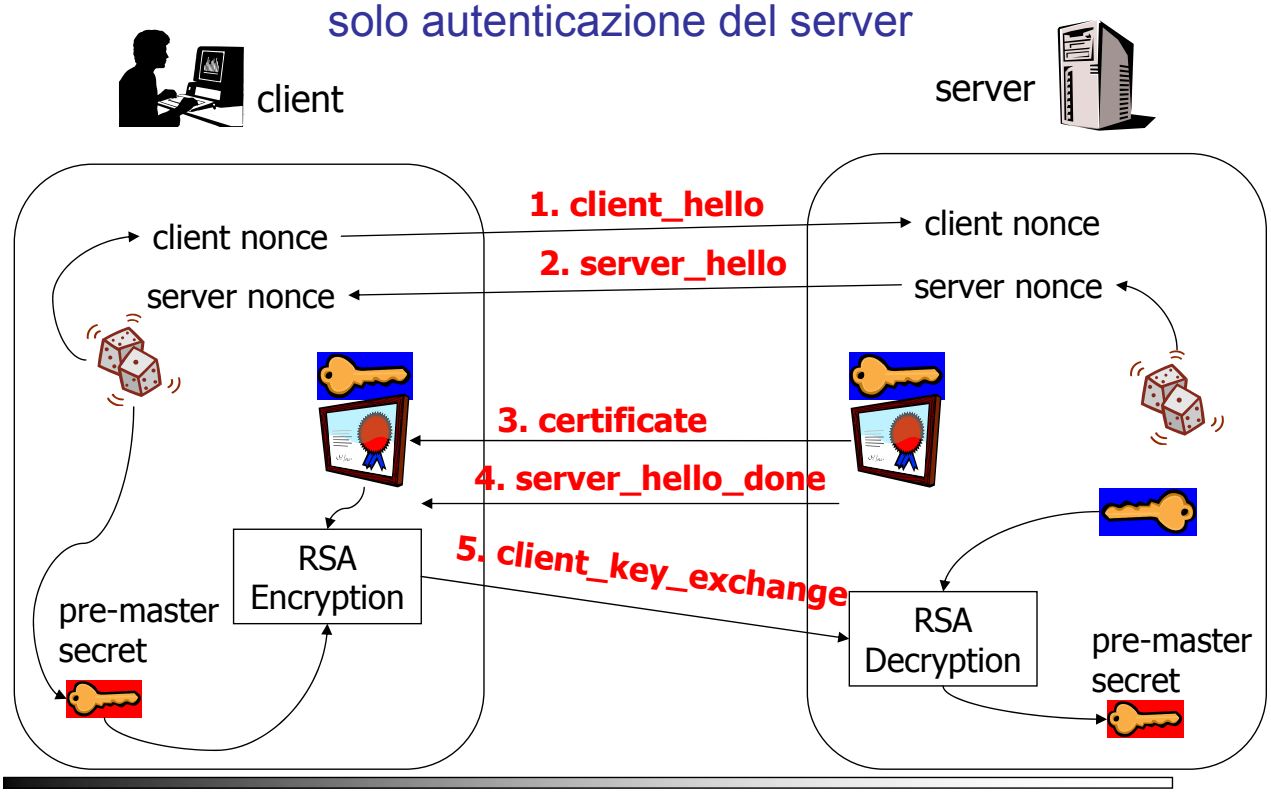
Il protocollo Handshake viene eseguito prima di inviare qualunque dato applicativo ed è la parte più complessa di SSL perché deve garantire interoperabilità

Protocollo Handshake: schema di principio (1)



Protocollo Handshake: schema di principio (2)

solo autenticazione del server



I messaggi di Hello

- In questa fase il client ed il server si dicono cosa sanno fare ed il client autentica il server
- Messaggio client_hello e server_hello
  - Versione di SSL
  - Random: timestamp (32 bit) + random byte[28]; client e server generano quantità random diverse
  - ID di sessione: in base al valore (1) viene creata una nuova sessione, (2) viene creata una connessione in una sessione esistente (3) vengono rinegoziati i parametri di una sessione esistente
  - Suite di cifratura (Cipher suite) specifica la lista degli algoritmi di cifratura supportati dal cliente in ordine di gradimento; il server sceglie
  - Metodo di compressione: lista dei metodi di compressione supportati dal client; il server sceglie

