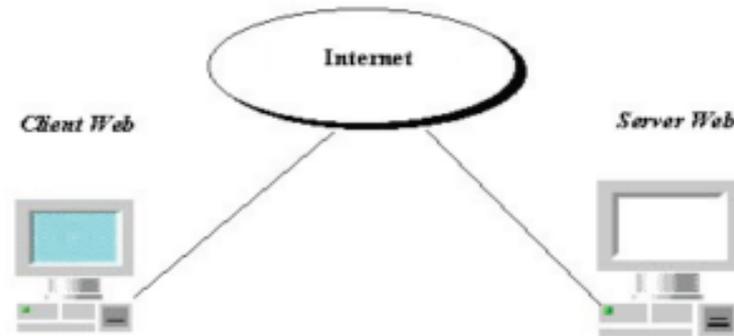


Comunicazioni sicure su Internet: HTTPS e SSL/TLS

HTTP - 1

- Come funziona nel dettaglio il Web?



- Uniform Resource Locator (**URL**) (Indirizzo simbolico pagina)
- Hyper Text Transfer Protocol (**HTTP**)
- Hyper Text Markup Language (**HTML**)

HTTPS (HTTP Secure) - 2

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

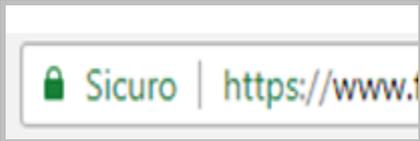
HTTPS è invece *Hyper Text Transfer Protocol over Secure Socket Layer /Transport Layer Security*.

Utilizza il **protocollo SSL/TLS** (*Secure Socket Layer /Transport Layer Security* - letteralmente *livello di socket sicuro/ sicurezza del livello di trasporto*) tra il livello di Trasporto e di Sessione.

L' **HTTPS** è:

- Sintatticamente identico allo schema **http://** ma con la **differenza** che gli accessi vengono effettuati sulla porta **443** (e non sulla **80**) - **https://**
- Tra il protocollo TCP e HTTP si interpone un livello di **crittografia/autenticazione**.

HTTPS - 3

- **HTTPS** verifica l'identità di un sito web e **crittografa** le informazioni inviate tra il sito web e il client e viceversa. Queste includono i cookie, i percorsi degli URL e i dati inviati tramite i moduli (form). **HTTPS** è progettato per impedire che queste informazioni vengano lette o modificate mentre sono in transito.
- Le **URL** di **HTTPS** iniziano con **https://**  e utilizzano la porta **443** di default, a differenza di **HTTP** le cui URL cominciano con **http://** e utilizzano la porta **80**.

HTTPS - 4

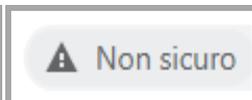
Come **riconoscere** una connessione **HTTPS**.

Per **incentivare** la **migrazione** verso **siti sicuri**, tutti i browser visualizzano ormai lo **status** dei website:

- **Un'icona a forma di lucchetto chiuso** di colore **grigio** o **verde** significa che il **sito è sicuro** ed ha un **certificato attendibile** (in Microsoft Edge o Chrome il **lucchetto grigio** indica: sito web crittografato e verificato; il **lucchetto verde** indica un certificato di convalida più esteso (**EV, Extended Validation**) che richiede un processo di verifica dell'identità molto rigoroso);



- **Un'icona a forma di cerchio** con il simbolo di **Informazioni** o **triangolo con !** significa **sito non sicuro**;



SSL/TLS *Secure Socket Layer /Transport Layer Security* - 5

Si tratta di un insieme di protocolli crittografici che aggiungono funzionalità di cifratura e autenticazione a protocolli preesistenti.

SSL: versione iniziale sviluppata da Netscape nel 1995 , poi evoluta nel protocollo standardizzato TLS nel 1999.

