

# SIC - Quiz 05- PKI

## Domanda 1

### Domanda 1

Risposta non ancora data

Punteggio max.: 1,00

🚩 [Contrassegna domanda](#)

Si visita un sito web e il browser mostra questo avviso:

`NET::ERR_CERT_DATE_INVALID`

Il certificato per questo sito è scaduto il 15 gennaio 2024.

Qual è il rischio di sicurezza principale se si procede?

Scegli un'alternativa:

- ☐ a. I dati del sito web verranno corrotti durante la trasmissione
- ☐ b. Il proprietario del sito ha dimenticato di rinnovare e non c'è rischio di sicurezza
- ☐ c. Il browser non sarà in grado di cifrare la connessione
- ☒ d. Un attaccante potrebbe presentare un vecchio certificato compromesso per impersonare il sito web

[Annulla la scelta](#)

## Domanda 2

### Domanda 2

Risposta salvata

Punteggio max.: 1,00

🚩 [Rimuovi contrassegno](#)

Un browser moderno esegue diversi controlli quando valida un certificato HTTPS. Quale dei seguenti motivi può causare il fallimento della validazione del certificato? (Selezionare tutti quelli applicabili)

Scegli una o più alternative:

- ☐ a. La chiave pubblica del certificato è di 4096 bit invece di 2048 bit
- ☒ b. La data corrente è successiva alla data "Not After" del certificato
- ☒ c. La catena del certificato è incompleta (mancano certificati intermedi)
- ☐ d. Il certificato include Subject Alternative Names (SAN)
- ☒ e. Il certificato è stato emesso da una Certificate Authority non presente nel trust store del browser
- ☐ f. Il certificato usa SHA-256 invece di SHA-1 per la firma
- ☐ g. Il Common Name (CN) del certificato è `example.com` (senza SAN) ma si sta visitando `www.example.com`

## Domanda 3

### Domanda 3

Risposta non ancora data

Punteggio max.: 1,00

🚩 Contrassegna domanda

Si sta configurando un ambiente di test e si genera un certificato self-signed. Il browser mostra:

`NET::ERR_CERT_AUTHORITY_INVALID`

Perché il browser rifiuta questo certificato?

Scegli un'alternativa:

- ☐ a. I certificati self-signed sono sempre scaduti
- ☐ b. Il certificato non è stato generato con la lunghezza di chiave corretta
- ☒ c. Il certificato non è firmato da una CA presente nel trust store del browser
- ☐ d. I certificati self-signed non possono cifrare correttamente il traffico

[Annulla la scelta](#)

## Domanda 4

### Domanda 4

Risposta salvata

Punteggio max.: 1,00

🚩 Contrassegna domanda

Un certificato per `secure.bank.com` viene presentato quando si visita `www.bank.com`. Il certificato è valido, non scaduto e firmato da una CA fidata.

Cosa dovrebbe accadere?

Scegli un'alternativa:

- ☒ a. Il browser dovrebbe mostrare un avviso perché il nome host non corrisponde al certificato
- ☐ b. Il certificato è valido finché il dominio base corrisponde
- ☐ c. La connessione dovrebbe procedere normalmente poiché il certificato è dello stesso dominio
- ☐ d. Il browser dovrebbe verificare se entrambi i domini risolvono allo stesso indirizzo IP

## Domanda 5

### Domanda 5

Risposta non ancora data

Punteggio max.: 1,00

🚩 [Contrassegna domanda](#)

Qual è lo scopo dei certificati intermedi in una catena di certificati?

Scegli un'alternativa:

- ☒ a. Creano una catena di fiducia tra il certificato end-entity e la CA root
- ☐ b. Forniscono certificati di backup se il certificato principale fallisce
- ☐ c. Cifrano la connessione con livelli aggiuntivi di sicurezza
- ☐ d. Memorizzano informazioni di revoca per il certificato end-entity

[Annulla la scelta](#)

## Domanda 6

### Domanda 6

Risposta non ancora data

Punteggio max.: 1,00

🚩 [Contrassegna domanda](#)

Un certificato è stato compromesso e revocato dalla CA. Quali meccanismi può usare un browser per verificare se un certificato è stato revocato? (Selezionare tutti quelli applicabili)

Scegli una o più alternative:


- ☐ a. Confronto dell'impronta digitale del certificato con una blockchain
- ☒ b. Online Certificate Status Protocol (OCSP) - interroga la CA sullo stato del certificato
- ☒ c. Certificate Revocation List (CRL) - scarica un elenco di certificati revocati
- ☐ d. Ricerca DNS del numero di serie del certificato

## Domanda 7

**Domanda 7**

Risposta salvata

Punteggio max.: 1,00

 **Contrassegna domanda**

Si ha un certificato wildcard per `*.example.com`. Quale di questi domini sono coperti dal certificato?