Cipher Suite

- La cipher suite specifica una lista di terne di algoritmi

  ⟨**Scambio chiavi**, **Cifrario**, **MAC**⟩

  alcune di queste terne sono state standardizzate

  SSL_RSA_WITH_3DES_EDE_CBC_SHA
- **I metodi di scambio delle chiavi supportati** sono:
  - **RSA** (encryption)
  - **Fixed Diffie-Hellman** (i parametri pubblici sono fissi e certificati)
  - **Ephemeral Diffie-Hellman** (i parametri pubblici sono creati di volta in volta e firmati)
  - **Anonymous Diffie-Hellman** (senza autenticazione)
  - …
- **I cifrari supportati** sono: **RC4, RC2, DES, 3DES, IDEA, …**
- **I MAC supportati** sono: **MD5, SHA-1**

Generazione delle chiavi

lato server e lato client

nei rispettivi messaggi di **Hello**

dati predefiniti | pre-master secret | client nonce | server nonce

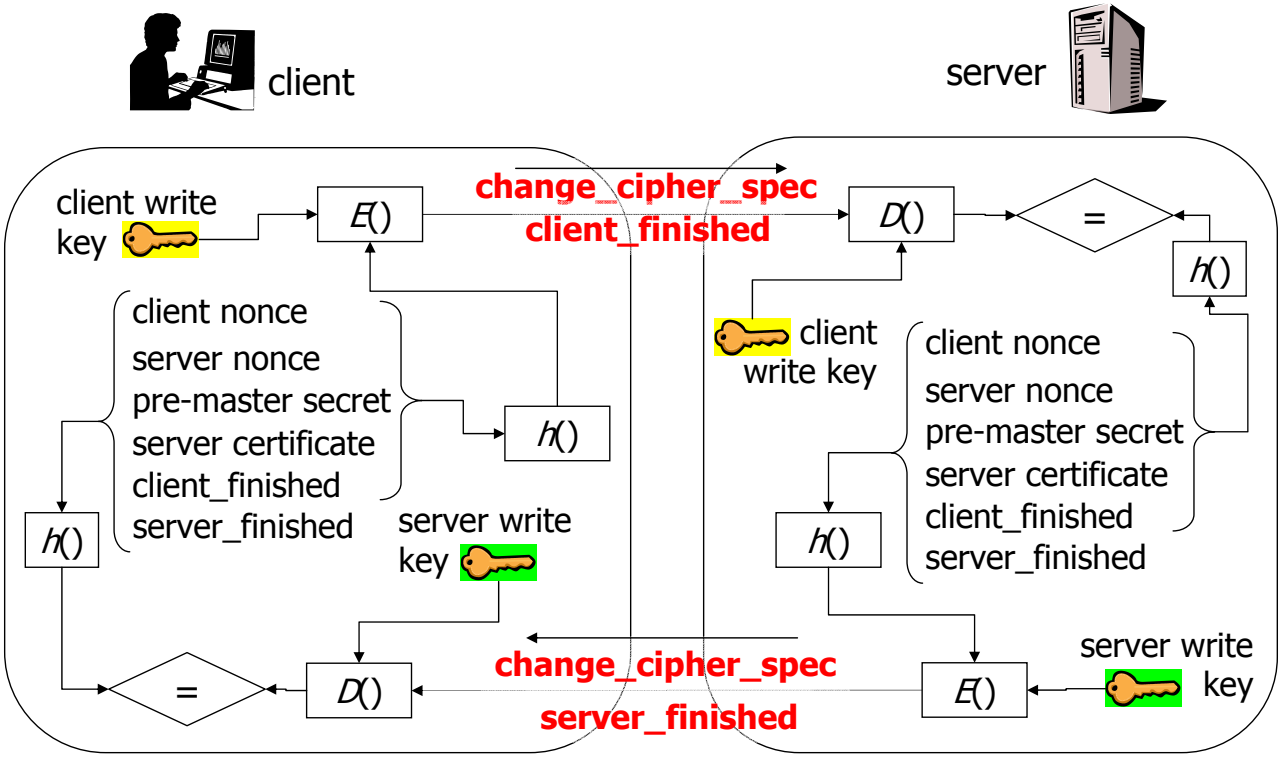
Pre-master secret è utilizzato come sorgente di entropia

Hash Multi-step

key block

- Server write MAC secret
- Client write MAC secret
- Server write key
- Client write key
- altro...