Protocolli SSL e TLS

Protocollo ↕	Publicato ↕	Status ↕
SSL 1.0	Non pubblicato	Non pubblicato
SSL 2.0	1995	Deprecato nel 2011 (RFC 6176 ^[2])
SSL 3.0	1996	Deprecato nel 2015 (RFC 7568 ^[2])
TLS 1.0	1999	Deprecazione pianificata per il 2020 ^[1]
TLS 1.1	2006	Deprecazione pianificata per il 2020 ^[1]
TLS 1.2	2008	
TLS 1.3	2018	

Il protocollo SSL/TLS provvede alla sicurezza del collegamento garantendo:

- **Autenticazione**: sicurezza dell'identità dei soggetti che comunicano (**crittografia asimmetrica**, ovvero a **chiave pubblica e privata** (ex. RSA)).
- **Riservatezza-Confidenzialità**: protezione dei dati da osservatori non autorizzati (la crittografia è usata dopo un **handshake (accordo)** iniziale per definire una **chiave simmetrica segreta di sessione (Diffie-Hellman)**. In seguito, per **crittografare i dati** è usata la **crittografia simmetrica (3DES, AES, IDEA ecc.)**).
- **Integrità**: sicurezza che il dato ricevuto è uguale al dato inviato (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** Message Digest, **SHA** Secure Hash Algorithm). In tal modo si verifica che i dati spediti tra client e server non siano stati **alterati** durante la trasmissione.

Transport Layer Security - 6

Funzionalità di TLS

- **Cifrare la connessione** al fine di garantire la **riservatezza** dei dati.
- **Autenticare il server** a cui si è connessi.

Funzionamento di TLS

- Il **server** invia al **client** un **certificato** attestante la **propria identità** e contenente la **propria chiave pubblica** (ad es. una chiave **RSA**).
- Il **client** **verifica l'identità** del **server** tramite **Certification Authority**. Poi genera una **chiave di sessione casuale** (o **Diffie-Hellman**) e la invia al server, **cifrandola** con la **chiave pubblica** del server.
- Il server **decifra** il messaggio con la propria **chiave privata** ed ottiene la **chiave di sessione**. Questa viene utilizzata per cifrare il successivo traffico dati con un **algoritmo simmetrico** (ad es. **3DES** o **AES** o **IDEA**).
- La **riservatezza** è quindi garantita dall'utilizzo **ibrido** di **cifratura simmetrica** e **asimmetrica**.
- L'**autenticazione** del server è **garantita** dal **certificato** rilasciato dalla **CA**.

Autorità di Certificazione -7

Lo **scambio di chiavi pubbliche** introduce un nuovo problema da risolvere.

Se ad esempio vogliamo comunicare in modo sicuro con Google, abbiamo bisogno della sua chiave pubblica e lo stesso vale per altri siti che vogliamo visitare (Facebook, Twitter, etc...).

Dato che esistono miliardi di siti web su Internet, come possiamo ottenere una **chiave pubblica** per ogni sito web che vogliamo visitare?

Ed è qui che entrano in scena le **Autorità di Certificazione** o **CA – Certification Authorities** come **DigiCert, Comodo, Symantec, GlobalSign, Google Trust Services, VeriSign, GeoTrust, Actalis**.

Lo scopo del **certificato digitale** è quello di garantire che una **chiave pubblica** sia **associata** alla vera **identità del soggetto** che la rivendica come propria.

Una **CA** è un'organizzazione di terze parti con 3 obiettivi principali:

- Rilasciare certificati digitali.
- Confermare l'identità del proprietario del certificato.
- Fornire la prova che il certificato è valido.

Nello scenario di **HTTPS** la **chiave pubblica** è rappresentata da un **certificato digitale**, più noto come **certificato SSL/TLS**. Un **certificato digitale** è un **certificato di identità elettronico**, cioè un **documento elettronico che associa l'identità di una persona ad una chiave pubblica**.

