Sicurezza informatica nel luogo di lavoro PA

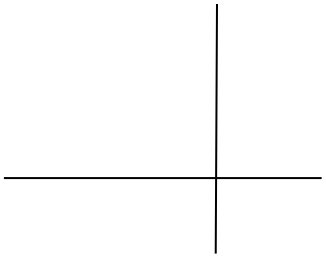
prof. Monica Palmirani

Definizione di sicurezza informatica

- Art. 32 GDPR «b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;»
- Sicurezza informatica:

«l'insieme dei mezzi e delle tecnologie tesi alla protezione dei sistemi **informatici** in termini di disponibilità, confidenzialità e integrità dei beni o asset **informatici**.»

Sicurezza informatica

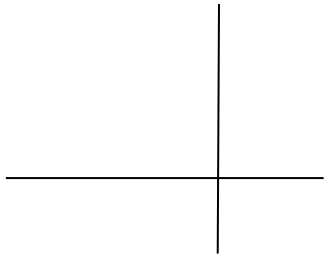


- Hardware
- Software
- Dati

- Fisica
- Logica
- Organizzativa

Sicurezza

- Sicurezza dell'autenticazione dei soggetti attori
  - autenticazione
- Sicurezza degli applicativi
  - autorizzazione e sicurezza degli applicativi WEB
- Sicurezza dell'integrità del dato
  - es. virus
- Sicurezza del sistema di rete
  - firewall e proxy
- Sicurezza del canale di trasmissione
  - es. VPN
- Sicurezza del computer
  - es. policy di password
- Sicurezza dei dispositivi
  - dischi e mobile



Autenticazione

Identificazione elettronica

- http://www.chyp.com/wp-content/uploads/2016/07/PRJ.1578-Digital-Identity-Issue-Analysis-Report-v1_6-1.pdf

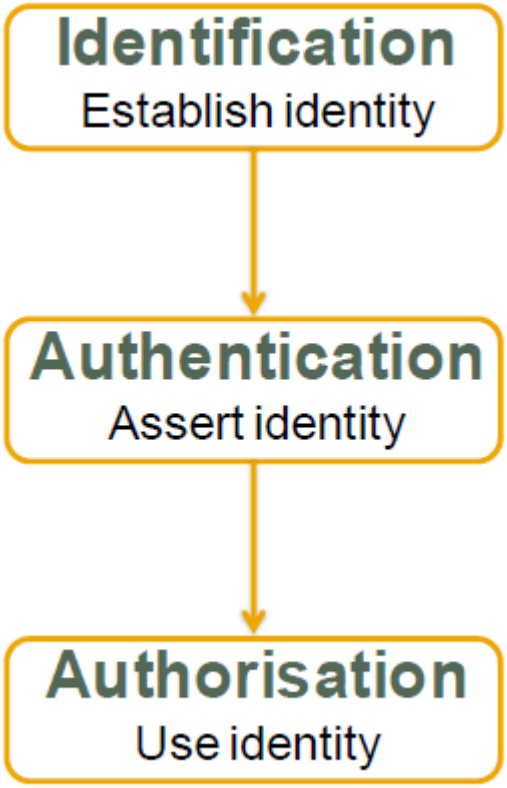


Figure 6: What is digital identity?

Articolo 3

Definizioni

Ai fini del presente regolamento si intende per:

1) «identificazione elettronica», il processo per cui si fa uso di dati di identificazione personale in forma elettronica che rappresentano un'unica persona fisica o giuridica, o un'unica persona fisica che rappresenta una persona giuridica;

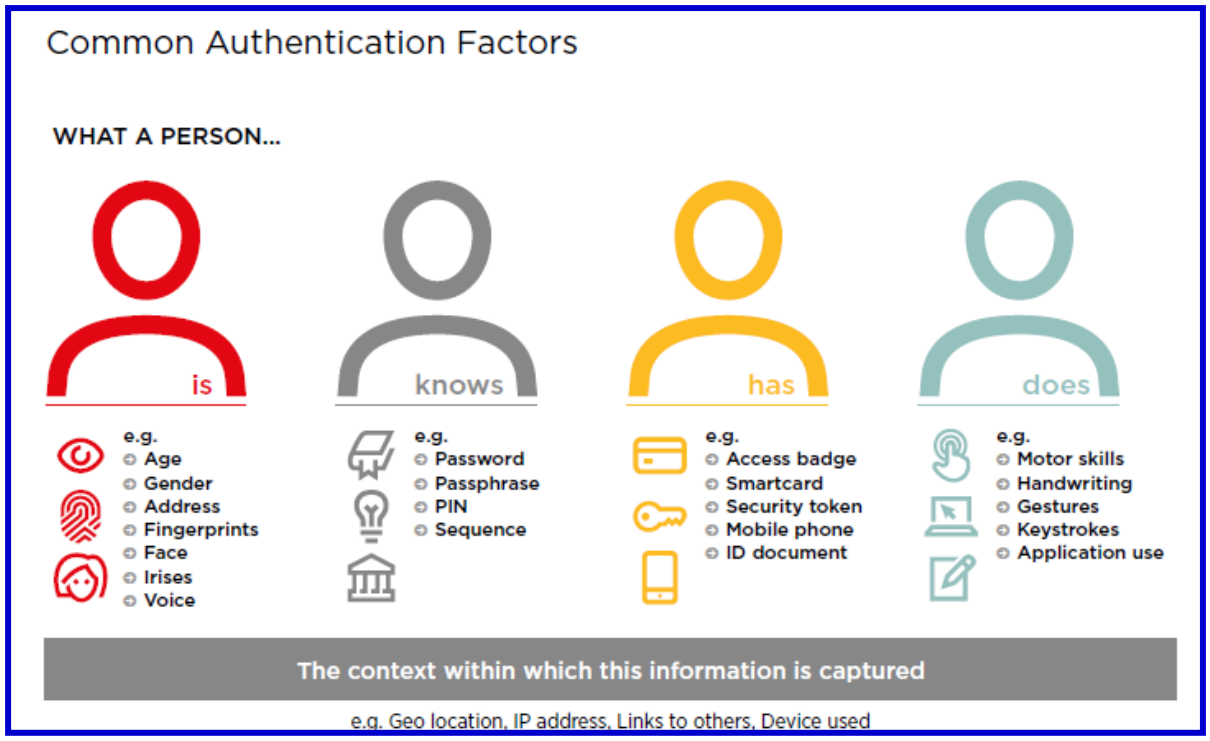
Regole di sicurezza

- Qualche cosa che sono
- Qualche cosa che conosco
- Qualche cosa che ho
- **Qualche cosa che faccio**

Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation

A joint World Bank Group – GSMA – Secure Identity Alliance Discussion Paper

JULY 2016



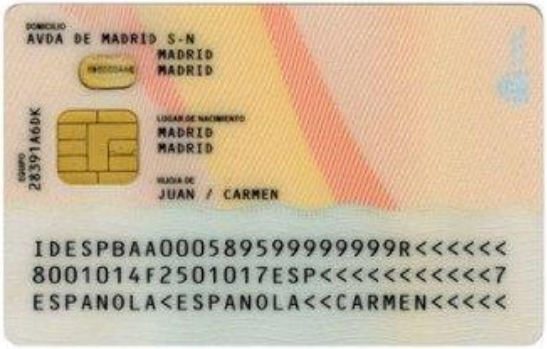
eID in Europe

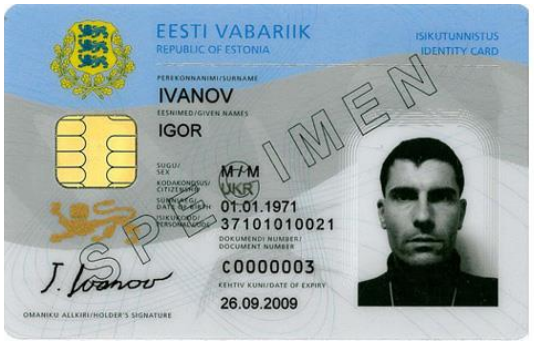
- Carta nazionale di identità elettronica (due fattori: card and pin)
- Carta nazionale dei servizi (due fattori : card and pin)
- Passwords+Token (due fattori : password and token)
- Password (un fattore : password)
- Sistemi biometrici (tre fattori : card+pin+biometric data)

See:

eID: carta di indentità elettronica

- Riparte il progetto carta di indentità elettronica





https://en.wikipedia.org/wiki/National_identity_cards_in_the_European_Economic_Area
CC BY-SA 4.0 (http://creativecommons.org/licenses/by-sa/4.0)], via Wikimedia Commons

- Le carte di identità elettroniche in Europa

Andrea SERVIDA
DG CONNECT, European Commission
Head of Unit "eGovernment and Trust"

European Commission

Countries with nationally supported eID schemes

Nearly all Member States (will) have a nationally supported eID scheme in place

Preliminary data from the ongoing CEF eID Stakeholder Analysis Report by Deloitte

