PIEMONTE
FONDI STRUTTURALI E DI INVESTIMENTO EUROPEI 2014/2020
fondo sociale europeo
ITS TECNOLOGIE DELL'INFORMAZIONE E DELLA COMUNICAZIONE

Certificati digitali e hashing

Sicurezza informatica

v 2.2 ~ mar 2021

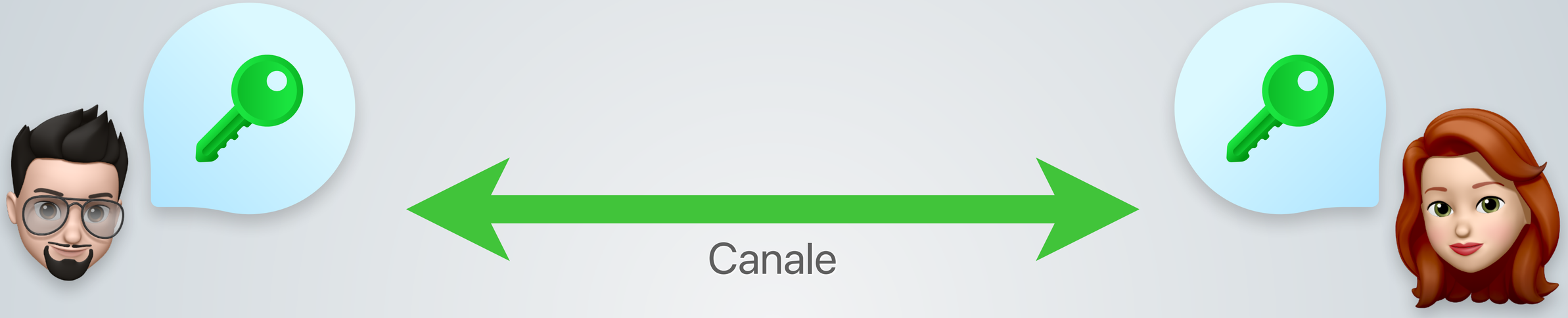
Prof. Marco Farina

marco.farina@its-ictpiemonte.it

t.me/marcofarina

in collaborazione con:
ISTITUTI TECNICI SUPERIORI
Ministero dell'Istruzione
UNIONE EUROPEA
REGIONE PIEMONTE
per una crescita intelligente, sostenibile ed inclusiva
www.regione.piemonte.it/europa2020
INIZIATIVA CO-FINANZIATA CON FSE

Risolvere il Man-in-the-middle



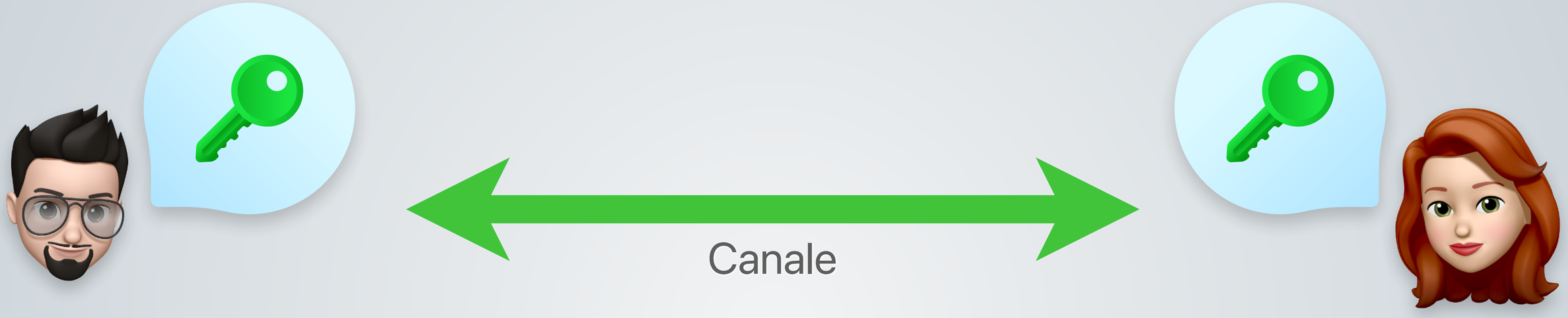
Come possiamo verificare che nessuno si sia messo in mezzo alla comunicazione?

Verifica manuale

Certificazione

(tra due lezioni...)

Risolvere il Man-in-the-middle



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

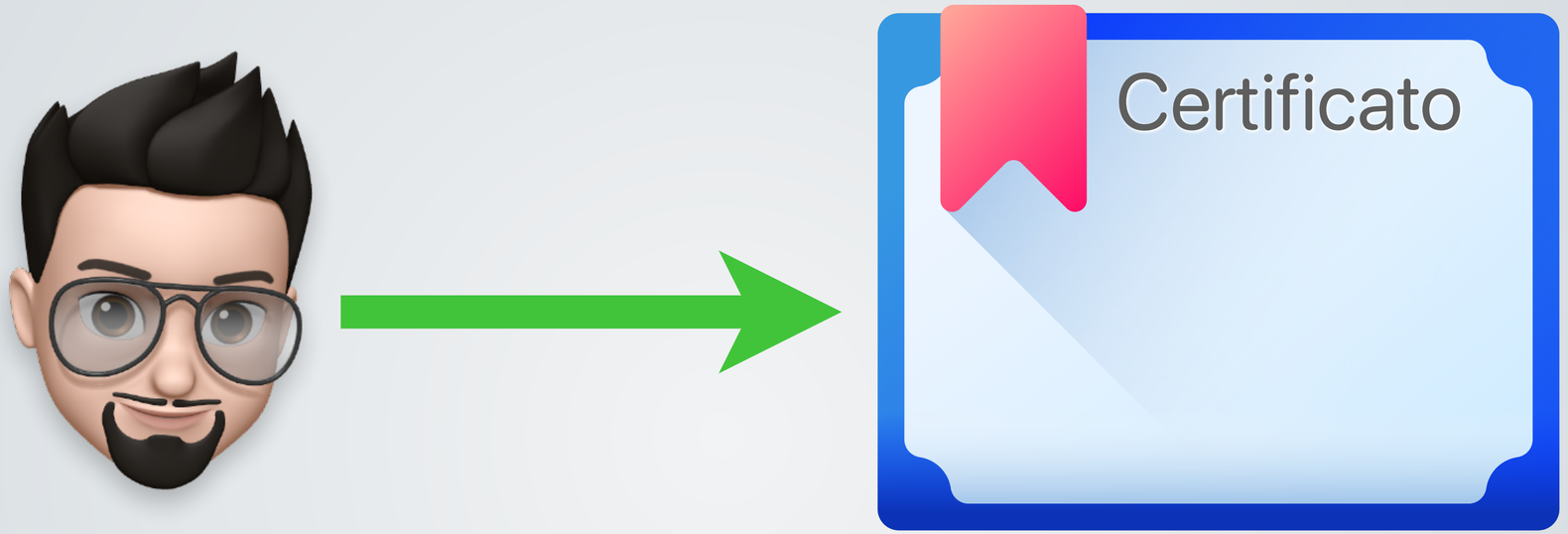
Verifica manuale

Certificazione

(tra due lezioni...)

Certificazione delle informazioni pubbliche

Certificazione delle informazioni pubbliche



L’informazione pubblica può essere falsificata, quindi:

- viene distribuita all’interno di un certificato;

Certificazione delle informazioni pubbliche

L'informazione pubblica può essere falsificata, quindi:

- viene distribuita all'interno di un certificato;

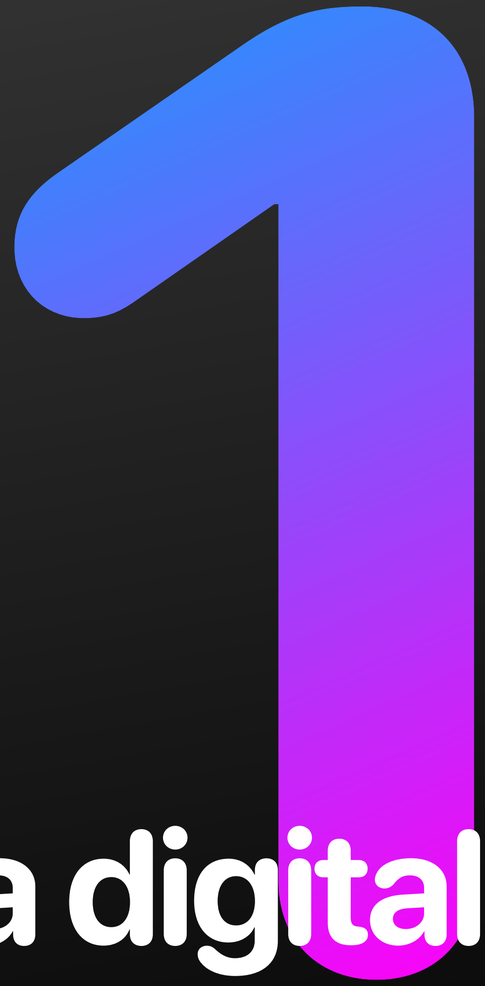
Certificazione delle informazioni pubbliche

L’informazione pubblica può essere falsificata, quindi:

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

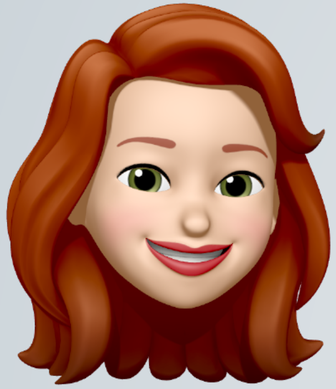
Chiave pubblica e info

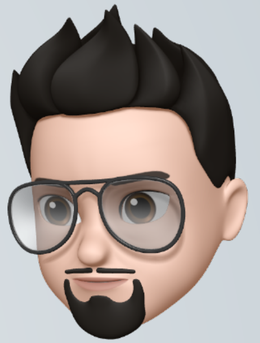
Firma digitale



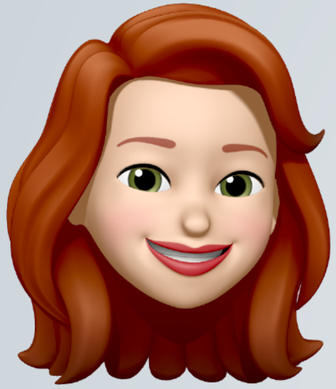
La firma digitale

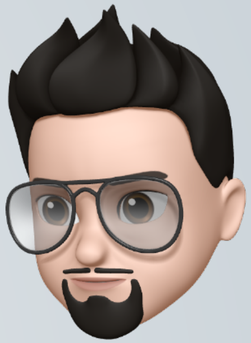
La firma digitale



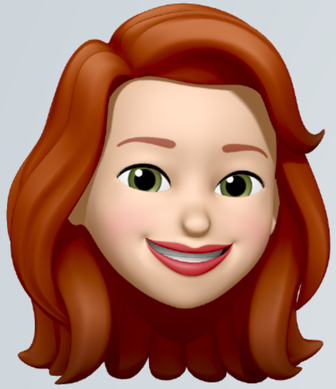


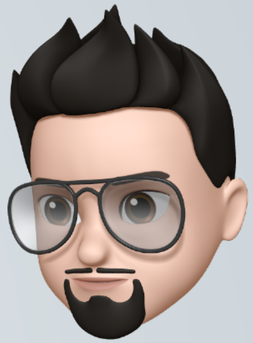
La firma digitale



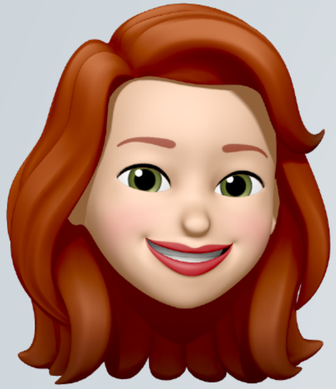


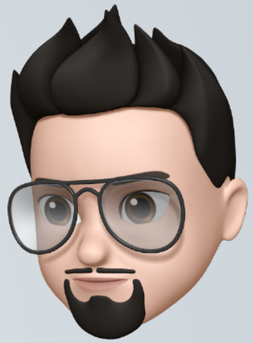
La firma digitale



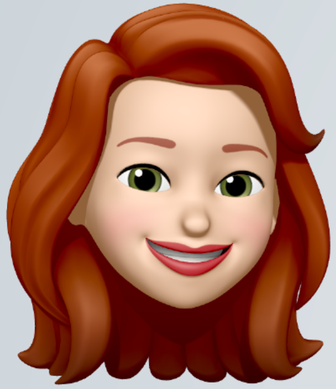


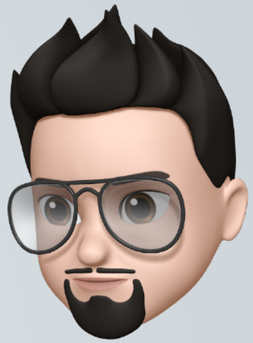
La firma digitale



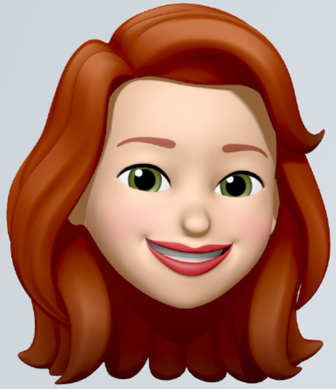


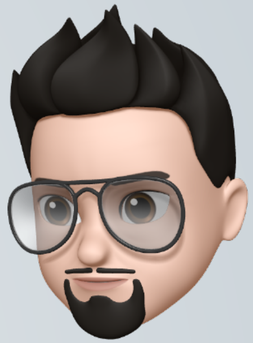
La firma digitale

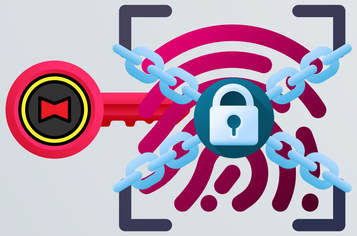




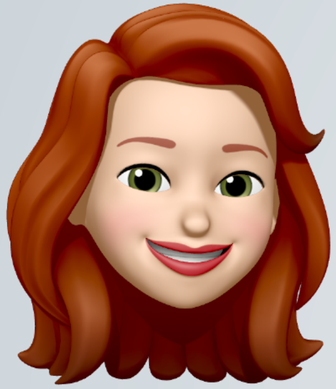
La firma digitale

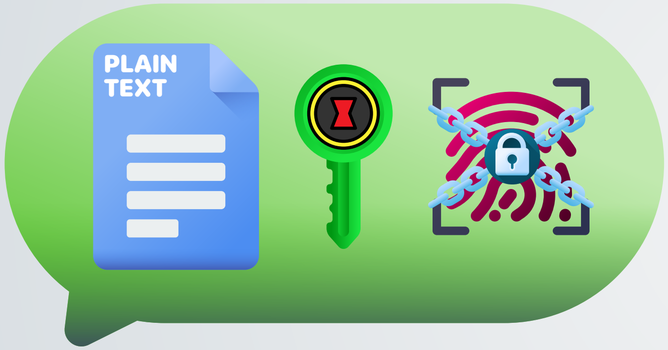


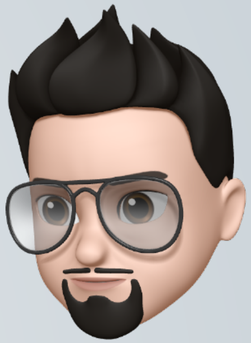




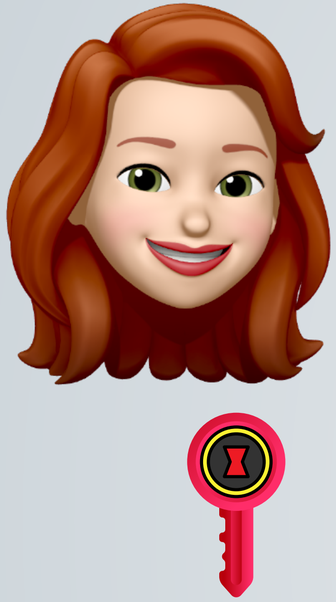
La firma digitale

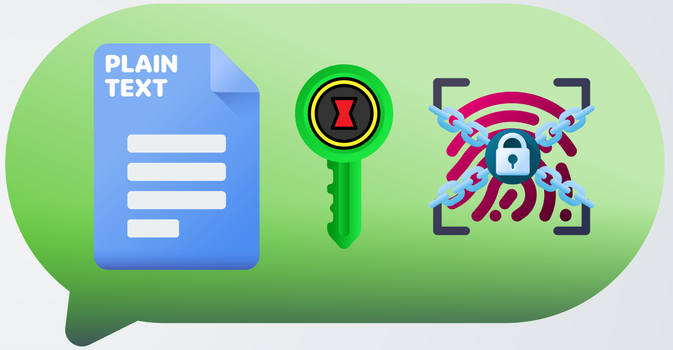




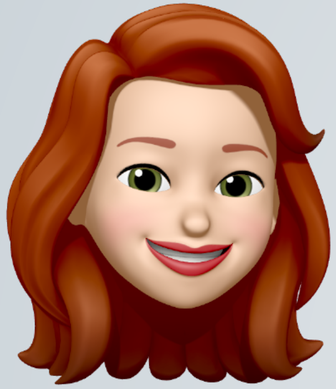


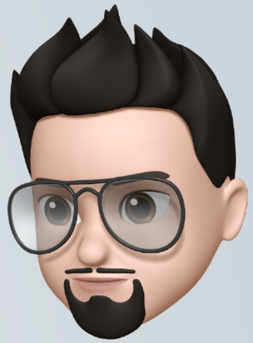
La firma digitale



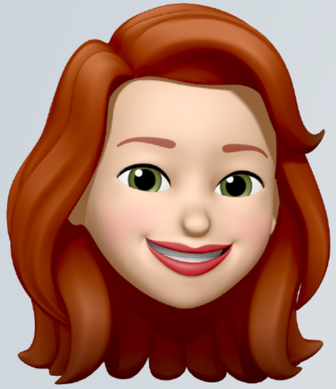


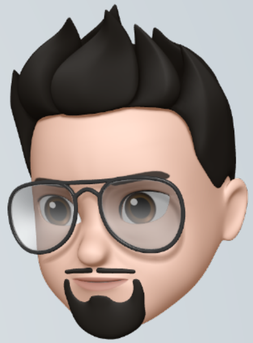
La firma digitale



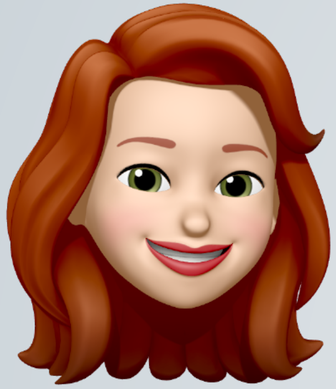


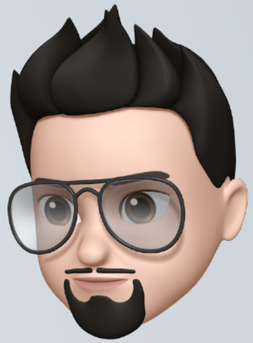
La firma digitale



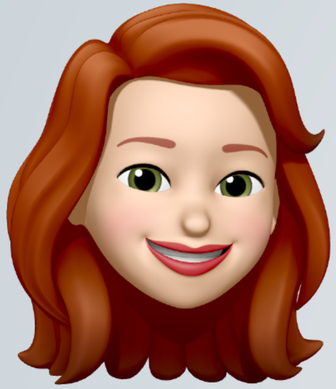


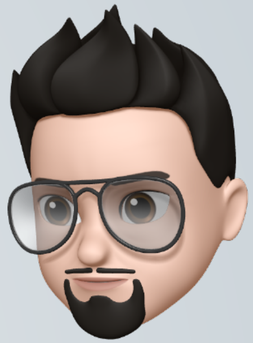
La firma digitale

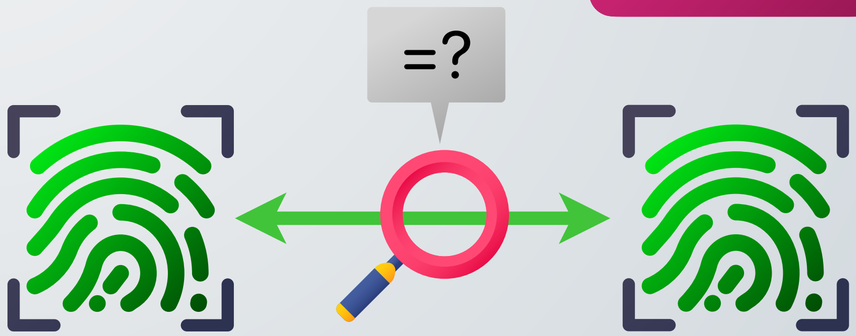




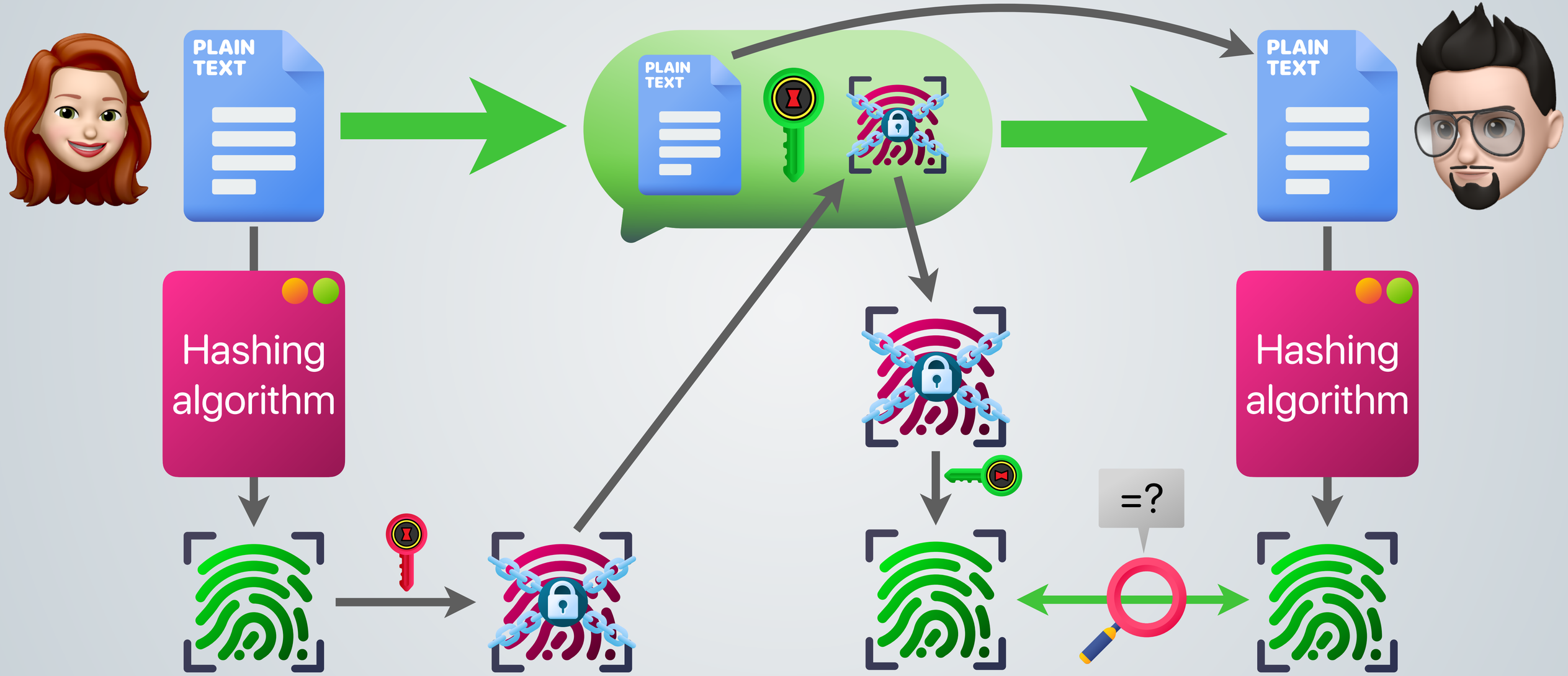
La firma digitale







La firma digitale



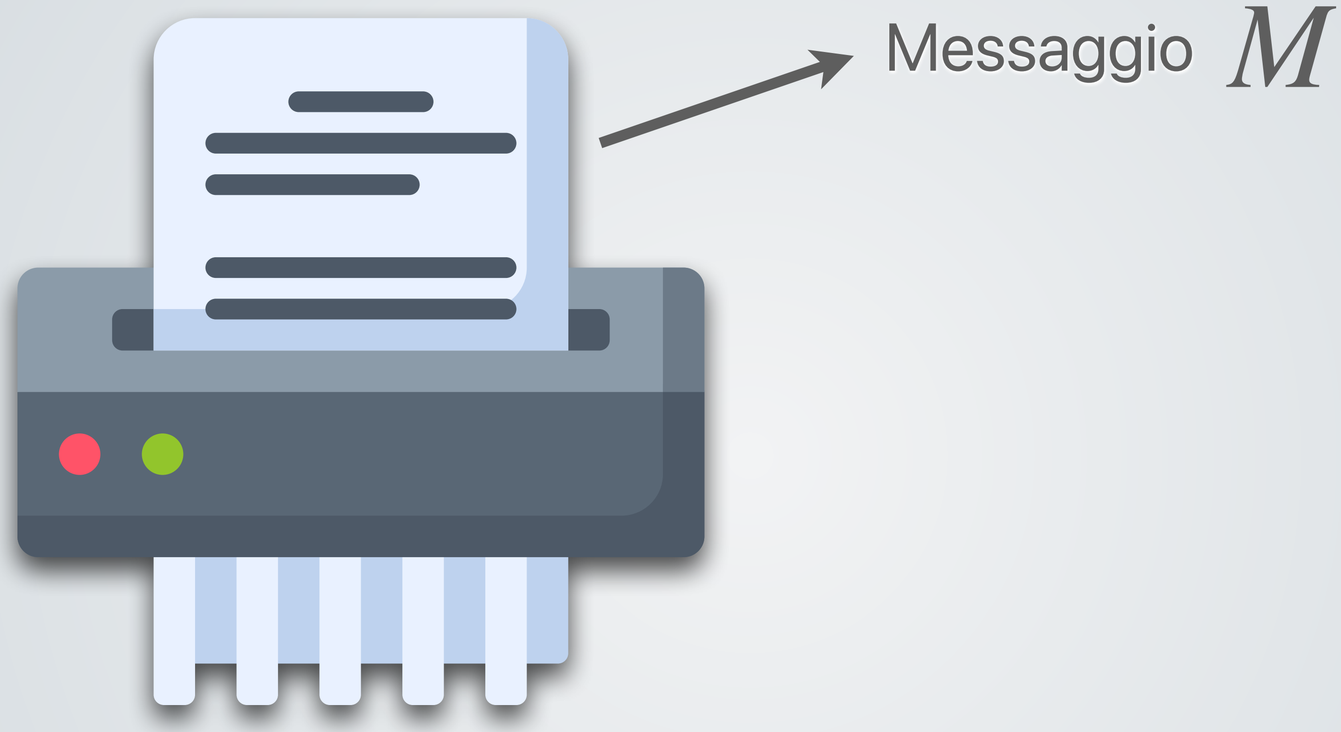
2

Algoritmi di hashing

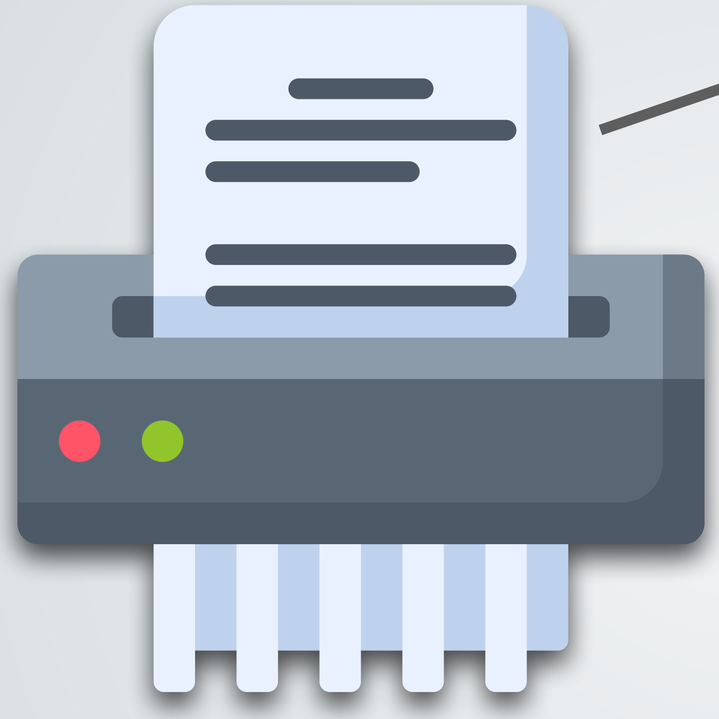
Le funzioni di hashing

Le funzioni di hashing

Le funzioni di hashing



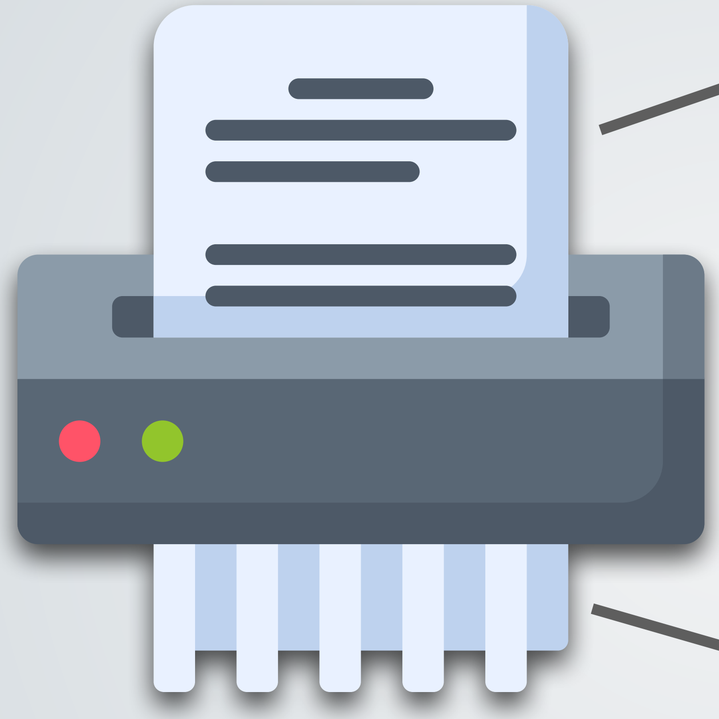
Le funzioni di hashing



Messaggio M

Funzione di hashing h

Le funzioni di hashing



Messaggio M

Funzione di hashing h

Hash H

$$H = h(M)$$

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

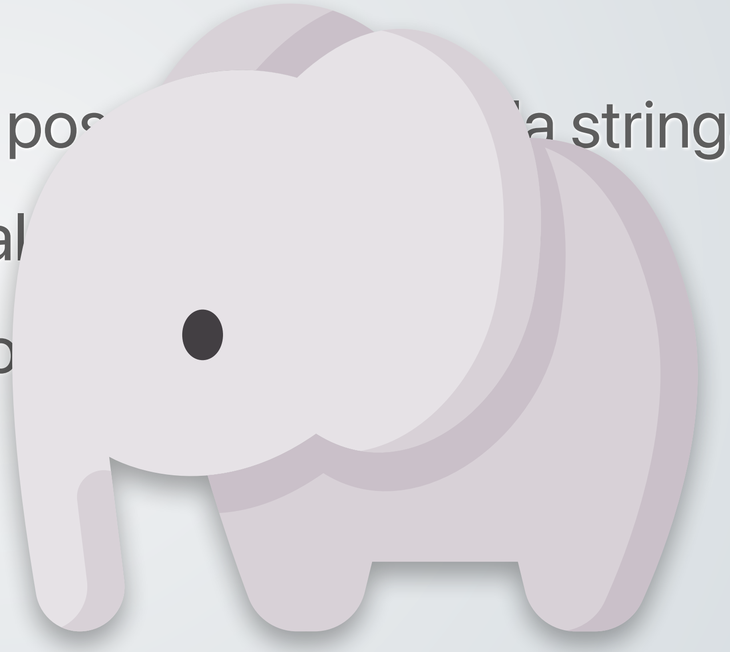
L'hash è una funzione non invertibile che mappa una stringa di lunghezza arbitraria in una stringa di lunghezza predefinita.

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

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

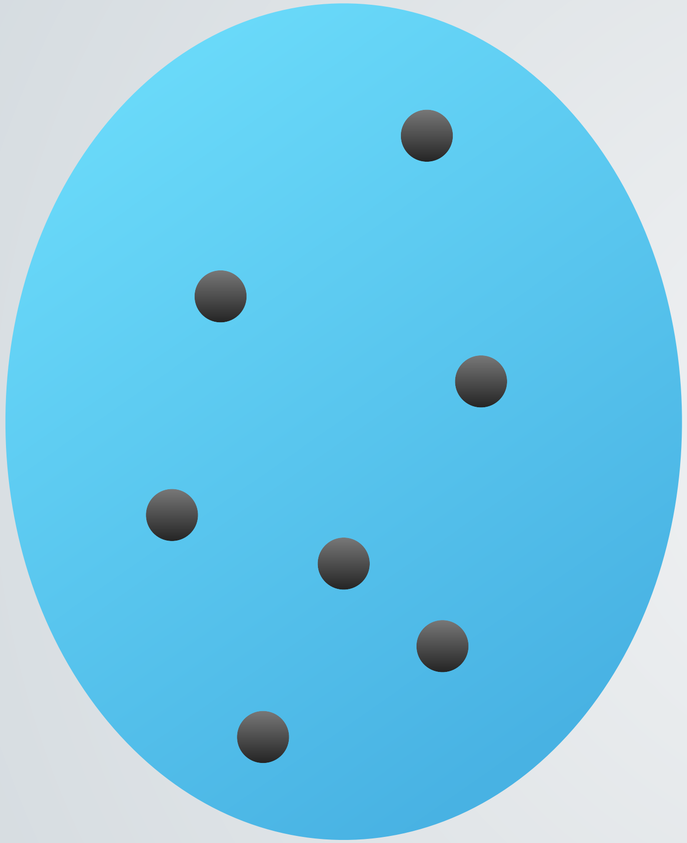
1. A partire dall'hash non è pos a stringa originale.
2. L'input può essere di qual
3. L'output ha una dimensio



DFCD3454

52ED879E

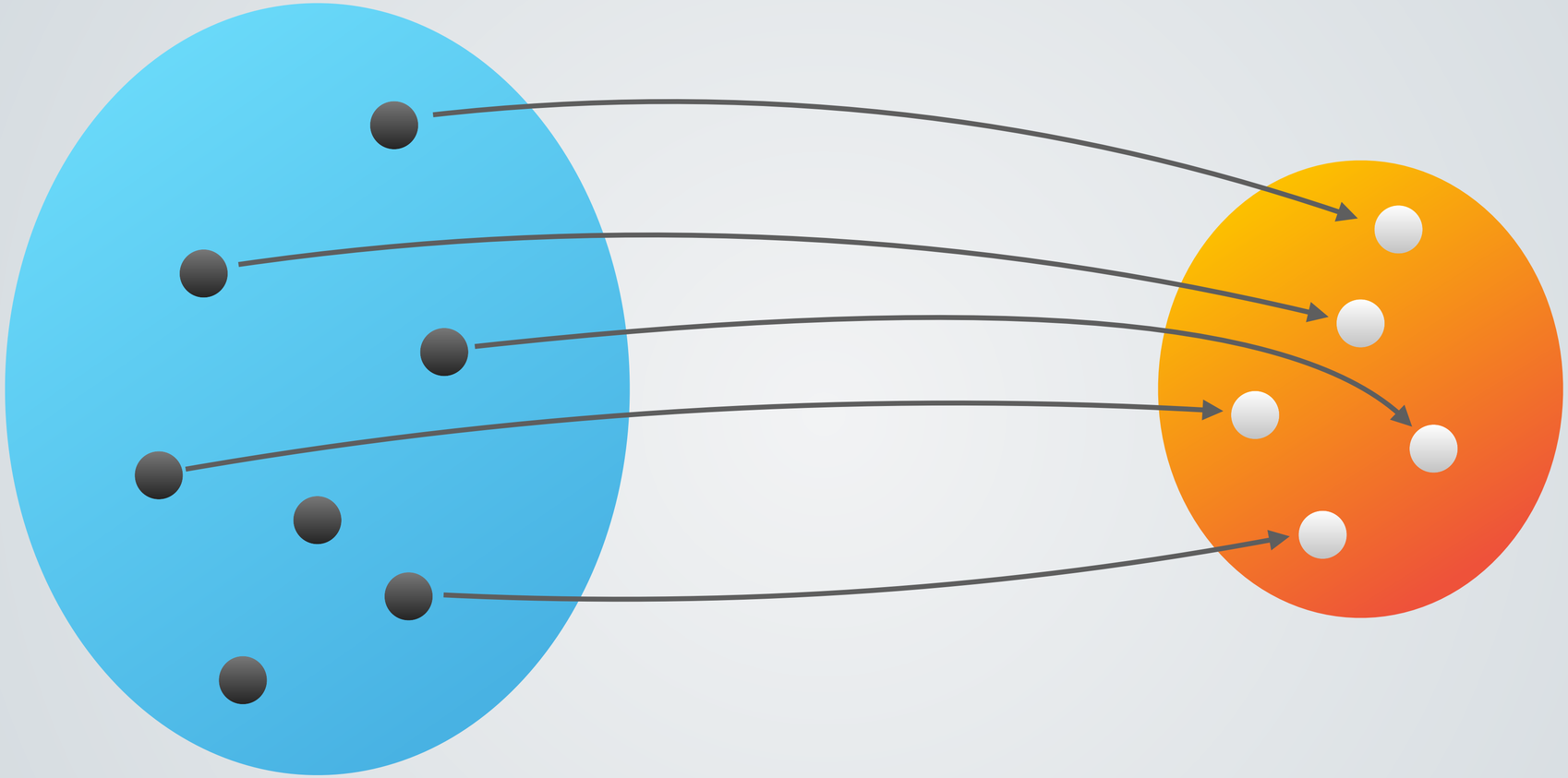
Qualquadra non cosa.