Certificato SSL/TLS - 8

Ora vediamo in che modo è possibile **ottenere un certificato SSL/TLS firmato da una Certification Authority**:

1. Il proprietario del sito web genera una **chiave pubblica** e una **chiave privata** (ex. **RSA**) ed invia un file di **richiesta di firma** del certificato (**CSR Certificate Signing Request**) e la sua **chiave pubblica** alla **CA**.
2. La **CA** crea quindi un **certificato personale basato sulla CSR**, dove sono indicati nome di dominio, nome del proprietario, data di scadenza e altre informazioni, appone la **firma digitale**, infine **crittografa** l'intero certificato con la **chiave pubblica** del sito e lo rimanda al proprietario del sito web.
3. Il **certificato** viene quindi **decifrato con la chiave privata** del proprietario del **sito web** ed, infine, **viene installato sul server**.

Il certificato è firmato digitalmente dall'autorità certificante (certification authority, CA) che quindi si fa garante dell'autenticità delle informazioni contenute nel certificato.

- **N.B.** La **firma digitale della CA** è **crittografata** dalla **chiave privata della CA** e può essere decifrata solamente con la **chiave pubblica della CA**, chiamiamo questa **chiave Certificato Radice (Root Certificate)**.
- Ogni dispositivo (pc, smartphone) ha, installato nel browser, un elenco di **certificati radice delle CA attendibili** e delle **CA intermedie**.

I Certificati SSL/TLS - 9

Il **Certificato Digitale** viene tipicamente distribuito mediante file **.DER** e contiene le seguenti **informazioni**:

- **nome del proprietario** a cui è stato rilasciato il Certificato.
- **il nome del dominio** associato al Certificato.
- **chiave pubblica** (2048 bit) del Certificato (visualizzabile in forma esadecimale).
- **nome della CA** che ha firmato il Certificato Digitale
- **numero di serie** del Certificato.
- **validità** del Certificato (data di inizio e data di scadenza)
- la **firma digitale** della **CA (CERTIFICATE SIGNATURE)** e l'algoritmo utilizzato per la firma (**MD5** o **SHA**): la **CA** si fa garante dell'**autenticità** delle informazioni contenute nel certificato.

Elenco Certificati Radice - 10

Elenco di **certificati radice** sul browser **google chrome** (Impostazioni -> Privacy e sicurezza -> Sicurezza -> Gestisci certificati):

Scopo designato: <Tutti>

Autorità di certificazione radice attendibili | Autori attendibili | Autori non attendibili

Rilasciato a	Emesso da	Data di s...	Nome
Chambers of Commerce Ro...	Chambers of Commer...	31/07/2038	Chambers of
Class 2 Primary CA	Class 2 Primary CA	07/07/2019	CertPlus Clas
Class 3 Public Primary Certifi...	Class 3 Public Primary ...	02/08/2028	VeriSign Clas
COMODO RSA Certification ...	COMODO RSA Certific...	19/01/2038	Sectigo (form
Copyright (c) 1997 Microsof...	Copyright (c) 1997 Mi...	31/12/1999	Microsoft Tim
DigiCert Assured ID Root CA	DigiCert Assured ID R...	10/11/2031	DigiCert
DigiCert Global Root CA	DigiCert Global Root CA	10/11/2031	DigiCert
DigiCert Global Root G2	DigiCert Global Root G2	15/01/2038	DigiCert Glob

Generale | Dettagli | Percorso certificazione

Informazioni sul certificato

Scopo certificato:

- Dimostra la propria identità ad un computer remoto
- Certifica che il software proviene dal relativo autore
- Protegge il software da modifiche dopo la pubblicazione
- Protegge i messaggi di posta elettronica
- Garantisce l'identità di un computer remoto
- Consente di firmare i dati con l'ora attuale