- Countries with eID schemes:
  AT, BE, DE, DK, EE, ES, FI, HR, HU, IT, IS, LT, LU, LV, MT, NL, NO, PT, RO, SE, SK, TR, UK
- Countries setting-up national eID schemes:
  BG, CY, CZ, EL, FR, SI
- Countries to be confirmed:
  IE, PL

Information provided by MSs (as of 1 January 2016):
eID cards in 15 MSs (6 planned), other eID means in 24 MSs
25 MSs having either an eID card or other eID means

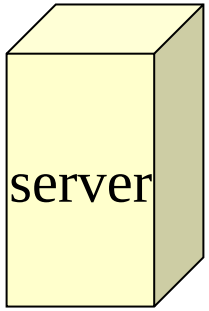
eID tools: carte nazionali dei servizi

OTP

- One Time Password:
  - codice: uno strumento che fornisce (mobile, token, email) codice unico (e.g., 30 seconds)
  - dinamico: il codice cambia
  - one-time: si usa una sola volta

Check between the two codes

4



seed + time = 225646 ⟺ 225646 = time + seed

1 **Local generation of the OTP**

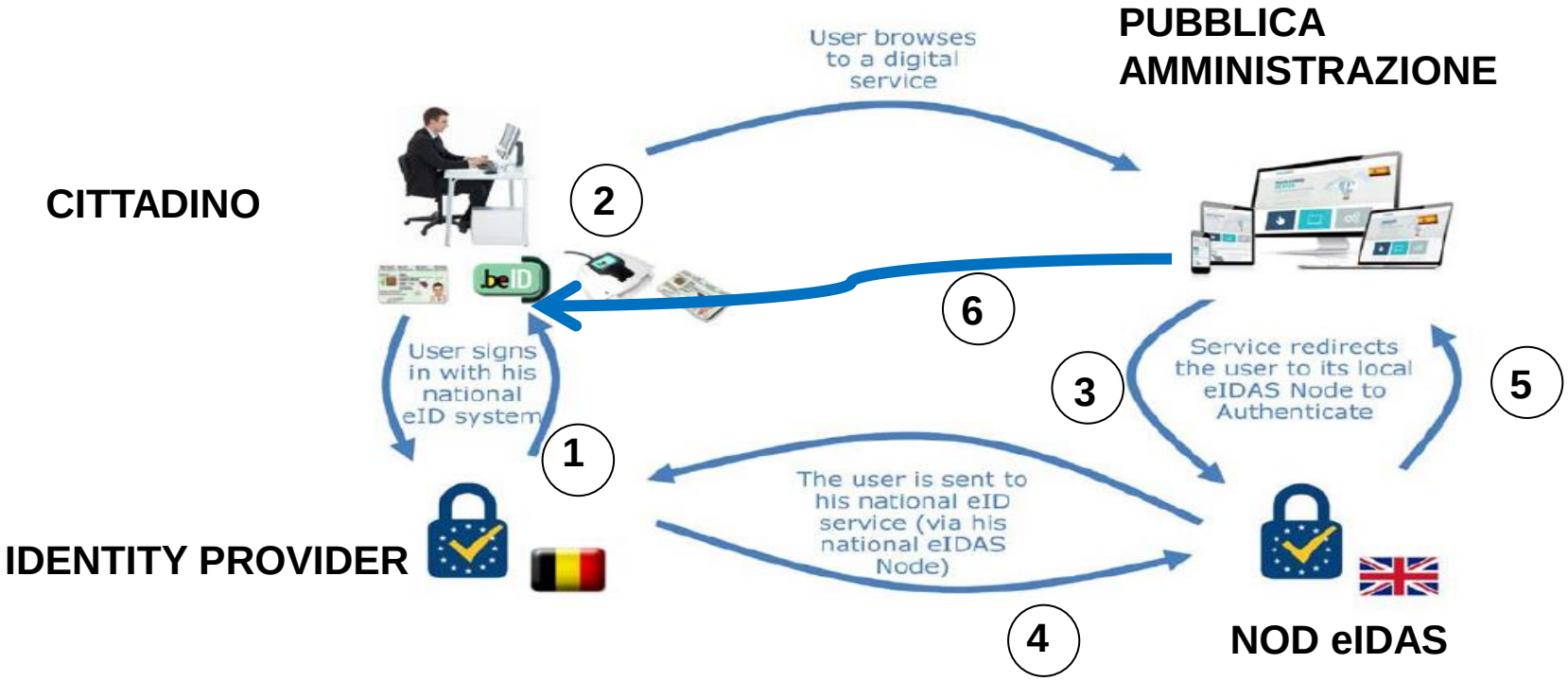
INPUT OF THE OTP in the system

2

Remote generation of the OTP

3

Goal del regolamento eIDAS: comunicazioni transfrontaliere



[Figure 4: eID authentication under eIDAS - user accessing a UK service with a foreign eID]

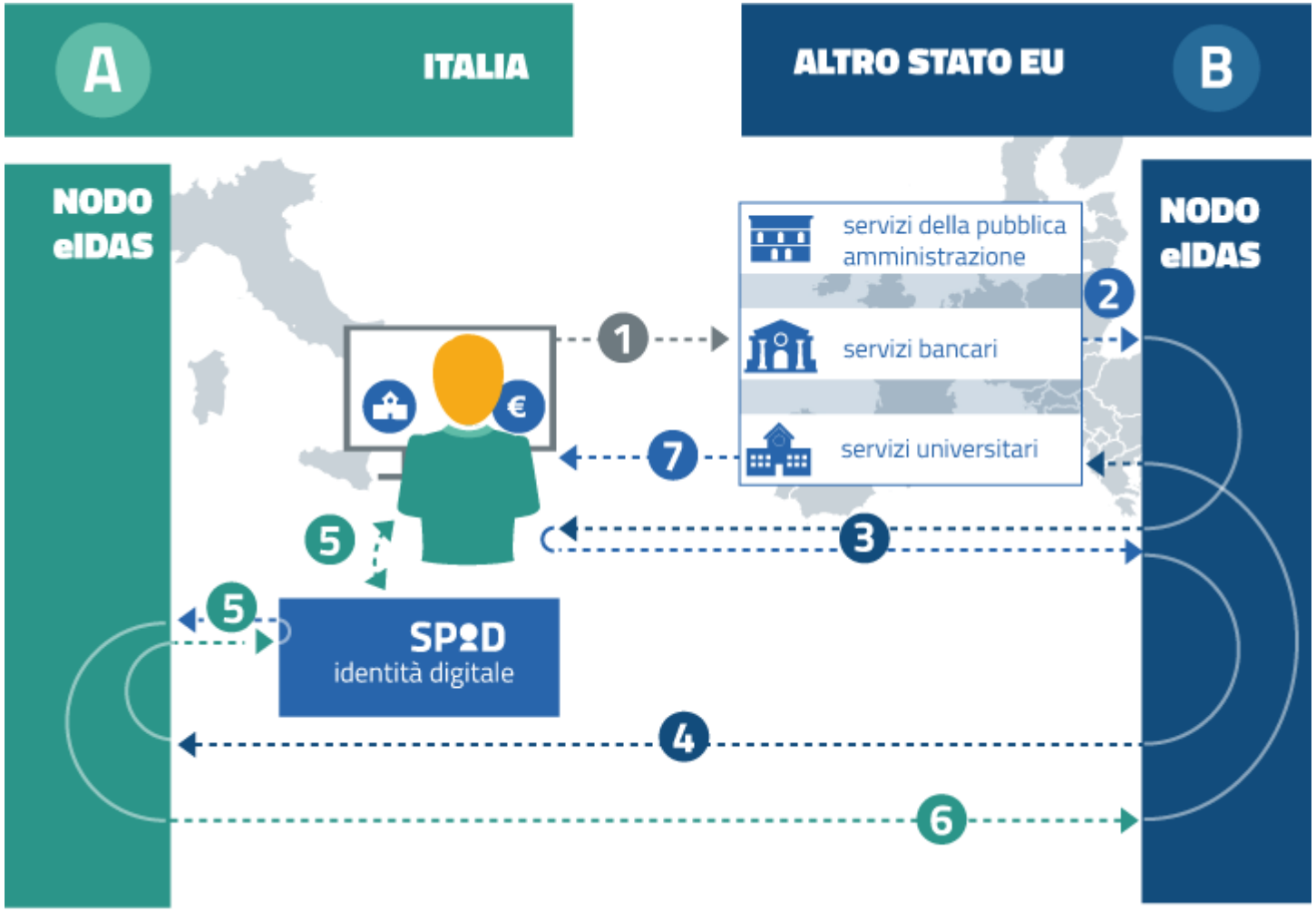
Il progetto FICEP - First Italian Crossborder eIDAS Proxy

