



Cofinanziato
dall'Unione europea



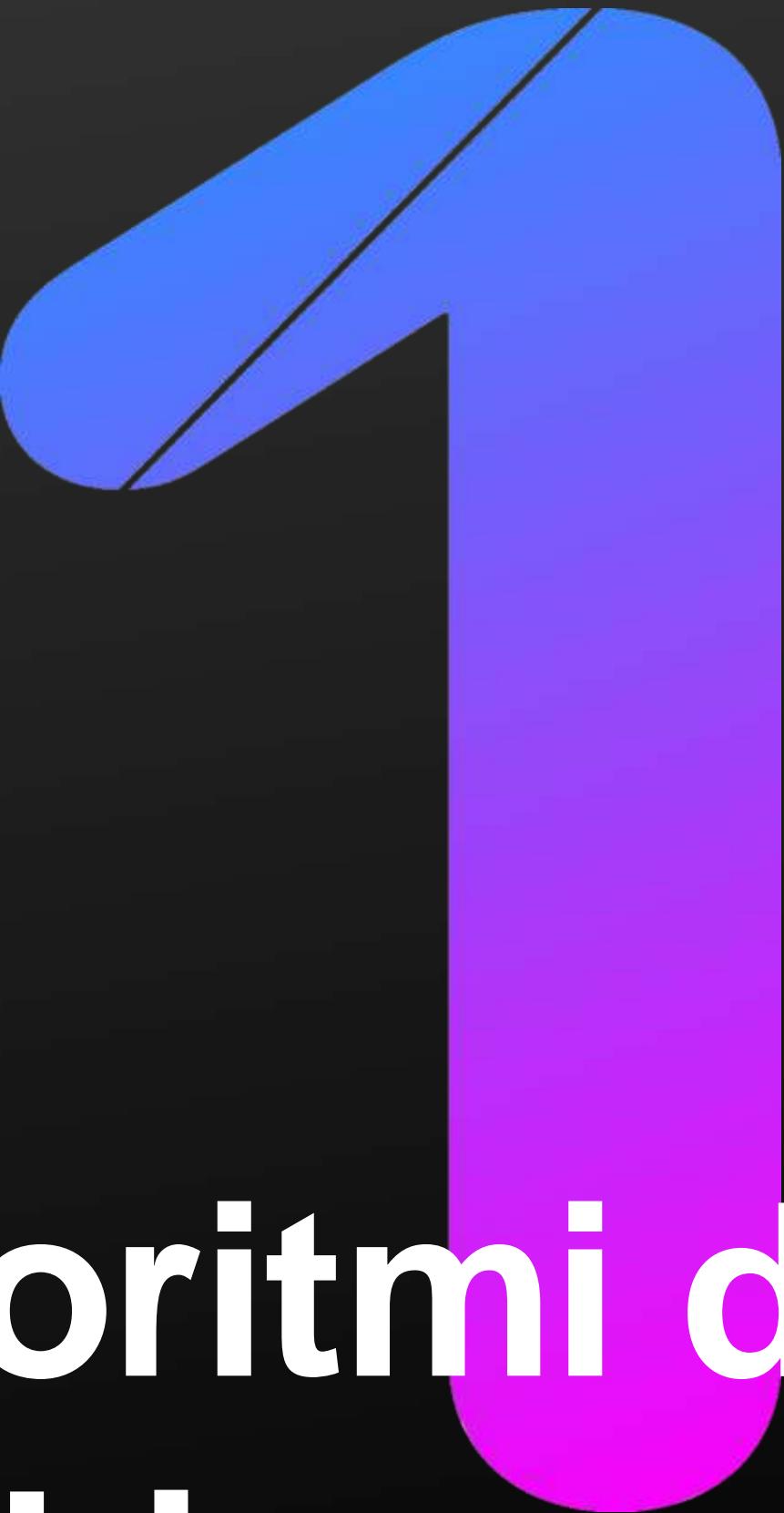
CERTIFICATI DIGITALI E HASHING

Sicurezza informatica

Elena Maria Dal Santo

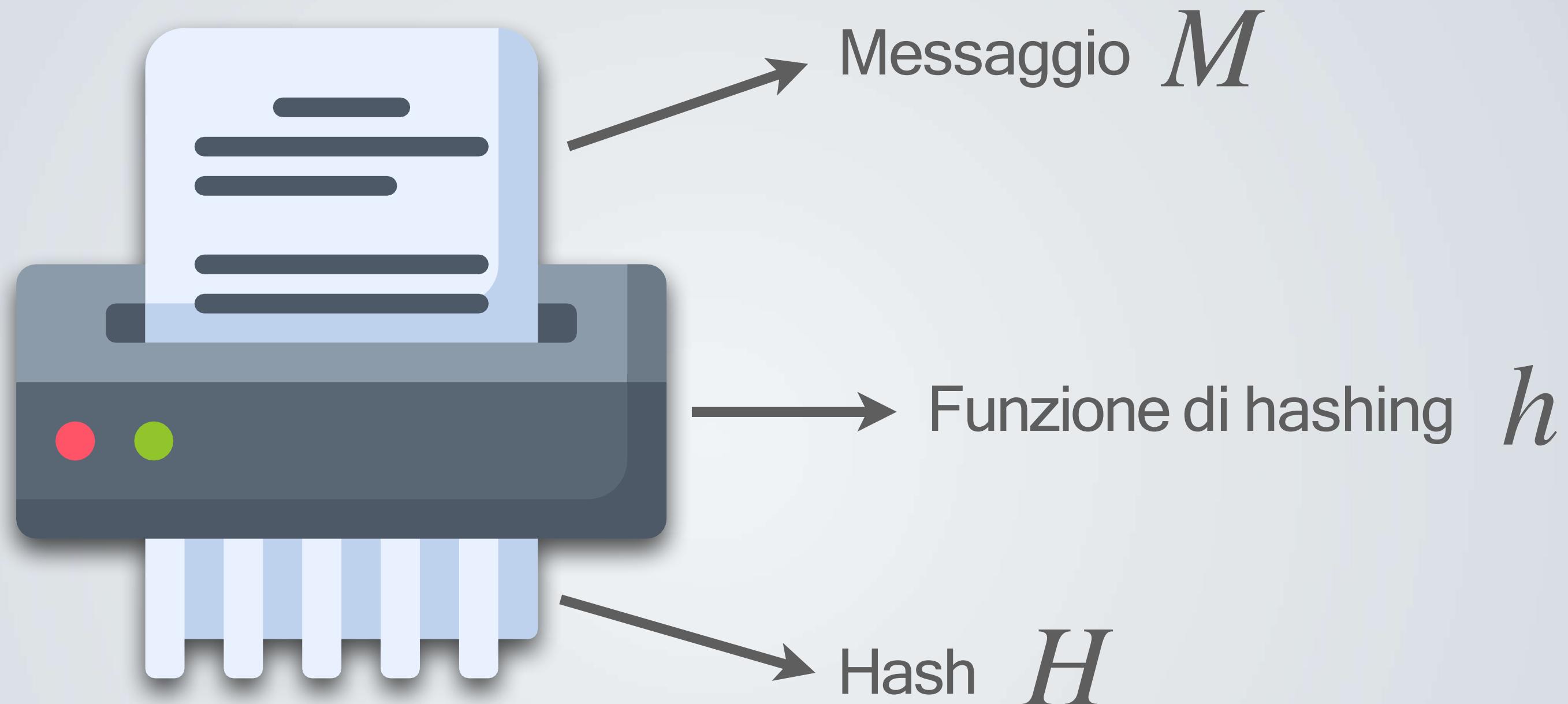
elenamaria.dalsanto@its-ictpiemonte.it





Algoritmi di hashing

Le funzioni di hashing

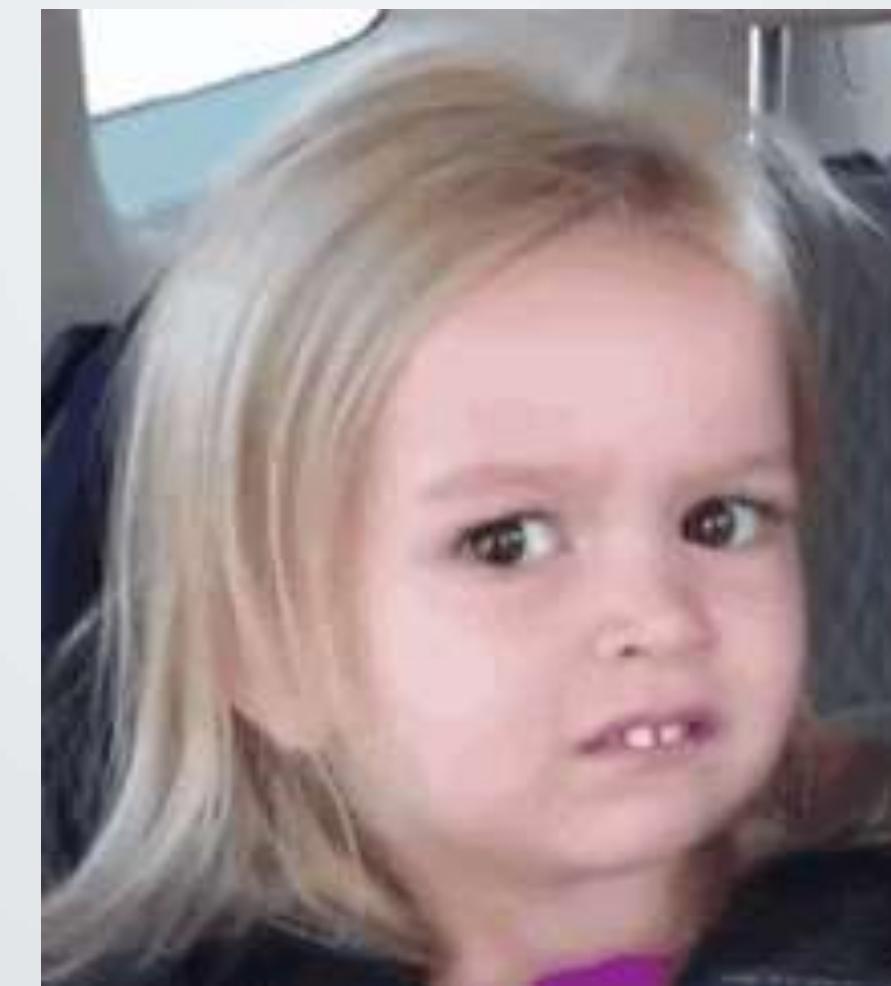


$$H = h(M)$$

Le funzioni di hashing



L'hash è una funzione non invertibile che mappa una stringa di lunghezza arbitraria in una stringa di lunghezza predefinita.