Rilasciato a: DigiCert Global Root CA

Rilasciato da: DigiCert Global Root CA

Valido dal 10/11/2006 al 10/11/2031

Generale | **Dettagli** | Percorso certificazione

Mostra: <Tutti>

Campo	Valore
Valido da	venerdì 10 novembre 2006 01:...
Valido fino a	lunedì 10 novembre 2031 01:0...
Soggetto	DigiCert Global Root CA, www...
Chiave pubblica	RSA (2048 Bits)
Parametri chiave pubblica	05 00
Identificatore chiave del so...	03de503556d14cbb66f0a3e21...
Identificatore chiave dell'au...	ID chiave=03de503556d14cb...
Utilizzo chiave	Firma digitale, Firma certificato

```
30 82 01 0a 02 82 01 01 00 e2 3b e1 11 72
de a8 a4 d3 a3 57 aa 50 a2 8f 0b 77 90 c9
a2 a5 ee 12 ce 96 5b 01 09 20 cc 01 93 a7
4e 30 b7 53 f7 43 c4 69 00 57 9d e2 8d 22
dd 87 06 40 00 81 09 ce ce 1b 83 bf df cd
3b 71 46 e2 d6 66 c7 05 b3 76 27 16 8f 7b
9e 1e 95 7d ee b7 48 a3 08 da d6 af 7a 0c
39 06 65 7f 4a 5d 1f bc 17 f8 ab be ee 28
d7 74 7f 7a 78 99 59 85 68 6e 5c 23 32 4b
```

Generale | Dettagli | **Percorso certificazione**

Percorso certificazione

DigiCert

Visualizza certificato

Stato certificato:
Il certificato specificato è valido.

Elenco Certificazioni Intermedie - 11

Elenco di **certificati di Autorità Intermedie** sul browser **google chrome** (Impostazioni -> Privacy e sicurezza -> Sicurezza -> Gestisci certificati):

Certificati

Scopo designato: <Tutti>

Autorità di certificazione intermedie | Autorità di certificazione radice attendibili | Autori atte

Rilasciato a	Emesso da	Data di s...	Nome
Entrust Certification Auth...	Entrust Root Certifica...	05/12/2030	<Nessuna>
Gandi Standard SSL CA 2	USERTrust RSA Certifi...	12/09/2024	<Nessuna>
GEANT OV RSA CA 4	USERTrust RSA Certifi...	02/05/2033	<Nessuna>
GeoTrust DV SSL CA	GeoTrust Global CA	25/02/2020	<Nessuna>
GeoTrust RSA CA 2018	DigiCert Global Root CA	06/11/2027	<Nessuna>
GeoTrust SSL CA - G3	GeoTrust Global CA	20/05/2022	<Nessuna>
GlobalSign Domain Validati...	GlobalSign Root CA	20/02/2024	<Nessuna>
GlobalSign Extended Valid...	GlobalSign	15/12/2021	<Nessuna>

Certificato

Generale | **Dettagli** | Percorso certificazione

Informazioni sul certificato

Scopo certificato:

- Dimostra la propria identità ad un computer remoto
- Garantisce l'identità di un computer remoto
- Criteri di rilascio