Ultimo aggiornamento 26 Luglio 2016

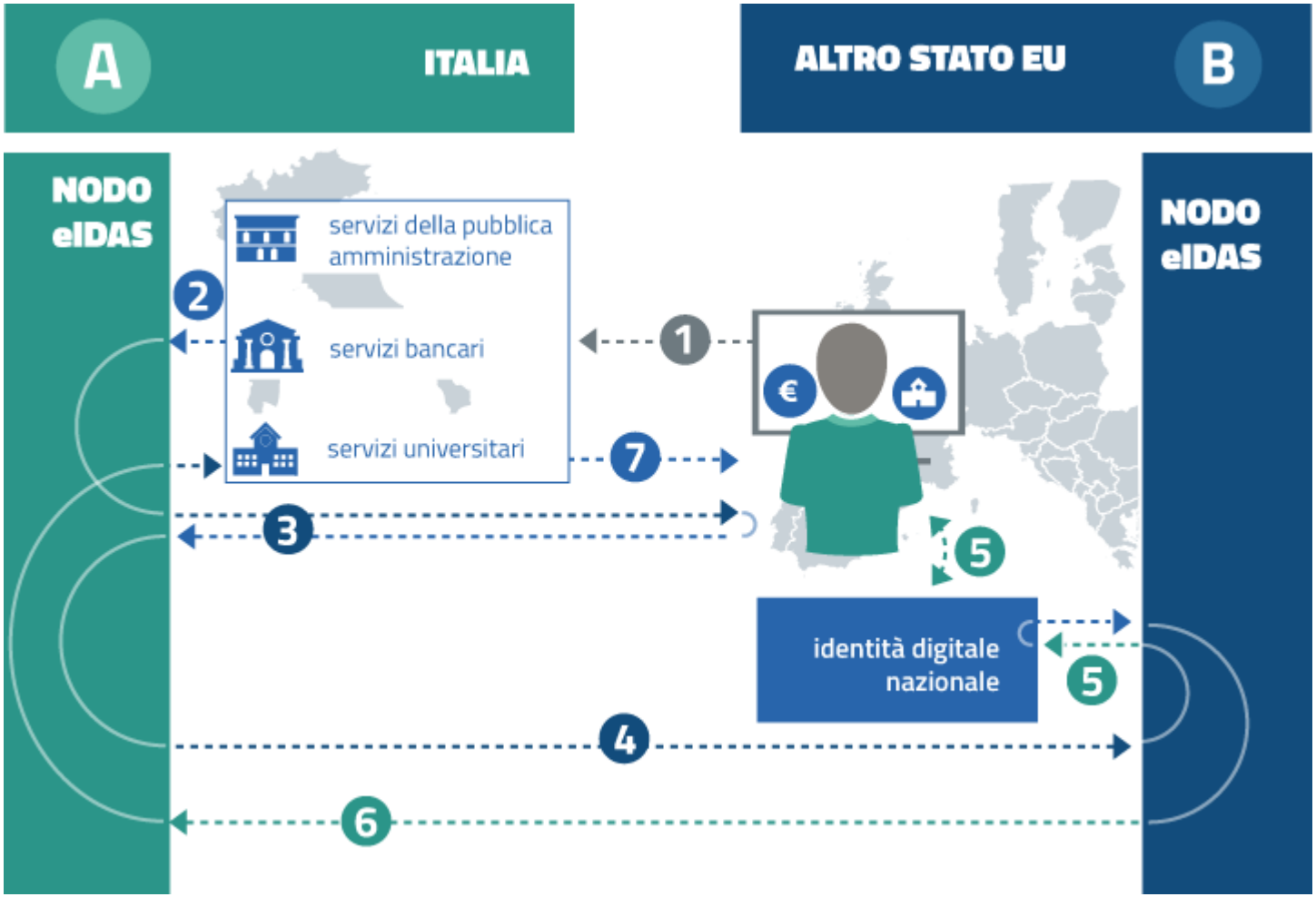
FICEP (First Italian Crossborder eIDAS Proxy) è il progetto nazionale finanziato dalla Commissione Europea per la realizzazione del nodo eIDAS italiano. FICEP è il primo "server trasfrontaliero italiano": la sua implementazione consentirà la circolarità delle identità digitali italiane fra tutti gli stati membri dell'Unione Europea.

AgID, in raggruppamento con Infocert S.p.a., Politecnico di Torino, Telecom Italia S.p.a., si è aggiudicata con il bando CEF-Telecom eID 2014 un finanziamento per la realizzazione del nodo eIDAS italiano.

Nodo eIDAS


A
ITALIA
ALTRO STATO EU
B
NODO eIDAS
NODO eIDAS
servizi della pubblica amministrazione
servizi bancari
servizi universitari
SPID
identità digitale
1
2
3
4
5
5
6
7

Nodo eIDAS


A
ITALIA
ALTRO STATO EU
B
NODO eIDAS
NODO eIDAS
servizi della pubblica amministrazione
servizi bancari
servizi universitari
identità digitale nazionale
1
2
3
4
5
5
6
7

Autenticazione

- Autenticazione è il procedimento attraverso il quale un *utente* (inteso come persona fisica, hardware, software, un applicativo) viene riconosciuto da un sistema informatico

- L'autenticazione avviene in questo modo:
  - *Identificazione fisica (per le persone fisiche)*
  - Rilascio delle credenziali ossia di id e password o dispositivi per il riconoscimento
  - Immissione nel sistema delle credenziali associate alla persona fisica
  - Utilizzo delle credenziali da parte dell'utente
  - Riconoscimento da parte del sistema dell'utente

Identificazione

- Per le persone fisiche l'autenticazione è preceduta *dall'identificazione*

- L'identificazione è una procedura organizzativa-tecnologica attraverso la quale si verifica:
  - l'identità fisica dell'individuo
  - le caratteristiche rispetto al servizio rilasciato (ruolo, stato civile, fedina penale, ecc.)
  - si rilasciano le credenziali
- Le procedure che assegnano credenziali senza un'opportuna identificazione rompono l'anello di congiunzione persona fisica→ codici digitali che la rendono riconoscibile in rete

Procedure di Identificazione

- Le procedure di identificazioni possono essere di tre tipi:
  - *De visu* – viene identificato l'individuo da personale preposto e vengono consegnate le credenziali
  - *Registrazione mista* – viene chiesta una registrazione via Internet dell'individuo alla quale farà seguito l'invio delle credenziali via e-mail o web nonché di una parte del PIN. La rimanente parte del PIN verrà inviata via raccomandata al destinatario. Questo meccanismo garantisce un certo grado di affidabilità ma non la certezza assoluta.
  - *Registrazione via Web* – viene chiesta una registrazione via Internet dell'individuo il quale riceverà le credenziali vie e-mail o web.

Credenziali

- Autenticazione basata su *password*
  - ID+password
  - ID+password+PIN
  - Misure minime di sicurezza – Allegato B – otto caratteri
  - Se non utilizzate da 6 mesi vengono disattivate
  - La password deve essere modificata almeno ogni 6 mesi, 3 mesi per i dati sensibili
- Autenticazione basata su *certificati*
  - Smart card con certificato
    - CSN
    - CIE
  - Protocolli: X.509, PGP, altri

Furto delle credenziali

- A scopo di frode
  - phishing
- A scopo di azioni criminose (terrorismo, etc.)
  - Creazione di false identità
- Log file
  - I sistemisti sono obbligati a tenere tracciate le operazioni compiute dagli utenti sul sistema per poter identificare con esattezza l'identificativo informatico abbinato alla persona specie in caso di illeciti, reati
  - L'obbligo è di almeno 6 mesi in archivi immodificabili e inalterabili - ***provvedimento del 27 novembre 2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema"***
  - Tutti gli utenti devono autenticarsi con credenziali personali e non generiche
  - Negli Internet point l'utente deve esibire il documento d'identità

Autenticazione del client e del server

- Autenticazione del client –
  - l'utente deve essere identificato dal server prima che questo rilasci i servizi
- Autenticazione del programma
  - Il programma invia un certificato con la firma del costruttore a garanzia di qualità e serietà
- Autenticazione del server
  - l'utente chiede di sapere l'identità esatta del server prima di effettuare un'operazione (pagamento elettronico, inserimento di dati sensibili, inserimento di dati identificativi)