Scegli un'alternativa:

- ☐ a. `example.com`, `example.org`, `example.net`
- ☒ b. `www.example.com`, `mail.example.com`, `api.example.com`
- ☐ c. Tutti i sottodomini nel formato `a.b.example.com`
- ☐ d. `example.com`, `www.example.com`, `sub.www.example.com`

[Annulla la scelta](#)

## Domanda 8

**Domanda 8**

Risposta non ancora data

Punteggio max.: 1,00

 **Rimuovi contrassegno**

Un web server presenta il suo certificato end-entity ma non include il certificato CA intermedio. La CA root è presente nel trust store del browser.

Cosa accade tipicamente?

Scegli un'alternativa:

- ☒ a. Il browser mostrerà un errore del certificato se non può costruire la trust chain (sebbene alcuni browser possano tentare di recuperare l'intermedio mancante)
- ☐ b. La connessione avrà successo perché la CA root è fidata
- ☐ c. Il browser scaricherà automaticamente il certificato intermedio mancante
- ☐ d. Il browser userà OCSP per recuperare il certificato mancante

[Annulla la scelta](#)

## Domanda 9

**Domanda 9**

Risposta non ancora data

Punteggio max.: 1,00

🚩 **Contrassegna domanda**

I certificati moderni usano Subject Alternative Names (SAN). Qual è il vantaggio di SAN rispetto all'uso del solo Common Name (CN)?

**Scegli un'alternativa:**

- ☐ a. SAN fornisce una cifratura più forte di CN
- ☐ b. SAN elimina la necessità di revoca del certificato
- ☒ c. SAN può specificare più nomi di dominio in un singolo certificato
- ☐ d. SAN permette al certificato di non scadere mai

[Annulla la scelta](#)

## Domanda 10

**Domanda 10**

Risposta non ancora data

Punteggio max.: 1,00

🚩 **Contrassegna domanda**

Si sta implementando HTTPS per `shop.example.com`. I requisiti sono:

- Supportare `shop.example.com` e `www.shop.example.com`
- I browser devono fidarsi del certificato per impostazione predefinita
- Il certificato dovrebbe essere valido per almeno 1 anno
- Deve usare algoritmi crittografici robusti

Cosa si dovrebbe fare? (Selezionare tutti quelli applicabili)

**Scegli una o più alternative:**

- ☒ a. Ottenere un certificato da una Certificate Authority pubblicamente fidata
- ☒ b. Includere sia `shop.example.com` che `www.shop.example.com` nei Subject Alternative Names
- ☐ c. Usare almeno chiavi RSA 2048-bit o ECC 256-bit
- ☐ d. Creare un certificato self-signed e distribuirlo a tutti gli utenti
- ☒ e. Usare un certificato wildcard per `*.example.com`
- ☐ f. Impostare il certificato per essere valido per 50 anni per semplificare il rinnovo

# Domanda 11

## Domanda 11

Risposta non ancora data

Punteggio max.: 1,00

🚩 Contrassegna domanda

Una pagina web caricata via HTTPS include un'immagine caricata via HTTP:

```
https://secure.example.com/page.html include 
```

Quale problema di sicurezza si presenta?

Scegli un'alternativa:

- ☐ a. La connessione HTTPS verrà automaticamente cambiata in HTTP
- ☐ b. La validazione del certificato fallirà per l'immagine
- ☒ c. Contenuto misto: la risorsa HTTP può essere intercettata e modificata da un attaccante
- ☐ d. L'immagine verrà comunque caricata con HTTPS

[Annulla la scelta](#)

# Domanda 12

## Domanda 12

Risposta non ancora data

Punteggio max.: 1,00

🚩 Contrassegna domanda

Perché i certificati CA root sono self-signed?

Scegli un'alternativa:

- ☐ a. I certificati root self-signed forniscono maggiore sicurezza
- ☐ b. Fa risparmiare denaro alla Certificate Authority
- ☒ c. Non c'è un'autorità superiore per firmarli; sono la radice della trust chain
- ☐ d. I certificati root non necessitano di firme

[Annulla la scelta](#)

# Domanda 13

## Domanda 13

Risposta non ancora data

Punteggio max.: 1,00

🚩 Contrassegna domanda

Quali informazioni sono tipicamente incluse in un certificato X.509? (Selezionare tutti quelli applicabili)

Scegli una o più alternative:

- ☒ a. Periodo di validità (date Not Before e Not After)
- ☐ b. Cronologia del browser
- ☐ c. Password degli utenti
- ☒ d. Chiave pubblica e algoritmo di firma
- ☒ e. Subject (a chi è rilasciato il certificato)
- ☐ f. Indirizzo IP del server
- ☒ g. Issuer (chi ha emesso il certificato)
- ☐ h. Chiave privata