Protocollo Handshake: schema di principio (3)

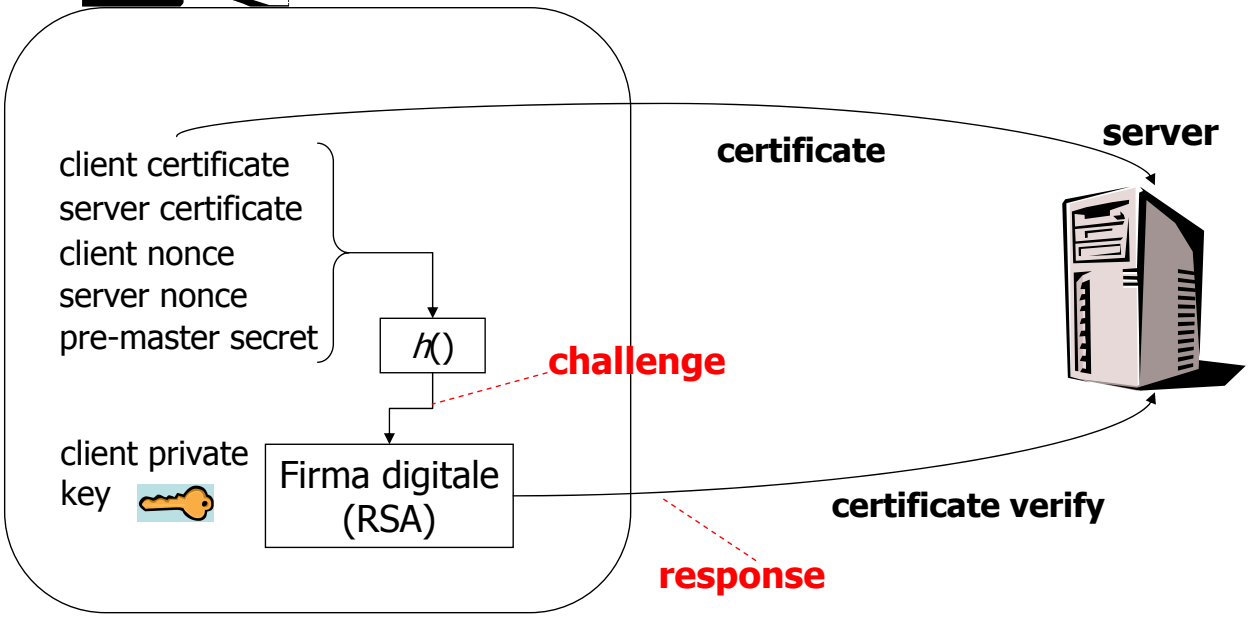


Autenticazione del client

- Il protocollo di Handshake autentica il server… ma come fa il server ad autenticare il client?
  - Una scelta tipica è quella di demandare l'autenticazione del client al livello applicativo sfruttando il canale sicuro instaurato da SSL per mezzo di user name e password, numero di carta di credito (!!),…
- Quanto è sicuro il canale SSL?
  - A causa delle restrizioni imposte dalla precedente normativa U.S. sulla esportazione di materiale crittografico, le vecchie versioni dei browser supportano solo chiavi di sessione a 40 bit (e chiavi pubbliche a 512 bit) invece dei 128 bit supportati dai browser più recenti
  - I vecchi browser sono ancora in uso; molti utenti sono ignari del problema
- SSL supporta anche l'autenticazione del client rispetto al server

Autenticazione del client: schema di principio (3)

- Il server richiede l'autenticazione del client con un messaggio **certificate request** dopo **server_hello**
- L'autenticazione è di tipo ***challenge-response***