Autorizzazione

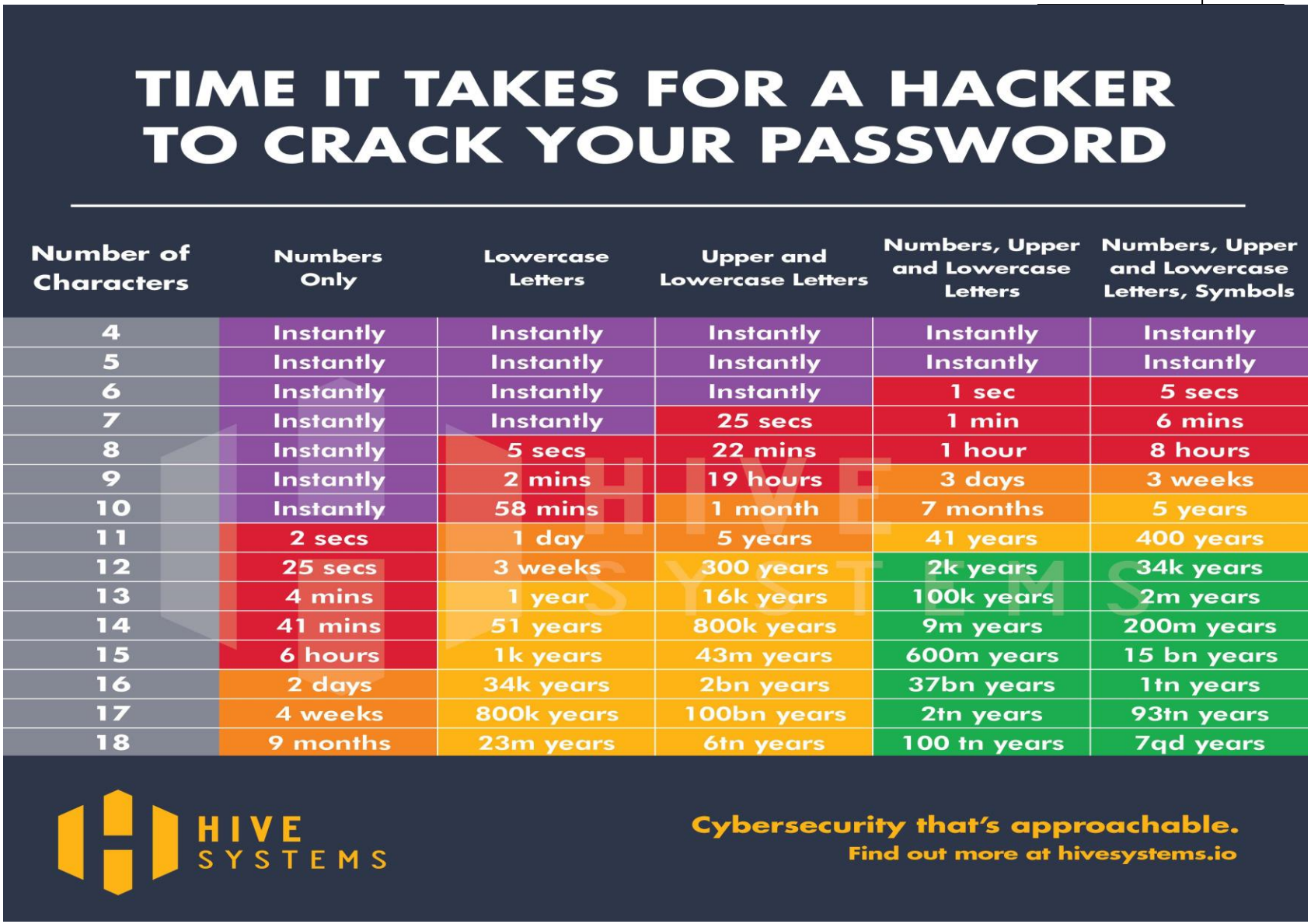
- Una volta autenticato l'utente ha l'autorizzazione ad effettuare determinate operazioni mantenute aggiornate dall'applicazione

- La tabella delle operazioni consentite per ogni utente è *la tabella delle autorizzazioni*

- Le autorizzazioni avvengono mediante due meccanismi:
  - Meccanismo dei permessi
  - Meccanismo dei biglietti

Password

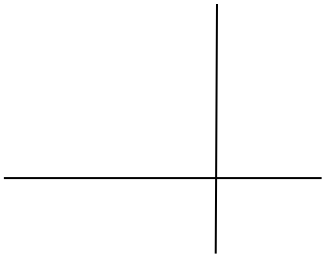
Cracking password



Password

- Non condividerla con i colleghi o familiari
- Non salvarla sul telefono
- Non trasmetterla via email

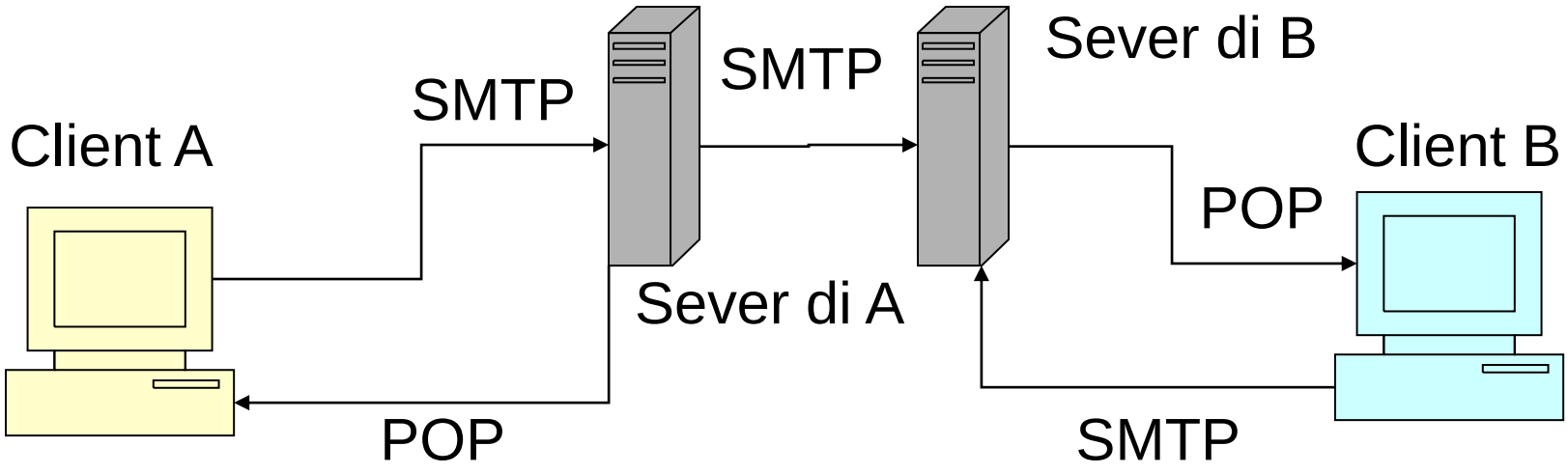
- Almeno 8 caratteri, non deve contenere riferimenti riconducibili all’utente o parole di senso compiuto
- Deve essere cambiata almeno ogni sei mesi
- Se si trattamento dati sensibili o giudiziari occorre cambiarla ogni 3 mesi



email

E-mail

- Il servizio di e-mail si basa su due protocolli: SMTP, POP
- SMTP port 25 (Symple mail transfer protocol) - trasferisce i messaggi da un host all'altro (centro di smistamento) – protocollo di spedizione
- POP port 110 (Post Office Protocol) - trasferisce i messaggi al destinatario (postino) – protocollo di ricezione
- MIME – protocollo per gestire gli allegati multimediali ed inviarli all'SMTP



Comportamenti scorretti con l'e-mail

- *flamming* - usare toni polemici, critici, logorroici, acidi approfittando del mascheramento indotto dal mezzo tecnologico
- *boombing* - invio di una mole massiccia di posta ad un server o ad una casella e-mail provocando la caduta del servizio di e-mail o del server o della casella in oggetto
- invio di *virus, worm, cavalli di troia, rootkit, malware*
- inivio di e-mail con identificativi falsi - scrivere e-mail falsificando il proprio identificativo, indirizzo di mittente, IP
- *phishing* – metodo per estorcere credenziali direttamente alle vittime con il metodo dell'inganno
- *spamming* – mail non desiderata
- *ransomware* – crittografia usata per bloccare i contenuti di un hard disk o di una banca dati con richiesta di riscatto in bitcoin

UniCredit
Factoring

Da UniCreditEu <mail@unicreditbulbank.bg>
Oggetto **Pid:681872912**
A Palmirani Monica
Data Tue, 20 Jun 2017 11:36:03 +0000
ID del Messaggio <6B.A0.06626.E6729495@mx01.unibo.it>
X-Account-Key account2
X-UIDL 273836

UniCredit

Ciao monica.palmirani@unibo.it,

Hai ricevuto un nuovo messaggio.

Continua

Grazie

Il vostro Unicredit

Perché lo spediamo? Prendiamo seriamente la sicurezza e vogliamo tenervi nel ciclo di azioni importanti nel tuo account. Non siamo riusciti a determinare se hai già utilizzato questo browser o dispositivo con il tuo account. Ciò può accadere quando si accede per la prima volta su un nuovo computer, telefono o browser, quando si utilizza la modalità di navigazione in modalità incognito o privata del browser oppure si elimina i cookie o quando qualcun altro accede al tuo account.