* Per ulteriori dettagli consultare l'informativa dell'Autorità di ce

Rilasciato a: GeoTrust RSA CA 2018

Rilasciato da: DigiCert Global Root CA

Valido dal 06/11/2017 al 06/11/2027

Certificato

Generale | **Dettagli** | Percorso certificazione

Mostra: <Tutti>

Campo	Valore
Valido fino a	sabato 6 novembre 2027 13:2...
Soggetto	GeoTrust RSA CA 2018, www....
Chiave pubblica	RSA (2048 Bits)
Parametri chiave pubblica	05 00
Identificatore chiave del so...	9058ffb09c75a8515477b1edf...
Identificatore chiave dell'au...	ID chiave=03de503556d14cb...
Utilizzo avanzato chiave	Autenticazione server (1.3.6....
Informazioni Autorità di cert	[1]Accesso alle informazioni su

```
30 82 01 0a 02 82 01 01 00 bf 8a d1 63 4d
e1 18 ea 87 5d e8 16 3c 8f 7f b6 be 87 17
37 a4 0c f8 31 3f 9f 45 54 40 21 d7 9d 07
9b ca 03 23 4a bd 9b ed 85 02 63 3f 9f 85
b9 ec 28 ef f2 86 22 db f8 4d 54 41 c5 b4
42 7f cf 33 17 01 0e 82 90 52 d3 c7 34 a4
c1 a1 01 da 32 a0 40 ad 1f 59 e4 33 fc a0
c3 96 ac 68 6c d3 e8 99 73 8c 26 10 77 cb
b7 3f 39 32 e8 d2 59 28 ee 07 86 e2 09 3b
```

Certificato

Generale | Dettagli | **Percorso certificazione**

Percorso certificazione

- DigiCert
 - GeoTrust RSA CA 2018**

Visualizza certificato

Stato certificato:

Il certificato specificato è valido.

Gerarchia di Certificati - 12

Ma come fidarsi della **Certification Authority**?

- L'identità di ogni **CA** è garantita a sua volta da un certificato rilasciato da una **CA "superiore"** ...
- Fino ad arrivare alla **root authority**, un'autorità certificante **non certificata da nessuno**, ovvero **certificata da se stessa**.
- Se la **root authority** è nota a livello mondiale e sottoposta a verifiche annuali da appositi organismi di controllo, possiamo ragionevolmente **fidarci** dei suoi **certificati**.

Root Authorities - 13

- Per questo motivo le **root authorities** fidate sono poche (meno di 40 in tutto il mondo), con **VeriSign** che detiene attualmente più del **50%** del mercato.
- I certificati delle root authorities sono “**self-signed**” in quanto non possono essere firmati da nessun'altra **CA**.
- Per garantire il processo di **verifica dei certificati**, tutti i **browser**, **client di posta elettronica**, e in generale ogni software che faccia uso di connessioni **TLS**, sono **distribuiti assieme ai certificati delle root authorities (Root Certificate - Certificati Radice)**.

Connessione HTTPS tra Browser e Server - 14

Ora vediamo come avviene la **connessione HTTPS** tra client browser e sito web, prendendo come esempio il sito <https://www.isisfermi.edu.it/> e **Actalis Domain Validation server CA G3** come **CA - Certification Authority**.
Cliccando sul **lucchetto grigio** davanti alla url e poi scegliendo **Certificato**:

Visualizzatore certificati: *.isisfermi.edu.it

Generali | Dettagli

Rilasciato a

Nome comune (CN)	*.isisfermi.edu.it
Organizzazione (O)	<Non parte del certificato>
Unità organizzativa (OU)	<Non parte del certificato>

Emesso da

Nome comune (CN)	Actalis Domain Validation Server CA G3
Organizzazione (O)	Actalis S.p.A.
Unità organizzativa (OU)	<Non parte del certificato>

Periodo di validità

Emesso in data	mercoledì 23 febbraio 2022 18:08:32
Scade in data	domenica 26 marzo 2023 19:08:32

Impronte digitali

Impronta digitale SHA-256	E0 FA 07 38 63 4A E6 3E 4F 77 E7 C6 41 4F 62 65 C6 88 A5 A5 08 26 BE A0 95 ED 18 3B 9B 41 0A 41
Impronta digitale SHA-1	7B 9A 9A E6 14 D3 D4 55 61 85 BF 73 35 11 25 27 D8 A7 12 6C

Visualizzatore certificati: *.isisfermi.edu.it

Generali | **Dettagli**

Gerarchia certificati

- Actalis Authentication Root CA
 - Actalis Domain Validation Server CA G3
 - *.isisfermi.edu.it

