Payment Card Industry
EMV® 3-D Secure 3DS SDK

Program Guide
Version 1.0

July 2018

Document Changes

Date	Version	Description
July 2018	1.0	Initial version of the 3DS SDK Program Guide.

Contents

1 Introduction

The *Payment Card Industry 3-D Secure (PCI 3DS) Security Requirements and Assessment Procedures for EMV® 3-D Secure SDK* ("PCI 3DS SDK Security Standard," or the "Standard") defines security requirements and testing procedures for 3-D Secure (3DS) Software Development Kits (3DS SDK) as defined in the *EMV® 3-D Secure 3DS SDK Specification*. The Standard provides a set of logical and physical security requirements as well as procedures for performing a 3DS SDK Evaluation. The PCI 3DS SDK Security Standard applies to entities that develop 3DS SDKs, as defined in the *EMV® 3-D Secure 3DS SDK Specification*. Prior to undergoing an Evaluation against the Standard, 3DS SDK Vendors should confirm with the Participating Payment Brand(s) whether they are required to validate compliance with the security objectives and requirements in the PCI 3DS SDK Security Standard. This *PCI 3DS SDK Program Guide* (referred to hereafter as "3DS SDK Program Guide") provides the requirements for 3DS SDKs to be listed by the PCI Security Standards Council (PCI SSC) as part of the 3DS SDK Program (the "Program"). PCI SSC maintains lists of 3DS SDK Products that have been assessed and validated in accordance with the PCI 3DS SDK Security Standard and this Program Guide.

1.1 Related Publications

The 3DS SDK Program Guide should be used in conjunction with the latest versions of the following PCI SSC publications, each is available through the Website, and the referenced *EMV 3-D Secure SDK Specification*:

Document name	Description
3DS SDK Attestation of Validation ("3DS SDK AOV")	3DS SDK AOV is a form for 3DS SDK Labs to attest to the results of a 3DS SDK Evaluation, as documented in the 3DS SDK Report on Validation.
3DS SDK Report on Validation ("3DS SDK ROV")	The 3DS SDK ROV Report Template is mandatory for completing a Report on Validation and includes detail on how to document the findings of a 3DS SDK Evaluation.
EMV® 3-D Secure SDK Specification	The *EMV® 3-D Secure SDK Specification* describes the specification for the 3DS SDK. Enhancements to the *EMV 3-D Secure Protocol and Core Functions Specification* that have an impact on the 3DS SDK are also included in this document.
Payment Card Industry 3-D Secure (PCI 3DS) Security Requirements and Assessment Procedures for EMV® 3-D Secure SDK	PCI 3DS SDK Security Standard.
Vendor Release Agreement ("VRA")	The VRA establishes the terms and conditions under which Validated 3DS SDKs are accepted and listed by PCI SSC.

1.2 Updates to Documents and Security Requirements

PCI SSC reserves the right to change, amend, or withdraw security requirements at any time. If such changes are required, PCI SSC will endeavor to work closely with its community of Participating Organizations, Vendors, and 3DS SDK Labs to help minimize the impact of any changes.

1.3 Terminology

Throughout this document the following terms have the meanings shown in the chart below.

Term	Meaning
3DS SDK	Acronym for 3-D Secure Software Development Kit.
3DS SDK Evaluation (or Evaluation)	Review of a 3DS SDK for purposes of validating the compliance of such 3DS SDK with the PCI 3DS SDK Security Standard as part of the 3DS SDK Program.
3DS SDK Laboratory (or 3DS SDK Lab)	PCI-recognized Lab that is qualified by PCI SSC to perform 3DS SDK Evaluations.
3DS SDK Program (or Program)	Refers to PCI SSC's program and requirements for qualification of 3DS SDK Labs, and validation and Acceptance of 3DS SDKs, as further described in this document and related PCI SSC documents, policies, and procedures.
3DS SDK Reference Number	Implementer and version of the 3DS SDK that is integrated with the 3DS Requestor App, assigned by EMVCo through the EMV 3-D Secure Testing and Approvals process when the 3DS SDK is approved. This reference number is a security asset of the 3DS SDK, and it shall be securely stored. During each transaction, this reference number shall be securely retrieved by the 3DS SDK and returned to the 3DS Requestor App. This number must be provided to the 3DS SDK Lab by the Vendor when submitting a 3DS SDK for Evaluation. Reference: *EMV® 3-D Secure 3DS SDK Specification v2.1.0*, Section 5.1.
3DS SDK Requirements	3DS Software Development Kit development and testing requirements as defined in the PCI 3DS SDK Security Standard.
3DS SDK ROV	3DS SDK Report of Validation containing details documenting results from an entity's 3DS SDK Evaluation for purposes of the 3DS SDK Program.
3DS SDK Vendor (or Vendor)	Developer or reseller of a 3DS SDK.