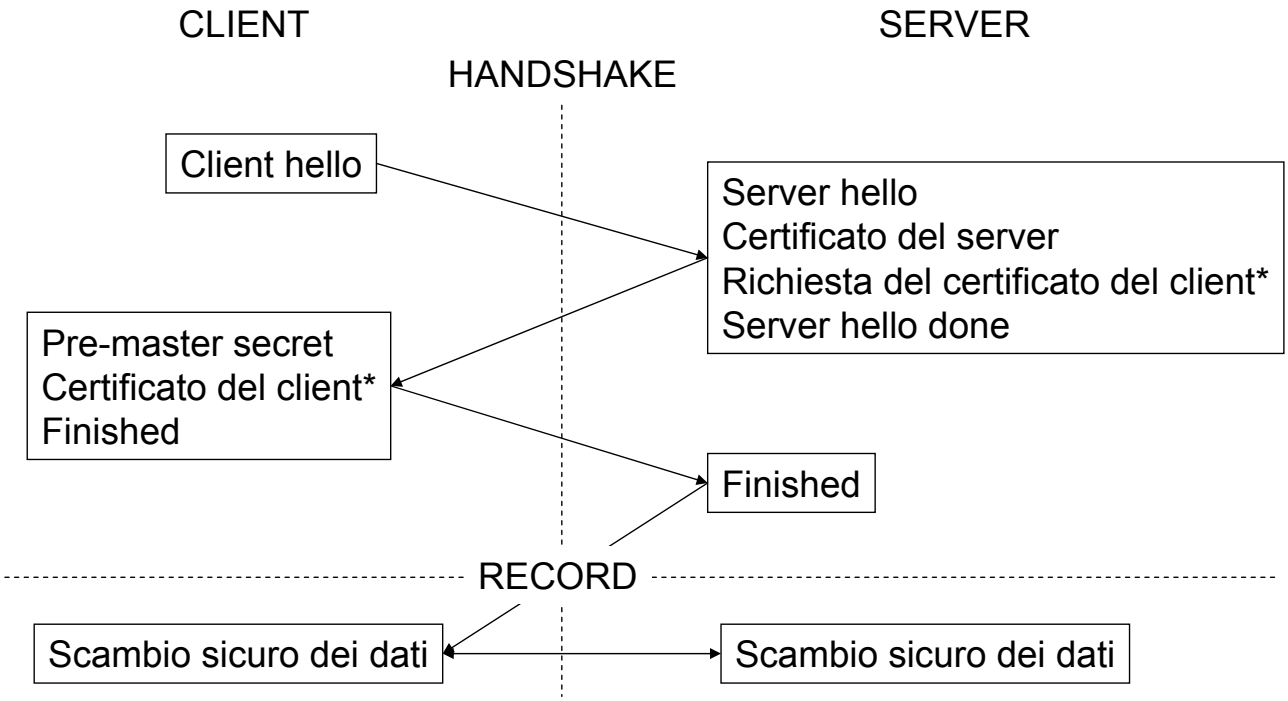
Sicurezza

- I nonce contenuti in client hello e server hello
  - Questi i nonce servono per costruire un master secret “fresco” ed evitare attacchi di tipo replay
- L’utilizzo di certificati
  - Protegge dal man-in-the-middle
- Le sequenze casuali
  - Il pre-master secret ed i nonce in client hello e server hello devono essere impredicibili
- Il protocollo Record
  - Numera il blocco in modo incrementale, lo autentica tramite il MAC e poi cifra tutto. Ciò evita replay, riordino e sostituzione in un blocco ma, se un blocco va perduto, i blocchi successivi devono essere ricreati e spediti nuovamente;
  - Il cifrario “protegge” il MAC