Tutti i messaggi
possibili

tutti gli hash
possibili.

Qualquadra non cosa.

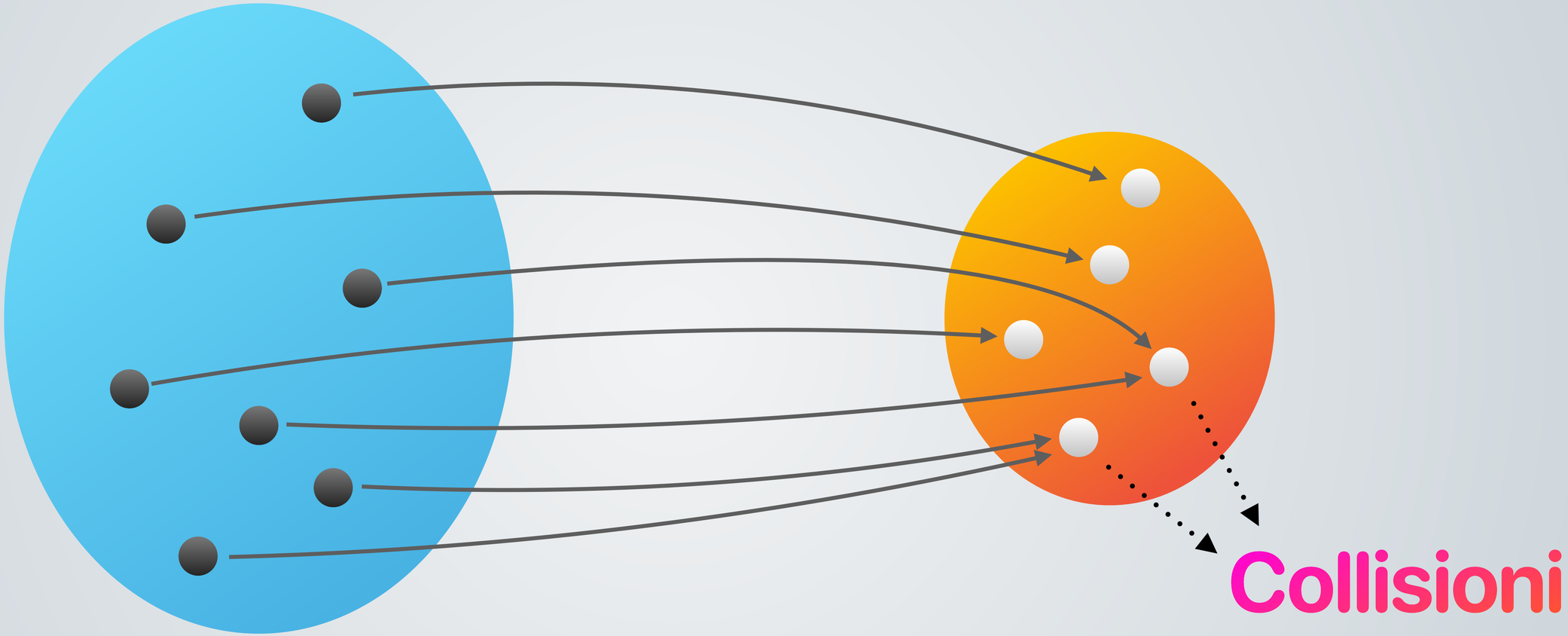


Tutti i messaggi possibili

sono di più di

tutti gli hash possibili.

Qualquadra non cosa.



Tutti i messaggi possibili

sono di più di

tutti gli hash possibili.

Resistenza alle collisioni

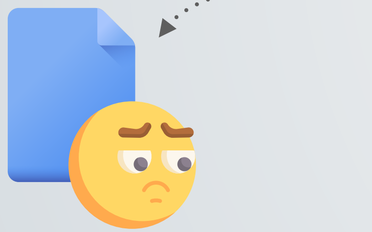
Resistenza debole

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

Resistenza alle collisioni

Resistenza debole

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

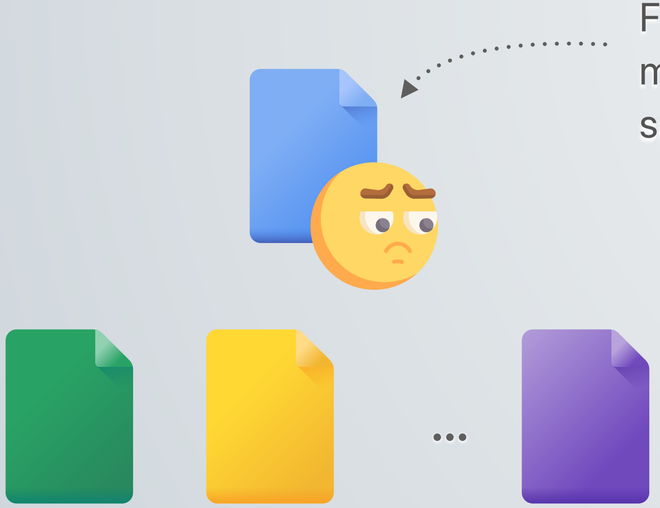


Fissato un messaggio ed il suo hash...

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 alle collisioni

Resistenza debole

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

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 $h(x) = h(y)$.

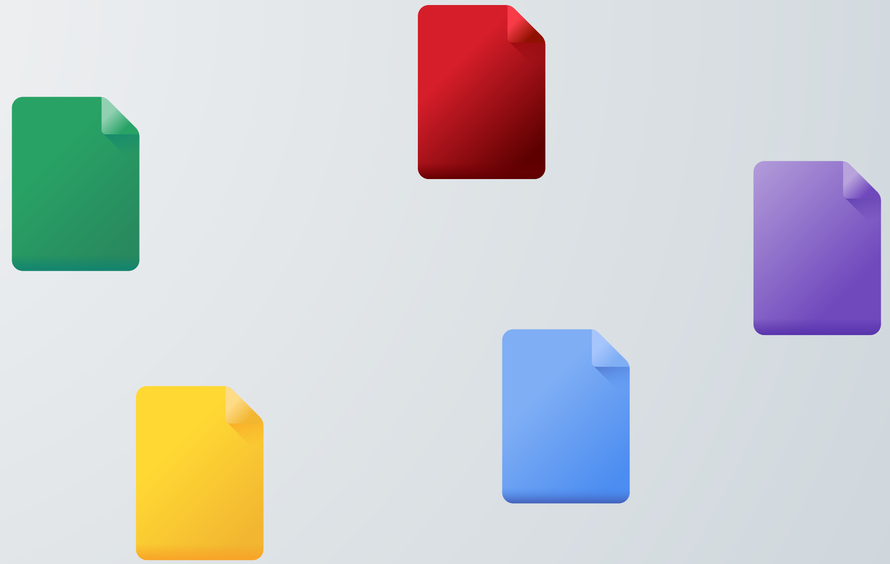
Resistenza alle collisioni

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 $h(x) = h(y)$.



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 $h(x) = h(y)$.

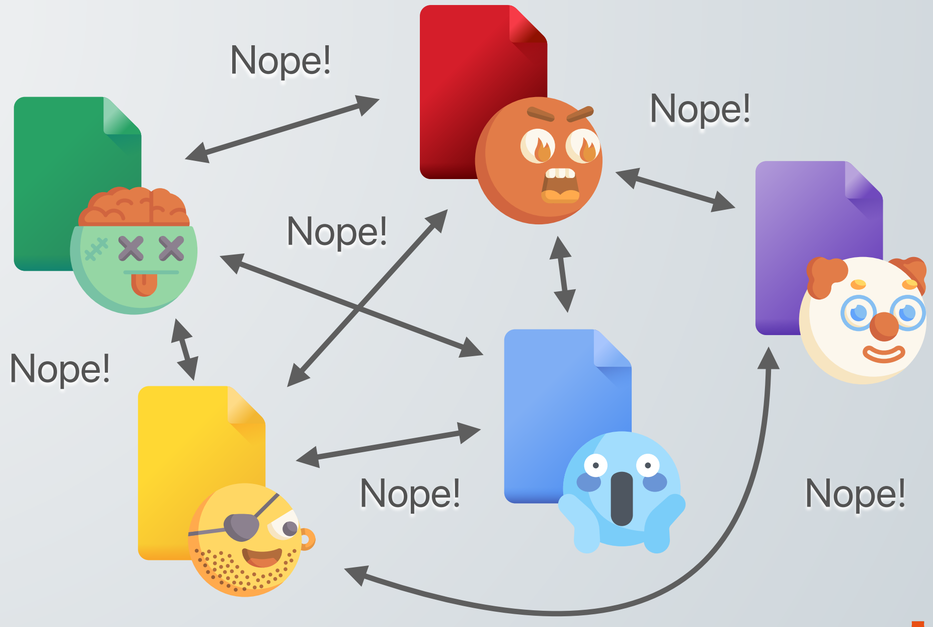
Resistenza alle collisioni

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 $h(x) = h(y)$.



Una semplice funzione di hashing

Una semplice funzione di hashing

Creiamo una funzione $h(x)$ che prende in input n bit e restituisce un *digest* lungo 5.

Una semplice funzione di hashing

Creiamo una funzione $h(x)$ che prende in input n bit e restituisce un *digest* lungo 5.

Input: `1011101001010 11`

Una semplice funzione di hashing

Creiamo una funzione $h(x)$ che prende in input n bit e restituisce un *digest* lungo 5.

Input: `1011101001010 11`

```
10111 ⊕
01001 ⊕
01011 =
```

Una semplice funzione di hashing

Creiamo una funzione $h(x)$ che prende in input n bit e restituisce un *digest* lungo 5.

Input: `101110100101011`

```
10111 ⊕
01001 ⊕
01011 =
-------
10101
```

Output: `10101`

Questa funzione prende il nome di *controllo di ridondanza longitudinale*.

Back in the days: MD5

Anno: 1991

Back in the days: MD5

Anno: 1991

Autore: Ron Rivest

Back in the days: MD5

Anno: 1991

Autore: Ron Rivest

Input:

Back in the days: MD5

Anno: 1991

Autore: Ron Rivest

Input: di qualunque lunghezza, ovviamente.

Back in the days: MD5

Anno: 1991

Autore: Ron Rivest

Input: di qualunque lunghezza, ovviamente.

Output: 128 bit

Back in the days: MD5

Anno: 1991

Autore: Ron Rivest

Input: di qualunque lunghezza, ovviamente.

Output: 128 bit

OpenSSL: `openssl dgst -md5 filename`

Back in the days: MD5

Anno: 1991

Autore: Ron Rivest

Input: di qualunque lunghezza, ovviamente.

Output: 128 bit

OpenSSL: `openssl dgst -md5 filename`

php: `md5($string)`

`md5_file($filename)`

PLEASE DON'T DO THAT

MD5 è deprecato per qualunque funzione di sicurezza.

PLEASE DON'T DO THAT

MD5 è deprecato per qualunque funzione di sicurezza.

```php
<?php
  $notSoSecureDigest = md5("monkey");
  $suchStringMuchSecurity = md5(md5("monkey"));
  $pleaseKillMeNow =
  md5(md5(md5(md5(md5(md5(md5(md5(md5(md5(md5("monkey"))))))))))));
?>
```

Secure Hash Algorithm

Secure Hash Algorithm

SHA è una famiglia di algoritmi.

SHA-1 **SHA-2** **SHA-3**

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

SHA-3

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
- ...

shattered.it

SHA-2

SHA-3

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
- ...

shattered.it

SHA-2

(2001)

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

SHA-3

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
- ...

shattered.it

SHA-2

(2001)

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

```
openssl dgst -sha256 filename
```

SHA-3

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
- ...

shattered.it

SHA-2

(2001)

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

```
openssl dgst -sha256 filename
```

SHA-3

(2015)

- algoritmo Keccak

(Si pronuncia kɛtʃæk,
un po' come ketchup,
ma con la k finale)