Le funzioni di hashing



L'hash è una **funzione non invertibile** che mappa una stringa di lunghezza arbitraria in una stringa di lunghezza predefinita.

1. A partire dall'hash non è possibile risalire alla stringa originale.

Le funzioni di hashing



L'hash è una funzione non invertibile che mappa una stringa di **lunghezza arbitraria** in una stringa di lunghezza predefinita.

1. A partire dall'hash non è possibile risalire alla stringa originale.
2. L'input può essere di qualunque dimensione.

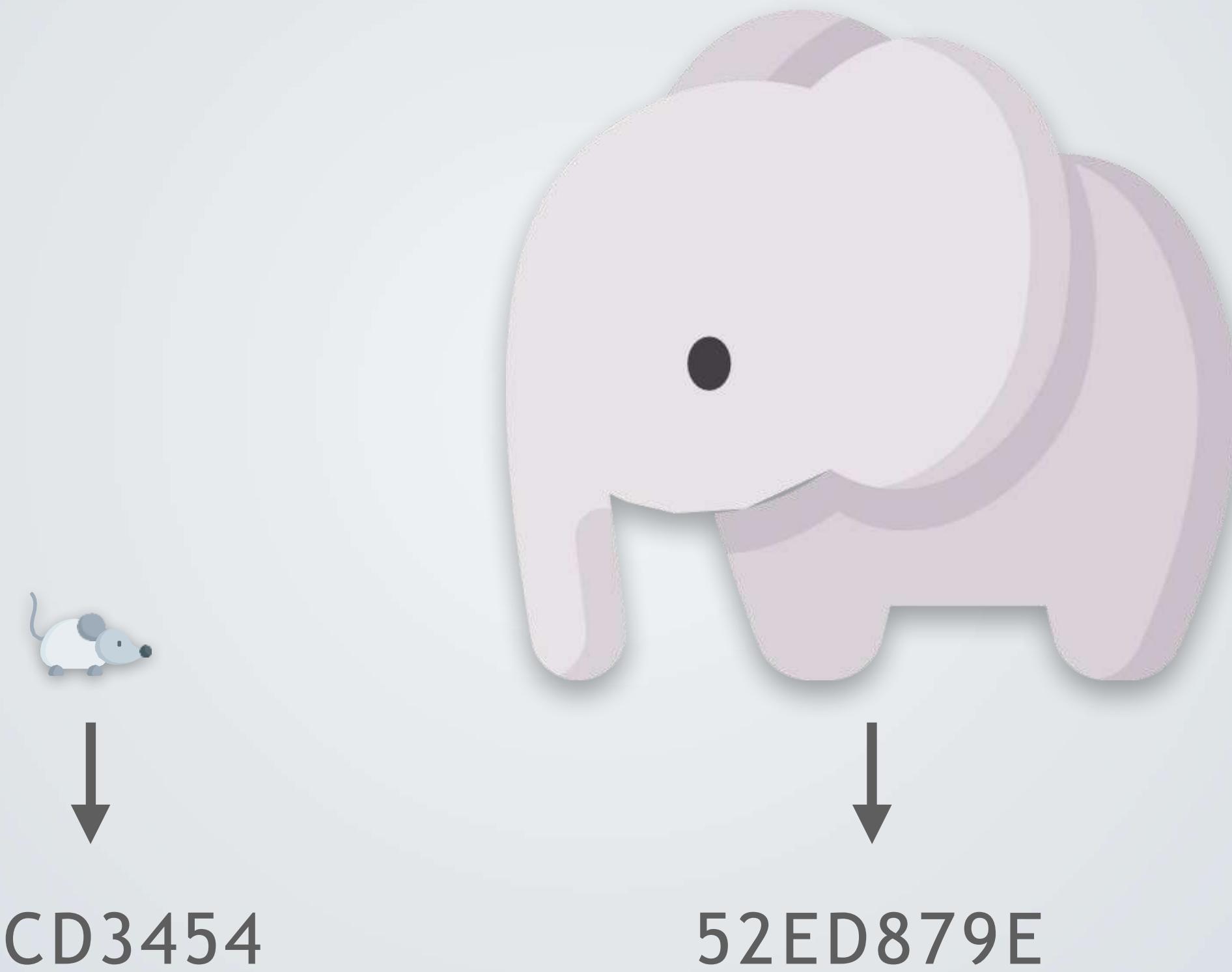
Le funzioni di hashing



L'hash è una funzione non invertibile che mappa una stringa di lunghezza arbitraria in una stringa di **lunghezza predefinita**.

1. A partire dall'hash non è possibile risalire alla stringa originale.
2. L'input può essere di qualunque dimensione.
3. L'output ha una dimensione fissa.

Le funzioni di hashing



Le funzioni di hashing

ATTENZIONE!

Input uguali generano hash uguali

→ Quando inserite la vostra password su Google per accedere al vostro account, Google non verifica che la password sia uguale a quella salvata! In realtà, Google non salva la vostra password, salva il suo hash. Quando inserite la password, Google ne genera l'hash e lo confronta con quello che aveva memorizzato. Se gli hash sono uguali, la password coincide con quella che avevate scelto ed è quindi giusta.

Ipotizziamo un attacco hacker. Il nemico riesce a clonare tutto il db di Google, e ha quindi accesso agli hash delle nostre password.

Con un attacco di forza bruta, il nemico inizia a confrontare gli hash delle parole con quelli rubati (attacco a dizionario), fino a trovare la nostra password.

Per evitare questo tipo di attacco possiamo “condire” il nostro hash con SALT e PEPPER



SALT

Sequenza casuale di bit, utilizzata insieme a una password come input di una funzione hash.

Un salt diverso viene generato per ogni password, e viene salvato insieme all'output della funzione hash.

Username	Password
user1	password123
user2	password123

Username	Valore del salt	Password + Salt	Hashed value = SHA256 (Password + Salt)
user1	E1F53135E559C253	password123E1F53135E559C253	72AE25495A7981C40622D49F9A52E4F1565C90F048F59027BD9C8C8900D5C3D8
user2	84B03D034B409D4E	password12384B03D034B409D4E	B4B6603ABC670967E99C7E7F1389E40CD16E78AD38EB1468EC2AA1E62B8BED3A

PEPPER

Sequenza casuale di bit, utilizzata insieme a una password come input di una funzione hash.

Differenze col salt:

- Sempre uguale, non viene generato per ogni password
- Non viene salvato

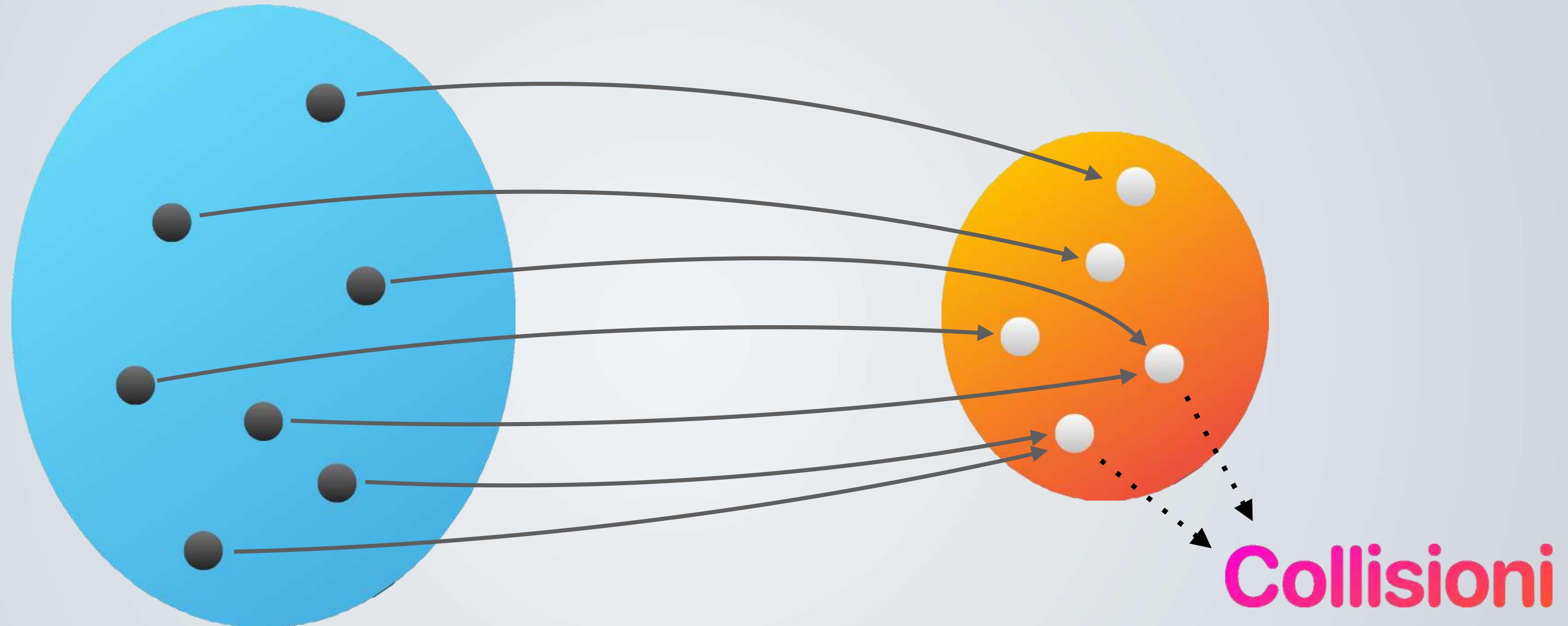
Username	Password
user1	password123
user2	password123