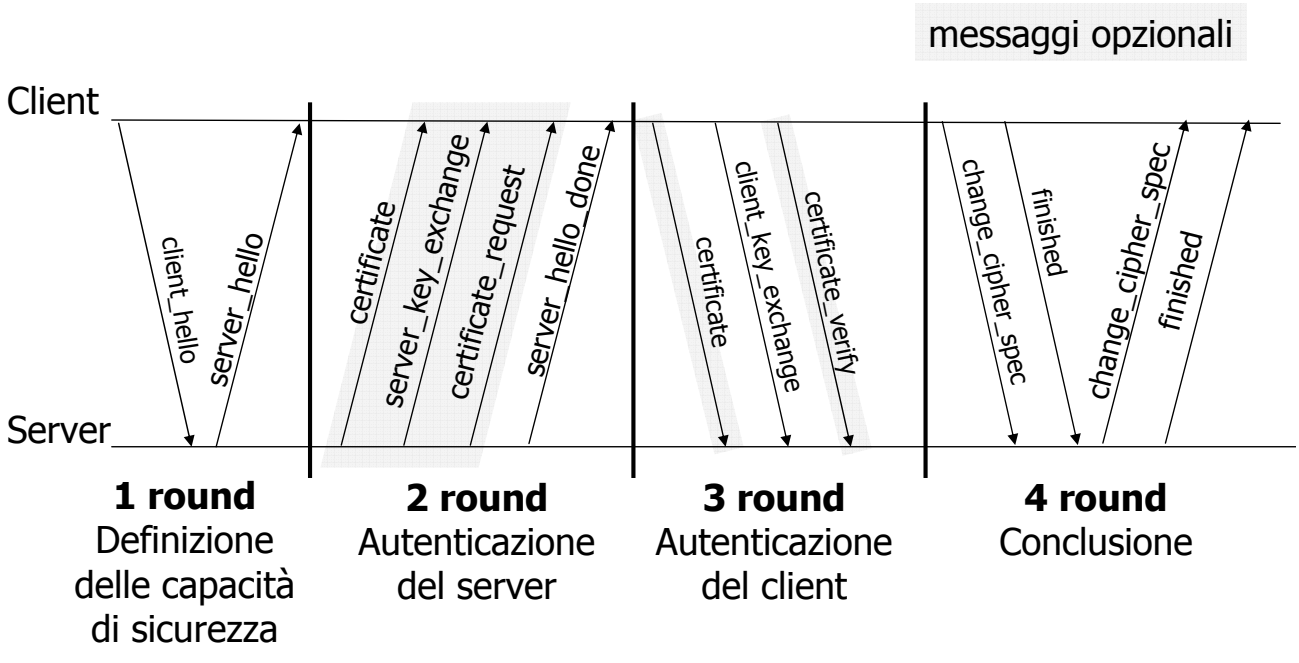
Protocollo Handshake: formato dei messaggi

TIPO	CONTENUTO
hello_request	nessun paramentro
client_hello	Versione, random, ID di sessione, suite di cifratura, metodo di compressione
server_hello	Versione, random, ID di sessione, suite di cifratura, metodo di compressione
certificate	Catena di certificati X.509v3
server_key_exchange	Parametri, firma
certificate_request	Tipo, autorità
server_hello_done	Nessun parametro
certificate_verify	Firma
client_key_exchange	Parametri, firma
finished	Valore hash