Header di un messaggio

bulgaria

Oggetto:Pid:681872912

Mittente:UniCreditEu <mail@unicreditbulbank.bg>

Data:20/06/2017, 13:36

A:<monica.palmirani@unibo.it>

Received:

from E13-MBX4-DR.personale.dir.unibo.it (10.12.1.74) by E13-MBX3-DR.personale.dir.unibo.it (10.12.1.73) with Microsoft SMTP Server (TLS) id 15.0.1263.5 via Mailbox Transport; Tue, 20 Jun 2017 15:47:26 +0200

Received:

from E13-MBX1-CS.personale.dir.unibo.it (10.12.1.71) by E13-MBX4-DR.personale.dir.unibo.it (10.12.1.74) with Microsoft SMTP Server (TLS) id 15.0.1263.5; Tue, 20 Jun 2017 15:47:26 +0200

Received:

from mx01.unibo.it (137.204.24.54) by mail.unibo.it (10.12.1.71) with Microsoft SMTP Server id 15.0.1263.5 via Frontend Transport; Tue, 20 Jun 2017 15:47:26 +0200

Received:

from dicht.dp.ua (dicht.dp.ua [195.24.152.234]) by mx01.unibo.it (unibo.it) with SMTP id 6B.A0.06626.E

IP della macchina

7 15:47:2

ukraina

)

Received:

from [52.173.189.212] (helo=brescia) by dicht.dp.ua with esmtp (Exim 4.77 (FreeBSD)) (envelope-from <mail@unicreditbulbank.bg>) id 1dNHP1-0004Pg-7z for monica.palmirani@unibo.it; Tue, 20 Jun 2017 14:32:59 +0300

ID-Messaggio:

<6B.A0.06626.E6729495@mx01.unibo.it>

Rispondi-a:UniCreditEu <mail@unicreditbulbank.bg>

Content-Type:text/html; charset="utf-8"

Content-Transfer-Encoding:

Return-Path:mail@unicreditbulbank.bg

Analisi dell'IP number 52.173.189.212

Email Share

WHOIS IP Lookup Tool

The IPWHOIS Lookup tool finds contact information for the owner of a specified IP address.

Enter a host name or an IP address:

52.173.189.212 Go »

Related Tools: DNS Traversal Traceroute Vector Trace Ping WHOIS Lookup

```
            Source: whois.arin.net
        IP Address: 52.173.189.212
              Name: MSFT
            Handle: NET-52-145-0-0-1
  Registration Date: 24/11/15
             Range: 52.145.0.0-52.191.255.255
               Org: Microsoft Corporation
        Org Handle: MSFT
           Address: One Microsoft Way
              City: Redmond
   State/Province: WA
       Postal Code: 98052
           Country: United States
      Name Servers:
```

Server in cloud computing
In USA

- In sintesi è un attacco di phishing

Phishing - definizione

Tecnica di *Ingegneria Sociale*

che mira al furto di identità *“identity theft”*

attuato mediante i più svariati mezzi (spesso tecnologici) per poter carpire dati riservati relativi alla identità elettronica dell’individuo

e poterli utilizzarli per commettere illeciti o reati

Le fasi del phishing

1) Creazione del sito clone o civetta e attacco al sito ufficiale per disattivarlo
2) Predisposizione del messaggio ed identificazione delle possibili vittime e adescamento: invio dell'e-mail
3) Recupero dei dati riservati
4) Frode informatica, utilizzo improprio dell'identità, atti terroristici, impersonificazione, ecc. (con coinvolgimento di terzi per il trasferimento del denaro in paesi privi di normazione al riguardo)
5) Cancellazione delle tracce

Come è sanzionato il phishing in EU

- Convenzione europea sul cybercrimine, approvata dal Consiglio d'Europa che lo tratta come frode informatica ma solo quando il reato si è già consumato nella sua fase n. 4
- Non esistono capi di accusa preventivi
- Si agisce *post-mortem*
- *Convenzione di Budapest del Consiglio d'Europa sulla criminalità informatica del 23.11.2001 (ratificata con Legge 18 marzo 2008 n. 48)*

Rimedi attuali

- Non pubblicare in Internet il proprio e-mail
- Strumenti anti-spamming, firewall, spyware
  - Lato server
  - Lato client
    - Poco efficaci
    - Falsi positivi
- Uso dell'informatica consapevole (evitare siti poco affidabili, pop-up menu, scaricare suonerie, scaricare .exe)
- Utilizzare solo siti con SSL, HTTPS, TLS
- Aggiornamento culturale

Definizione di SPAM e SPAMMING

- *Junk*: invio di posta non sollecitata in genere
  - Unsolicited Bulk E-mail – UBE (es. catene di S'Antonio, appelli umanitari, mobilitazioni sociali, ecc.)
  - Unsolicited Commercial E-mail – UCE
- *Spamming*: (spam -SPiced hAM)
  - invio di messaggi non sollecitati di natura prevalentemente commerciale mediante telefono, fax, sms e-mail
  - inviati in grandi quantità, reiterati, da mittente spesso sconosciuto, mascherato, falsificato.

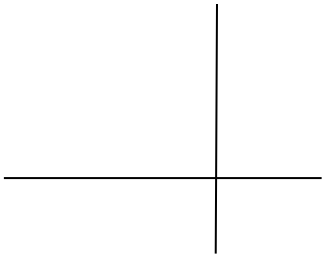
Origini di SPAM e SPAMMING

- http://www.spam.com/ - la vera SPAM

- PRIMO SPAM
  http://www.templetons.com/brad/spamreact.html -
  DEC 3 maggio 1978 ARPANET directory

- http://www.detritus.org/spam/skit.html -
  31 marzo 1993 la scenetta di “**Monthy Pyton**”

Opt-in e Opt-out



- Opt-in e Opt-out : due diversi approcci
  - Opt-in: inviare solo a chi ha fornito preventivo consenso
  - Opt-out: il destinatario deve agire al fine di essere “espulso” dalle liste di invio

Opt-in e Opt-out

- Opt-in:
  - consentito lo spamming solo a chi ha fornito preventivo consenso
  - Approccio Europeo - **L'art. 13 della direttiva 2002/58/CE**
  - tutelante della persona
  - tutela a priori
- Opt-out:
  - consentito lo spamming sempre fino a disdetta dell'interessato
  - il destinatario deve agire al fine di essere "espulso" dalle liste di invio
  - Approccio americano, coreano, giapponese
  - tutela il libero mercato, la concorrenza fra imprese
  - tutela a posteriori

Garante per la protezione dei dati personali

- **Provvedimento generale del Garante maggio 2003**
- ***Spamming.* Regole per un corretto invio delle *e-mail* pubblicitarie - Provvedimento generale**
- "La utilizzazione per scopi promozionali e pubblicitari è possibile solo se il soggetto cui riferiscono i dati ha manifestato in precedenza un consenso libero, specifico e informato."
- Questo vale anche se è un software a inviare i messaggi in automatico
- Questo assetto, basato su una scelta dell'interessato c.d. di opt-in, è stato ribadito nel 1998 (con il d.lg. n. 171) prima ancora che una recente direttiva comunitaria lo estendesse a tutti i Paesi dell'Unione europea (n. 2002/58/CE in fase di recepimento in Italia, pubblicata sulla G.U.C.E. n. L 201 del 31 luglio 2002).

Web

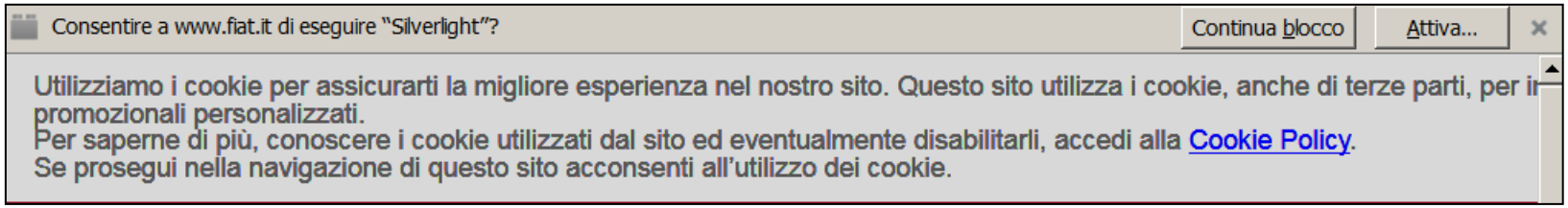
Caratteristiche dell' HTTP

- HTTP è un protocollo "**stateless**" ossia senza memoria di stato
- Per questo sovente da una pagina HTML all'altra i parametri inseriti si perdono
- Ad ogni richiesta si attiva una connessione diversa di TCP/IP - connessione non persistente
- La versione HTTP 1.1 risulta essere persistente – rimane "**attaccata**"
- Un modo per evitare la perdita di stato è l'uso di sessioni e di cookies

I cookie

- Il cookie è il meccanismo usato da alcuni server Web per tenere traccia degli utenti che hanno acceduto al sito
- Il server scrive sul computer dell'utente un file con informazioni relative alla navigazione più un codice identificativo
- La volta successiva il server può leggere dal cookie le informazioni che interessano al sito e sapere a chi sono riferite: per esempio può personalizzare la presentazione con un messaggio del tipo:

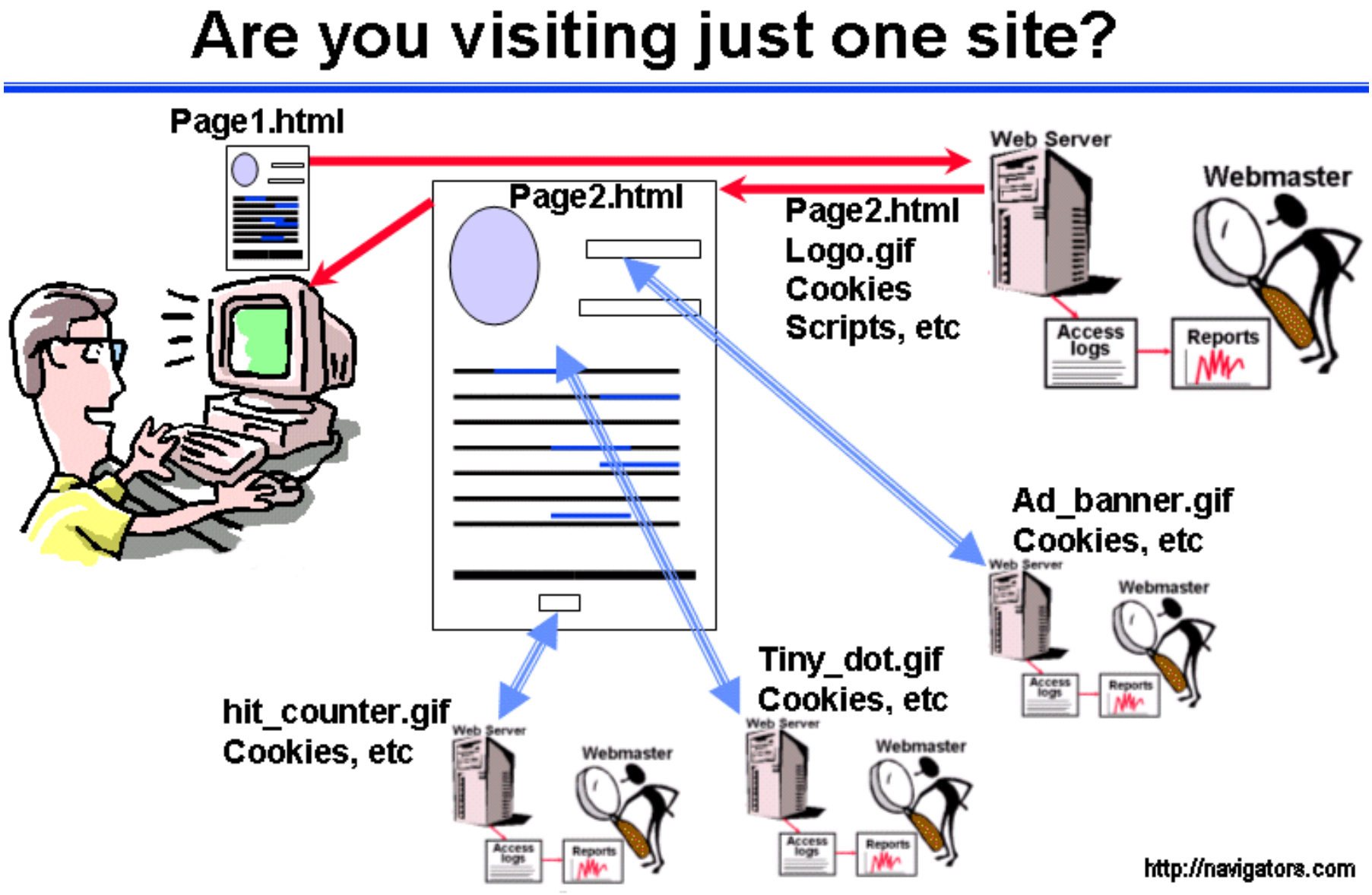
"Benvenuto Mario Rossi è la terza volta che ci visita"



Come funziona un cookie

- La prima volta che l'utente si collega ad un server questo aggiunge un file sulla macchina dell'utente contenente un numero identificativo univoco che identifica l'utente stesso
- La volta successiva che l'utente si collega, il server rintraccia dal file il numero di identificativo (ID) e riesce ad associare così l'utente
- Spesso nei siti vengono proposti banner pubblicitari in linea con le scelte che stiamo compiendo sul sito perché all'interno dei cookie si possono memorizzare le nostre preferenze

HTTP, stateless and cookies



Come è fatto un cookie

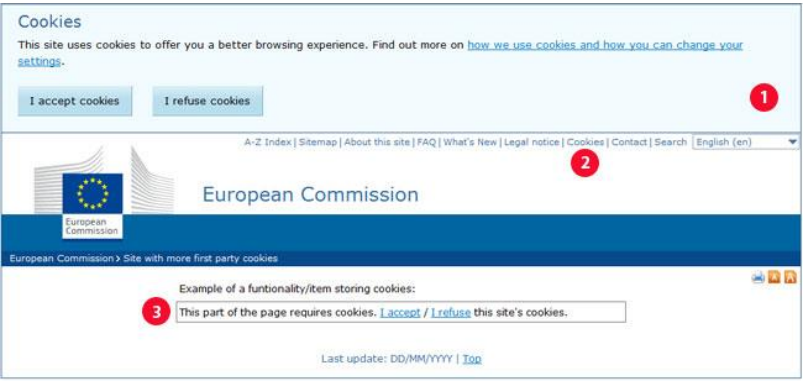
- Apache151.26.160.113.30625101601452075 5iol.it/063331840029646475134389648029477495*IOLADVIDA61165535iol.it/0260366336302117591421896480294774 95*IOLADVLCTCLP0099iol.it/03092983040294952609434489602947836 5*

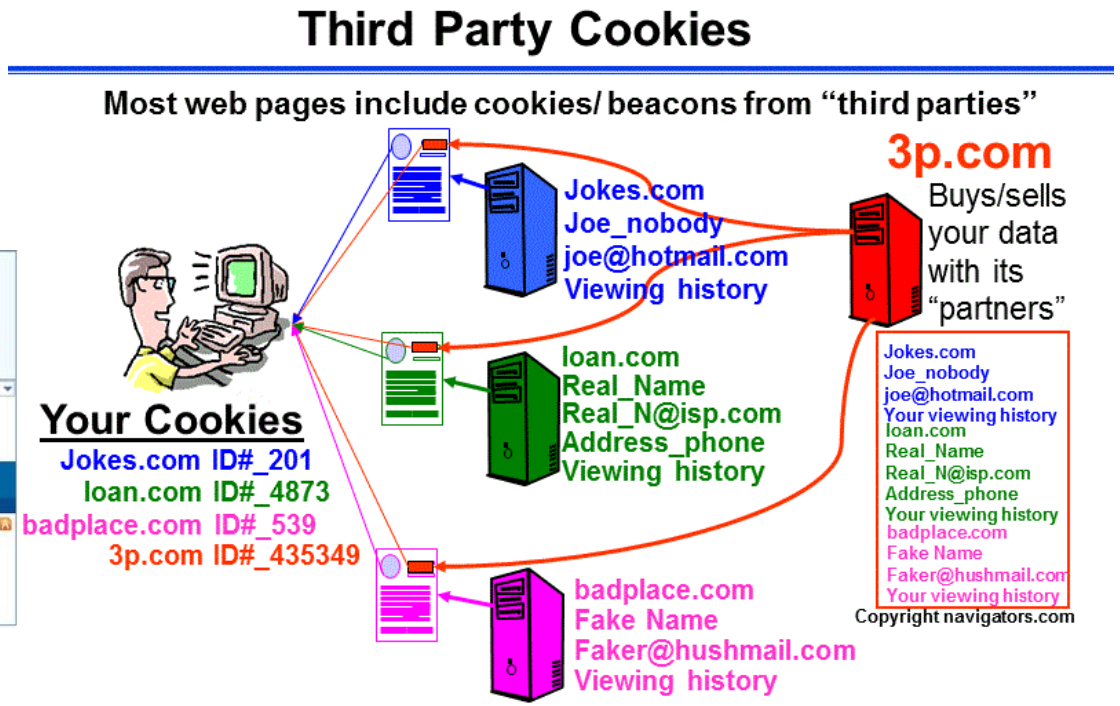
  Un cookie può violare la legge sulla privacy:

  - fornendo o vendendo informazioni sulle abitudini dell'utente
  - creando occasioni in cui le informazioni sono palesate per errore a terzi
  - monitorando senza adeguati premessi le abitudini degli utenti

Third party cookies

- The third party cookies need a consent by the end user
- EU Cookies Law
  http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:IT:PDF





The "third party site" can compile an extensive profile on you, and sell this information to companies that are online and offline. Google Analytics is embedded in 50% of the top 1 million websites

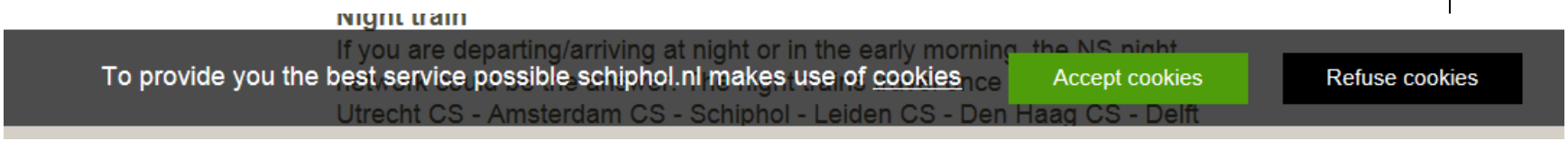
Approfondimento - Pagine statiche e dinamiche: uso dei cookies