Username	Stringa di cui fare l'hashing	Valore di output dell'hash = SHA256(Password + pepper)
user1	password123+44534C70C6883DE2	D63E21DF3A2A6853C2DC675EDDD4259F3B78490A4988B49FF3DB7B2891B3B48D
user2	password123+44534C70C6883DE2	D63E21DF3A2A6853C2DC675EDDD4259F3B78490A4988B49FF3DB7B2891B3B48D

Uno schema completo di salvataggio delle password comprende l'utilizzo sia del salt che del pepper



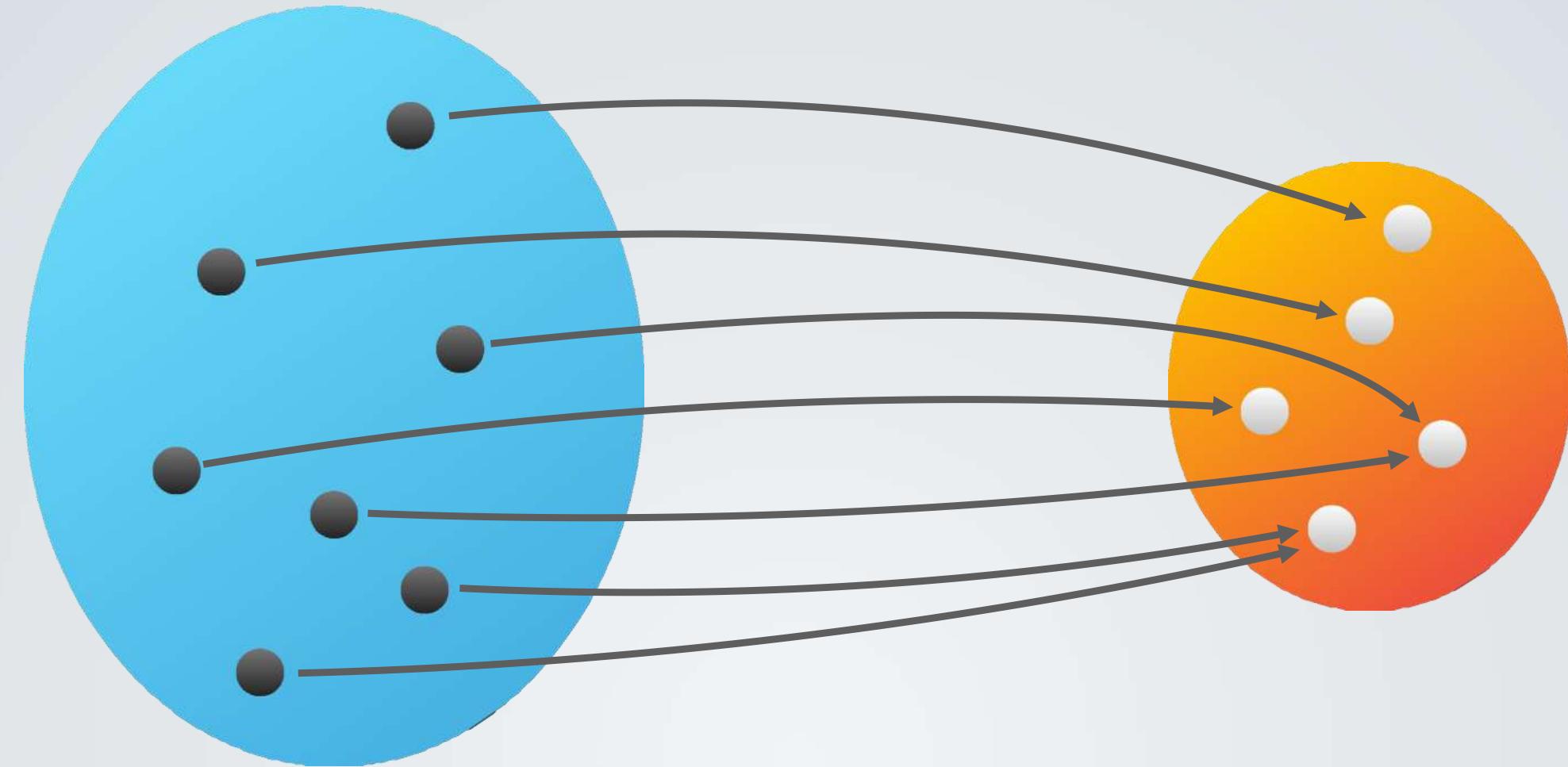
Qualquadra non cosa.



Tutti i messaggi
possibili

sono di più di

tutti gli hash
possibili.



Si ha una **collisione** quando due diversi input producono lo stesso output

Potenzialmente, la maggior parte delle funzioni hash da luogo a collisioni, ma con una buona funzione esse avvengono raramente.

Resistenza alle collisioni

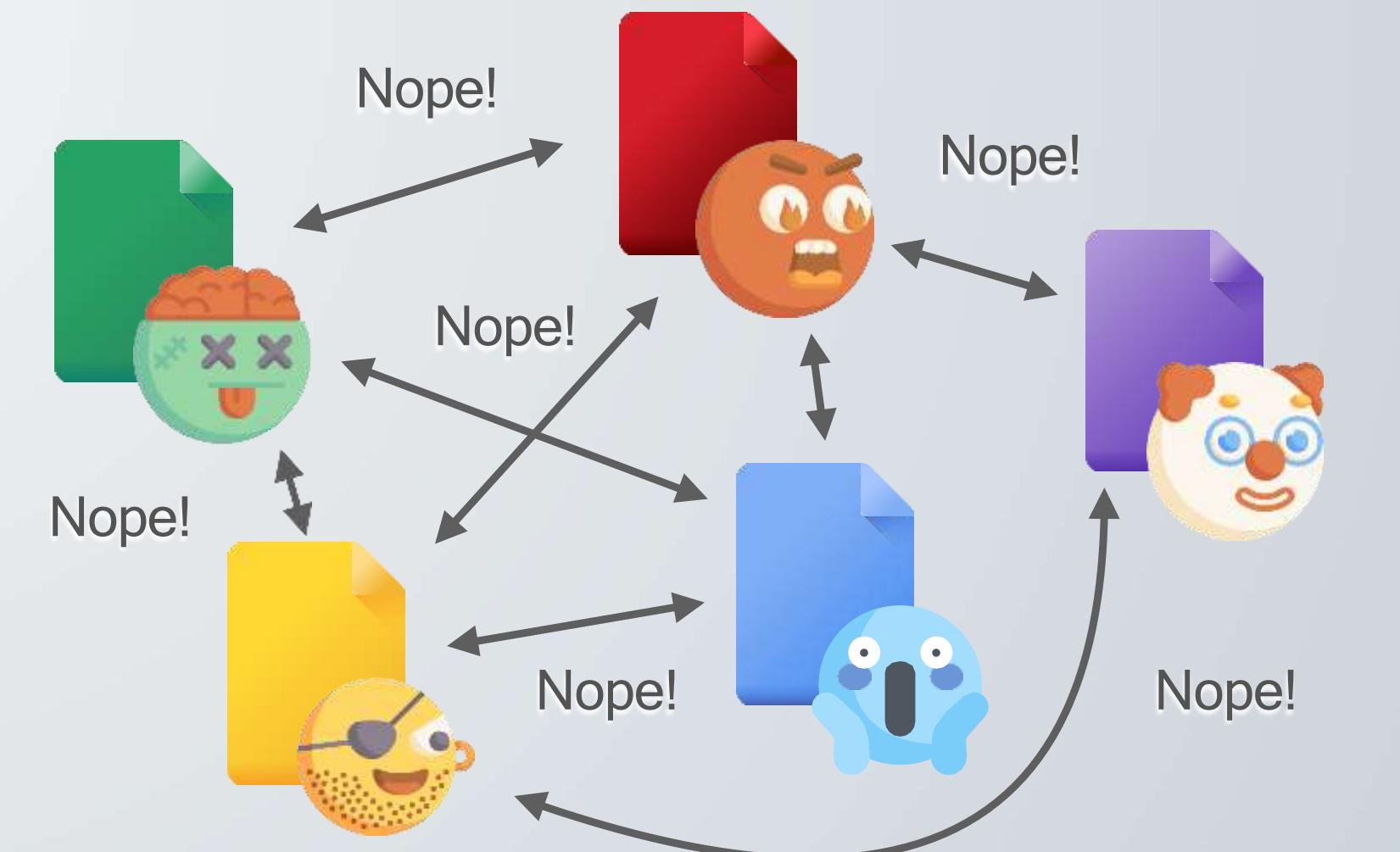
Resistenza debole

Data una stringa x è computazionalmente impossibile trovare la stringa $y \neq x$ tale che $h(y) = h(x)$.