I protocolli Handshake: visione d'insieme



Il Protocollo Handshake: visione d'insieme

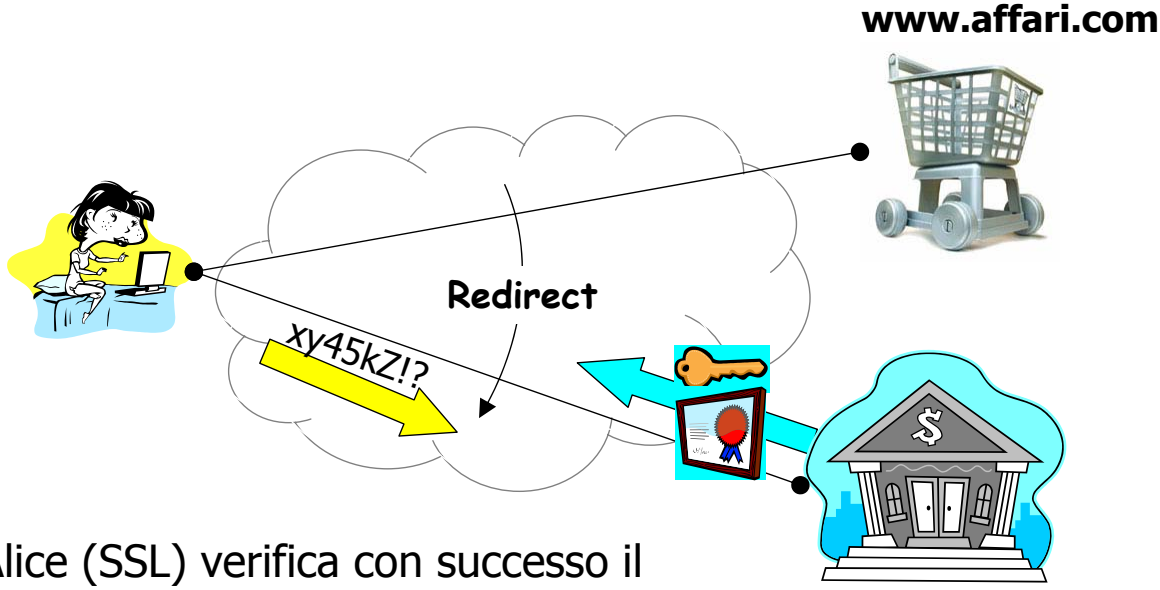


Gli altri protocolli di SSL

- Il protocollo change cipher spec è costituito da un solo messaggio (in chiaro) che ha come obiettivo quello di rendere operativa la cipher suite negoziata
- Il protocollo alert è utilizzato per comunicare al peer i messaggi di allarme relativi a SSL:

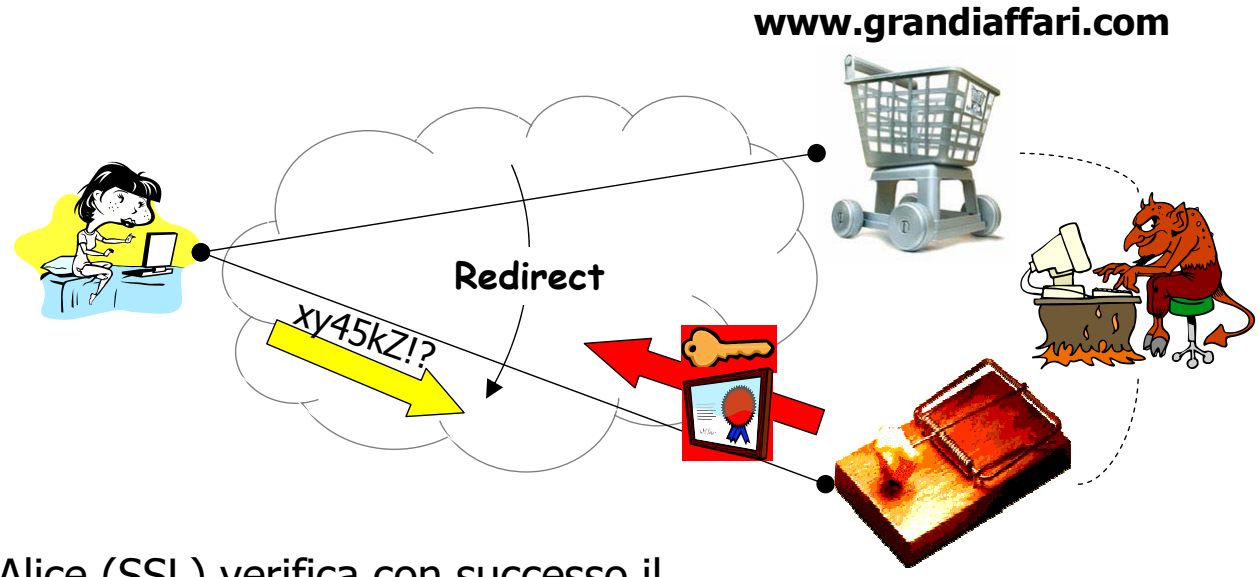
unexpected_message	no_certificate
bad_record mac	bad_certificate
decompression_failure	unsupported_certificate
handshake_failure	certificate_revoked
illegal_parameter	certificate_expired
	certificate_unknown

Il certificato è quello giusto?



Alice (SSL) verifica con successo il certificato della banca, stabilisce la connessione ed invia la propria PWD alla banca

Il certificato è quello giusto?



- Alice (SSL) verifica con successo il certificato dell'avversario, stabilisce la connessione ed invia la propria PWD alla banca

Il certificato è quello giusto?

