Payment Card Industry

3-D Secure (PCI 3DS)

Security Requirements and Assessment Procedures for EMV® 3-D Secure SDK

Technical FAQs for use with Version 1.1

August 2022

Introduction

This document addresses frequently asked questions (FAQs) related to the *PCI 3DS Security Requirements and Assessment Procedures for EMV® 3-D Secure SDK* (hereafter referred to as the PCI 3DS SDK Security Standard). Throughout this FAQ document:

- The use of "PCI 3DS SDK Security Standard" or "PCI 3DS SDK" refers to the current version of the *PCI 3DS Security Requirements and Assessment Procedures for EMV® 3-D Secure SDK*, as published on the PCI SSC website (www.pcisecuritystandards.org).
- The use of "EMVCo 3DS SDK Specification" refers to the *EMV® 3-D Secure SDK Specification*, as published by EMVCo (www.emvco.com).

Further information about use and applicability of the PCI 3DS SDK Security Standard can be found in the "Introduction", "Terminology", and "Scope of Security Requirements" sections within the standard itself, as well as in the general PCI Glossary on the PCI SSC website: https://www.pcisecuritystandards.org/pci_security/glossary.

PCI 3DS SDK: Technical FAQs

These technical FAQs provide answers to questions regarding the application of the security requirements defined in the *PCI Security Requirements and Assessment Procedures for EMV® 3-D Secure SDK* (hereafter referred to as the *PCI 3DS SDK Security Standard*). The FAQs are an integral part of those requirements and shall be fully considered during the PCI 3DS SDK evaluation process.

New questions or questions updated for clarity are in **red**.

General Questions

Q1 **April 2021: Can 3DS Authentication Challenge Data (i.e., CReq/CRes data) be stored temporarily for debugging or troubleshooting purposes?**

A *No, 3DS SDK vendors should never debug their code or troubleshoot issues with their software using live or production CReq/CRes data. Debugging and/or troubleshooting these products should always be performed in a development or test environment using test data. Where the 3DS SDK vendor does not have access to appropriate test functionality—for example, access to test Directory Server (DS), Access Control Server (ACS), 3DS Server (3DSS) functionality—the 3DS SDK vendor should manually generate their own CReq/CRes test data for debugging or troubleshooting purposes.*

Q2 **April 2021: Are there any 3DS SDK data elements not included in the Sensitive 3DS SDK Data Elements table that should be treated as "sensitive data"?**

A *No. For the purposes of the PCI 3DS SDK Security Standard, all 3DS SDK Data Elements that require confidentiality and/or integrity protection are included in the "Sensitive 3DS SDK Data Elements" table. 3DS SDK data elements not explicitly referenced in that table are not considered sensitive per the PCI 3DS SDK Security Standard. The 3DS SDK vendor may define additional data protection requirements for certain 3DS SDK data elements that are not defined in the PCI 3DS SDK Security Standard. Please contact the 3DS SDK vendor for more information of vendor-specific data protection requirements.*

Q3 **February 2022: Is partial testing of a platform (OS and/or hardware) allowed where full testing has been performed on another version of the OS or hardware? I.e., is it possible to account for only the delta differences between platform 'x' and platform 'y' in order to avoid redundant testing?**

A *Yes, where possible, provided the following conditions are met:*

- *The partial testing is only permitted where the OS and Hardware platform is from the same OEM vendor for the same product where the only difference between the partially tested platform and the fully tested platform is between the version of the OS or the hardware (not both).*
- *The latest (most recent) version must be fully tested.*
- *Partial testing must not overlook any differences between versions that requires analysis and testing to a governing PCI 3DS SDK requirement. I.e., the scope of the evaluation must be complete.*

While partial testing may be possible, the amount of analysis and testing required will dynamically depend on the delta differences between the fully tested platform. Whether or not partial testing will be possible and/or beneficial compared to fully testing the platform will depend on each unique use case.

The 3DS SDK lab must clearly document within the PCI 3DS SDK ROV:

- *The OS and Hardware platform that was fully tested.*
- *The OS and Hardware platform that was only partially tested, and which OS and Hardware platform was fully tested that accounts for the possibility to perform the subsequent partial testing.*
- *The delta differences between the fully tested OS and Hardware platform and the partially tested OS and Hardware platform, including the resources (e.g., documentation, testing, etc.) used to determine and validate the differences (and therefore, the similarities).*
- *How the partial testing satisfies all the applicable requirements and assessment procedures.*

Requirement 1.1

Q4 **August 2022: Requirement 1.1 (Security Checks) states in T.1.1.7 to "confirm the 3DS SDK detects when its code or execution has been tampered with." It may not be possible for a 3DS SDK to implement integrity mechanisms that can satisfy this criterion. In the event it is not technically achievable, how should the requirement be assessed?**