Campi certificato

- Non prima
- Non dopo
- Oggetto
 - Info sulla chiave pubblica del soggetto
 - Algoritmo chiave pubblica del soggetto
 - Chiave pubblica del soggetto**
 - Estensioni
 - Limitazioni di base certificato

Valore campo

Modulo (2048 bit):
A9 7A 3D 4A 68 FE 4D AC 6A 6D 30 EF 3E A2 17 E3
66 38 08 AB DD F5 6C ED B9 F8 71 A9 CB 33 6D 33
7A EF 6F 5A 35 14 18 C9 B1 49 B3 2B 5F AB 1D 67
B3 80 89 4D 66 FA 82 BB 5E 7C BA BF 40 21 FE 2A

Esporta...

Connessione HTTPS tra Browser e Server - 15

Visualizzatore certificati: *.isisfermi.edu.it

Generali **Dettagli**

Gerarchia certificati

▼ Actalis Authentication Root CA

▼ Actalis Domain Validation Server CA G3

*.isisfermi.edu.it

Actalis è una **Certification Authority** qualificata per l'erogazione di servizi certificati e riconosciuta in tutto il mondo per l'emissione di **certificati SSL Server**.

Dal 2009 parte del **Gruppo Aruba**, la cui capogruppo è **Aruba S.p.A.**, società italiana leader nei servizi di data center, cloud, web hosting, email e registrazione di nomi di dominio, **Actalis** oggi serve importanti funzioni della Pubblica Amministrazione Centrale italiana, oltre ad aziende private di ogni settore e dimensione a livello internazionale.

Sito: <https://www.actalis.com/>

Durante una connessione **HTTPS** avvengono **due passaggi**:

- L'**handshake** (letteralmente **stretta di mano**) per **convalidare il certificato del sito web**.
- La **creazione di una connessione sicura** tra **client e sito web**.

Handshake - 16

Ecco cosa succede durante la **stretta di mano** tra **browser** e **sito web**:

- Il **Client** invia al **Server** **HTTPs** un **ClientHello message** contenente la versione di **TLS/SSL** impostata sul client più la cosiddetta **cipher suite**, (insieme di codici), cioè un elenco dei protocolli di **Autenticazione** (tipo **RSA**), **Crittografia** (tipo **3DES**, **AES**, **IDEA**) con relativa **profondità di chiave** e **Funzioni HASH** (tipo **MD5** e **SHA**) **supportati** dal **browser** utilizzato per la richiesta.
- Il **Server** risponde inviando in chiaro una **lista di Protocolli Scelti** (fra quelli supportati dal browser), la sua **chiave pubblica** + il **certificato digitale di autenticazione** (firmato da **Actalis Domain** con la sua chiave privata).
- Per **verificare l'autenticità del certificato**, il **browser** preleva dall'elenco dei **certificati radice o intermedi** la **chiave pubblica** di **Actalis Domain** e tenta di **decodificare la firma digitale del certificato** che è stata **crittografata tramite la chiave privata** di **Actalis Domain**.
- Se è in grado di **decifrare** la **firma digitale del certificato** passa allo step successivo di creazione di una **connessione sicura col server**, altrimenti mostra all'utente un avviso di **Certificato non Valido** come si può vedere dalla figura seguente.

Avviso Fallimento Handshake - 17



La connessione non è privata

Gli utenti malintenzionati potrebbero provare a carpire le tue informazioni da **untrusted-root.badssl.com** (ad esempio, password, messaggi o carte di credito). [Ulteriori informazioni](#)

NET::ERR_CERT_AUTHORITY_INVALID

Invia automaticamente a Google [alcune informazioni sul sistema e alcuni contenuti delle pagine](#) per contribuire a rilevare app e siti pericolosi. [Norme sulla privacy](#).

AVANZATE

Torna nell'area protetta

Connessione Sicura a Chiave Simmetrica - 18

Come già detto, con la richiesta della pagina di www.isisfermi.edu.it, il server di Isisfermi invia la sua **chiave pubblica** al browser.