Term	Meaning
Accepted, or listed	A 3DS SDK is deemed to have been "Accepted" or "listed" (and "Acceptance" is deemed to have occurred) when PCI SSC has: i. Received the corresponding 3DS SDK Report on Validation from the 3DS SDK Lab; ii. Received the fee and all documentation required with respect to the 3DS SDK as part of the Program; iii. Confirmed that: a) The 3DS SDK ROV is correct as to form, b) The 3DS SDK Lab properly determined that the 3DS SDK is eligible to be a 3DS SDK, c) The 3DS SDK Lab adequately reported the 3DS SDK compliance of the 3DS SDK in accordance with Program requirements, and d) The detail provided in the 3DS SDK ROV meets PCI SSC's reporting requirements; and iv. Listed the 3DS SDK on the List of 3DS SDKs; provided that PCI SSC may suspend, withdraw, terminate, revoke, cancel, or place conditions upon (including without limitation, complying with remediation requirements) Acceptance of any 3DS SDK in accordance with applicable 3DS SDK Program policies and procedures.
Delta Evaluation	Partial 3DS SDK Evaluation performed only against applicable 3DS SDK Requirements when changes to a listed 3DS SDK impact only a subset of 3DS SDK Requirements.
EMVCo Letter of Approval	Approval letter provided by an EMVCo Lab to a 3DS SDK Vendor to confirm that the 3DS SDK that is the subject of that letter underwent and passed EMVCo functional testing.
List of Validated 3DS SDKs	Refers to the authoritative list of Validated 3DS SDKs appearing on the Website.
Listing or listing	Refers to the listing and related information regarding a 3DS SDK on the List of 3DS SDKs.
Participating Payment Brand	A global payment card brand or scheme that is also a limited liability company member of PCI SSC (or affiliate thereof).
PCI-recognized Lab	A security laboratory qualified by PCI SSC under the PCI SSC PCI-recognized Laboratory program.
Portal	Defined in Section 6.2, "Delivery of the 3DS SDK ROV and Related Materials."
Validated 3DS SDK	A 3DS SDK that has been Accepted and with respect to which such Acceptance has not been terminated, suspended, withdrawn, revoked, or canceled.

Term	Meaning
Vendor Release Agreement (or VRA)	The then-current version of (or successor document to) the Payment Card Industry Vendor Release Agreement on the form then Approved by PCI SSC for Vendors participating in the 3DS SDK Program, as from time to time amended and made available on the Website.
Website	The then-current PCI SSC web site (and its accompanying web pages), which at the time of publication is available at www.pcisecuritystandards.org.
Wildcard	A character that may be substituted for a defined subset of possible characters in an application version scheme. In the context of a 3DS SDK, wildcards can optionally be used to represent a non-security impacting change. A wildcard is the only variable element of the Vendor's version scheme, and is used to indicate there are only non-security-impacting changes between each version represented by the wildcard element.

2 Roles and Responsibilities

Several stakeholders are involved in maintaining and managing PCI SSC standards. The following describes the high-level roles and responsibilities as they relate to the PCI 3DS SDK Security Standard and 3DS SDK Program:

2.1 PCI Security Standards Council

PCI SSC maintains various PCI standards, supporting programs and related documentation. In relation to the PCI 3DS SDK Security Standard, PCI SSC:

- Maintains the PCI 3DS SDK Security Standard.
- Maintains supporting documentation to assist entities implementing and assessing to the PCI 3DS SDK Security Standard including: reporting templates, attestation forms, frequently asked questions (FAQs), and guidance.
- Maintains the list of approved 3DS SDK versions and qualified 3DS SDK Labs on the Website.
- Maintains a quality assurance program for qualified Labs.

2.2 Participating Payment Brands

The Participating Payment Brands develop and enforce their respective programs related to compliance with PCI SSC standards, including, but not limited to:

- Requirements, mandates, and deadlines for compliance to PCI SSC standards
- Required validation frequencies for brand-specific programs
- Fines or penalties for non-compliance

2.3 EMVCo

EMVCo is the global technical body owned by American Express, Discover, JCB, Mastercard, UnionPay, and Visa that facilitates the worldwide interoperability and acceptance of secure payment transactions by managing and evolving the EMV specifications and related testing processes. Adoption of EMV specifications and associated approval and certification processes promotes a unified international payments framework, which supports an advancing range of payment methods, technologies, and acceptance environments.