3

I certificati digitali

Certificare la chiave pubblica

Certificare la chiave pubblica

Certificare la chiave pubblica

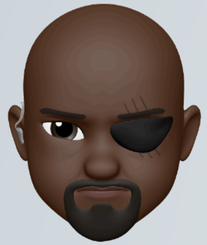
Certificare la chiave pubblica

Certificare la chiave pubblica

Certificare la chiave pubblica

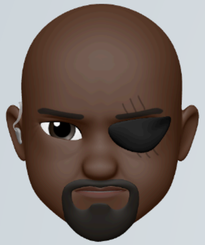
Public Key Infrastructure

Public Key Infrastructure



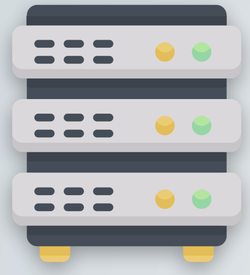
Subject

Public Key Infrastructure



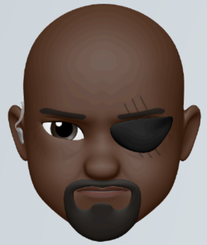
Subject

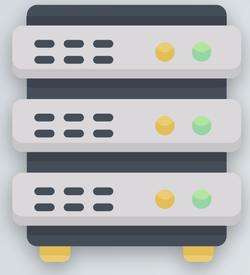
Web Server
`avengers.com`



Public Key Infrastructure

Web Server