A *The 3DS SDK must implement integrity checking mechanisms as per requirement 1.1. The 3DS SDK Lab must determine if the implementation is sufficient. In the event there are technical limitations to the efficacy of the integrity implementation, the 3DS SDK Lab must clearly document within the PCI 3DS SDK ROV:*

- *The extent that the integrity mechanisms implemented mitigate the compromise of the 3DS SDK.*
- *The technical (logical) limitations of the run-time integrity implementation, and why these limitations cannot be resolved.*
- *The residual risk to the integrity of the 3DS SDK that exists due to the technical limitations.*

Requirement 1.2

Q5 **April 2021: How is the 3DS SDK expected to perform checks to determine whether the 3DS SDK was installed from an approved source?**

A *This requirement is under revision. Some platforms and versions provide functions or APIs to determine the source from which an application package was installed (for example: PackageManager.getInstallSourceInfo on Android). Where such methods or APIs are unavailable, it is not expected that the 3DS SDK provide for such functionality.*

Q6 **April 2021: How is the 3DS SDK expected to respond when checks indicate the 3DS SDK was not installed from an approved source? The requirement states that the 3DS SDK should make the information available to the ACS, but Assessment Procedure T.1.2.4 indicates that the 3DS SDK should terminate 3DS transaction processing upon detection.**

A *This requirement is under revision. Per the requirement, the information is expected to be made available to the ACS for further decision-making where possible. It is not*

expected that the 3DS SDK terminate 3DS transaction processing unless instructed by the ACS.

Q7 April 2021: How is the 3DS SDK expected to convey the results of checks to determine whether the 3DS SDK was installed from an approved source to the ACS? The ACS does not provide any dedicated fields to report this information.

A *This requirement is under revision. It may be possible to pass the results of the checks to the ACS along with other general device information. It is not expected that the ACS provider develop custom server-side functionality to accommodate this information beyond what is specified in the EMV® 3-D Secure SDK Specification.*

Q8 April 2021: How can 3DS SDKs be submitted for publishing in an appropriate App Store if it must first be installed from an approved source? Would testing by the respective App Store prior to publishing fail because of this requirement?

A *This requirement is under revision. This requirement was not intended to complicate testing or acceptance by App Store providers. If such functionality prevents a 3DS SDK from being tested and accepted by an appropriate App Store, then such checks may be disabled.*

Where automated checks are not possible, procedural and/or contractual methods to ensure the 3DS SDK is installed from an approved source may be used to satisfy this requirement. In such instances, the 3DS SDK Lab(s) should request documentation from the 3DS SDK vendor that verifies such methods are in place.

Requirement 1.3

Q9 February 2022: Requirement 1.3 (Run-Time Integrity) states in T.1.3.1 to "verify that the security of the SDK cannot be compromised after the initialization phase by tampering with the execution code or parameters." It may not be possible for a 3DS SDK to implement run-time integrity mechanisms that can satisfy this criterion. In the event it is not technically achievable, how should the requirement be assessed?

A *The 3DS SDK must implement run-time integrity mechanisms as per requirement 1.3. The 3DS SDK Lab must determine if the implementation is sufficient. In the event there are technical limitations to the efficacy of the run-time integrity implementation, the 3DS SDK Lab must clearly document within the PCI 3DS SDK ROV:*

- *The extent that the run-time integrity mechanisms implemented mitigate the compromise of the 3DS SDK.*
- *The technical (logical) limitations of the run-time integrity implementation, and why these limitations cannot be resolved.*
- *The residual risk to the run-time integrity of the 3DS SDK that exists due to the technical limitations.*

Requirement 2.2

Q10 February 2022: In regard to Requirement 2.2 (Clearing of Sensitive 3DS SDK Data Elements), it may not be technically possible to delete all sensitive 3DS SDK data elements (in reference to Table 2 in the 3DS SDK Standard) depending on the particular architecture and the management of memory due to the underlying platform (e.g., the OS and/or hardware). In the event this is the case, how should this requirement be

assessed?

A *The 3DS SDK must meet Requirement 2.2 in regard to all sensitive 3DS SDK data elements under its control. If there are relevant 3DS SDK sensitive data elements that cannot be securely deleted due to technical (logical) constraints of the architecture, the 3DS SDK Lab must clearly document those data elements and the reasoning as to why they cannot be securely deleted.*

Requirement 3.1

Q11 April 2021: Do PCI 3DS SDK requirements for ensuring the authenticity of public keys apply to Directory Server (DS) public keys? Test Requirement 3.1.10 indicates that the use any self-signed certificates is prohibited unless the authenticity of the key is ensured through the use of a secure cryptographic module (SCD).

A *No. DS public keys certificates are generated and signed by the Directory Server Certificate Authority which is typically operated the payment system responsible for a specific DS. The 3DS SDK is required to use DS public keys to encrypt device information before sending it to the 3DS Requestor App which is then forwarded to the 3DS Server to use in the construction of the Authentication Request (AReq). It is not expected that the 3DS SDK store these public key certificates in a secure cryptographic device (SCD).*