2.4 3DS SDK Vendors

3DS SDK Vendors are responsible for:

- Ensuring their 3DS SDK meets 3DS SDK Requirements, including (but not limited to) successfully passing an evaluation as specified in the PCI 3DS SDK Security Standard;
- Complying with the Vendor Release Agreement including the adoption and implementation of Vulnerability Handling Policies (further described in the VRA) consistent with industry best practices;
- Adhering to their defined software versioning methodology as validated and documented in the 3DS SDK ROV.

Vendors submit their 3DS SDK and supporting documentation to the 3DS SDK Lab for review and authorize their 3DS SDK Lab to submit the resulting 3DS SDK ROVs and related information to PCI SSC.

2.5 3DS SDK Labs

PCI SSC qualifies 3DS SDK Labs to assess 3DS SDKs for compliance with the PCI 3DS SDK Security Standard. In order to perform 3DS SDK Evaluations, a 3DS SDK Lab must have been qualified by PCI SSC and remain in good standing (or in compliance with remediation requirements, if applicable) as both a PCI-recognized Lab and a 3DS SDK Lab. All PCI-recognized Labs and 3DS SDK Labs are listed on the Website. Labs identified on the Website as 3DS SDK Labs are the only laboratories recognized by PCI SSC as qualified to perform 3DS SDK Evaluations.

Note: *Not all PCI-recognized Labs are 3DS SDK Labs.*

Organizations wishing to become a PCI-recognized 3DS SDK Lab must first be an EMVCo-recognized Security Laboratory. If this baseline criterion has been satisfied, organizations interested in becoming a PCI-recognized 3DS SDK Lab must, in the first instance, contact the SDK Program Manager at 3DS@pcisecuritystandards.org for further information.dxc

3DS SDK Labs are responsible for:

- Performing Evaluations of 3DS SDKs in accordance with the PCI 3DS SDK Security Standard;
- Providing an opinion regarding whether the 3DS SDK meets 3DS SDK Requirements;
- Documenting each Evaluation in a 3DS SDK ROV using the 3DS SDK ROV Report Template;
- Providing adequate documentation within the 3DS SDK ROV to demonstrate the 3DS SDK's compliance with the 3DS SDK Requirements;
- Submitting the 3DS SDK ROV and/or any change submissions to PCI SSC, along with the 3DS SDK Attestation of Validation signed by both the evaluating 3DS SDK Lab and Vendor;
- Maintaining an internal quality assurance process for their Evaluation efforts;
- Staying up to date with PCI SSC statements and guidance, industry trends and best practices;
- Satisfying all applicable 3DS SDK Program requirements at all times.

3 Overview of 3DS SDK Evaluation Processes

3DS SDKs must first undergo functional testing as defined in the *EMV® 3-D Secure 3DS SDK Specification* prior to security testing as defined in the PCI 3DS SDK Security Standard. The 3DS SDK Evaluation process typically includes the following steps:

1. The Vendor participates in the EMVCo process for 3DS SDK Functional Testing, completes the testing, and if successful, receives a Letter of Approval and 3DS SDK Reference Number from EMVCo.

   ***Note**: Eligibility for 3DS SDK Evaluation as part of the PCI SSC 3DS SDK Program is limited to 3DS SDKs that have obtained EMVCo functional approval and are able to provide the Letter of Approval.*

   The EMVCo Letter of Approval and 3DS SDK Reference Number must be obtained and presented by the Vendor to the 3DS SDK Lab before 3DS SDK Evaluation may commence under the PCI SSC 3DS SDK Program.

2. The Vendor contacts the Participating Payment Brands to determine whether the 3DS SDK is eligible or required to validate compliance with the PCI 3DS SDK Security Standard.
3. The Vendor contracts with a 3DS SDK Lab to perform the 3DS SDK Evaluation and provides the 3DS SDK Lab its EMVCo Letter of Approval and 3DS SDK Reference Number.
4. The 3DS SDK Lab performs the 3DS SDK Evaluation following the “Evaluation Procedures” for each security objective and associated requirements specified within the PCI 3DS SDK Security Standard.
5. The 3DS SDK Lab completes the 3DS SDK Report on Validation (ROV) and 3DS SDK Attestation of Validation (AOV) in accordance with applicable PCI SSC templates, guidance, and instructions.
6. The 3DS SDK Lab submits the 3DS SDK ROV and 3DS SDK AOV, along with any other requested documentation, to PCI SSC via the Portal.
7. If required, remediation activities are performed by the Vendor to address security objectives or requirements that are not in place, or security controls that were not sufficiently evidenced. The 3DS SDK Lab will then perform follow-up testing and provide PCI SSC with an updated 3DS SDK ROV.
8. Upon receipt of a satisfactory 3DS SDK ROV and 3DS SDK AOV, and compliance with any other applicable Program requirements, PCI SSC will acknowledge the successful completion of the Evaluation process by recognizing the assessed version of the 3DS SDK on a list of “Approved 3DS SDKs” on its Website. Processes for reassessing updated versions of Approved 3DS SDKs are discussed in Section 5 of this Program Guide, “Managing a Validated 3DS SDK.”