Resistenza forte

È computazionalmente impossibile trovare una qualsiasi coppia (x,y) tale che $h(x) = h(y)$.





La scoperta di anche solo una collisione è motivo sufficiente per considerare deprecato un algoritmo di hashing (perché indica il fatto che potremmo calcolarne altre in un tempo computazionalmente sensato)

Secure Hash Algorithm

SHA è una famiglia di algoritmi.

SHA-1

(deprecato dal 2011)

- Digital Certificate signatures
- Email PGP/GPG signatures
- Software vendor signatures
- Software updates
- ISO checksums
- Backup systems
- Deduplication systems
- GIT
- ...

SHA-2

(2001)

- SHA-224
- SHA-256
- SHA-384
- SHA-512

SHA-3

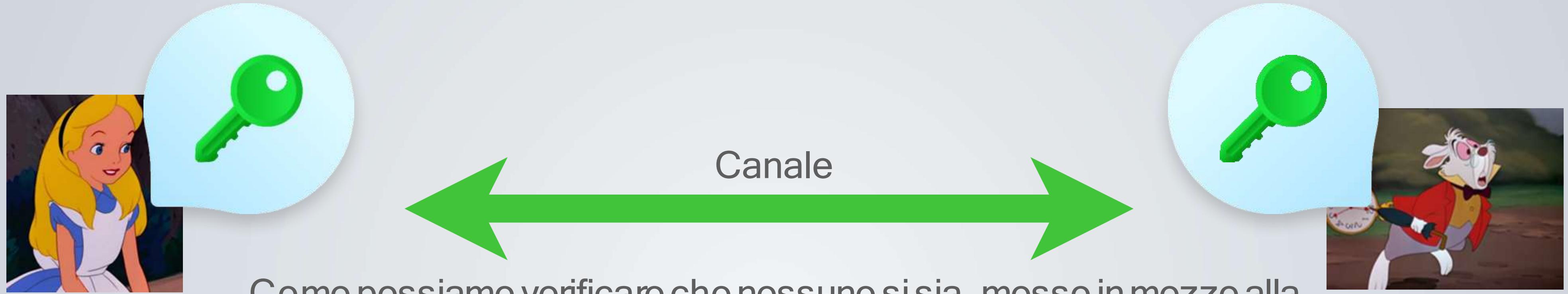
(2015)



Certificati digitali



Risolvere il Man-in-the-middle



Come possiamo verificare che nessuno si sia messo in mezzo alla comunicazione?

Verifica manuale

Certificazione

(le vedremo più avanti...)



Io sono Alice,
ecco la mia
chiave pubblica!



IO sono Alice!



Certificazione delle informazioni pubbliche



L'informazione pubblica può essere falsificata, quindi:

- viene distribuita all'interno di un certificato;
- il certificato è firmato digitalmente e non può essere contraffatto.

Chiave pubblica e info

Firma digitale

Certificati digitali

Un certificato digitale contiene:

- Informazioni sulla chiave
- Informazioni sull'identità del proprietario
- Firma digitale dell'entità che ha verificato la validità dei contenuti



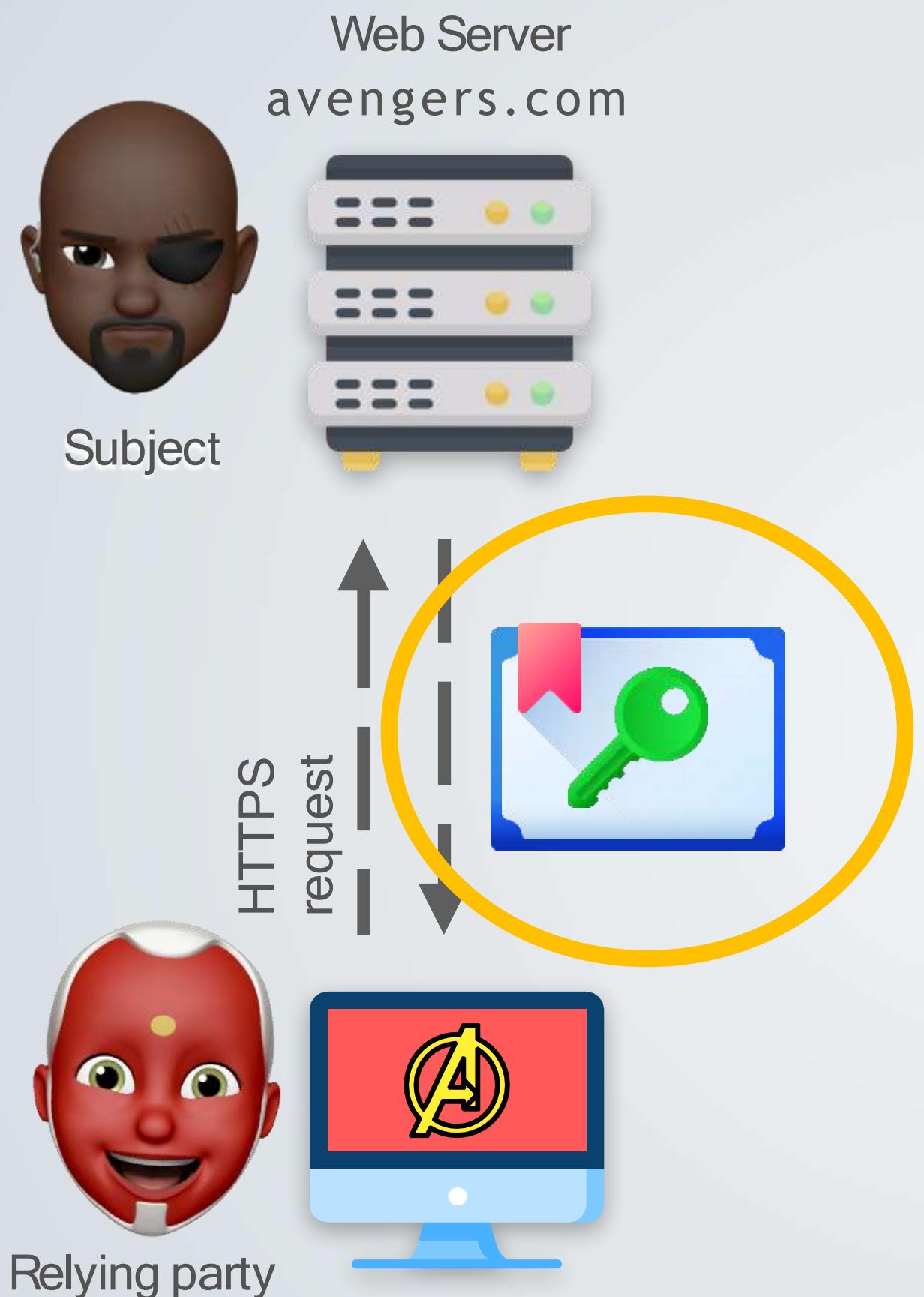
Certificati digitali

Un **certificato digitale** è un documento elettronico che attesta l'associazione univoca tra una chiave pubblica e l'identità di un soggetto.

Il soggetto dichiara così di utilizzare la chiave pubblica per procedure di cifratura asimmetrica e/o autenticazione tramite firma digitale.