- Le pagine possono essere statiche o dinamiche:
- Statiche quando esistono già sottoforma di file statici. Si riconoscono perché l'URL finisce con html o htm
- Dinamiche ossia che il server le crea al volo sulla base delle richieste dell'utente e quindi vengono confezionate anche in base al comportamento dell'utente – profilo utente
- Per mantenere traccia del profilo dell'utente i server scaricano non solo la pagina html nel client ma anche un micro file chiamato cookie che tiene traccia dei comportamenti dell'utente e li comunica la volta successiva al server o ai server collegati
- I cookies sollevano problemi di tutela dei dati personali

Approfondimento: i cookie

- I cookies possono quindi identificare ed autenticare l'identità del visitatore
- Questo meccanismo è usato soprattutto per identificare l'utente di volta in volta e per raccogliere dati statistici e comportamentali relativi all'utente: numero di volte che accede al sito, voci scelte, preferenze, etc.
- Si usa il cookie e non l'IP perché spesso l'utente non è identificabile attraverso l'IP in quanto usa un IP dinamico e non fisso oppure da uno stesso IP si collegano più utenti

Cookeis buoni e cattivi



- Buoni
  - si chiudono nella sessione lasciando il PC pulito
  - agevolano l'applicazione nel passaggio di dati
  - fanno *cache* di pagine
  - aiutano il passaggio all'interno di diverse applicazioni collegate
- Cattivi
  - profilano senza consenso
  - utilizzano il profilo per far comparire banner, spam, notizie
  - inviano i dati personali a diversi siti non noti

Direttiva EU cookies

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:en:PDF

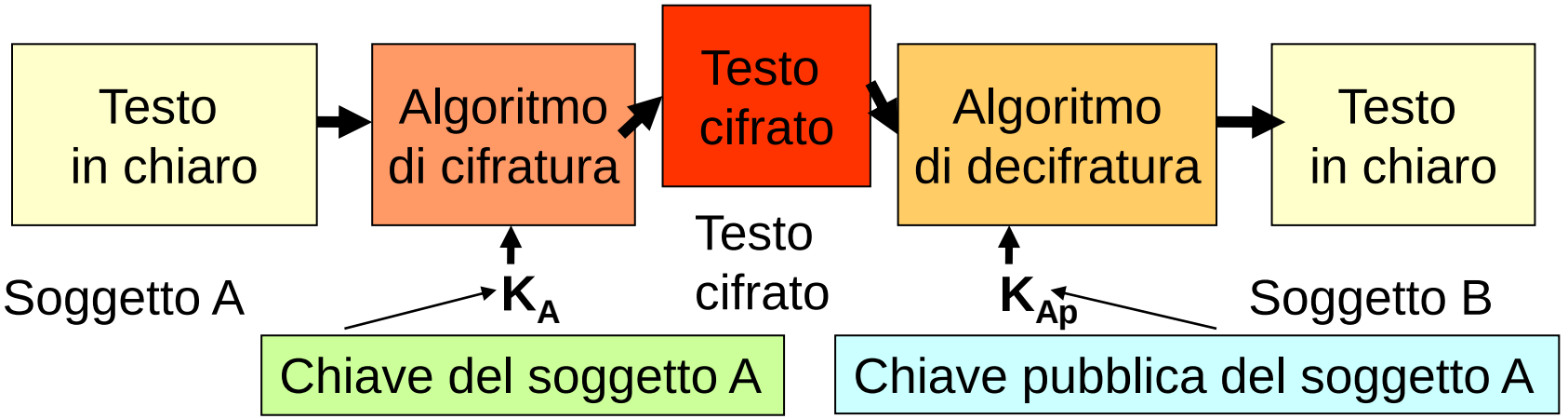
Crittografia

Obbiettivo della Crittografia

- L'obiettivo della crittografia è quello di mascherare il testo originario di un messaggio attraverso regole di traduzione di cui sono a conoscenza solo il mittente e il destinatario
- Il metodo consente di tenere sotto controllo
  - l'integrità del dato
  - l'autenticazione del mittente
  - la riservatezza del contenuto
- La crittografia non risolve altri problemi quali la falsificazione, la sostituzione di persona, la sicurezza del canale di trasmissione

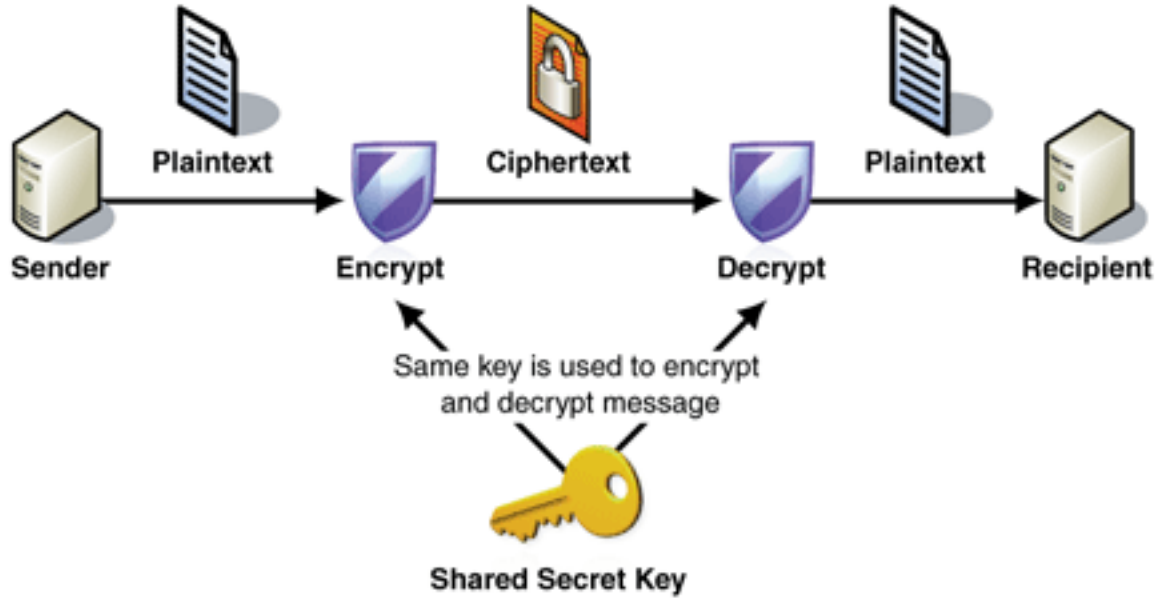
La crittografia moderna basata sulla chiave

- Il meccanismo di crittografia trasforma il testo originale in un testo cifrato non facilmente leggibile
- L'oggetto della trasformazione viene detto testo in chiaro (plain-text o cleartext), l'oggetto risultato della trasformazione viene detto testo cifrato (chipertext)
- Il processo di trasformazione avviene mediante un algoritmo di cifratura, un algoritmo di decifratura, delle chiavi segrete che contribuiscono alla trasformazione del testo

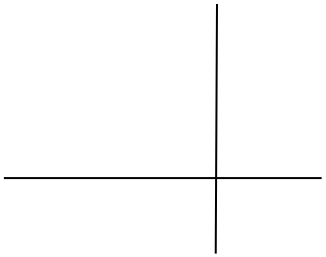


Crittografia simmetrica

- Ci si scambia una chiave crittografica
- I due attori crittografano con questa chiave
- Importante avere un canale alternativo e sicuro per lo scambio delle chiavi



Sistemi a chiave pubblica
Public Key Infrastructure - PKI



- Nei sistemi a chiave pubblica si usa una coppia di chiavi: una pubblica nota sia al mittente che al ricevente - in realtà nota al mondo intero - e una chiave privata per ogni soggetto (mittente e ricevente)
- In definitiva si avranno due coppie di chiavi:
  - una pubblica per il mittente
  - una pubblica per il ricevente
  - una privata per il mittente
  - una privata per il ricevente

<la funzione di hash

- Per garantire l'integrità del messaggio si usa una funzione matematica di *hash* che costruisce un riassunto del messaggio stesso detto *digest o impronta digitale del documento*
- Il *digest* è una stringa di lunghezza fissa calcolata sul contenuto del messaggio – *impronta digitale del documento*
- Due messaggi diversi danno origine a due impronte diverse
- Due messaggi uguali forniscono la stessa impronta
- Due messaggi diversi possono, in via ipotetica, dare origine a due impronte uguali ma la probabilità che accada è talmente piccola da definire tali funzioni *collision free*
- Dal digest non è possibile risalire al documento - *one-way function*
- Funzioni di hash ammesse delle regole tecniche sono: SHA-256, RIPEMD-160