4 Preparation for the 3DS SDK Evaluation

Prior to commencing a 3DS SDK Evaluation, Vendors should take the following preparatory actions:

- Review 3DS SDK Requirements, including the PCI 3DS SDK Security Standard and related documentation located at the Website;
- Determine/assess the 3DS SDK's readiness to comply with the PCI 3DS SDK Security Standard by:
  - Performing a gap analysis between the 3DS SDK's security functionality and the 3DS SDK Requirements;
  - Correcting any gaps;
  - Optionally having the 3DS SDK Lab perform a pre-Evaluation or gap analysis of a Vendor's 3DS SDK. If the 3DS SDK Lab notes deficiencies that would prevent a compliant result, the 3DS SDK Lab will provide to the Vendor a list of 3DS SDK features to be addressed before the formal review process begins

Note: *Refer to Section 3, "Overview of 3DS SDK Evaluation Processes," for details on 3DS SDK eligibility and validation testing.*

4.1 Required Documentation and Materials

As a requirement for the Evaluation, the Vendor must provide the appropriate documentation and software to the 3DS SDK Lab. All completed 3DS SDK related materials such as install media, manuals, the Vendor Release Agreement, the 3DS SDK Reference Number and all other materials related to the Evaluation and participation in the 3DS SDK Program must be delivered to the 3DS SDK Lab performing the Evaluation, not to PCI SSC.

Examples of software, documentation, and other items to submit to the 3DS SDK Lab include, but are not limited to:

1. The 3DS SDK (e.g., compiled software, source code, associated libraries if applicable, documentation, etc.)
2. The necessary hardware and software accessories to perform:
   - Simulated payment transactions
   - Operational support functions on the 3DS SDK
3. Documentation that describes all functions used for data input and output that can be used by third-party 3DS SDK users (i.e., customers or developers)—for example, applicable functions associated with capture, authorization, settlement, and chargeback flows;
4. Documentation that relates to installing and configuring the 3DS SDK, or which provides information about the 3DS SDK. Such documentation includes but is not limited to:
   - Software Installation Guide or Instructions (as provided to customers or developers);
   - Vendor's software versioning methodology for the 3DS SDK;
   - Vendor's Vulnerability Handling Policies; and
   - Change control documentation;

Note: *The 3DS SDK Lab may request additional material as necessary. The Vendor must work with the 3DS SDK Lab to work out how the testing will be accomplished, including use of any test harnesses.*

5. Additional documentation—such as diagrams and flowcharts—that will aid in the 3DS SDK review; and
6. The Vendor's executed VRA.

4.2 3DS SDK Review Timeframes

The amount of time necessary for a 3DS SDK Evaluation, from the start of an Evaluation to listing on the Website, can vary widely depending on factors such as:

- How close the 3DS SDK is to being compliant at the start of the Evaluation process: Modifications to the 3DS SDK will cause delays.
- Whether the 3DS SDK's documentation meets all 3DS SDK Requirements at the start of the Evaluation: Extensive documentation rewrites will cause delays.
- Prompt payment of the all applicable fees due to PCI SSC—PCI SSC will not commence review of the 3DS SDK ROV until all applicable fees have been received.
- Quality of the 3DS SDK Lab's submission to PCI SSC:
  - Incomplete or erroneous submissions—for example, missing or unsigned documents, incomplete or inconsistent submissions—will result in delays in the process.
  - If PCI SSC reviews the 3DS SDK ROV more than once, providing comments back to the 3DS SDK Lab to address each time, this will increase the length of time for the review process.

Evaluation timeframes provided by a 3DS SDK Lab should be considered estimates, since they may be based on the assumption that the 3DS SDK is able to successfully meet all 3DS SDK Requirements quickly. If problems are found during the review or acceptance processes, discussions between the 3DS SDK Lab, the Vendor, and/or PCI SSC may be required. Such discussions may significantly impact review times and cause delays and/or may even cause the review to end prematurely (for example, if the Vendor decides it does not want to make the necessary 3DS SDK changes to achieve compliance or it is determined that the 3DS SDK is not eligible for 3DS SDK Validation).

4.3 3DS SDK Lab Fees

The prices and fees charged by 3DS SDK Labs are negotiated between the 3DS SDK Lab and the Vendor.