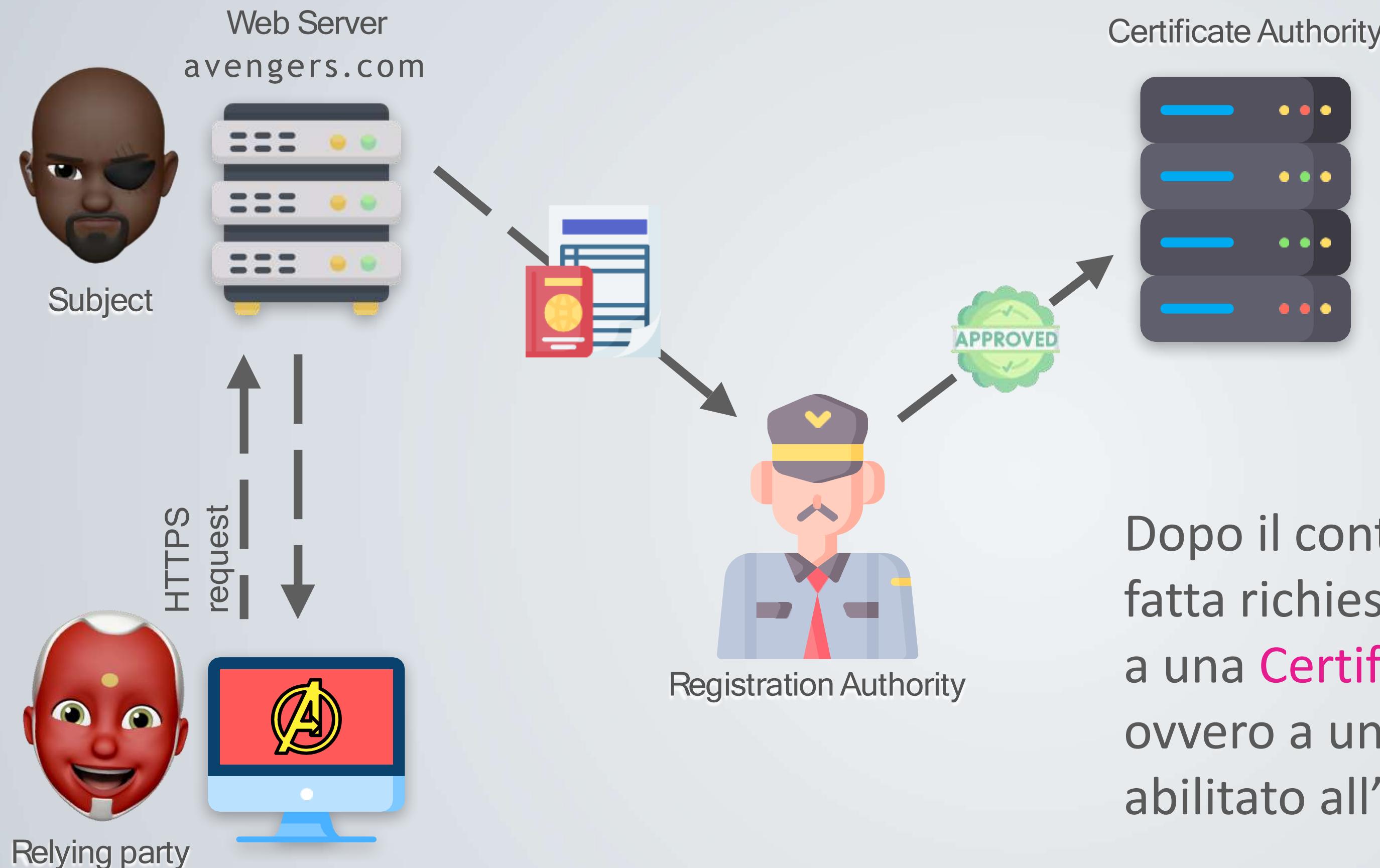
Certificare la chiave pubblica





A e B si vogliono scambiare dei messaggi con la crittografia asimmetrica, ma vogliono essere sicuri dell'identità dell'altro.

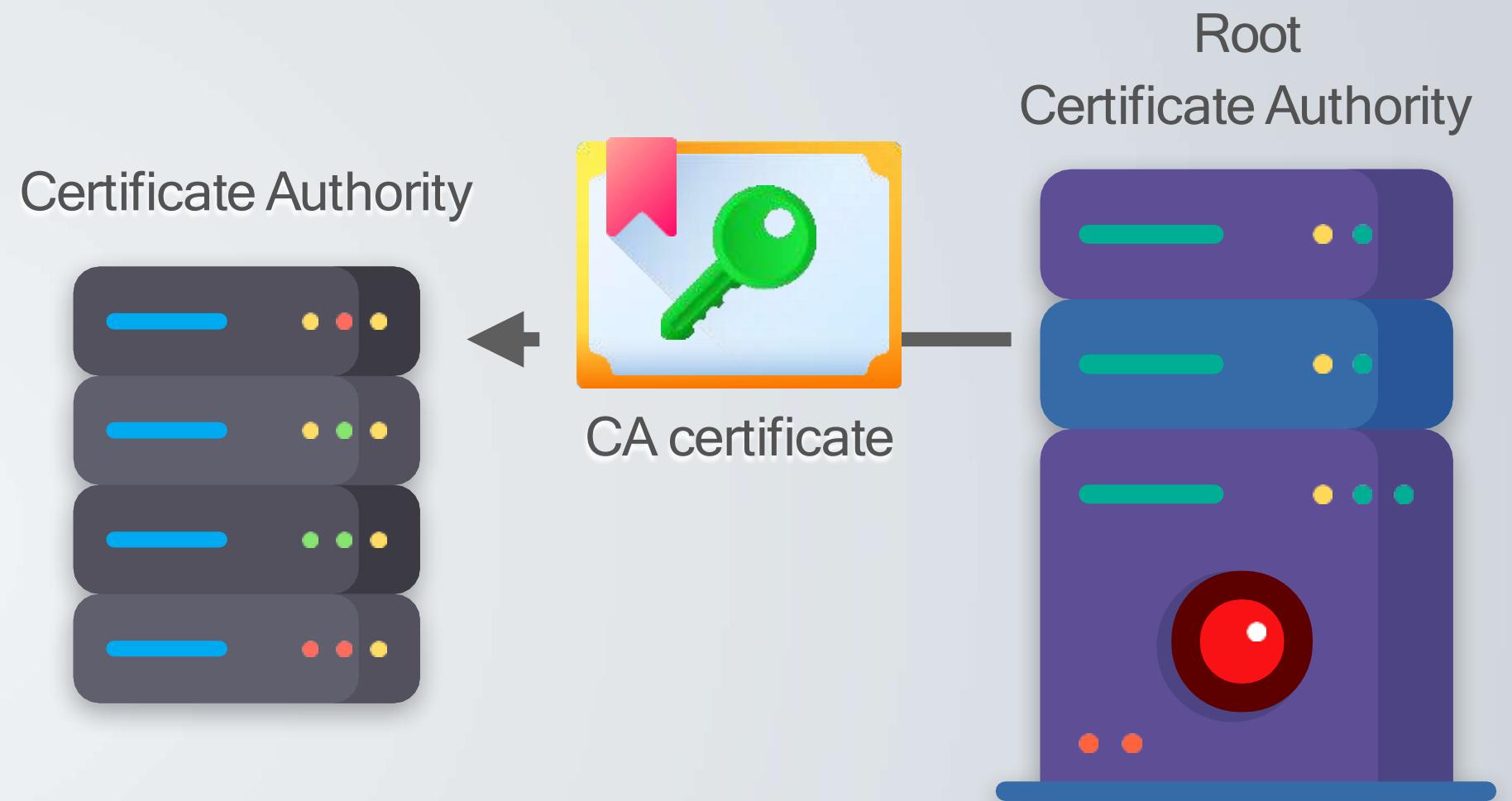
Come si ottiene un certificato?



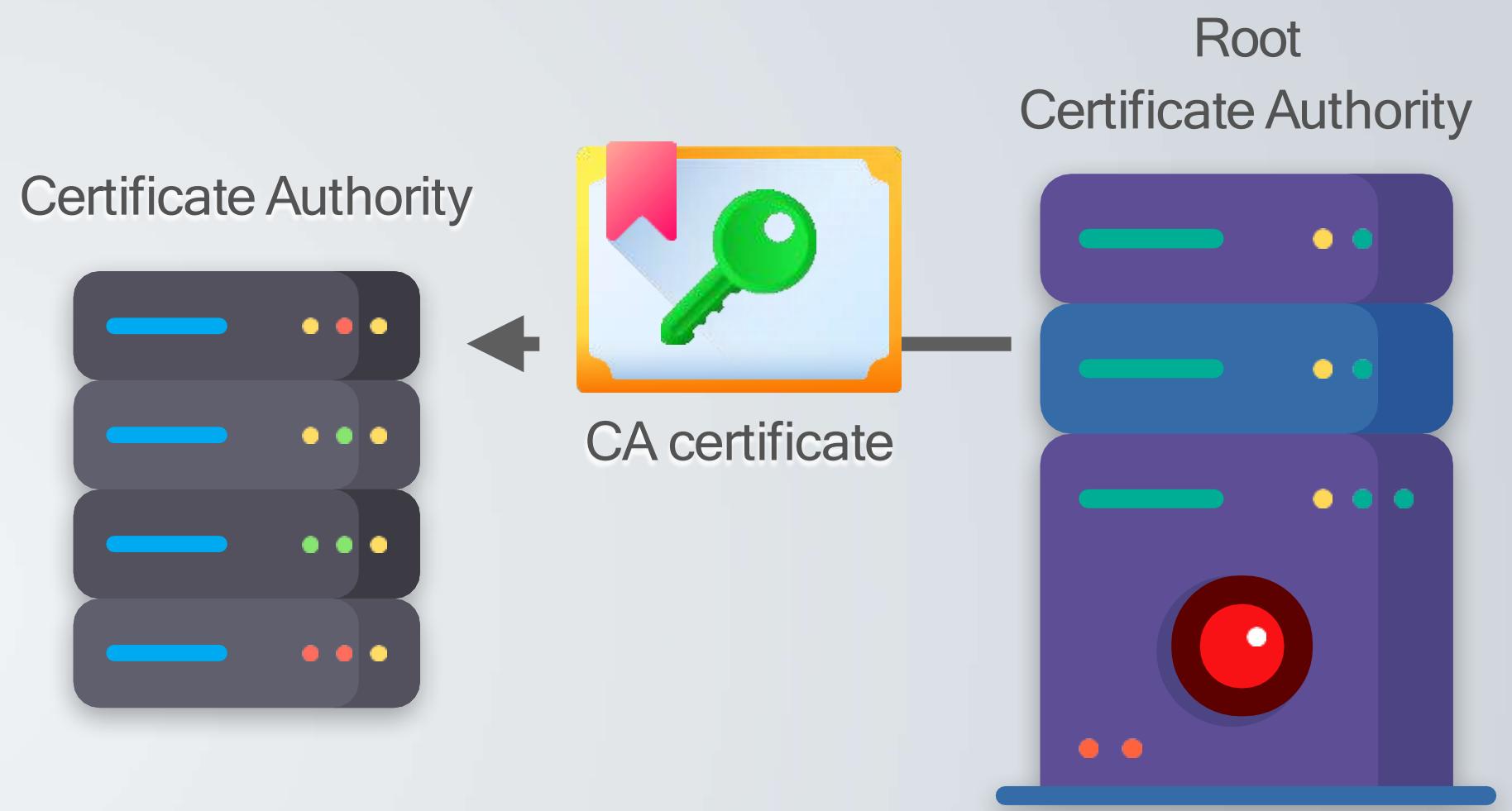
Dopo il controllo dei documenti, viene fatta richiesta di emissione certificato a una **Certificate Authority (CA)**, ovvero a un soggetto terzo, di fiducia e abilitato all'emissione di certificati

Perché ci fidiamo di una CA? Perché è a sua volta certificata!

