DUMPSBOSS.

Card Production Security Assessor (CPSA)QualificationExam

PCI SSC CPSA

Version Demo

Total Demo Questions: 7

Total Premium Questions: 74

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

QUESTION NO: 1

A vendor uses codes from a chip manufacturer to 'unlock' chips and prepare them for use by adding applications and keys. Which of the following best describes this process?

A. Data creation

B. Data preparation

C. Manufacture

D. Pre-personalization

ANSWER: D

Explanation:

Pre-personalization is correct because it describes a controlled production stage in which an integrated-circuit chip is prepared before issuer-specific card personalization. A chip supplier may provide codes, keys, or other secure mechanisms that enable an approved card-production entity to activate or unlock chip functions. The entity can then load or enable payment applications, application parameters, and cryptographic keys needed for the chip to support later personalization and use in the payment ecosystem.

This activity is distinct from simply creating cardholder or issuer data: its purpose is to establish the chip's functional and cryptographic readiness. In a secure card-production environment, pre-personalization must be performed under defined authorization, key-management, access-control, and traceability procedures. Those controls protect sensitive chip assets and help ensure that only authorized applications and keys are introduced before the card reaches the subsequent personalization stages. PCI SSC's card-production standards address security controls throughout the card-production and provisioning lifecycle, including protection of sensitive materials and cryptographic processes. See the PCI SSC Card Production standards page and EMVCo's EMV technology resources for relevant industry context on chip payment applications and secure implementation.

QUESTION NO: 2

Which of the follow best describes a Technical FAQ?

A. Technical FAQs only apply to the specific technology as the FAQ defines it

B. Technical FAQs can be submitted to PCI SSC at any time

C. Use of the Technical FAQs is mandatory, they shall be used during an assessment

D. Use of the Technical FAQs is optional, they are considered guidance

ANSWER: D

Explanation:

Use of the Technical FAQs is optional, they are considered guidance. PCI SSC publishes Frequently Asked Questions to provide clarification and supporting information on PCI SSC standards, programs, and related technologies. A Technical FAQ helps stakeholders understand how a particular technology, implementation, or circumstance relates to PCI SSC requirements; it is not itself a PCI SSC standard, requirement, or mandatory assessment procedure. Accordingly, an assessor should use applicable Technical FAQs as an authoritative source of PCI SSC clarification and as useful guidance when interpreting a scenario, but the assessment determination must remain grounded in the applicable card-production security standard, validation requirements, and program documentation. Technical FAQs may also be revised, superseded, or retired as technology and PCI SSC guidance evolve, so assessors should consult the current published material when it is relevant to the scope being assessed. PCI SSC's document library and FAQ resources are available through the PCI SSC Document Library and the PCI SSC FAQ portal.

QUESTION NO: 3

During an assessment, the vendor explains that its HSA access-control system grants entry to any employee with a valid badge. The system does not verify whether a second authorized person is present. What is the principal concern?

A. The system does not enforce dual presence

B. The system should grant access to all employees during production hours

C. The system should allow guards to enter the HSA without a badge

D. The system should replace all badges with physical keys

ANSWER: A

Explanation:

The HSA access-control system does not enforce dual presence. High Security Areas protect sensitive card-production assets, materials, and processes. Dual presence requires two authorized individuals to be physically present when the applicable access or activity occurs. A system that permits a single authorized employee to enter alone does not enforce that safeguard, even where the employee holds a valid badge.

Badge validity confirms an individual's authorization but does not establish the required presence of a second authorized person. The vendor should ensure that HSA entry arrangements support both the applicable authorization conditions and the required dual-control and dual-presence principles. PCI SSC publishes relevant program materials through its Document Library.

QUESTION NO: 4

A vendor's security manager asks an assessor to remove a non-compliant finding from the ROC because the corrective action will be completed shortly after the assessment. What should the assessor do?