4.4 Technical Support throughout Testing

To expedite the Evaluation process, it is recommended that the Vendor designate an individual with sufficient technical knowledge to act as a liaison throughout the review, providing assistance with any questions that may arise. The Vendor's designated contact should be on call to discuss issues and respond to questions from the 3DS SDK Lab.

4.5 3DS SDK Report on Validation

For each 3DS SDK Evaluation, the resulting report must follow the 3DS SDK Report on Validation (3DS SDK ROV) template and instructions, as outlined in the 3DS SDK ROV Template and 3DS SDK ROV Reporting Instructions.

The 3DS SDK Lab must prepare each 3DS SDK ROV based on evidence obtained by following the PCI 3DS SDK Security Standard.

Each 3DS SDK ROV must be accompanied by a 3DS SDK Attestation on Validation (3DS SDK AOV) in the form available through the Website, signed by a duly authorized officer of the 3DS SDK Lab, that summarizes whether the 3DS SDK is in compliance or is not in compliance with the PCI 3DS SDK Security Standard, and any related findings.

4.6 Vendor Release Agreement (VRA)

Among other things, the VRA covers confidentiality issues, the Vendor's agreement to 3DS SDK Program requirements, policies and procedures, and gives permission to the Vendor's 3DS SDK Lab to release 3DS SDK ROVs and related materials to PCI SSC for review. The VRA also requires Vendors to adopt and comply with industry standard Vulnerability Handling Policies.

At the beginning of each Evaluation process for each 3DS SDK, along with the 3DS SDK and other required documents and materials, the Vendor must submit to the 3DS SDK Lab a copy of the Vendor's signed Vendor Release Agreement on the then most current VRA form available on the Website.

The Vendor‘s signed copy of the then-current version of the VRA available on the Website must then be delivered directly to PCI SSC by the 3DS SDK Lab, along with the corresponding 3DS SDK ROV.

It should be noted that PCI SSC will not review any 3DS SDK ROV or update thereto without the then-current VRA on file from the relevant Vendor.

Accordingly, if the 3DS SDK Lab submits any 3DS SDK ROV or update to PCI SSC for a given Vendor, and at that time, the VRA last submitted to PCI SSC for that Vendor is not the then-current VRA form available on the Website, the 3DS SDK Lab must obtain from the Vendor and submit to PCI SSC a copy of the Vendor's signed VRA on the most current VRA form available on the Website.

So long as an executed current VRA is on file with the PCI SSC for the relevant Vendor, it is not required to re-submit the same VRA with each subsequent 3DS SDK ROV for the same Vendor.

4.7 PCI 3DS SDK Acceptance Fees

Vendors are also required to pay a 3DS SDK Acceptance Fee to PCI SSC. For each new 3DS SDK submission, the 3DS SDK Acceptance Fee will be invoiced and payment must be received by PCI SSC before the 3DS SDK submission will be reviewed, and if applicable, Accepted and added to the List of Validated 3DS SDKs. Upon Acceptance, PCI SSC will sign and return a copy of the 3DS SDK Attestation of Validation to both the Vendor and the 3DS SDK Lab.

Note: *The Vendor pays all 3DS SDK Evaluation-related fees directly to the 3DS SDK Lab (these fees are negotiated between the Vendor and the 3DS SDK Lab).*

PCI SSC will invoice the Vendor for all PCI 3DS SDK Acceptance Fees and the Vendor will pay these fees directly to PCI SSC.

There are no annual recurring PCI SSC fees associated with the Acceptance of a Validated 3DS SDK. There are however, PCI SSC fees associated with Vendor updates to Validated 3DS SDKs. Please see the Website for more information.

Program fees are nonrefundable and are subject to change upon posting of revised fees on the Website.

5 Managing a Validated 3DS SDK

Following a successful Evaluation, the 3DS SDK will be Validated for a period of two years from the date that the Evaluated version of the product was first Accepted.

Note: *PCI SSC reserves the right to withdraw Acceptance as indicated in Section 5.5.5.*

5.1 Changes to Listed 3DS SDKs

Vendors may update listed 3DS SDKs for various reasons. The table below provides a summary of the four types of change scenarios from a 3DS SDK perspective:

Change Type	Description
High Impact	Changes to the 3DS SDK where **any** of the following apply: ▪ Four or more 3DS SDK Requirements are affected; ▪ Half or more of all 3DS SDK Requirements/sub-Requirements are affected; ▪ Half or more of the 3DS SDK's functionality or half or more of its code-base is changed; **or** ▪ Addition of tested platform/operating system to include on the List of Validated 3DS SDKs. High Impact changes require the Vendor to submit the new version of the 3DS SDK for a full 3DS SDK Evaluation. *See Section 5.1.3.4, "High Impact Changes," for details.*
Low Impact	Changes to the 3DS SDK where **all** of the following conditions are met: ▪ Three or fewer 3DS SDK Requirements are affected; ▪ Less than half of all 3DS SDK Requirements/sub-Requirements are affected; **and** ▪ Less than half the 3DS SDK's functionality is affected and less than half the 3DS SDK's code-base is changed. Low Impact changes may be eligible for partial or "Delta" Evaluation. *See Section 5.1.3.3, "Low Impact Changes," for details.*
No Impact	Non-security-related changes that have no impact to PCI 3DS SDK Security Standard related functions, tested platforms, operating systems, or dependencies and no impact on any of the 3DS SDK Requirements. No Impact changes may be eligible for partial or "delta" Evaluation. *See Section 5.1.3.2, "No Impact Changes," for details.*
Administrative	Changes to the 3DS SDK listing or changes to how the 3DS SDK is described in the List of Validated 3DS SDKs, for example, corporate identity or 3DS SDK name changes. *See Section 5.1.3.1, "Administrative Changes," for details.*

Note: *While the 3DS SDK Vendor may choose to continue to support and/or release updates for expired 3DS SDK versions, PCI SSC does not list changes for expired 3DS SDKs.*

5.1.1 Wildcards

All 3DS SDK changes must result in a new 3DS SDK version number; however, whether this affects the version number listed on the Website depends on the nature of the change and the 3DS SDK Vendor's defined, documented versioning methodology. The use of wildcards may be permitted for managing the versioning methodology for No Impact changes only.

Note: *Wildcards may only be substituted for elements of the version number that represent non-security impacting changes; the use of wildcards for any change that has an impact on security or any of the 3DS SDK Requirements is prohibited.*

Only those applications that have had the Vendor's wildcard versioning methodology assessed and validated by a 3DS SDK Lab are eligible for wildcard usage and listing on the Website with wildcards. Vendors do not need to notify PCI SSC of changes falling within the scope of wildcard usage; therefore, any such changes will not result in an update to the 3DS SDK listing on the Website. See Appendix C, "3DS SDK Software Versioning Methodology," for additional information regarding the use of wildcards.

5.1.2 Delta Evaluations

It may not be necessary to fully reassess the entire 3DS SDK if a 3DS SDK Lab confirms the change has limited impact on the 3DS SDK. Low Impact and No Impact changes to listed 3DS SDKs may be eligible for partial re-Evaluation, or Delta Evaluation.

Note: *Only Low Impact and No Impact changes are eligible for Delta Evaluation.*

See 5.1.3, "Change Types," for additional information.

As part of the Delta Evaluation process, the entire 3DS SDK must be evaluated to determine which 3DS SDK Requirements are affected by the change. Delta Evaluations involve the 3DS SDK Lab assessing the changes documented in the Vendor Change Analysis against the applicable subset of 3DS SDK Requirements.

Delta Evaluations must:

- Be performed by the 3DS SDK Lab that performed the last full Evaluation and validation of the 3DS SDK;
- Include all 3DS SDK Requirements affected by the change;
- Include verification that all other 3DS SDK Requirements are not affected by the change;
- Include 3DS SDK functionality testing; and
- Be completed using the same major version of the PCI 3DS SDK Security Standard as used for the full validation.

Note: *It is strongly recommended that the Vendor uses the 3DS SDK Lab that performed the last full 3DS SDK Evaluation, as changing 3DS SDK Labs requires a full Evaluation.*

5.1.3 Change Types

Since the number of possible 3DS SDK changes and their impacts cannot be determined in advance, 3DS SDK changes must be assessed on a per-case basis. Vendors should contact the 3DS SDK Lab for guidance.

Note: *The determination of the type of change depends on the nature of the change and its impact on the 3DS SDK or 3DS SDK Requirements. Working with the Vendor, 3DS SDK Labs have an understanding of the 3DS SDK and are empowered to determine the change type that represents the proposed change.*

The Vendor prepares documentation of the change (Vendor Change Analysis) and submits the Vendor Change Analysis to the 3DS SDK Lab for review. The 3DS SDK Lab then determines whether a full Evaluation or Delta Evaluation of the 3DS SDK is required. This decision is based on the degree to which the changes impact the security and/or 3DS SDK related functions of the 3DS SDK, the impact to 3DS SDK Requirements and/or the scope of the changes being made. If the 3DS SDK Lab is unable to determine the applicable change type, the 3DS SDK Lab may consult with PCI SSC on an as-needed basis to determine if a change is too great to be eligible for Delta Evaluation.