- Il problema è che SSL opera ad un livello più basso di quello applicativo

➔ È l'applicazione che deve (indurre l'utente a) verificare che il nome richiesto sia uguale al nome contenuto nel certificato verificato

- ESEMPIO: Netscape
  - Il browser *notifica* all'utente se l'URL specificato dal browser e quello contenuto nel certificato del server sono diversi
  - L'utente decide se proseguire la connessione oppure no (interfaccia utente!!!)
  - In linea di principio non è detto che il controllo eseguito dal browser Netscape sia sufficiente per ogni tipo di applicazione Web-based

Acquisti in rete con SSL

Acquisti in rete mediante carta di credito

Decreto legislativo 22 maggio 1999, n. 185, di attuazione della direttiva 97/7/CE

Art. 8 - Pagamento mediante carta

1. Il consumatore può effettuare il pagamento mediante carta ove ciò sia previsto tra le modalità di pagamento, da comunicare al consumatore al sensi dell'articolo 3, comma 1, lettera e), del presente decreto legislativo.

2. L'istituto di emissione della carta di pagamento riaccredita al consumatore i pagamenti dei quali questi dimostri l'eccedenza rispetto al prezzo pattuito ovvero l'effettuazione mediante l'uso fraudolento della propria carta di pagamento da parte del fornitore o di un terzo, fatta salva l'applicazione dell'articolo 12 del decreto-legge 3 maggio 1991, n. 143, convertito, con modificazioni, dalla legge 5 luglio 1991, n. 197. L'istituto di emissione della carta di pagamento ha diritto di addebitare al fornitore le somme riaccreditate al consumatore.

Acquisti in rete mediante carta di credito

- **Gli istituti di emissione**, cui compete l'autorizzazione dell'operazione di pagamento, nonché i soggetti che rendono tecnicamente possibile la transazione on-line, **sono tenuti a controllare la correttezza del numero della carta e la data della sua scadenza ma non anche la corrispondenza tra il numero fornito e l'effettivo titolare**

- Gli istituti di emissione verificano la corrispondenza tra numero della carta di credito comunicato per effettuare una transazione on-line ed il nominativo fornito da colui che la effettua.

  Ad esempio, l'Address Verification Service (AVS) verifica che l'indirizzo di consegna sia quello con cui il possessore della carta è registrato

- In Europa il grado di sicurezza nelle transazioni on-line è minore e quindi il commercio elettronico è destinato ad incontrare resistenze anche da parte dei fornitori di che sopportano rischi elevati

Acquisti in rete mediante carta di credito

- Il fornitore di beni o servizi on-line **è tenuto ad accollarsi il rischio** della rivalsa degli istituti di emissione qualora, in caso di uso fraudolento delle carta, questi riaccreditano le corrispondenti somme al legittimo titolare.

- La legge **non consente** al fornitore di liberarsi dall'obbligo della restituzione delle somme agli istituti di emissione qualora dimostri
  1. di avere usato tutte le cautele necessarie e possibili ad evitare l'uso fraudolento della carta di credito
  2. che il fatto è stato causato dal caso fortuito.

- I fornitori dovranno usare tutte le cautele del caso per potere, nel caso di uso fraudolento di carte di credito, perlomeno rintracciare l'illegittimo utilizzatore e rivalersi su questo.

  Le conseguenze derivanti dall'addebito delle somme riaccreditate al titolare della carta potrebbero poi essere annullate contraendo una assicurazione a copertura dei danni (economici) derivanti da tale circostanza.

Acquisti in rete con SSL

Foglio informativo sulle operazioni e servizi offerti alla clientela

(cariprato)

Caratteristiche e rischi tipici

Struttura e funzione economica

CARTE DI DEBITO e CARTE DI CREDITO

Strumenti di pagamento rilasciabili a clienti della Banca che consentono:
- Acquisto di beni;
- Prestazione di servizio presso esercenti convenzionati.
- Ottenimento di contante presso sistemi automatici o sportelli bancari convenzionati.