avengers.com

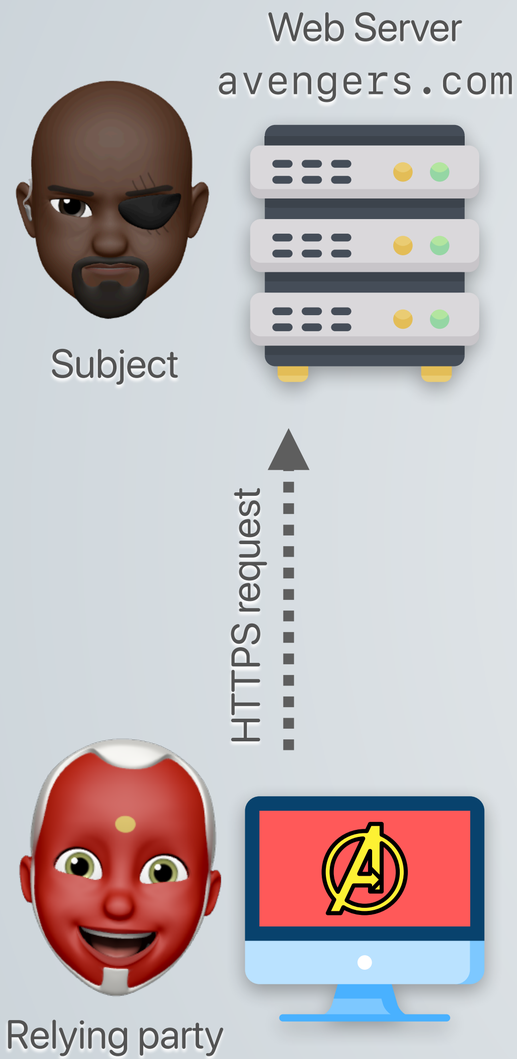




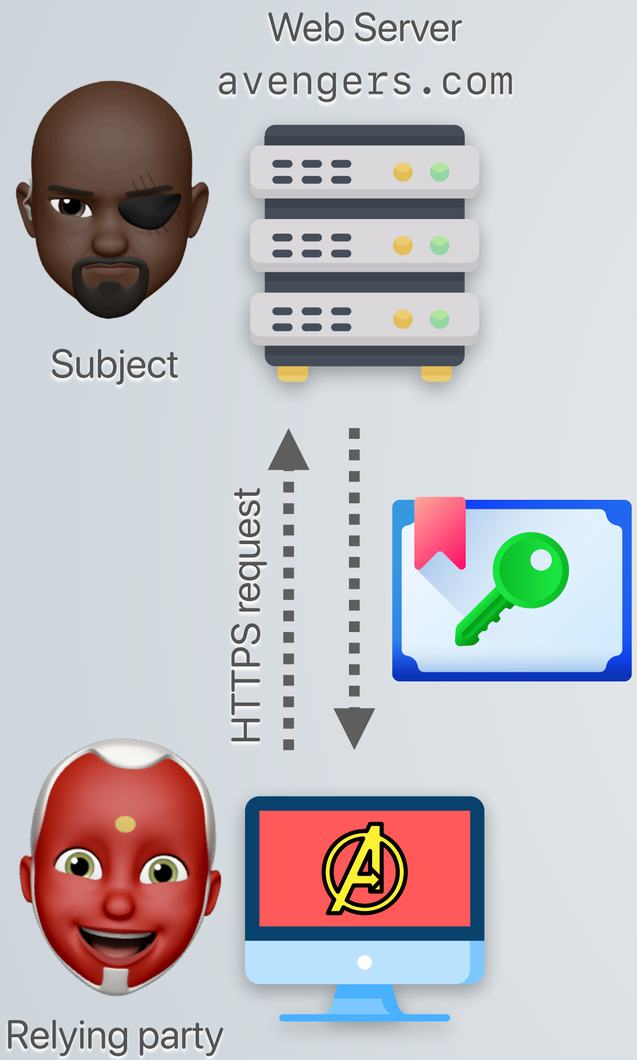
Subject

Relying party

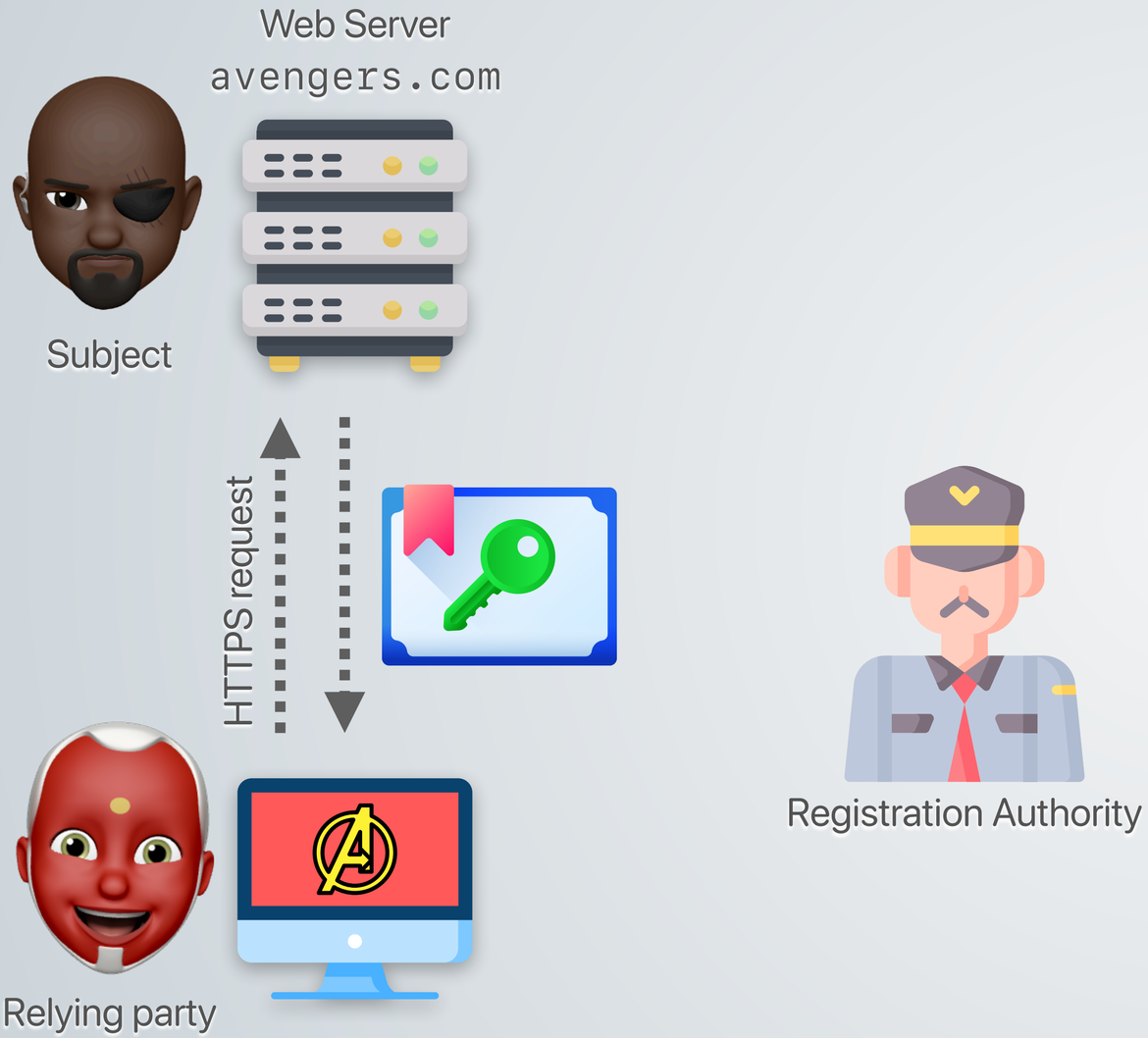
Public Key Infrastructure



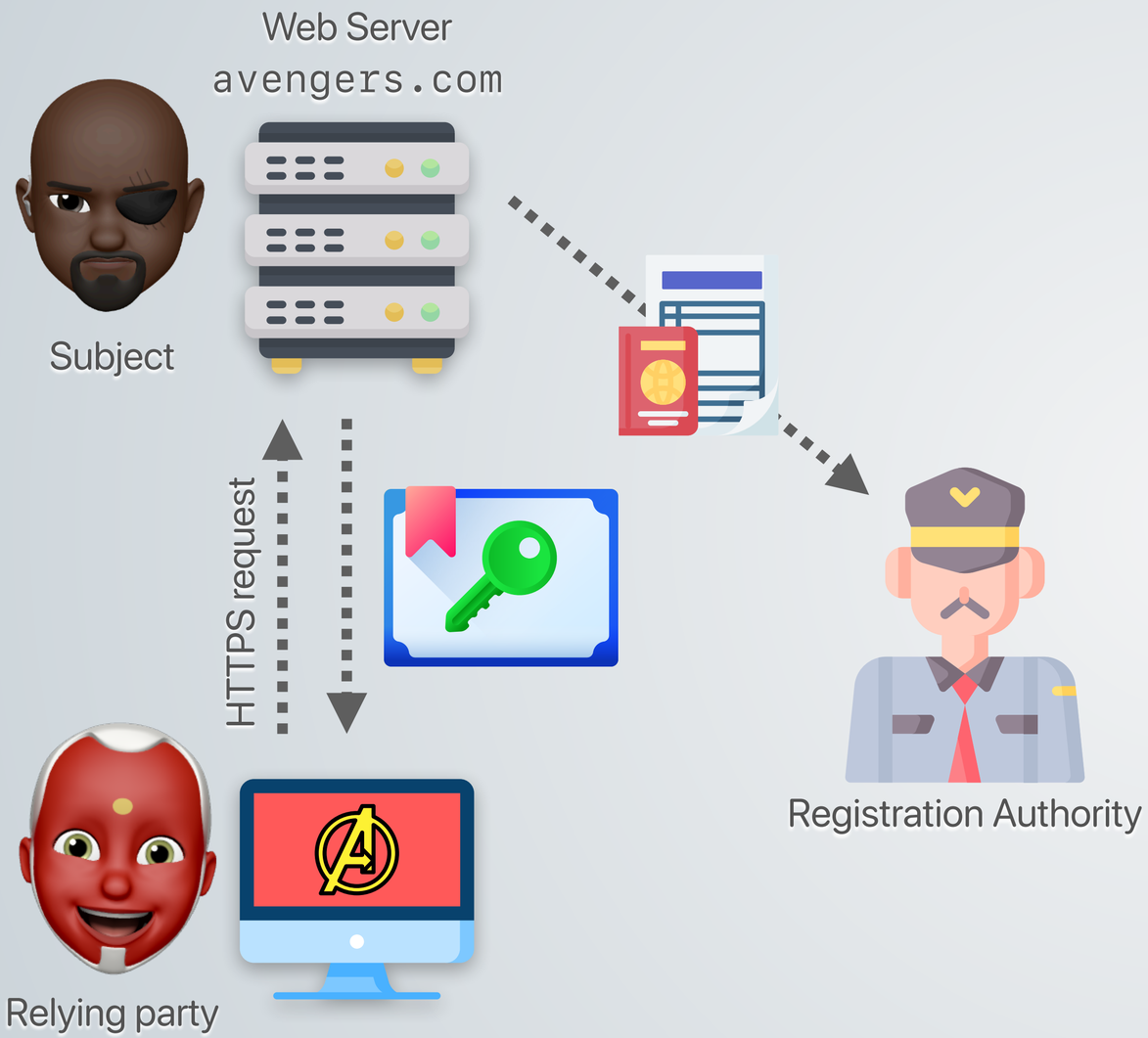
Public Key Infrastructure



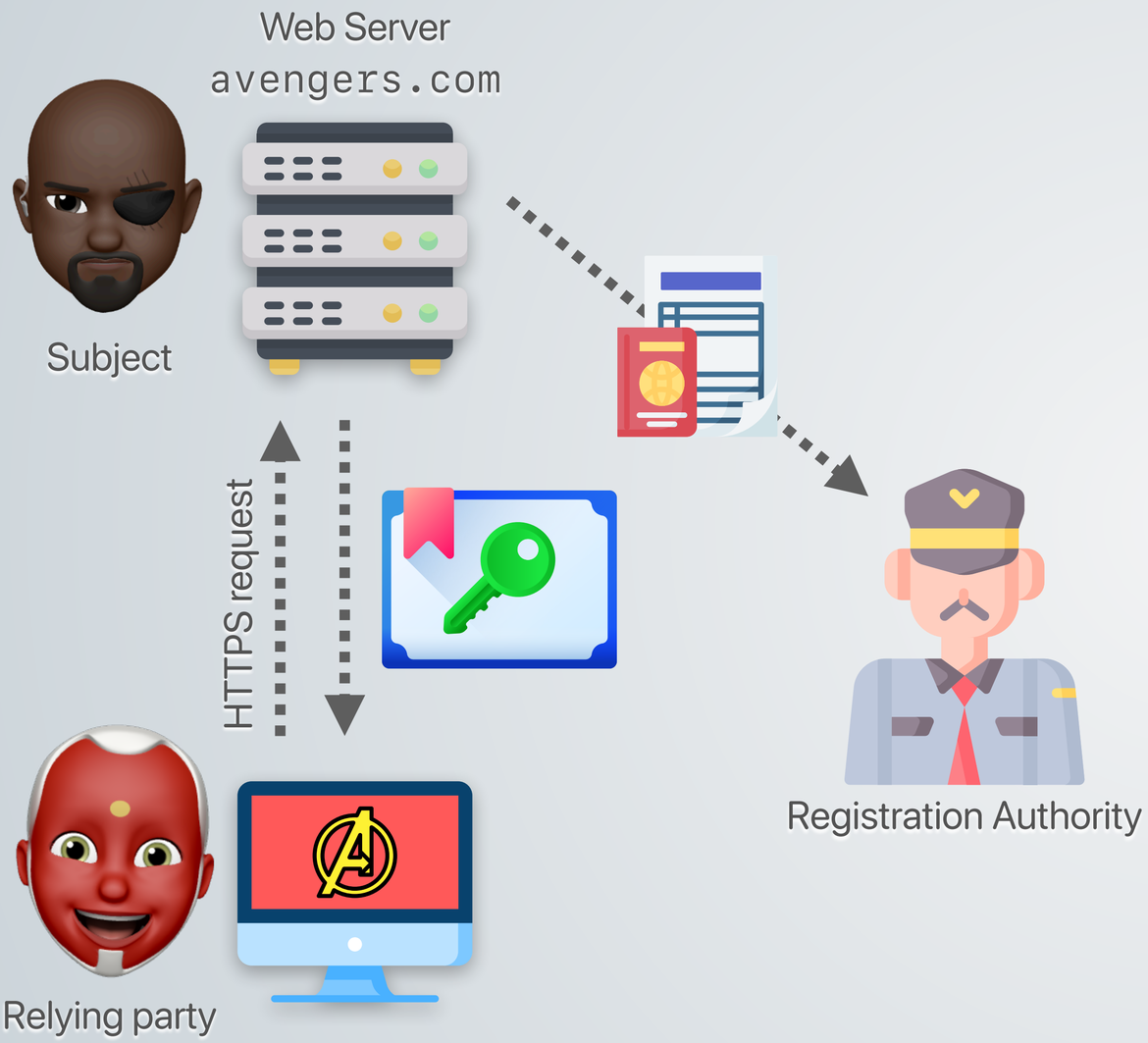
Public Key Infrastructure



Public Key Infrastructure

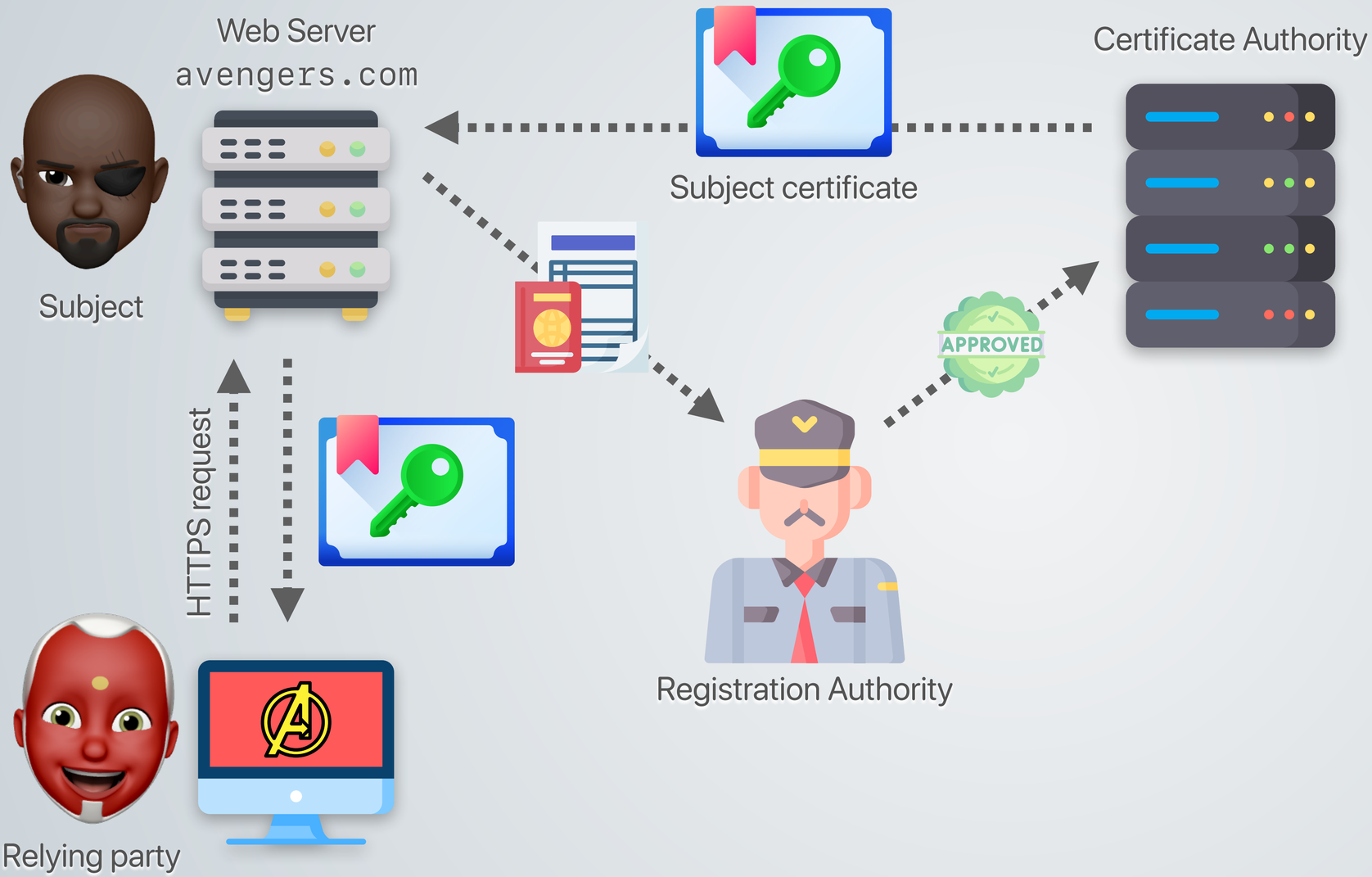


Public Key Infrastructure

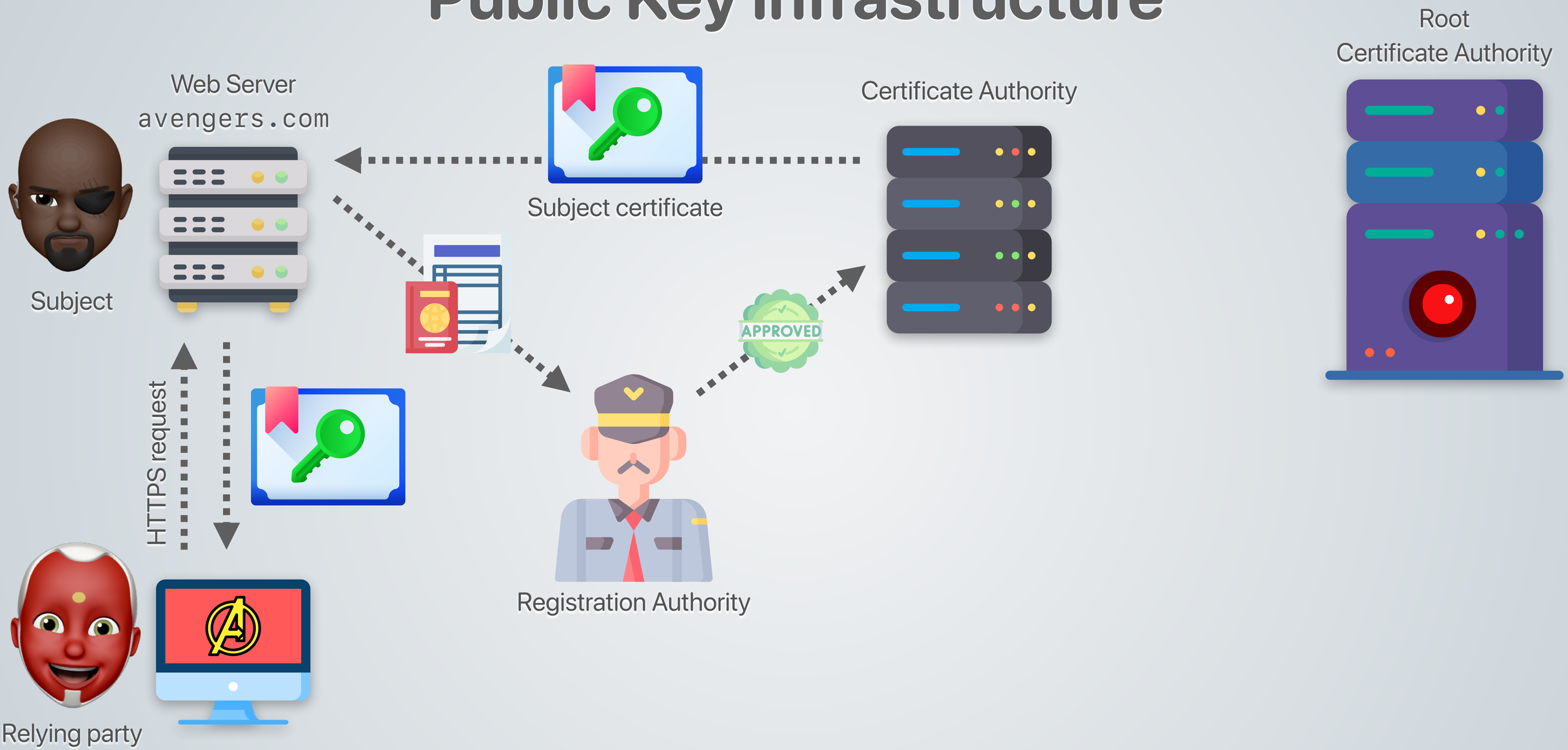


Public Key Infrastructure

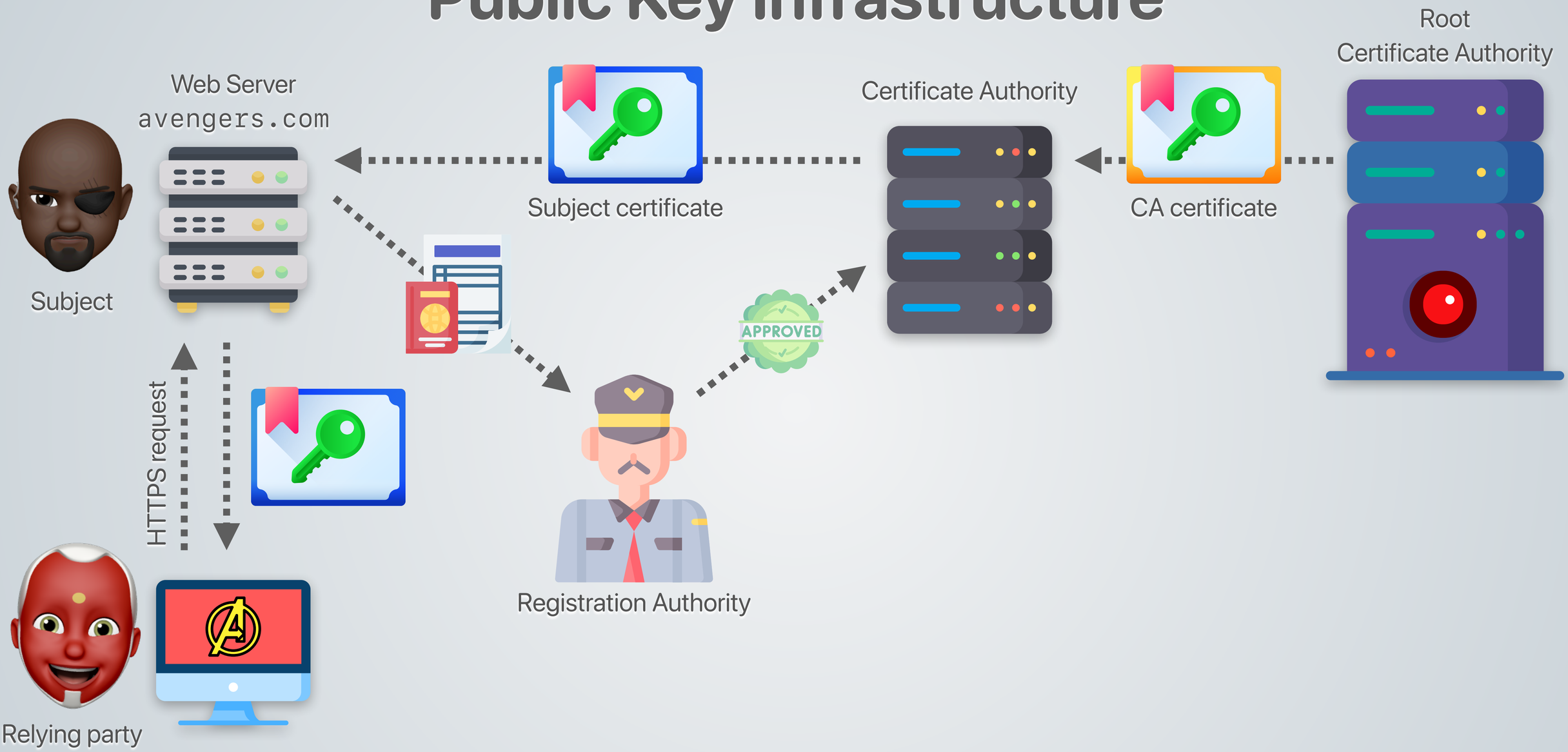
Public Key Infrastructure



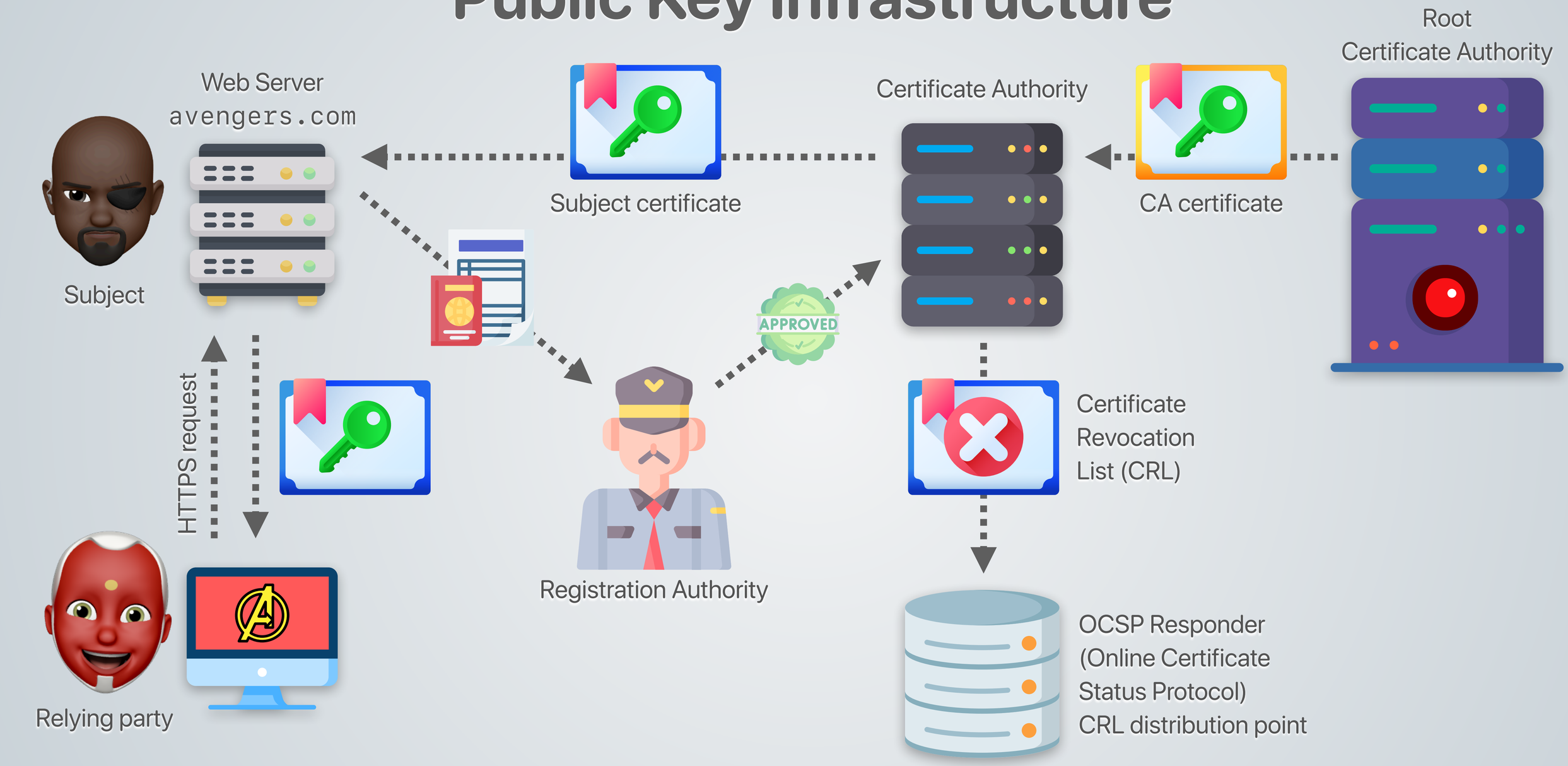