The table below summarizes Delta Evaluation eligibility for the various change types.

Change Type	Wildcards	Evaluation Type
High Impact	Wildcard usage not permitted	Full Evaluation required
Low Impact	Wildcard usage not permitted	Eligible for Delta Evaluation
No Impact	Wildcard usage permitted	Eligible for Delta Evaluation
Administrative	N/A	N/A

The following sections provide details about each listed 3DS SDK change type, the supporting documentation that must be generated, and the processes to be followed in order to successfully effect changes to the validation of a listed 3DS SDK.

5.1.3.1 Administrative Changes

Administrative changes are limited to updates where no 3DS SDK changes have occurred but the Vendor wishes to request a change to the way the 3DS SDK is currently listed on the List of Validated 3DS SDKs on the Website. Administrative changes include, but are not limited to, changes to the 3DS SDK name or corporate entity name.

The Vendor prepares a Vendor Change Analysis and submits it to the 3DS SDK Lab for review.

If the 3DS SDK Lab agrees with the Vendor Change Analysis:

i. The 3DS SDK Lab must notify the Vendor that it agrees;

ii. The Vendor prepares and signs a 3DS SDK Attestation of Validation and sends it to the 3DS SDK Lab;

iii. If applicable, the Vendor completes a new Vendor Release Agreement;

iv. The 3DS SDK Lab completes the 3DS SDK Change Impact in Appendix B;

v. The 3DS SDK Lab signs the 3DS SDK Attestation of Validation to show that it concurs and forwards it, along with the 3DS SDK Change Impact document—and if applicable, new Vendor Release Agreement—to PCI SSC;

vi. PCI SSC will then issue an invoice to the Vendor for the applicable change fee; and

vii. Upon payment of the invoice PCI SSC will review the 3DS SDK Attestation of Validation and 3DS SDK Change Impact document for quality assurance purposes.

If the 3DS SDK Lab does not agree with the Vendor that the change, as documented in the Vendor Change Analysis, has no impact on any functions of the 3DS SDK, the 3DS SDK Lab returns the Vendor Change Analysis to the Vendor and works with the Vendor to consider the actions necessary to address the 3DS SDK Lab's observations.

Following a successful PCI SSC quality assurance review of the change, PCI SSC will:

i. Amend the List of Validated 3DS SDKs on the Website accordingly with the new information; and

ii. Sign and return a copy of the 3DS SDK Attestation of Validation to both the Vendor and the 3DS SDK Lab. The expiry date of the newly listed 3DS SDK and version number will be the same as that of the parent 3DS SDK.

For quality issues associated with any aspect of the submission, PCI SSC communicates those issues to the 3DS SDK Lab. PCI SSC reserves the right to reject any 3DS SDK Change Impact document if it determines that a change described therein and purported to be an Administrative Change by the 3DS SDK Lab or Vendor is ineligible for treatment as an Administrative Change.

5.1.3.2 No Impact Changes

No Impact changes are limited to changes that have no impact to 3DS SDK Requirements or 3DS SDK security, PCI 3DS SDK Security Standard related functions, tested platforms, operating systems, or dependencies. Examples of No Impact changes include, but are not limited to user-interface changes, database-schema modifications, updates to reporting modules, and changing/deleting payment gateways.

If the Vendor has chosen to use a wildcard versioning methodology for managing No Impact changes, the wildcard usage must adhere to the requirements in this Program Guide and be consistent with that documented as part of the Vendor's versioning methodology. Vendors do not need to notify PCI SSC of changes falling within the scope of wildcard usage, nor will such changes result in any update to the 3DS SDK listing on the Website.

Note: *Administrative and No Impact changes cannot be used to transition between major versions of standards. Major version changes to the Standard require a full Assessment.*

If the Vendor has chosen **not** to use a wildcard versioning methodology for managing No Impact changes, the Vendor prepares and submits a Vendor Change Analysis to the 3DS SDK Lab that performed the last full validation of the application.

The Vendor prepares and submits a Vendor Change Analysis to the 3DS SDK Lab that performed the last full validation of the 3DS SDK.

If the 3DS SDK Lab agrees that the change (as documented by the Vendor in the Vendor Change Analysis) meets the No Impact change criteria:

i. The 3DS SDK Lab must notify the Vendor that it agrees;

ii. The Vendor prepares and signs a 3DS SDK Attestation of Validation, and sends it to the 3DS SDK Lab;

iii. If applicable, the Vendor completes a new Vendor Release Agreement;

iv. The 3DS SDK Lab completes the 3DS SDK Change Impact template in Appendix B;

v. The 3DS SDK Lab signs the 3DS SDK Attestation of Validation to show that it concurs and forwards it, along with the 3DS SDK Change Impact document—and if applicable, new Vendor Release Agreement—to PCI SSC;

vi. PCI SSC issues an invoice to the Vendor for the applicable change fee; and

vii. Upon payment of the invoice, PCI SSC reviews the 3DS SDK Attestation of Validation and 3DS SDK Change Impact document for quality assurance purposes.