La **Root Certificate Authority** è una CA che firma da sé il proprio certificato. Ciò significa che, in autonomia, crea chiave pubblica e privata, crea la richiesta di rilascio di un certificato e la firma con la sua chiave privata.



Non esiste, da un punto di vista architetturale, alcuna autorità garante al di sopra della Root CA → vengono fornite garanzie giuridiche e non tutte le CA possono essere Root CA.





Il certificato digitale richiesto dall'utente viene così emesso e può essere utilizzato per confermare la propria identità nelle comunicazioni online

Il certificato può essere validato online
(ad esempio da una Validation Authority) e può esserne anche
controllato lo stato di validità (tramite la
Certificate Revocation List)



La **Certificate Revocation List** è una lista di certificati che sono stati revocati dalla CA prima della scadenza, e che non dovrebbero più essere considerati attendibili.

I motivi della revoca includono compromissione della chiave privata, certificato rilasciato in modo improprio, pubblicazione di documenti falsi, ecc

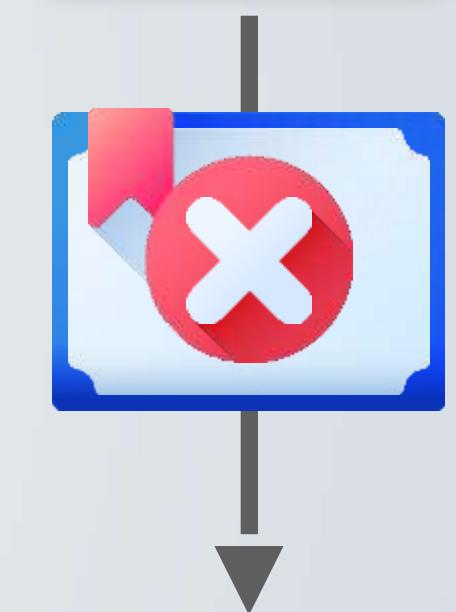
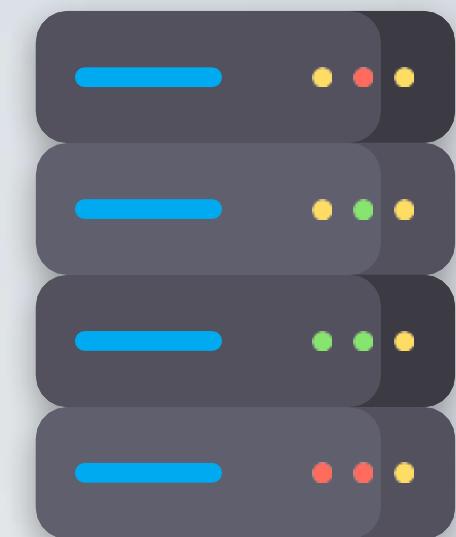
La revoca è IRREVERSIBILE.



Relying party



Certificate Authority



Certificate
Revocation
List (CRL)

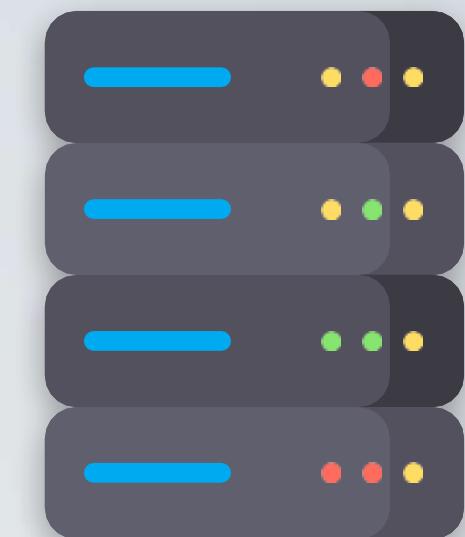


OCSP Responder
(Online Certificate
Status Protocol)
CRL distribution point

La CRL può essere interrogata utilizzando un **Online Certificate Status Protocol**, ovvero un protocollo online che permette di ottenere informazioni sullo stato di un certificato.

Utile perché consente di non scaricare l'intera CRL e ottenere l'intero certificato, ma fornisce solo le informazioni essenziali.

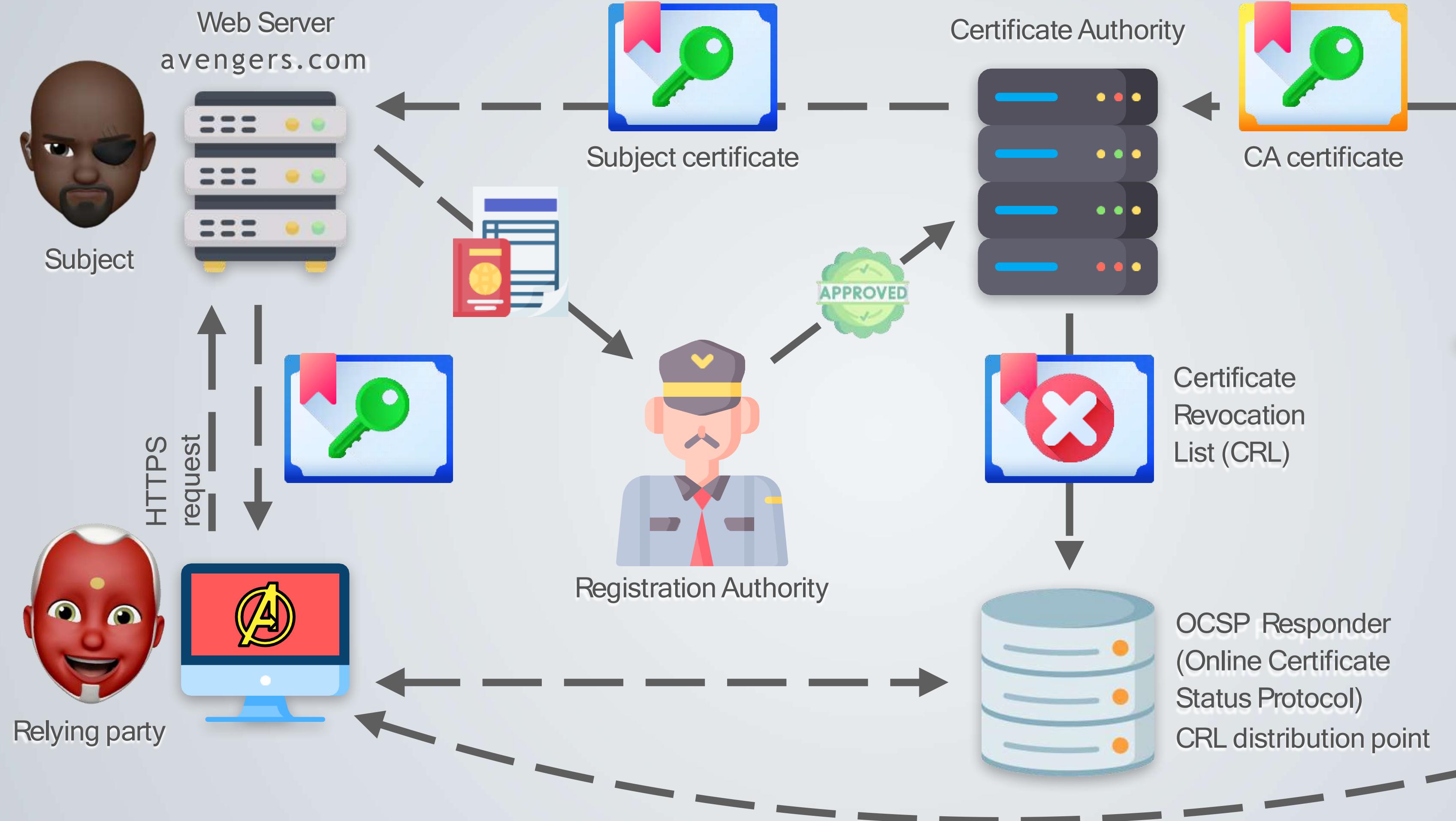
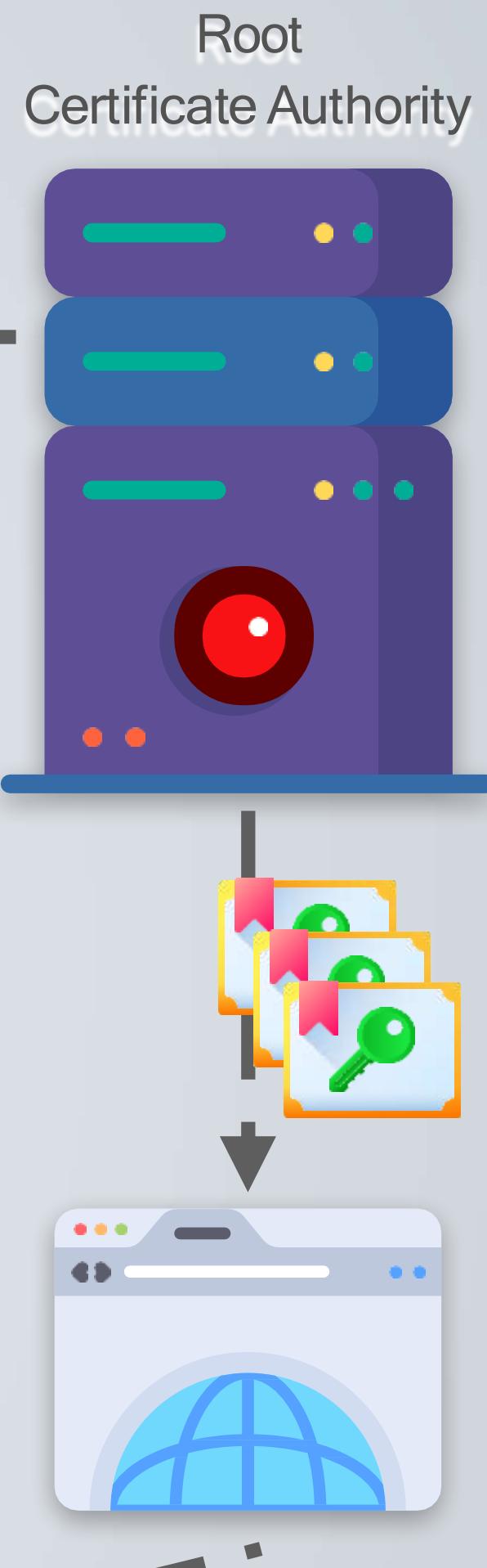
Certificate Authority