Tutti i dati cifrati con questa **chiave pubblica** possono essere decifrati solo dalla **chiave privata** di Isisfermi.

- Dopo aver **convalidato** il **certificato**, il browser crea una nuova **chiave simmetrica di sessione** (o una **pre-shared key Diffie-Hellman**) facendone una copia. Queste chiavi saranno usate per crittografare e decrittografare i dati.
- Il browser quindi **crittografa** la **chiave simmetrica di sessione** con la **chiave pubblica di Isisfermi** ed invia tutto al server di Isisfermi .
- Il server di Isisfermi decodifica la **chiave simmetrica di sessione** con la sua **chiave privata**.
- Ora server e browser hanno entrambi una copia della **chiave simmetrica di sessione** creata dal browser. Nessun altro ha questa chiave, quindi solo server e browser **possono cifrare e decifrare** i dati in **maniera sicura**.
- Quando Isisfermi invia dati al browser, prima li cifra con la chiave di **simmetrica di sessione** e il browser decodifica i dati con la sua copia di questa chiave. Lo stesso avviene se è il browser ad inviare i dati.
- **Client** e **Server** trasmettono i dati codificandoli con la **chiave simmetrica** concordata. In coda ad ogni messaggio l'**End Point autenticato** (il server, oppure **entrambi** in caso di **autenticazione bilaterale**), aggiunge la propria **Firma Digitale** che consiste in una **impronta SHA256 univoca** cifrata con la **chiave privata**. Il ricevente, utilizzando il **Certificato Digitale** del mittente, **verifica** la **Firma Digitale** che garantisce sia l'**integrità** del **messaggio** sia l'**autenticità** del **mittente**.

Funzionamento HTTPS - 19

Riepilogo passo dopo passo.

1. **Isisfermi** richiede un **certificato** a **Actalis Domain**.
2. **Actalis Domain** verifica che è davvero **Isisfermi** che sta effettuando la richiesta.
3. **Isisfermi** invia a **Actalis Domain** la propria **chiave pubblica**.
4. **Actalis Domain** usa la propria **chiave privata** per firmare digitalmente la **chiave pubblica** di **Isisfermi**.
5. **Actalis Domain** dà a **Isisfermi** la **chiave pubblica** firmata, questa rappresenta ora il **Certificato SSL/TLS** di **Isisfermi**.
6. **Lo studente** si collega col suo browser al sito web di **Isisfermi** ed inizia la fase di **handshake** (protocolli e hash supportati).
7. **Isisfermi** invia al browser il **Certificato SSL/TLS**.
8. **Utilizzando** la **chiave pubblica** di **Actalis Domain**, che si trova nell'archivio dei **certificati radice** del browser, viene verificata la firma di **Actalis Domain** sul **Certificato SSL/TLS** di **Isisfermi** .

Funzionamento HTTPS - 20

9. Se tutto ok, viene generata una **chiave segreta simmetrica di sessione** e si utilizza la **chiave pubblica** di Isisfermi, ovvero il **Certificato SSL/TLS**, per **crittografarla**.
10. Viene inviata a Isisfermi la **chiave segreta simmetrica di sessione** cifrata con la **chiave pubblica** di Isisfermi (in alcuni casi si utilizza **pre-shared key Diffie-Hellman**).
11. Isisfermi **decifra** la **chiave segreta di sessione** con la propria **chiave privata** e la trattiene.
12. Il **browser** dello studente e Isisfermi utilizzano la **chiave segreta simmetrica di sessione** condivisa per **cifrare** le **comunicazioni successive**.
13. Così viene raggiunta l'**autenticazione** e la **segretezza** e finché **Actalis Domain** è ritenuta una **CA attendibile**, lo studente può essere certo che i **certificati di Isisfermi** saranno **sicuri e affidabili**.