Public Key Infrastructure



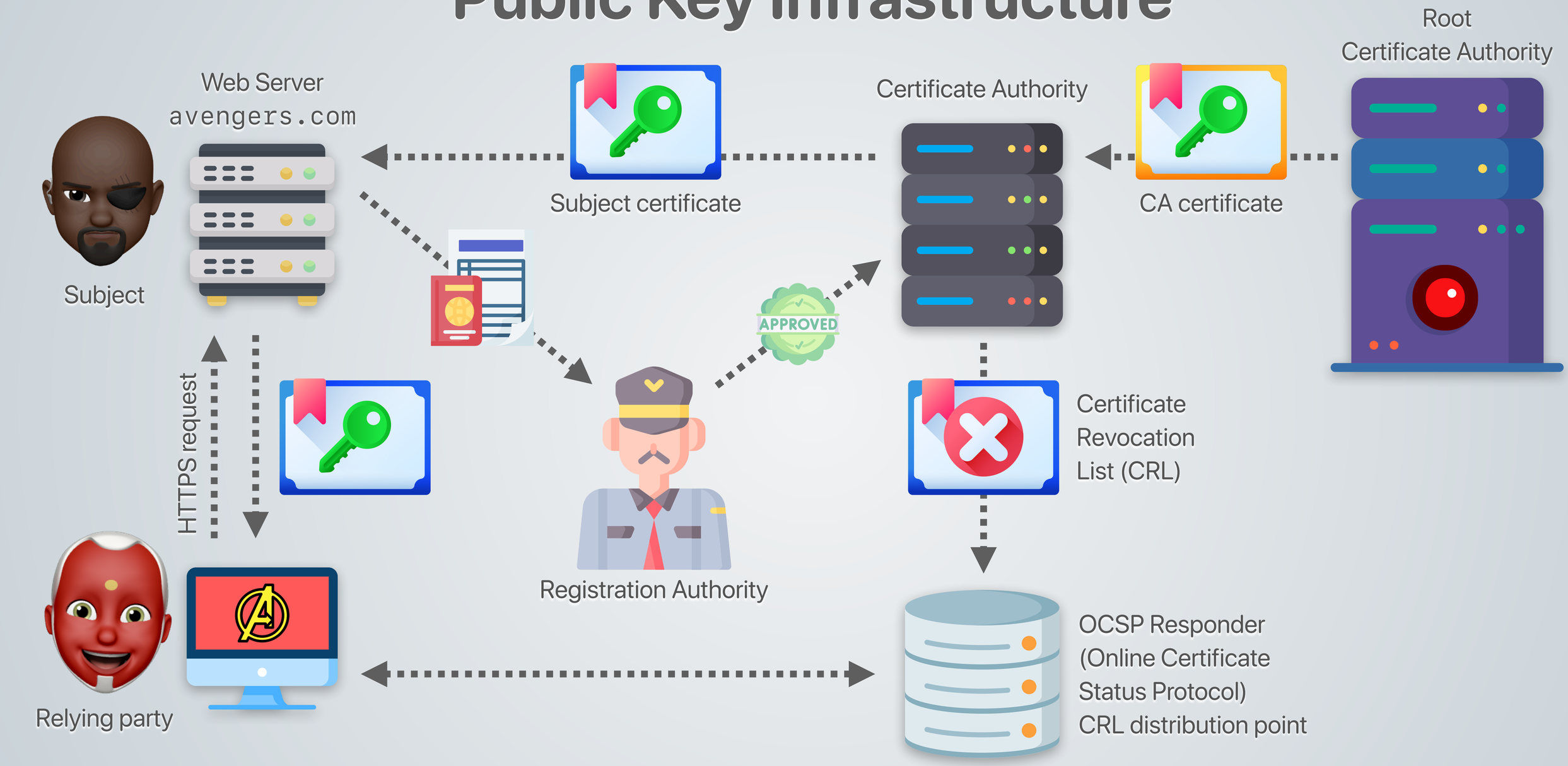
Public Key Infrastructure



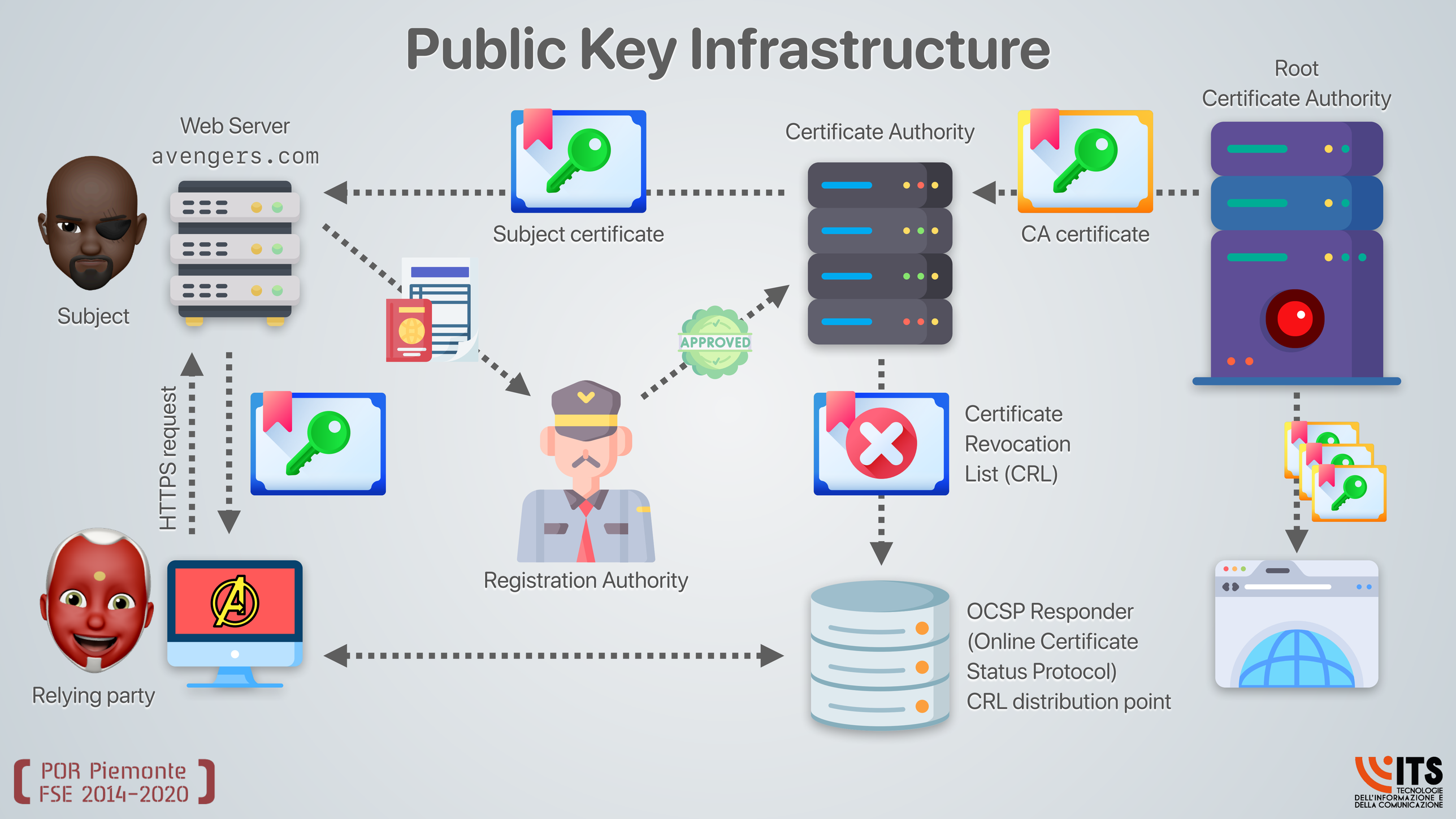
Public Key Infrastructure



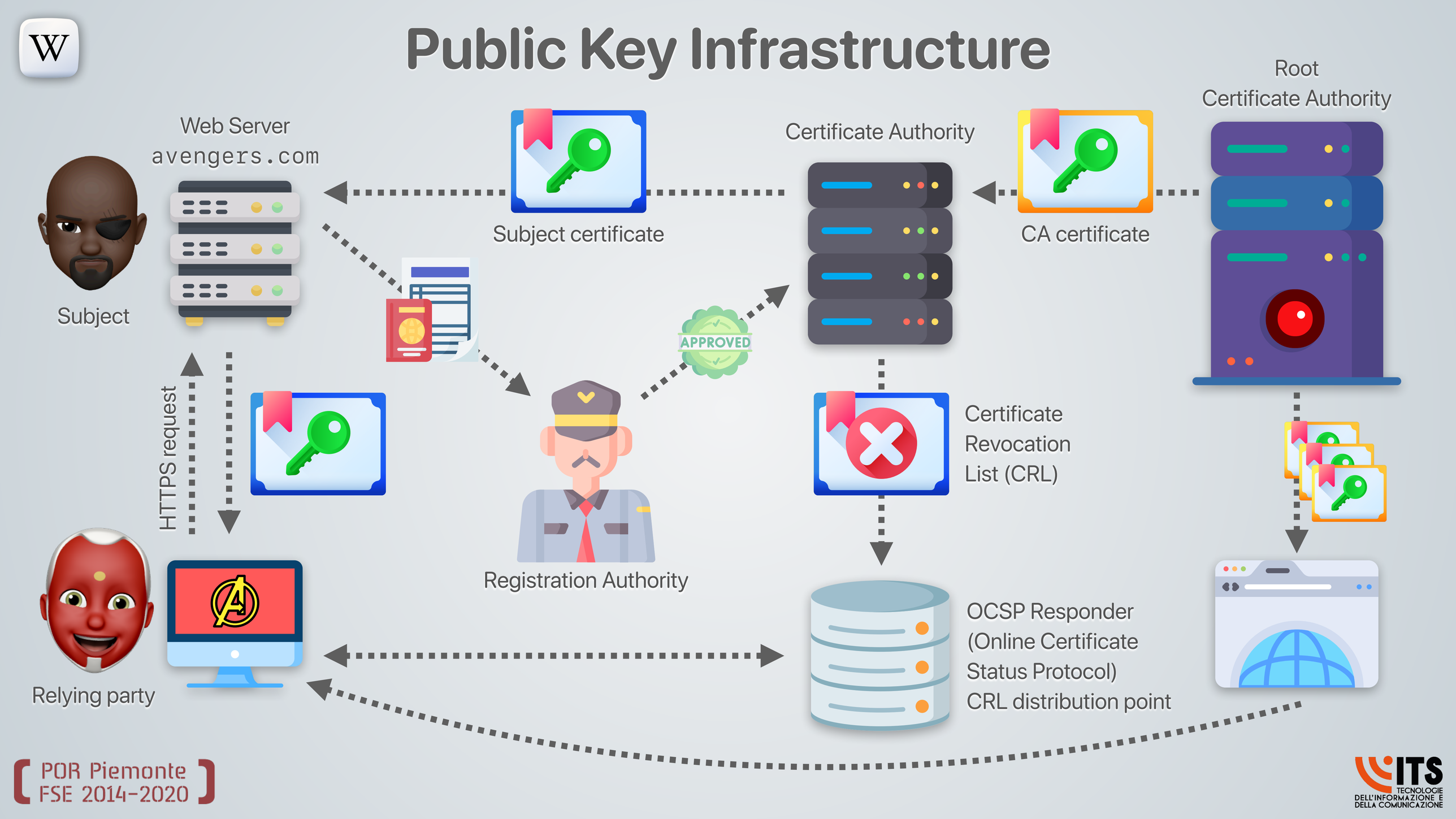
Public Key Infrastructure



Public Key Infrastructure



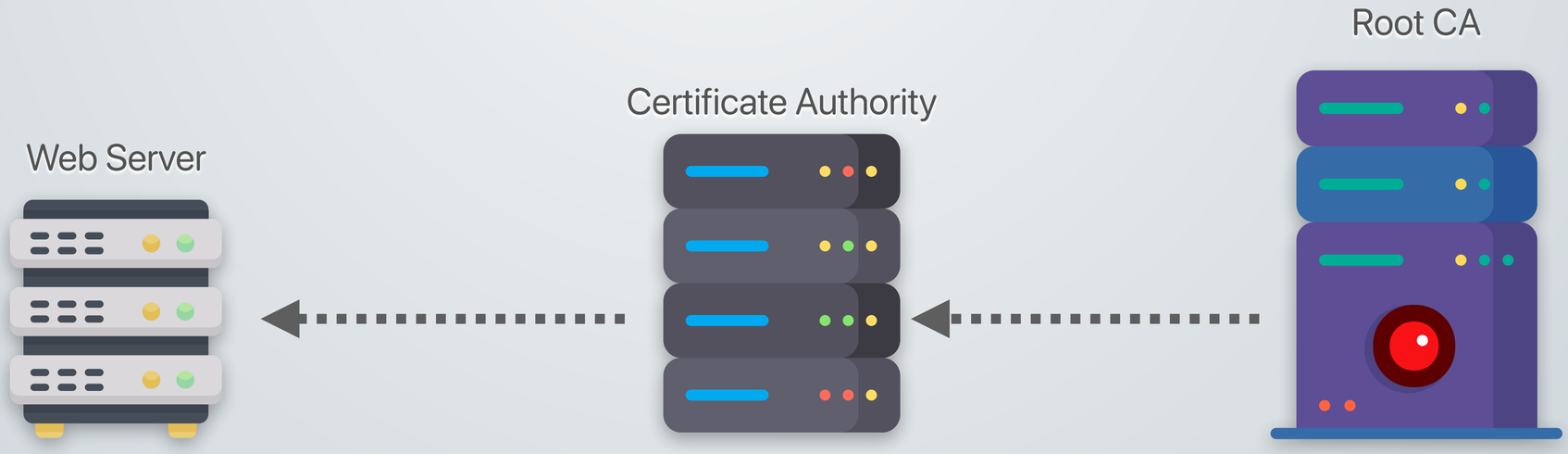
Public Key Infrastructure



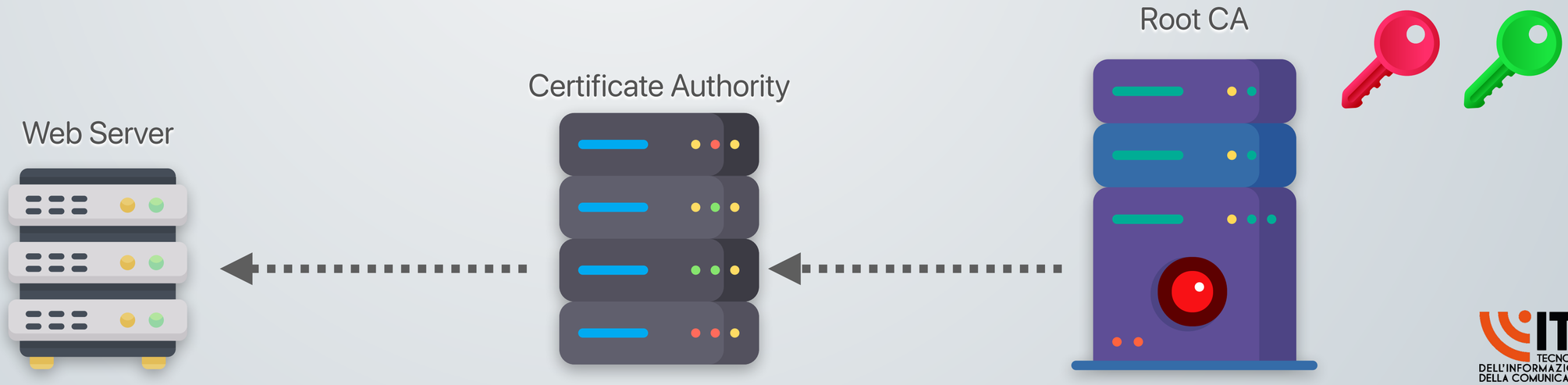
POR Piemonte
FSE 2014-2020

ITS
TECNOLOGIE
DELL'INFORMAZIONE E
DELLA COMUNICAZIONE

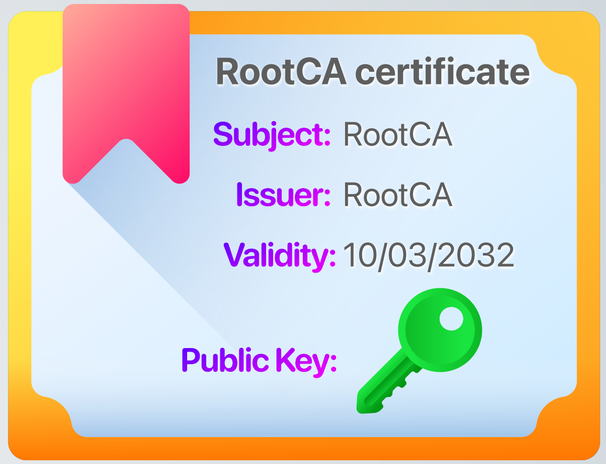
X.509 Certificate issuance

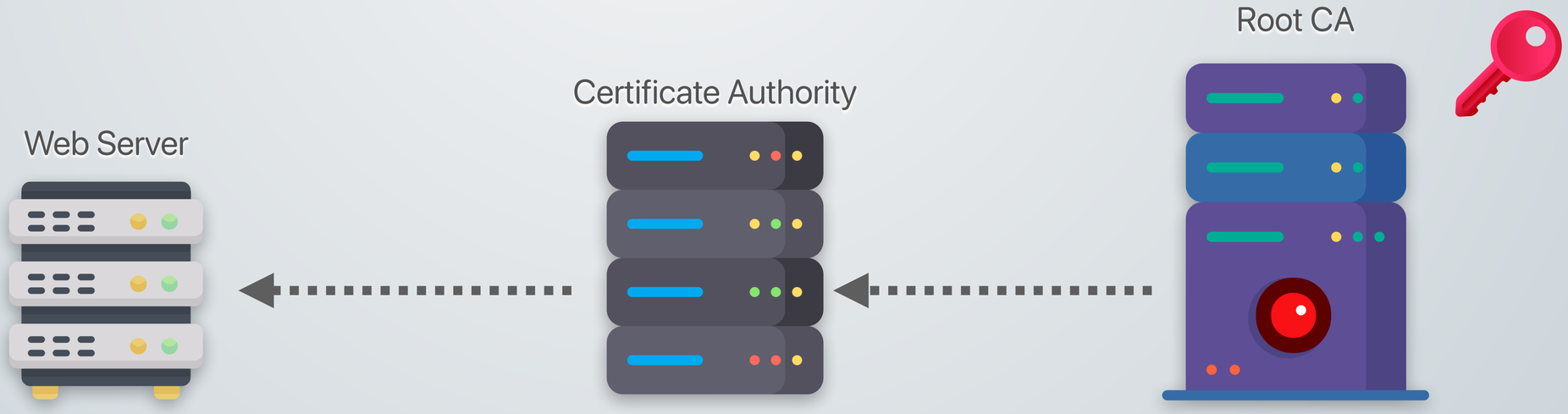