Certificate
Revocation
List (CRL)

OCSP Responder
(Online Certificate
Status Protocol)
CRL distribution point





Chi sono le CA?



digicert®

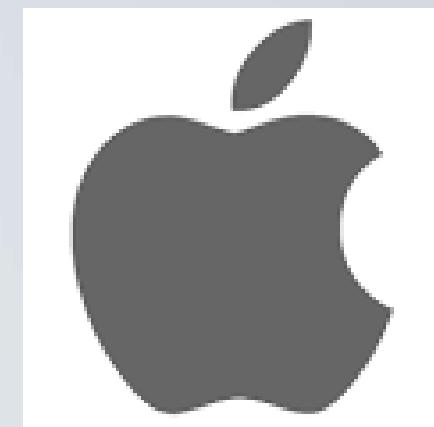
COMODO
Certification Authority



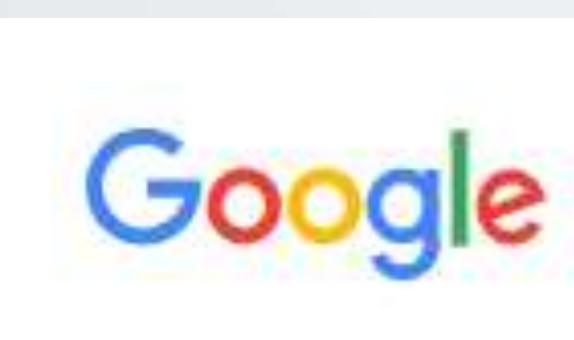
aruba.it



Chi sono le Root CA?



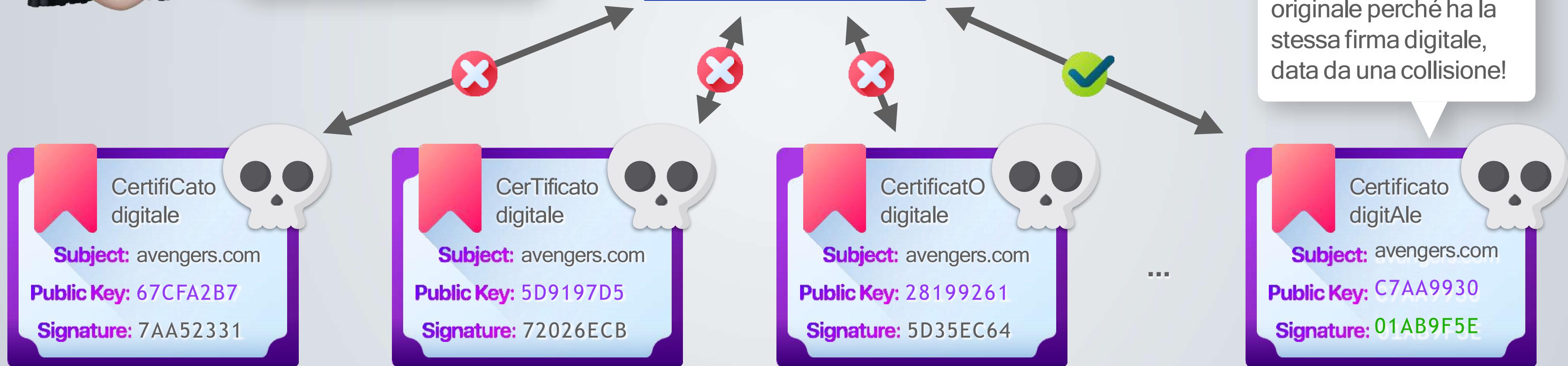
Chambers of Commerce Root Certificate



Come fare danni?



Se riuscissi a trovare una collisione potrei creare un certificato falso!

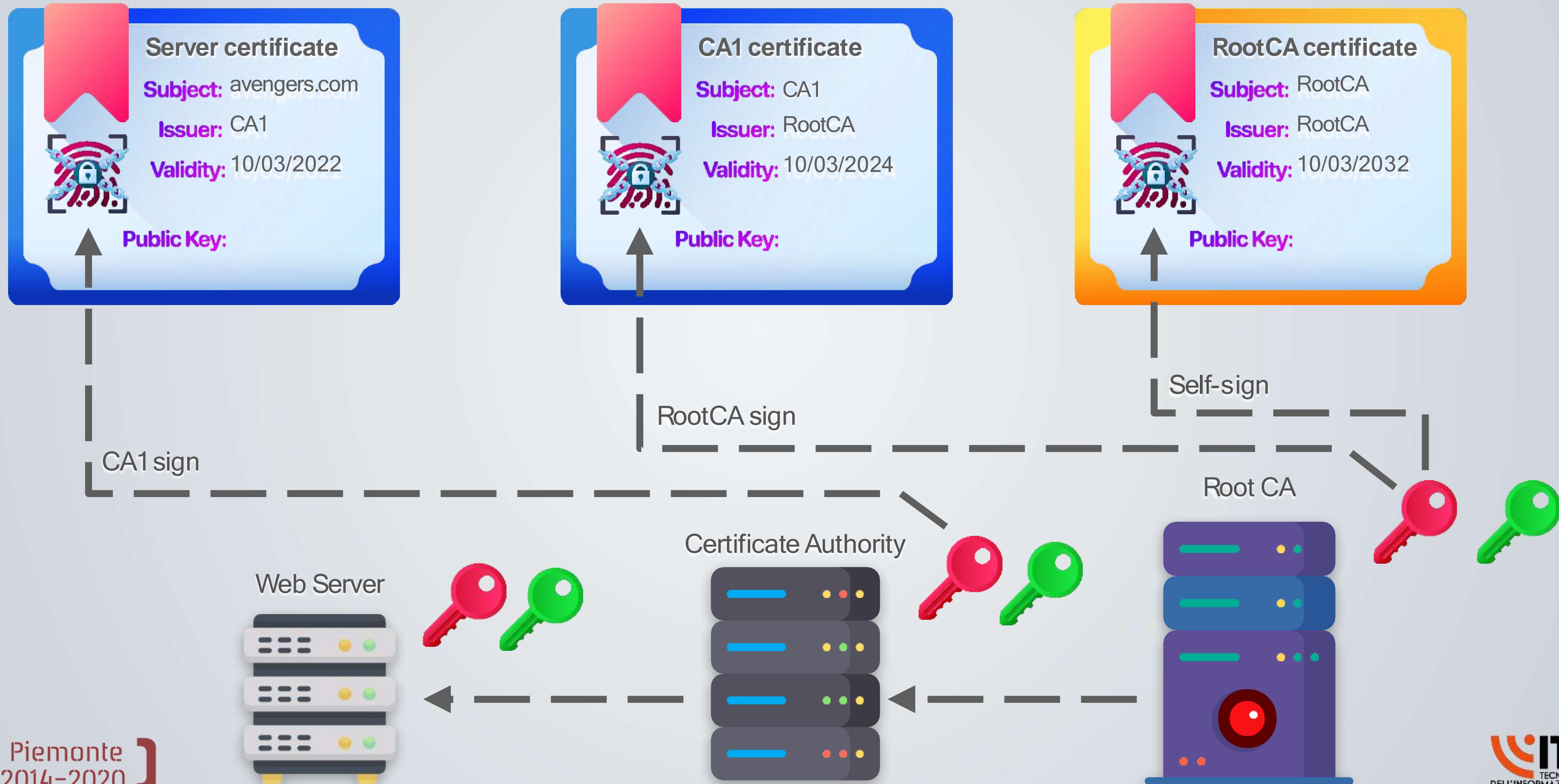


L'algoritmo di hash scelto è estremamente importante!



HTTPS e TLS

X.509 Certificate issuance



X.509 Certificate issuance

X.509 è uno standard usato per definire il formato dei certificati a chiave pubblica e delle CA.

Secondo questo standard, ogni certificato digitale contiene 3 voci principali:

- 1.Il certificato** (contenente ID dell'algoritmo, numero seriale, emittente, richiedente, informazioni sulla validità e sulla chiave pubblica del richiedente, ecc)
- 2.L'identificativo dell'algoritmo di firma del certificato**
- 3.La firma del certificato**

X.509 Certificate issuance

Uno degli usi più diffusi di X.509 è nell'ambito internet, dove il certificato **SSL/TSL** (che segue gli standard di X.509) viene usato nell'omonimo protocollo per rendere sicure le comunicazioni tra un sito web e il nostro browser.

TLS e SSL

TLS (**Transport Layer Security**) e il suo predecessore SSL (Secure Socket Layer) sono protocolli crittografici che permettono una comunicazione sicura tra mittente e destinatario all'interno della rete internet, fornendo autenticazione, integrità e confidenzialità dei dati.

L'autenticazione è unilaterale → il server si identifica presso il client, ma non avviene il contrario

NB. Questi protocolli sono ampiamente utilizzati soprattutto perché la struttura protocolare della rete internet non prevede di per sé alcuna funzionalità di sicurezza (quando è nata veniva utilizzata come rete per scambio di informazioni tra ricercatori nella comunità scientifica, solo successivamente è diventata patrimonio di tutti)

Transport Layer Security



Privacy

Algoritmi crittografici per nascondere il traffico dati.