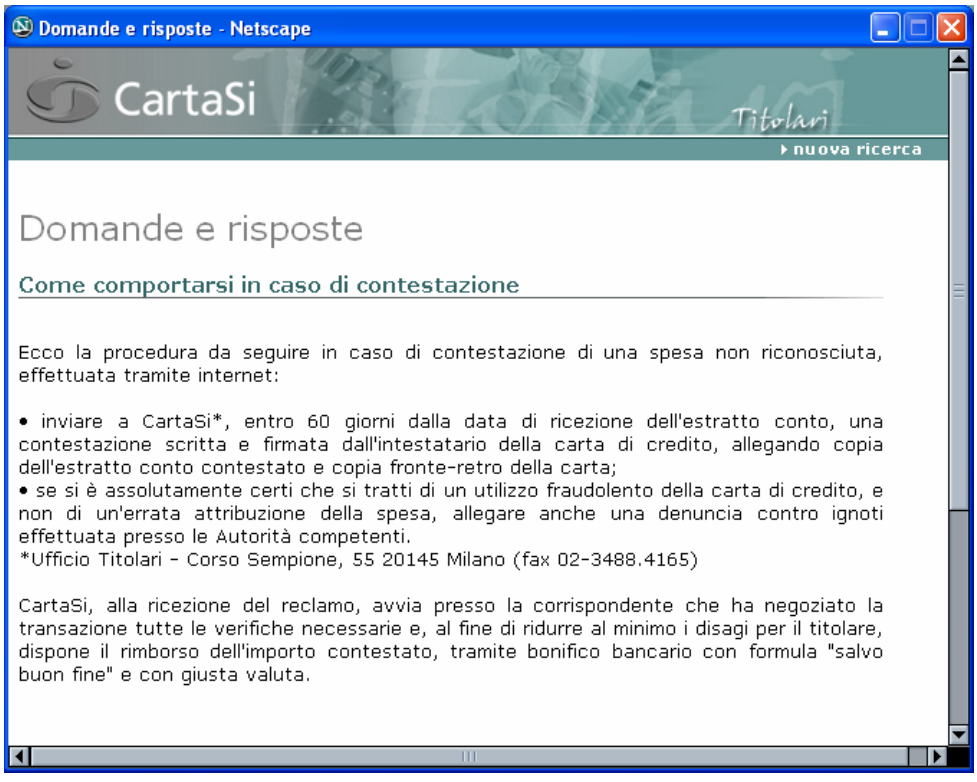
Funzione Bancomat: è il servizio in forza del quale la banca (emittente), attraverso il rilascio di una Carta, consente al correntista (c.d. "titolare") di effettuare prelievi di denaro — entro massimali di utilizzo stabiliti dal contratto - presso sportelli automatici (ATM) contraddistinti dal marchio Bancomat, digitando un codice segreto (c.d. P.I.N., "Personal Identification Number").
Funzione PagoBANCOMAT: è il servizio in forza del quale il correntista può compiere acquisti di beni e servizi presso esercizi commerciali convenzionati che espongono il marchio "PagoBANCOMAT", digitando il citato codice segreto.
L'utilizzo del sistema di pagamento è consentito nei limiti giornaliero e mensile, entro limiti di importo contrattualmente previsti, determinato dal momento dell'emissione e dalla capienza di conto corrente al momento dell'addebito.

Principali rischi (generici e specifici)

Il rischio relativo ad eventuali utilizzi fraudolenti effettuati con le Carte di Pagamento è limitato a 150 € per evento se il Titolare ha ottemperato e rispettato quanto indicato dalla "Raccomandazione della Commissione Europea del 30 giugno 1997 n. 97/489"

In sintesi il titolare è tenuto a:
- Firmare la carta nel caso che la stessa sia munita di apposita banda di scrittura;
- Osservare la massima attenzione nella custodia della carta e PIN e la massima riservatezza nell'uso del medesimo;
- Bloccare la carta nel caso di furto, smarrimento o uso fraudolento della medesima, confermando l'evento con denuncia o dichiarazione di smarrimento.

Acquisti in rete con SSL



Limiti di SSL

- *SSL è un protocollo sicuro ben progettato che utilizza algoritmi sicuri e robusti*
- *SSL però presenta i seguenti limiti*
  - l'utente ha l'onere di controllare le informazioni di sicurezza
  - SSL è vulnerabile allo spoofing dei nomi
  - SSL protegge solo la comunicazione