X.509 Certificate issuance

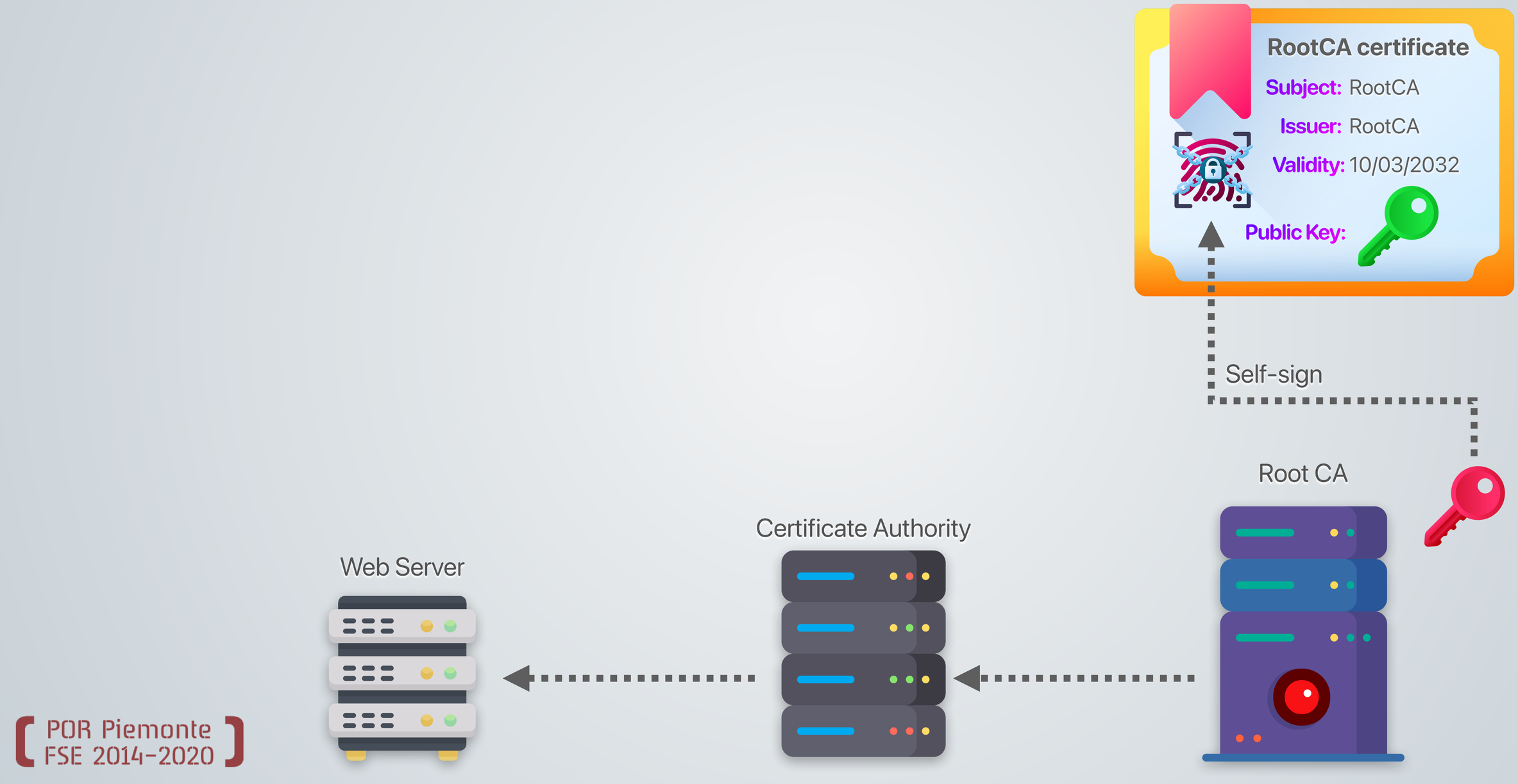


X.509 Certificate issuance

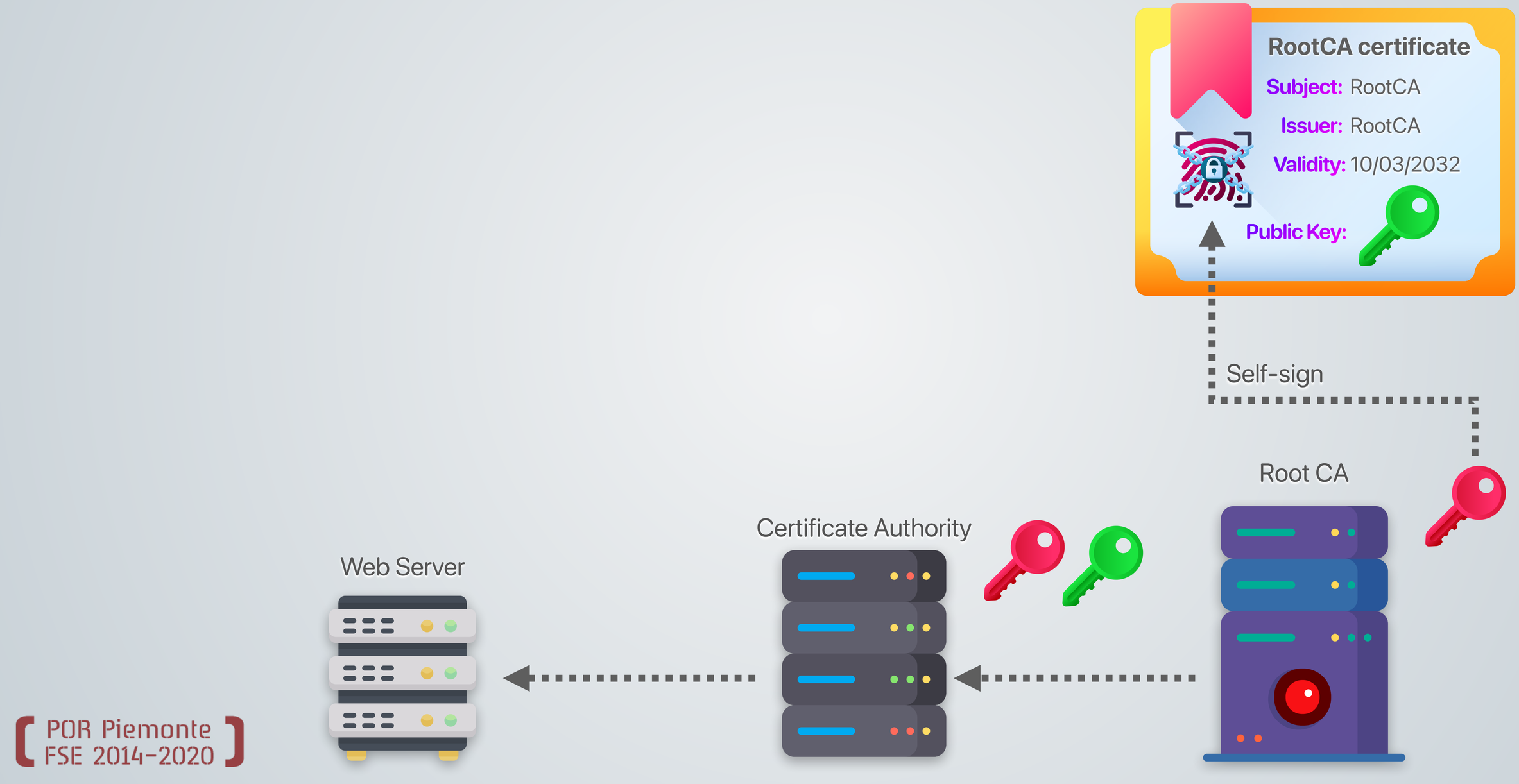




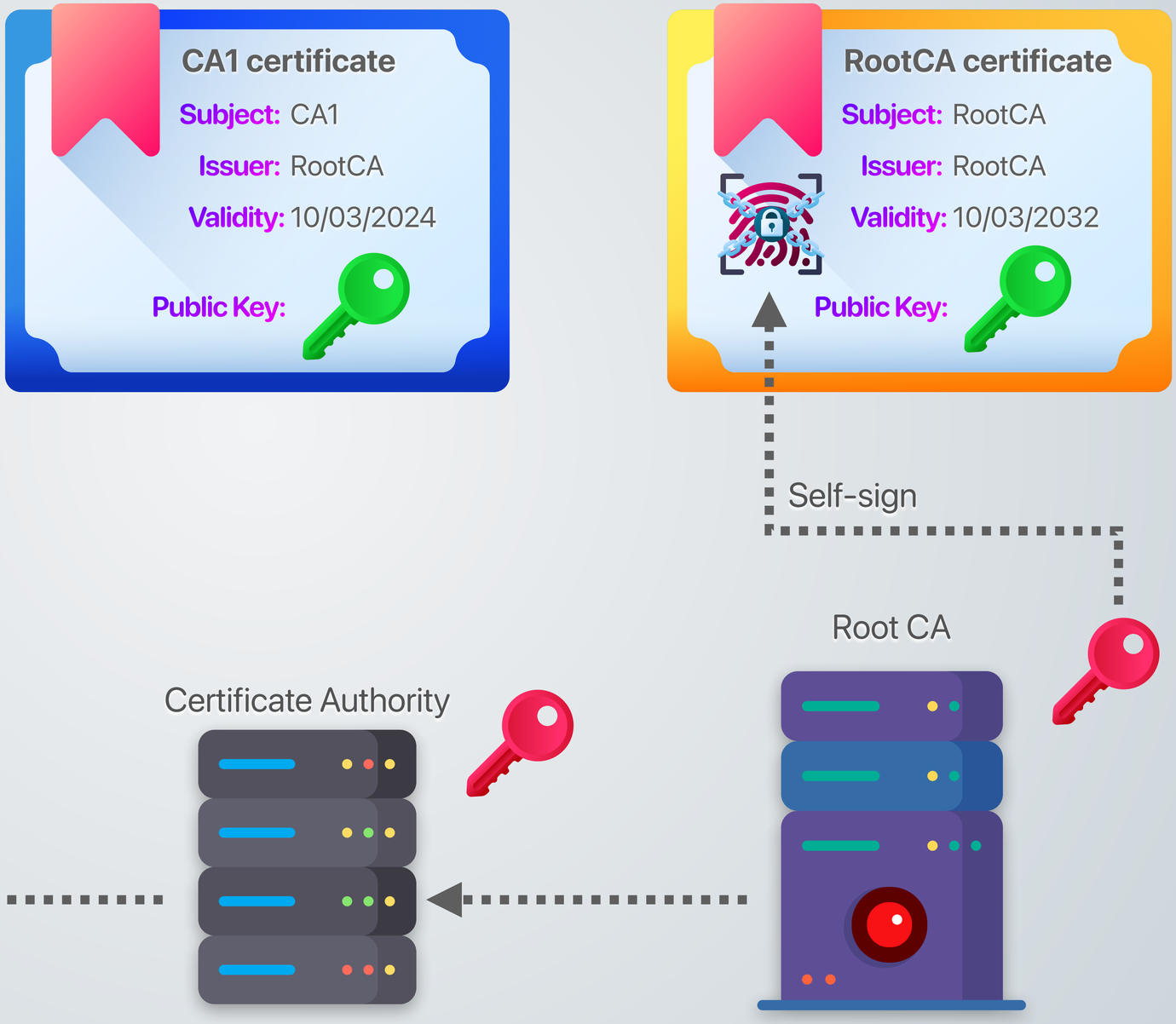
X.509 Certificate issuance



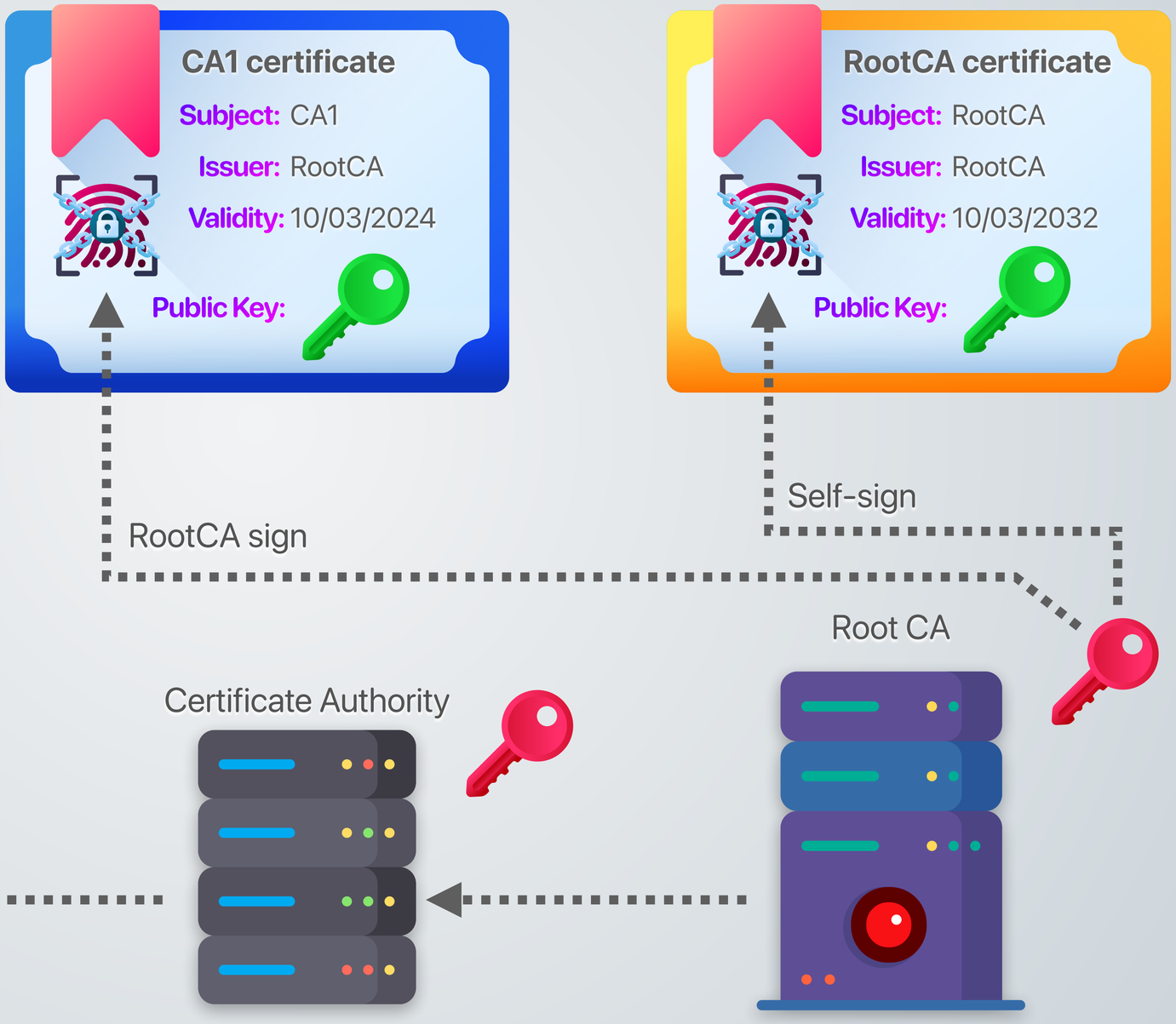
X.509 Certificate issuance



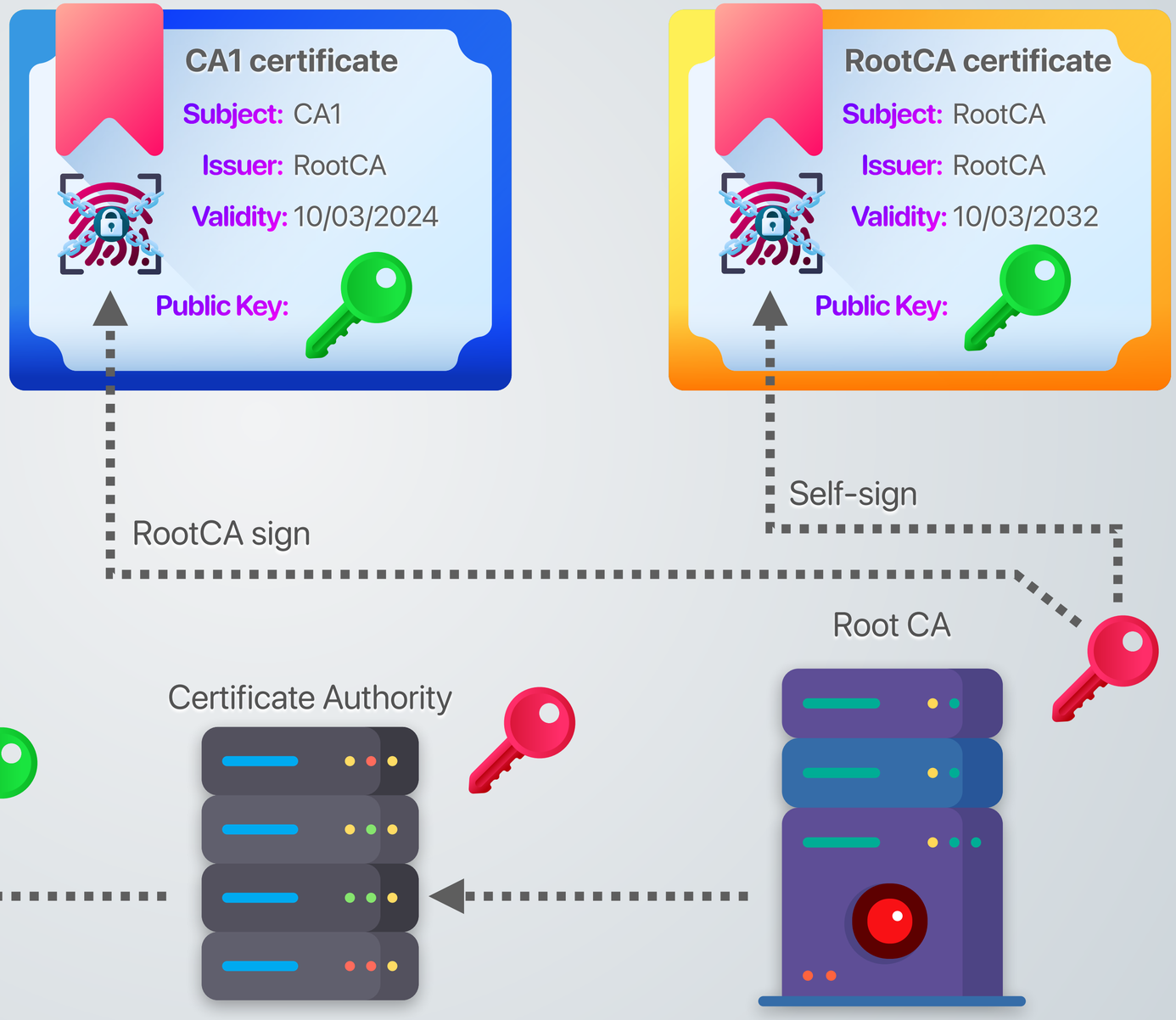
X.509 Certificate issuance



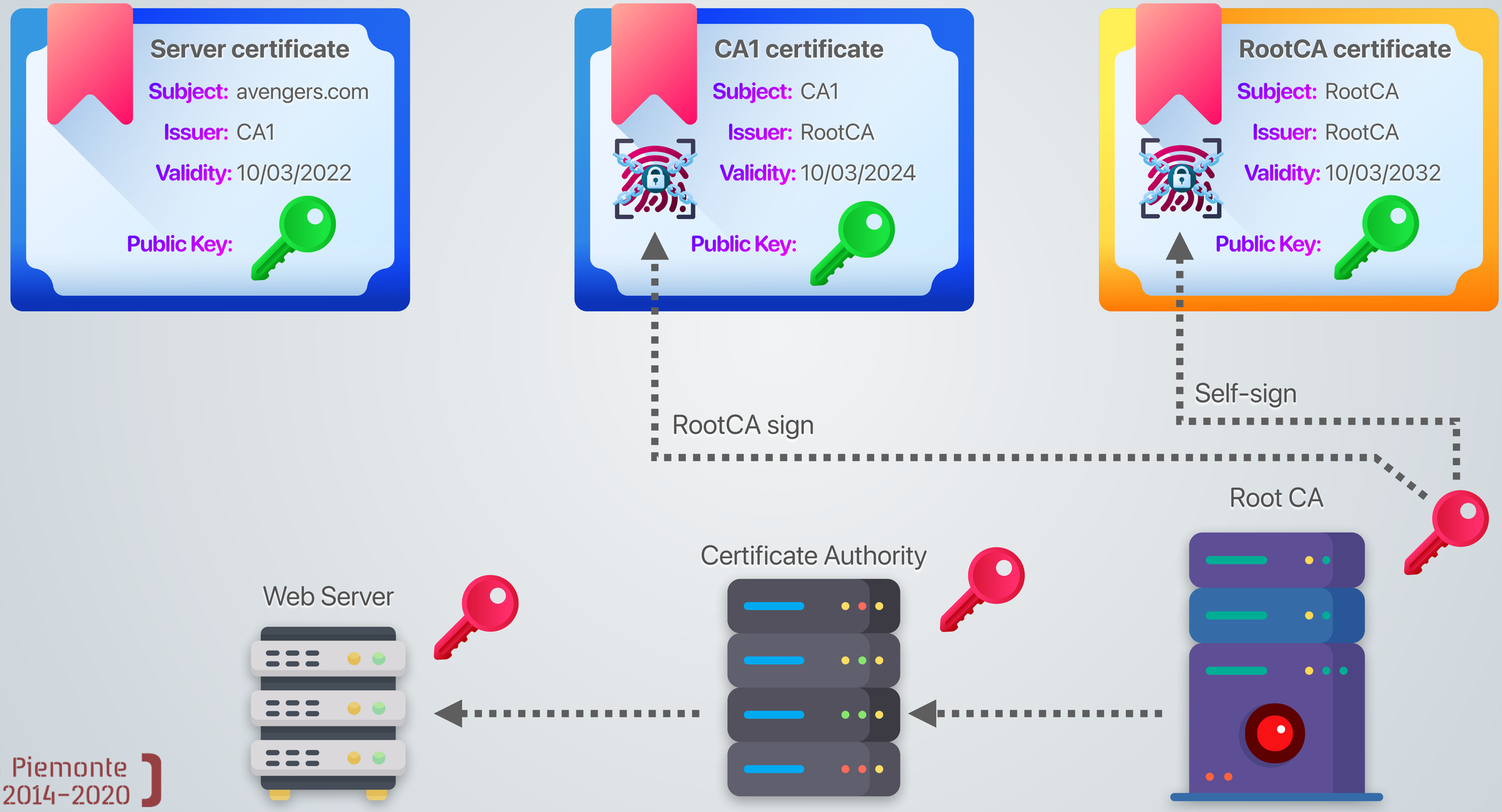
X.509 Certificate issuance



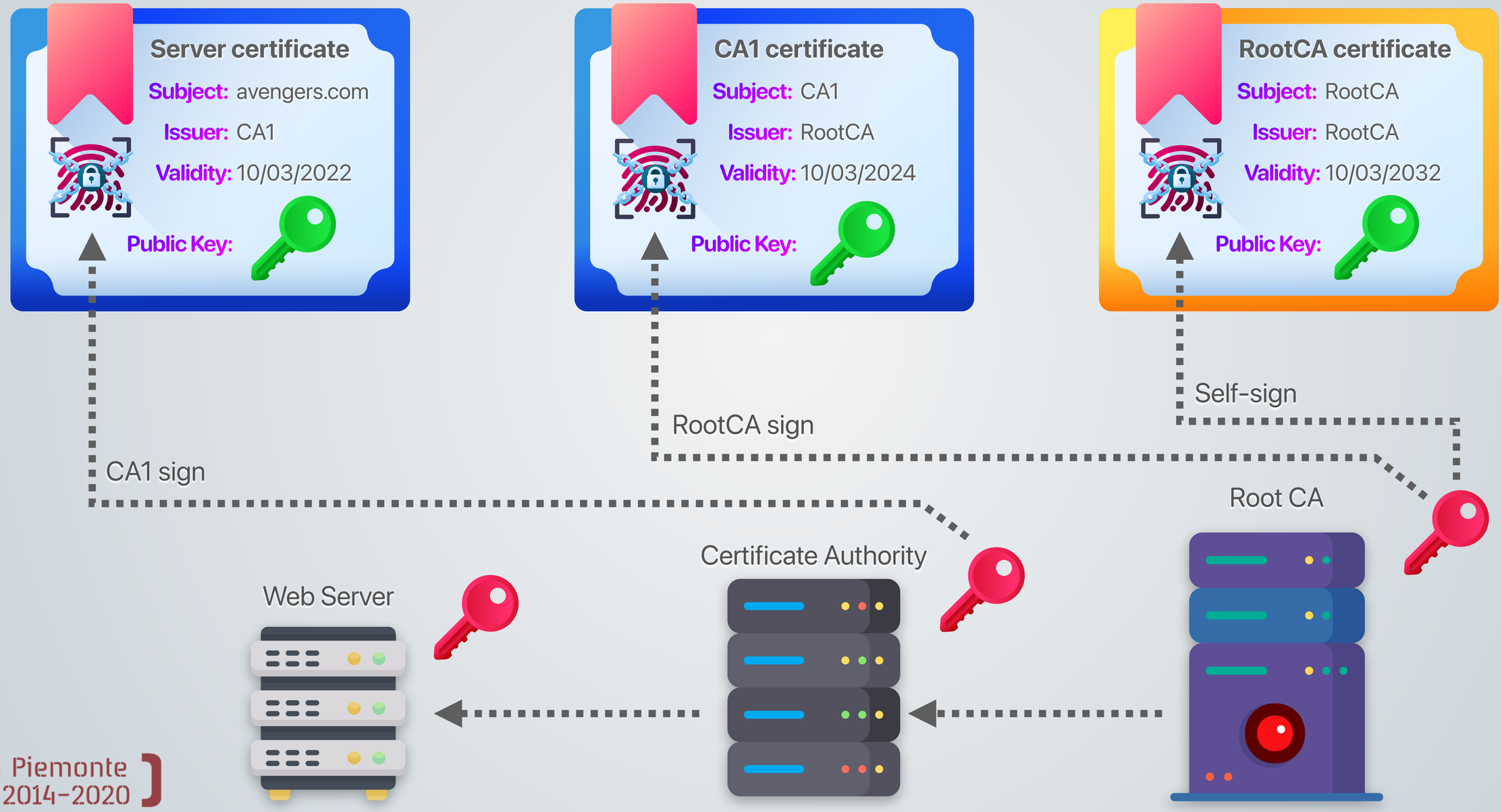
X.509 Certificate issuance



X.509 Certificate issuance



X.509 Certificate issuance



Perché le collisioni sono pericolose?

