CERTLABZ CERTIFICATION BOARD

Certified Crypto Wallet Security Practitioner (CCWS)

Ten Sample Questions

These ten questions are written at the difficulty of the live exam. Six carry a figure, a data table, a configuration or a code listing; four are plain scenario questions, as on the live paper. Every one is a scenario a working crypto wallet security practitioner would meet, and none of them appears in the live question bank.

The live exam is multistage adaptive: how you score on one stage selects the difficulty of the next, so no two candidates sit the same paper. It is a performance-based exam: each form can carry up to 5 to 12 performance-based questions alongside the multiple-choice questions, which means you build, sequence or complete something rather than only choosing from a list. Answers and full explanations follow each question here; the live exam does not disclose item-level answers.

Question 1

Domain 1: Wallet and Key Foundations

DATA

Sarah Miller maps each key to its role, with one role missing.

Key	Role
Private key	Signs transactions
Public key	(to choose)
Wallet address	Receives funds
Passphrase	Adds extra secret

Table 1.1 Keys and their roles.

What is the public key role?

A. Stores the funds
B. Verifies a signature
C. Pays the network fee
D. Deletes the wallet

Correct answer: B
A public key lets others verify a signature made with the matching private key, so the missing role is to verify a signature. Funds sit on the ledger, fees are set per transaction, and no key deletes a wallet.

Question 2 Domain 2: Wallet Types and Storage DATA

James Carter compares wallet types by whether the keys stay offline.

Wallet type	Keys offline
Hardware wallet	Yes
Paper wallet	Yes
Mobile hot wallet	No
Exchange account	No

Table 2.1 Wallet types and key exposure.

Which type keeps keys most exposed online?

A. Paper wallet
B. Hardware wallet
C. Cold storage
D. Mobile hot wallet

Correct answer: D
A mobile hot wallet stays connected to the internet, so its keys are the most exposed of the choices. Hardware and paper wallets keep keys offline, which is why they are called cold storage.

Question 3 Domain 3: Seed Phrases and Backups CONFIG

Emma Wilson reviews a sample recovery phrase used only for training.

```
word 01  sample
word 02  example
word 03  placeholder
word 04  demo
...      (12 words total)
```

Listing 3.1 A demo recovery phrase.

How should this phrase be stored?

A. Offline on paper
B. In a chat message
C. On a shared drive

D In a browser note

Correct answer: A
A recovery phrase should be written down and kept offline, away from any connected device or account. Storing it in chats, shared drives, or browser notes exposes it to theft if those systems are breached.

Question 4 — Domain 4: Threats and Attacks — DATA

Olivia Davis maps each threat to how it reaches a victim, with one method missing.

Threat	Method
Phishing site	Fake login page
Clipboard malware	(to choose)
Fake support	Impersonates staff
SIM swap	Hijacks phone number

Table 4.1 Threats and delivery methods.

What does clipboard malware do?

A Guesses the passphrase
B Swaps the paste address
C Freezes the ledger
D Prints the seed phrase

Correct answer: B
Clipboard malware silently swaps a copied wallet address for the attacker address when it is pasted, so funds go to the wrong place. It does not guess secrets, freeze ledgers, or print phrases.

Question 5 — Domain 5: Secure Transactions and Signing — CONFIG

Liam Anderson checks a sample transaction on the hardware wallet screen before approving.

```
To      0xEXAMPLE...1234
Amount  0.50 sample
Fee     0.001 sample
Status  awaiting confirm
```

Listing 5.1 A demo transaction to confirm.

What should he verify before signing?

A The device colour
B The screen brightness
C The battery level

D The address and amount

Correct answer: D
He should confirm the destination address and amount on the device screen match what he intended before signing. Checking those details on the trusted screen catches swapped addresses or altered amounts that malware may show elsewhere.

Question 6

Domain 6: Recovery, Custody and Compliance

CONFIG

Ava Thompson lists the custody options a small team is weighing.

```
Self custody   user holds keys
Custodial      provider holds keys
Multi sig      several approvers
Shared backup  split recovery
```

Listing 6.1 Custody options.

Which option removes any single point of failure for signing?

A Multi signature
B Self custody
C Custodial only
D One paper backup

Correct answer: A
Multi signature requires several approvers to sign, so no single lost or stolen key can move funds alone. Self custody and a single paper backup each rest on one secret, and custodial only shifts trust to one provider.

Question 7

Domain 1: Wallet and Key Foundations

A new user thinks the wallet app itself stores their coins, so they believe reinstalling the app will lose the funds forever. What is the accurate view?

A Funds live in the app
B Coins sit on the ledger
C Deleting burns the coins
D The app mints the coins

Correct answer: B
Coins are recorded on the shared ledger, and the wallet only holds the keys that control them. Reinstalling and restoring from the recovery phrase brings access back, so the funds are not tied to the app itself.

Question 8

Domain 3: Seed Phrases and Backups

A support chat asks David Brown to type his twelve recovery words to verify his account before it can help him. What should he do?

A. Send half the words
B. Share it once only
C. Never share the phrase
D. Email it securely

Correct answer: C
A recovery phrase should never be shared with anyone, since anyone who holds it can take the funds. Real support never needs it, so the request is a clear sign of a scam, whether asked in full, in part, or by email.

Question 9 — Domain 4: Threats and Attacks

A pop up promises free tokens if the user connects their wallet and approves a request to spend any amount of their assets. What is the safe response?

A. Approve to claim
B. Raise the limit
C. Decline the request
D. Share the address

Correct answer: C
An open ended approval to spend any amount lets a malicious contract drain the wallet later, so the request should be declined. Free token offers that demand broad spending approval are a common draining scam.

Question 10 — Domain 6: Recovery, Custody and Compliance

A small group keeps its only wallet backup on one laptop in one office, and a fire or theft would wipe out every copy at once. What best reduces this risk?

A. Add a longer password
B. Store copies in two places
C. Use a faster laptop
D. Delete the backup

Correct answer: B
Keeping backups in two separate secure locations means a single fire, theft, or failure cannot destroy every copy at once. A longer password or faster laptop does not address the single point of loss, and deleting the backup makes recovery impossible.

Published by the CertLabz Certification Board, a division of CertLabz LLC. Companion to objectives document CCWS-001. https://certlabz.com/certifications/certified-crypto-wallet-security-practitioner.html