Esempio di hash con MD5

- Testo: Nel cammin di nostra vita mi ritrovai in una selva oscura

  0fc273b475a3479d0e9f2200lc695c1e

  digest o impronta

- Modifica con una semplice andata a capo

  9a63075b13e84cb75e7ada3c351f14e1

- Ho inserito il numero di pagina

  be7dbc971a01ec88670bd5b3456a2c03

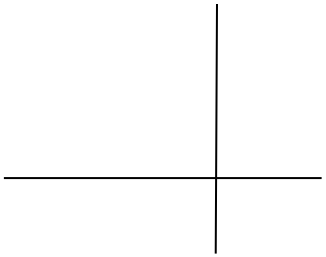
- Ma se inserisco in un file Word o PDF una macro il meccanismo di hash non rileva cambiamenti. Per questo è importante firmare solo formati dati privi di macro le quali possono mutare nel tempo alterando l'integrità del documento

Impronta e hash

- Impronta di una generica sequenza di testo è la sequenza di simboli di lunghezza predefinita generata mediante l'applicazione di una opportuna funzione di *hash*

- DPCM 8 febbraio 1999, ne dà una definizione
- *"l'impronta di una sequenza di simboli binari è una sequenza di simboli binari di lunghezza predefinita generata mediante l'applicazione alla prima di un'opportuna funzione di hash"*

- Hash è una funzione matematica che genera, a partire da una generica sequenza di simboli, un'altra sequenza di simboli (impronta) in modo che risulti "impossibile", a partire da questa, risalire matematicamente alla sequenza che l'ha generata



Sicurezza Web

Sicurezza del WEB

- Con l'introduzione del commercio elettronico il grado di sicurezza della rete Internet e delle connessioni HTTP si sono evolute al fine di assicurare la correttezza, l'integrità e la riservatezza delle transazioni in rete
- SSL - *secure socker layer* - Netscape - garantisce la cifratura e l'autenticazione della comunicazione fra client e server Web. Abbinato a questo troviamo l'TLS - Transport Layer Security del livello di trasporto
- SSL garantisce:
  - autenticazione del server
  - autenticazione del client
  - una sessione cifrata per la trasmissione dati

SSL

- Si accede ad un sito protetto da SSL via browser e la sicurezza è garantita da una chiave simmetrica cifrata condivisa fra client e server
- l'url che compare è https invece che http
- inizia la fase di handshake (stretta di mano) fra server e client
- il server invia il certificato
- il client genera una chiave pubblica sulla base del certificato ricevuto e una simmetrica che cifra con la chiave pubblica appena costruita - RSA a chiave pubblica
- il client invia la chiave simmetrica cifrata al server
- ora il client e il server condividono una chiave simmetrica di connessione attraverso la quale possono cifrare e decifrare i dati che si trasmetteranno

Limiti dell'SSL

- Tutto il procedimento non garantisce che chi sta comunicando sia autorizzato a compiere operazioni, transizioni, pagamenti con carta di credito

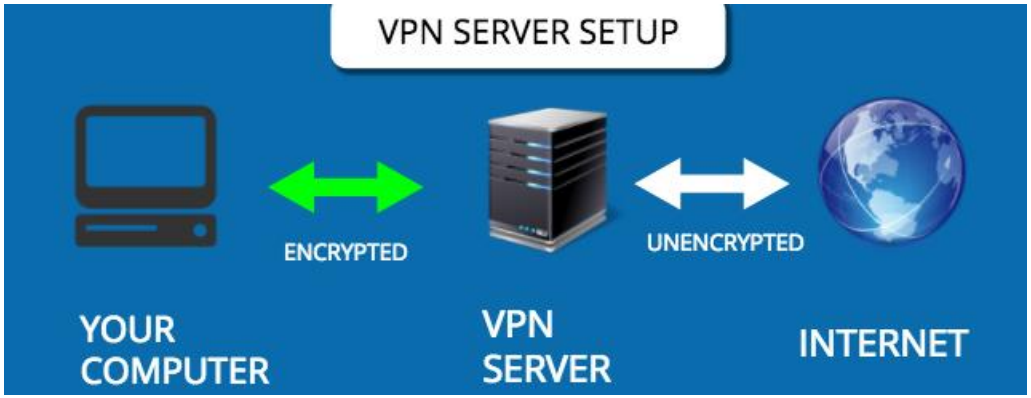
- Il client potrebbe inserire una carta di credito falsa o rubata che il meccanismo SSL non è in grado di tutelare l'effettiva bontà della transazione

- SSL garantisce solo la sicurezza, l'integrità e l'autenticazione e non garantisce da operazione fraudolente

VPN Virtual Private Network

- Permette di realizzare un canale sicuro crittografato
- **Fase 1. Autenticazione**
- **Fase 2. Tunnelling**:
- **Fase 3. Criptaggio**

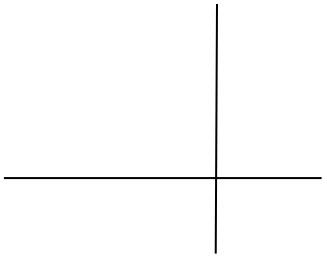
- Crittografia simmetrica
- Invio delle chiavi su canale alternativo o con crittografia asimmetrica



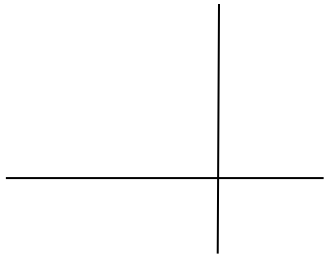
I Firewall

- dispositivo hardware dotato di software programmabile che costituisce una barriera di protezione fra la rete interna e la rete esterna. La barriera viene implementata con diverse tecniche:
  - monitoraggio di tutti i pacchetti in entrata e in uscita
  - controllo dei servizi Internet ammessi in entrata e in uscita
  - effettua un filtraggio degli IP secondo una stop-list e regole di security policy
  - implementa una barriera protettiva nei confronti degli utenti interni alla rete
  - effettua filtraggi sui comportamenti (blocca spamming, virus, inibisce accessi a siti nella stop-list, etc.)
- esistono simulazioni software dei meccanismi hardware

I Proxy

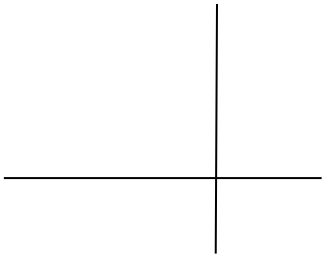


- Dispositivo software e/o hardware che viene installato fra la rete interna e la rete esterna. Il sistema software simula quello hardware con meno efficacia.
- Consente di filtrare le richieste in uscita in modo che si possano risparmiare uscite inutili
  - Es. le richieste via HTTP passano attraverso il proxy il quale consente di gestire una sorta di “memoria storica” delle richieste più recenti e quindi di evitare l’accesso continuo verso l’esterno
- Consente di direzionare le richieste dall’esterno sulla rete interna limitatamente ad una lista di utenti
- Il proxy consente anche un grado di programmabilità come filtro o monitoring di liste di IP number



Antivirus

Virus



- Tutti i virus attraversano quattro fasi:
  - fase latente
  - fase di propagazione
  - fase di innesco
  - fase di esecuzione

Virus

- Bomba logica - istruzioni inserite all'interno del sistema che scattano al verificarsi di un determinato evento. Esempio: una data, un determinato comportamento dell'utente, l'esecuzione di un certo programma, etc. A questo punto le istruzioni lesive vengono innescate e parte il danneggiamento di tutto o di parte del sistema

- cavalli di troia - meccanismi veicolati attraverso i normali programmi di gestione o le normali attività quotidiane di generica utilità. Una determinata istruzione scatena l'attacco inserito in un normale contesto.

Virus

- Virus - sono programmi che sono in grado di infettare parti del sistema. I virus informatici, analogamente ai virus biologici, contengono istruzioni in grado di replicare copie di se stesso diffondersi in modo subdolo fino a creare danni visibili. I metodi di replicazione sono molteplici: prelevare la lista delle e-mail spedite ed inviare in modo casuale il virus a questi destinatari, infettare i documenti che si trasmettono via dischetto o via e-mail, infettare file particolari di sistema, etc.

Virus

- Worm - programmi che utilizzano la rete per diffondersi. I worm possono usare la posta elettronica, la connessione in remoto, replicarsi in remoto su un altro sistema.
- Batteri - i batteri hanno lo scopo di auto-replicarsi senza in genere danneggiare direttamente il sistema. Il sistema collassa per “infezione” ovvero per esempio perché un file si è replicato n volte occupando tutto l’hard disk o perché ha occupato tutta la RAM. A questo punto l’accesso al sistema è impedito
- Spyware – programmi che una volta installati controllano le attività dell’utente
- Ransomware - limita l'accesso del dispositivo che infetta, richiedendo un riscatto

Rimedi

- Rilevazione
- Identificazione
- Rimozione
- Recupero backup

- Pacchetti di uso comune, Norton, McCaffe, etc.
- Lato client e lato server
  - Le protezioni lato server possono creare illeciti e reati riconducibili a violazioni della tutela dei dati personali, apertura non autorizzata della corrispondenza
- ditte specializzate che eseguono monitoraggio costante dei sistemi