Perché le collisioni sono pericolose?

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

Perché le collisioni sono pericolose?

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

Certificato Digitale

Subject: avengers.com

Public Key: 3F4AC50A

Signature: 01AB9F5E

CertifiCato digitale

Subject: avengers.com

Public Key: 67CFA2B7

Signature: 7AA52331

Perché le collisioni sono pericolose?

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

Certificato Digitale

Subject: avengers.com

Public Key: 3F4AC50A

Signature: 01AB9F5E

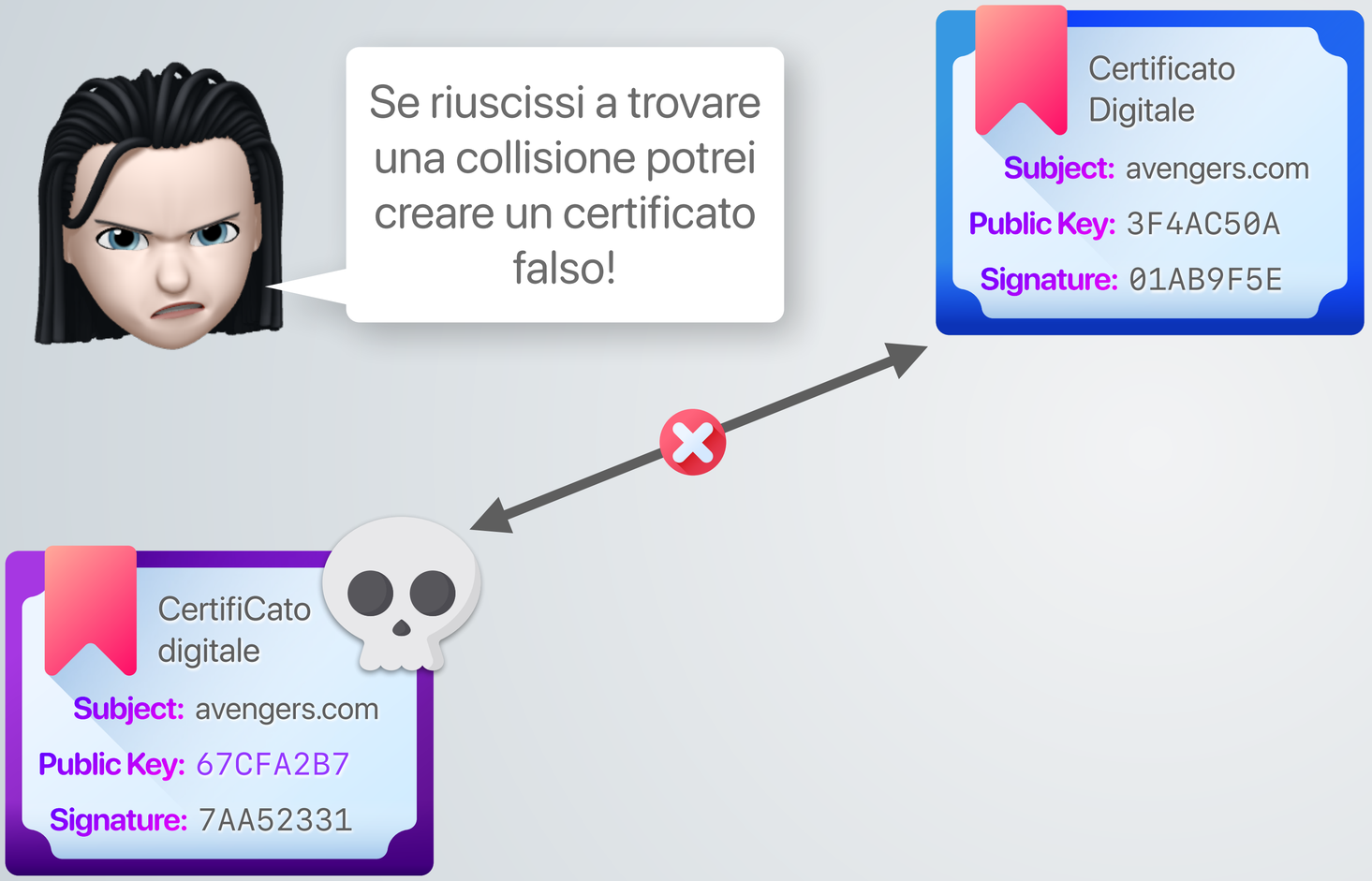
CertifiCato digitale

Subject: avengers.com

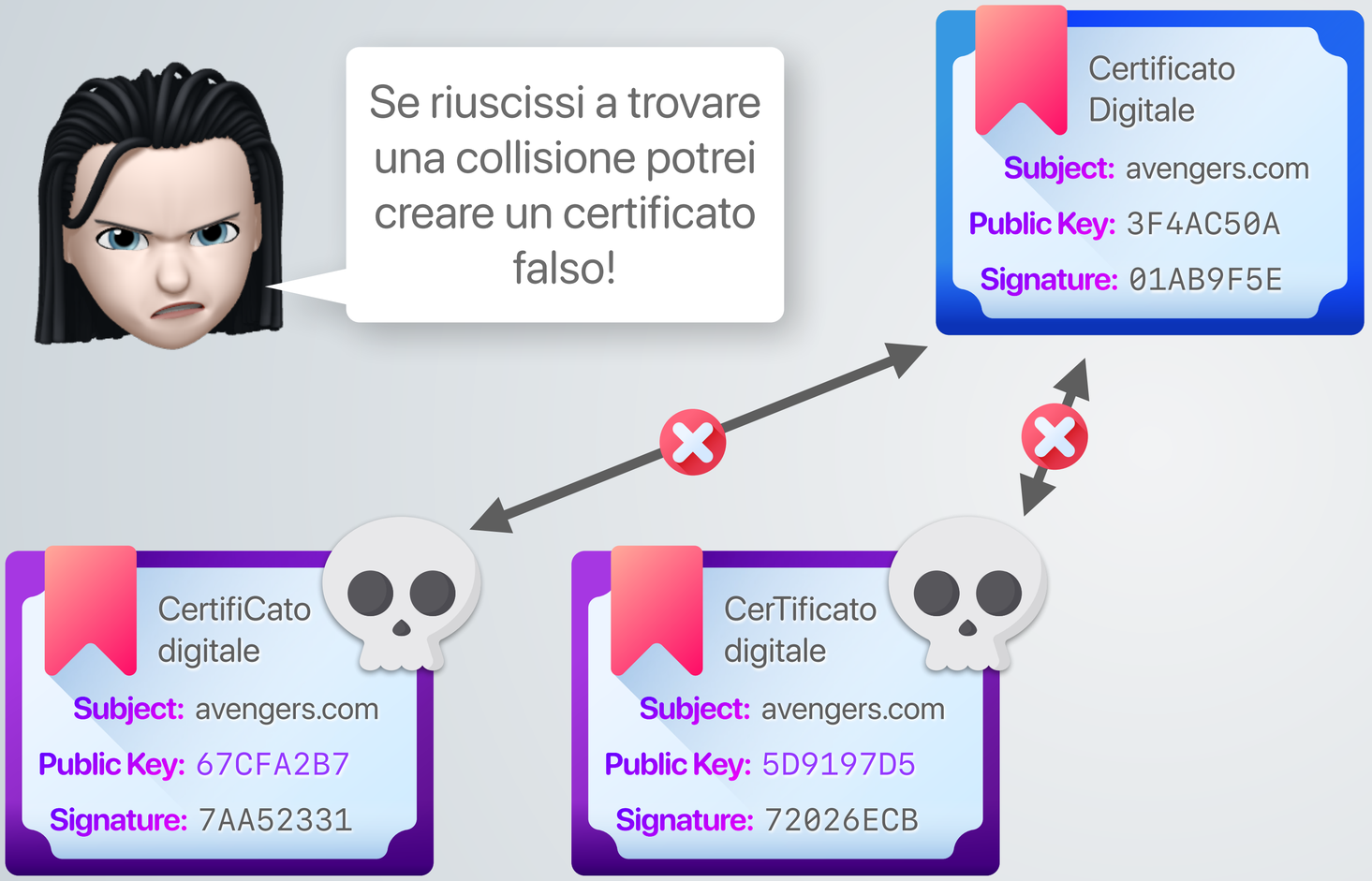
Public Key: 67CFA2B7

Signature: 7AA52331

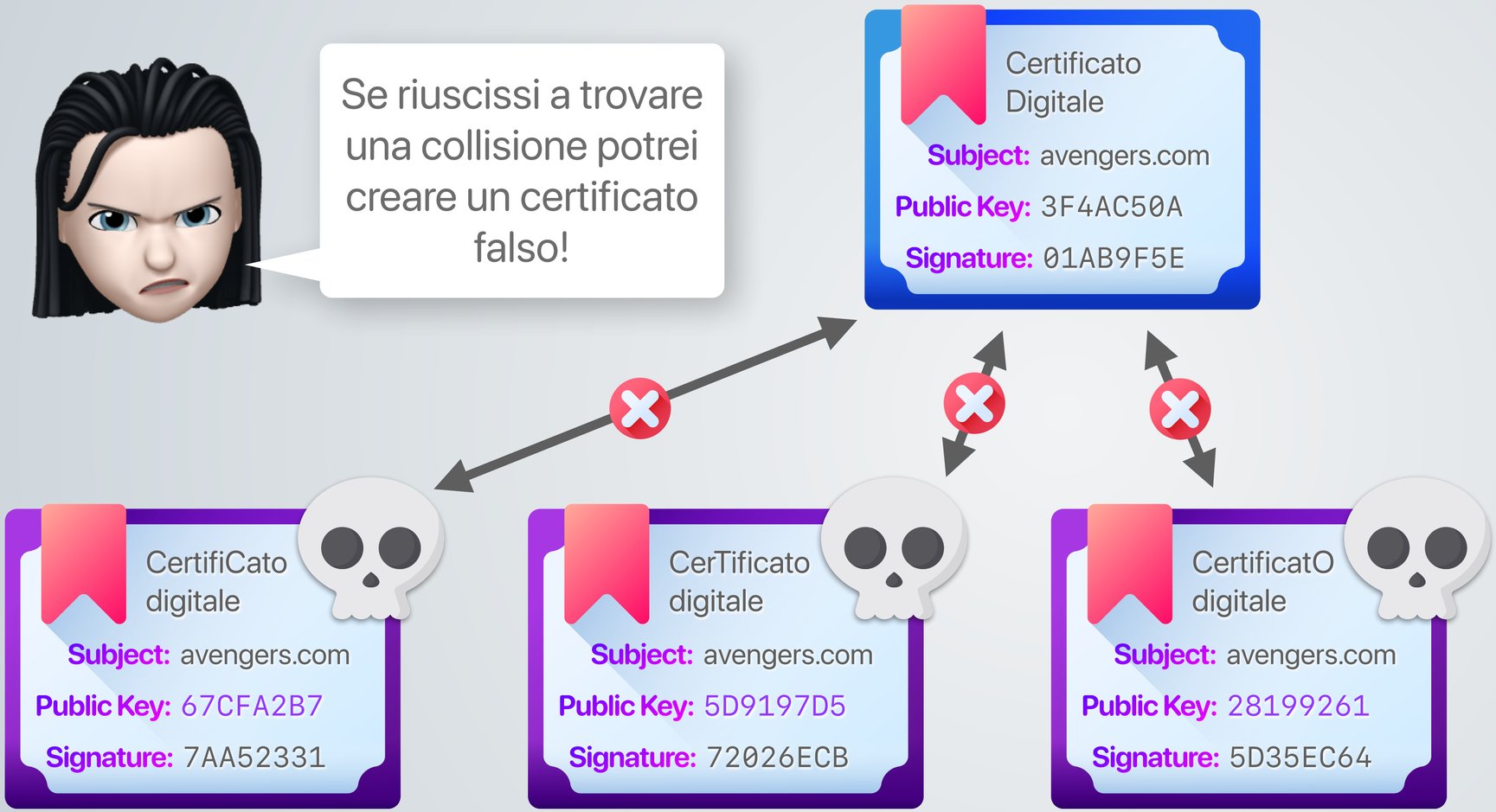
Perché le collisioni sono pericolose?



Perché le collisioni sono pericolose?



Perché le collisioni sono pericolose?



Perché le collisioni sono pericolose?

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

Certificato Digitale
Subject: avengers.com
Public Key: 3F4AC50A
Signature: 01AB9F5E

CertifiCato digitale
Subject: avengers.com
Public Key: 67CFA2B7
Signature: 7AA52331

CerTificato digitale
Subject: avengers.com
Public Key: 5D9197D5
Signature: 72026ECB

CertificatO digitale
Subject: avengers.com
Public Key: 28199261
Signature: 5D35EC64

...

Certificato digitAle
Subject: avengers.com
Public Key: C7AA9930
Signature: 01AB9F5E

Perché le collisioni sono pericolose?

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

Certificato Digitale
Subject: avengers.com
Public Key: 3F4AC50A
Signature: 01AB9F5E

Questo certificato, con una chiave pubblica falsificata, può essere sostituito a quello originale perché ha la stessa firma digitale, data da una collisione!

CertifiCato digitale
Subject: avengers.com
Public Key: 67CFA2B7
Signature: 7AA52331

CerTificato digitale
Subject: avengers.com
Public Key: 5D9197D5
Signature: 72026ECB

CertificatO digitale
Subject: avengers.com
Public Key: 28199261
Signature: 5D35EC64

...

Certificato digitAle
Subject: avengers.com
Public Key: C7AA9930
Signature: 01AB9F5E

L'algoritmo di hash scelto è estremamente importante!

4

HTTPS e TLS

Considerazioni sulla web security

Considerazioni sulla web security

Complessità

I contenuti web sono straordinariamente complessi e possono nascondere problemi di sicurezza.

Considerazioni sulla web security

Complessità

I contenuti web sono straordinariamente complessi e possono nascondere problemi di sicurezza.

Escalation

I server web possono essere exploitati e usati come trampolino verso la rete aziendale interna.

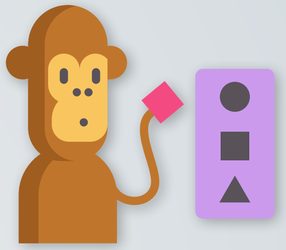
Considerazioni sulla web security

Complessità

I contenuti web sono straordinariamente complessi e possono nascondere problemi di sicurezza.

Escalation

I server web possono essere exploitati e usati come trampolino verso la rete aziendale interna.

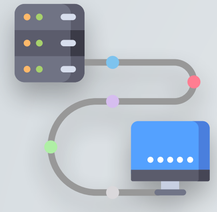


Utonti

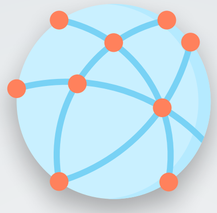
Gli utenti tipici dei servizi web non sono addestrati alle tematiche della security.

Approcci alla web security

Approcci alla web security



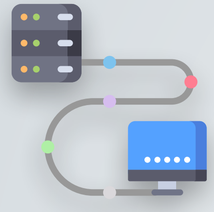
Network



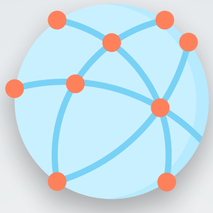
Transport

Application

Approcci alla web security



Network



Transport

Application

HTTP	FTP	SMTP
TCP		
IP/IP Sec		

HTTP	FTP	SMTP
TLS/SSL		
TCP		
IP		

	S/MIME	HTTPS
Kerberos	SMTP	HTTP
UDP	TCP	
IP		

Transport Layer Security

Transport Layer Security

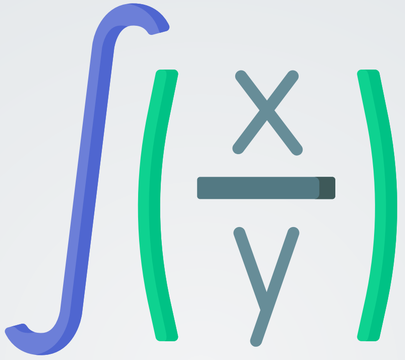
Privacy

Algoritmi crittografici per nascondere il traffico dati.

Transport Layer Security

Privacy

Algoritmi crittografici per nascondere il traffico dati.



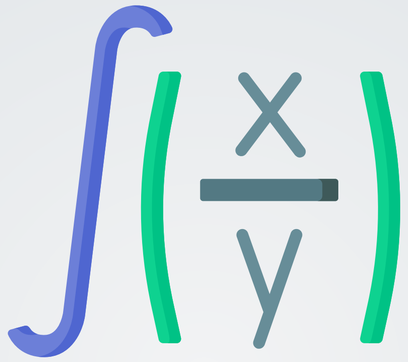
Integrità

I dati non vengono alterati durante il transito in rete.

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.

SSL/TLS

SSL/TLS

Fase 1

Negoziazione fra le parti
degli algoritmi da utilizzare

SSL/TLS

Fase 1

Negoziazione fra le parti
degli algoritmi da utilizzare

Fase 2

Scambio delle chiavi
e autenticazione

SSL/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

SSL/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:

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://

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

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

- l'URL del documento richiesto;
- il contenuto del documento;
- il contenuto dei form riempiti dall'utente;
- i cookie scambiati tra browser e web server;
- il contenuto dell'header HTTP.

Puoi trovare TLS in...

Puoi trovare TLS in...

Web

HTTPS

VPN

e-mail

S/MIME

instant message

Esercizio: S/MIME

https://extrassl.actalis.it/portal/uapub/freemail