A. Retain the non-compliant finding in the ROC

B. Remove the finding if the vendor provides a remediation date

C. Mark the requirement Not Applicable

D. Allow the vendor to determine the final finding status

ANSWER: A

Explanation:

The assessor should retain the non-compliant finding in the ROC. Assessment findings must reflect the controls that were in place and operating effectively at the time of assessment. A planned corrective action, even where it is expected to be completed soon, is not evidence that the requirement was met during the assessment period.

The vendor may document its remediation plan and subsequently provide evidence that the deficiency has been corrected through the applicable process. However, changing a finding merely because remediation is planned would misrepresent the assessment result and undermine the integrity of the report. PCI SSC publishes assessor-program and reporting resources through its Document Library.

QUESTION NO: 5

A cardholder downloads a payment application to a mobile phone. The issuer then sends payment credentials securely to the application through the mobile network after the phone has been activated. Which of the following best describes the issuer's activity?

A. Card personalization

B. Host Card Emulation (HCE) provisioning

C. Secure Element (SE) provisioning

D. Over-the-air (OTA) provisioning

ANSWER: D

Explanation:

Over-the-air (OTA) provisioning is correct because payment credentials are being delivered remotely to a mobile device through a wireless communications channel after the device is in use. OTA provisioning describes the secure remote loading, updating, or management of payment credentials or applications without requiring the cardholder to visit a physical location or connect the device directly to personalization equipment.

The presence of a mobile application does not, by itself, make the activity Host Card Emulation or Secure Element provisioning. Those terms describe the environment in which credentials are stored or used. The defining feature in this scenario is the remote delivery method. PCI SSC information on card production and provisioning is available through the Card Production and Provisioning standards page.

QUESTION NO: 6

Before you go on-site, the vendor's primary contact communicates a legitimate reason for delaying the assessment for several months. Who can approve the change in the report delivery schedule?

A. Vendor senior management

B. Payment brands

C. Affected issuers

D. PCI SSC

ANSWER: D

Explanation:

PCI SSC can approve a change to the report delivery schedule. The PCI Security Standards Council administers the card-production security assessment program and its associated assessor qualification processes. As the program administrator, it maintains oversight of assessment-cycle obligations and the timing for submitting assessment reporting. A vendor's legitimate operational reason for postponing an assessment does not, by itself, revise the required reporting timetable. The proposed delay must be communicated through the applicable PCI SSC process so that the Council can review the circumstances, determine whether the requested schedule change is appropriate, and formally approve the revised delivery date. This centralized approval preserves consistent governance, ensures that exceptions are documented, and maintains the integrity of the assessment and reporting process across participating vendors and assessors. The assessor should therefore avoid treating a vendor request as authorization to alter the reporting schedule; instead, the assessor should obtain PCI SSC approval before relying on a revised deadline. PCI SSC's role in developing, administering, and supporting security standards and related programs is described on the PCI Security Standards Council About Us page. Additional program and standards resources are available through the PCI SSC Standards portal.

QUESTION NO: 7

A vendor receives cardholder information and keys from a bank. The vendor then performs the following:

* Uses its HSM to create keys

* Creates cardholder information specific to each cardholder, including name and PAN

* Formats the data for the hardware that will put it on a card

* Writes it to an encrypted file

Which of the following best describes this process?

A. Data creation

B. Data preparation

C. Manufacture

D. Pre-personalization

ANSWER: B

Explanation:

Data preparation is the correct description because it covers the controlled processing of issuer-supplied cardholder information and cryptographic key material into secure, card-specific personalization data. In this scenario, the vendor generates or derives the necessary keys within an HSM, associates the data with an individual cardholder and PAN, and formats the resulting records for use by the equipment that will personalize the physical card. Producing an encrypted output file is also a core data-preparation activity: it protects sensitive personalization data and key-related information while it is stored or transferred to the subsequent personalization environment.

The important boundary is that the described work creates and securely packages the logical data needed for a card; the actual act of placing that information onto the card is performed later by the card-personalization hardware. PCI SSC's Card Production and Provisioning requirements address the security of these connected production activities, including protection of account data, cryptographic keys, and the systems that prepare personalization data. See the PCI SSC Card Production and Provisioning standards overview and the PCI SSC Document Library for the applicable requirements and supporting terminology.