Integrità

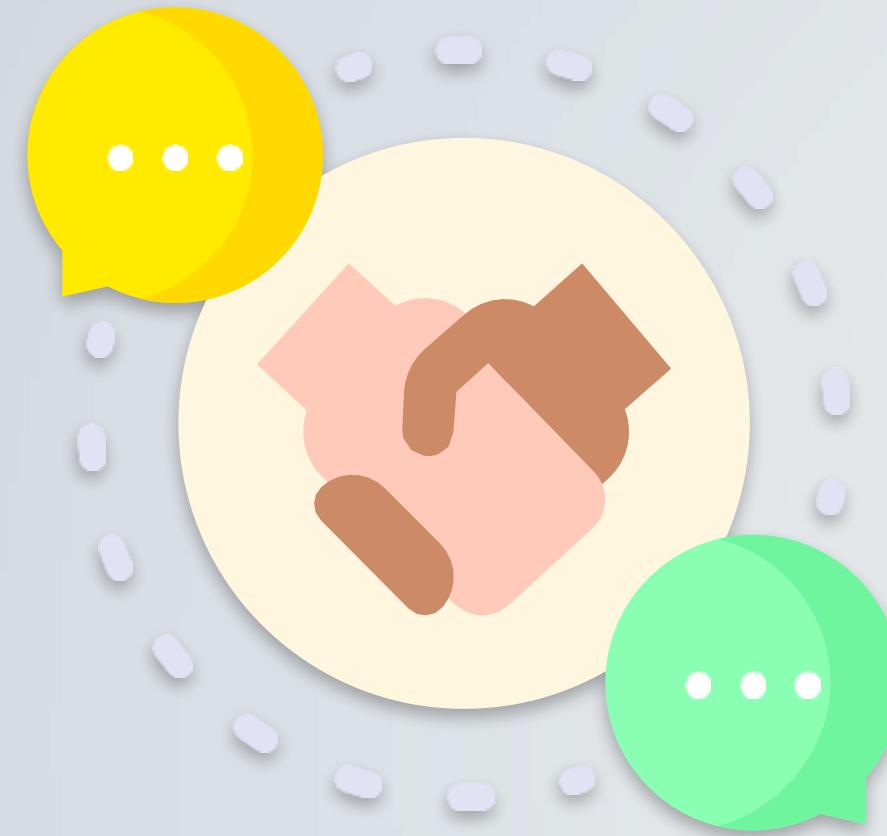
I dati non vengono alterati durante il transito in rete.



Identificazione

Il certificato digitale permette di identificare l'altra parte coinvolta.

Le 3 fasi di TLS



Fase 1

Negoziazione fra le parti
degli algoritmi da utilizzare



Fase 2

Scambio delle chiavi
e autenticazione



Fase 3

- Cifratura simmetrica e
autenticazione dei messaggi

Diffie-Hellman

RSA

AES-256

HMAC-SHA



https://

HTTPS è la combinazione di HTTP e SSL/TLS che implementa una connessione sicura tra browser (client) e web server, fornendo:

- Autenticazione del sito
- Integrità dei dati
- Protezione della privacy

HTTPS utilizza i certificati digitali per attestare l'identità del sito Web visitato.



https://

Con l'utilizzo di HTTPS viene usata (solitamente) la porta 443 e viene invocato TLS che cifra:

- L'URL della pagina richiesta
- Eventuali parametri della query e body (messaggio)
- Intestazioni di connessione (headers)
- Cookies



https://

ATTENZIONE!

Poiché IP e numero di porta fanno parte del protocollo di trasmissione TCP (e non di https stesso), non possono essere protetti.

Possiamo solo proteggere il contenuto della comunicazione.



https://

Un utente dovrebbe fidarsi di una connessione HTTPS verso un sito web se e solo se tutti i punti seguenti sono verificati:

- Il sito web fa uso di un certificato digitale
- Il certificato è stato emesso da una CA nota/fidata
- Il certificato risulta valido (= è valida la firma al suo interno)
- Il certificato identifica il sito web (ad esempio quando il browser visita "<https://example.com>", il certificato ricevuto è appropriatamente quello relativo a "example.com" e non di qualche altra entità)
- Il protocollo SSL/TLS utilizzato è sufficientemente sicuro

Puoi trovare TLS in...



Web

HTTPS



VPN



e-mail



instant message



VPN (Virtual Private Network)

Rete privata virtuale che garantisce

- Privacy
- anonimato
- sicurezza dei dati



attraverso un canale di comunicazione riservato (tunnel VPN) tra dispositivi che non necessariamente si trovano nella stessa rete locale. Il tunnel è quindi creato sopra un'infrastruttura di rete pubblica.



VPN ad accesso remoto

Consentono agli utenti di accedere a un server su una rete privata tramite rete internet (es. collego un pc con il server dell'azienda tramite VPN)

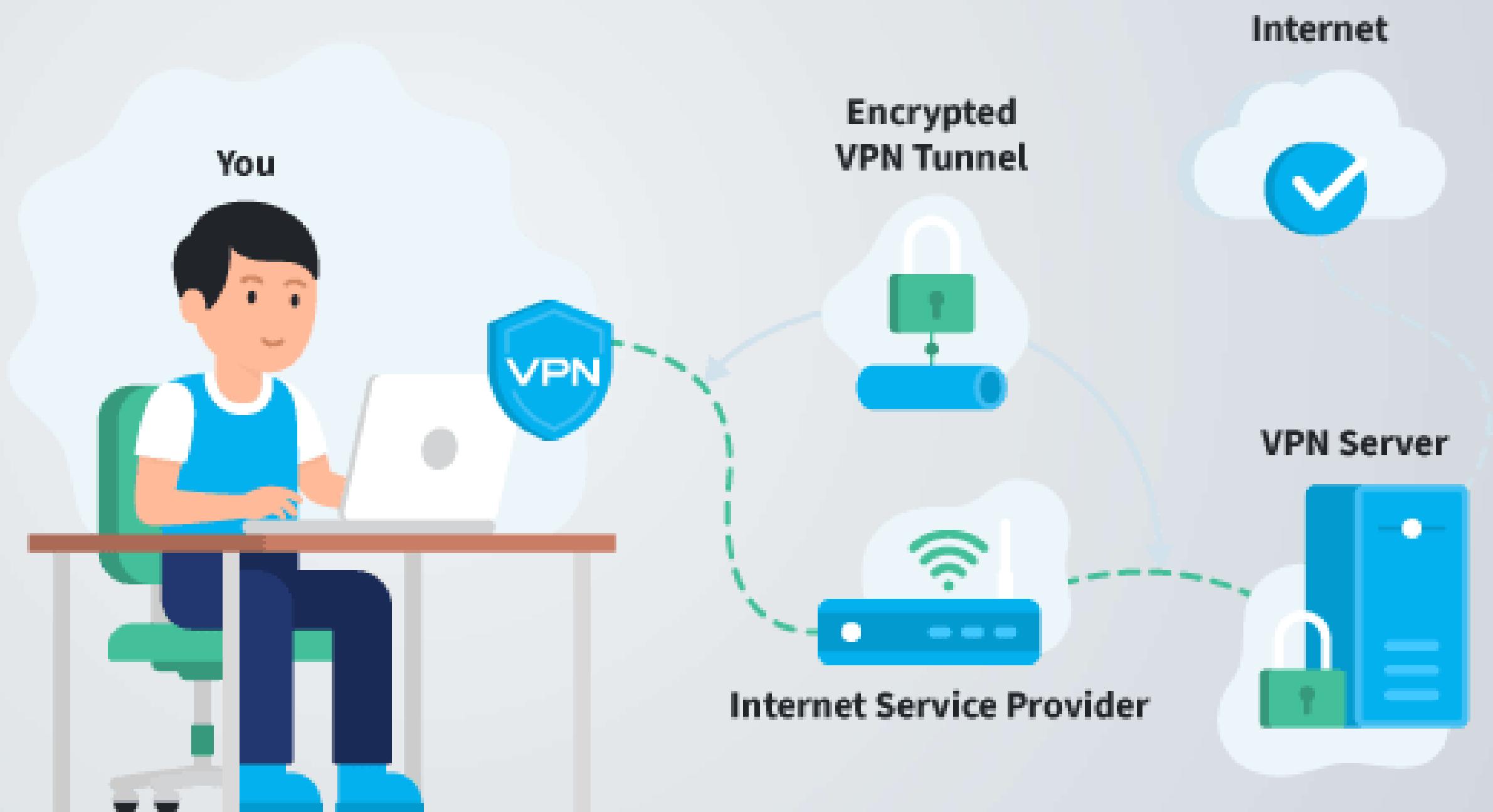
Idealmente, è come avere a disposizione un canale dedicato e privato

VPN site-to-site

Utilizzate per connettere in una rete privata (sempre tramite rete internet) uffici dislocati in più sedi o di più organizzazioni.

Ogni sede ha un router dedicato che si occupa di comunicare con gli altri nodi della VPN.

Tra le due entità comunicanti viene costruito un tunnel, all'interno del quale vengono incapsulati i dati



In base alla loro sicurezza, le VPN possono essere classificate in:

- **Trusted**
un provider assicura la creazione di percorsi dotati di specifiche caratteristiche di sicurezza e pertanto idonei all'utilizzo per scambio di informazioni
- **Secure**
garantisce la creazione di un tunnel attraverso protocolli di crittografia. I dati che viaggiano sul tunnel sono pertanto inaccessibili a tentativi di intercettazione
- **Hybrid**
unione delle due