If the 3DS SDK Lab does not agree with the Vendor that the No Impact change (as documented in the Vendor Change Analysis) meets the No Impact change criteria, the 3DS SDK Lab will return the Vendor Change Analysis to the Vendor and work with the Vendor to consider the necessary actions to address the 3DS SDK Lab's observations.

Following a successful PCI SSC quality assurance review of the change PCI SSC will:

i. Amend the List of Validated 3DS SDKs on the Website accordingly with the new information; and

ii. Sign and return a copy of the 3DS SDK Attestation of Validation to both the Vendor and the 3DS SDK Lab. The expiry date of the newly listed 3DS SDK will be the same as that of the parent 3DS SDK.

For quality issues associated with any aspect of the submission, PCI SSC communicates those issues to the 3DS SDK Lab. PCI SSC reserves the right to reject any 3DS SDK Change Impact document if it determines that a change described therein and purported to be a No Impact change by the 3DS SDK Lab or Vendor is ineligible for treatment as a No Impact change.

5.1.3.3 Low Impact Changes

Low Impact changes are limited to changes to the 3DS SDK where all of the following conditions are met:

- Three or fewer high-level 3DS SDK Requirements are affected;
- Less than half of all 3DS SDK Requirements/sub-Requirements are affected; and
- Less than half the 3DS SDK's functionality is affected and less than half the 3DS SDK's code-base is changed.

Note: *It is strongly recommended that the Vendor uses the 3DS SDK Lab that performed the last full 3DS SDK Evaluation, as changing 3DS SDK Labs requires a full Evaluation.*

While Low Impact changes are not eligible for wildcard versioning, they are eligible for Delta Evaluation. Examples of Low Impact changes to PCI 3DS SDK Security Standard related functions of a Validated 3DS SDK include, but are not limited to:

- Inclusion of updates or patches to validated OS versions upon which the 3DS SDK was previously validated;
- Inclusion of updates or patches to supported third-party databases with which the 3DS SDK was previously validated;
- Additions or deletions of supported payment processors;
- Inclusion of updates or patches to supported middleware with which the 3DS SDK was previously validated;
- Recompilation of unchanged code base with either the same compiler using different flags or with a completely different compiler;
- Changes to the software versioning methodology for the 3DS SDK;
- Inclusion of non-security-related patches to the 3DS SDK.

Since the number of possible 3DS SDK changes and their impacts cannot be determined in advance, the type of Evaluation performed for Low Impact changes may be considered on a per-case basis. Vendors should contact the 3DS SDK Lab that performed the last full validation of the 3DS SDK for guidance. The 3DS SDK Lab determines whether a full Evaluation or Delta Evaluation of the 3DS SDK is required, based on the degree to which the changes impact the security and/or PCI 3DS SDK Security Standard related functions of the 3DS SDK, the impact to 3DS SDK Requirements and/or the scope of the changes being made.

The Vendor prepares and submits a Vendor Change Analysis (for example, using the 3DS SDK Change Impact document in Appendix B is acceptable) to the 3DS SDK Lab that performed the last full Evaluation of the 3DS SDK.

If the 3DS SDK Lab agrees that the change (as documented by the Vendor in the Vendor Change Analysis) meets the Low Impact change criteria and is eligible for a Delta Evaluation:

i. The 3DS SDK Lab must notify the Vendor that it agrees;

ii. The 3DS SDK Lab performs a delta review of the 3DS SDK for the 3DS SDK Requirements affected by the Low Impact change;

iii. The 3DS SDK Lab tests the 3DS SDK's functionality;

iv. The 3DS SDK Lab completes a 3DS SDK Change Impact document in Appendix B and makes redline changes to the original 3DS SDK ROV as appropriate;

v. The Vendor prepares and signs a 3DS SDK Attestation of Validation and sends it to the 3DS SDK Lab;

vi. If applicable, the Vendor completes a new Vendor Release Agreement;

vii. The 3DS SDK Lab signs the 3DS SDK Attestation of Validation to show that it concurs and forwards it, along with the "redline" version of the 3DS SDK ROV and the 3DS SDK Change Impact document (and if applicable, new Vendor Release Agreement) to PCI SSC;

viii. PCI SSC issues an invoice to the Vendor for the applicable change fee; and

ix. Upon payment of the invoice, PCI SSC will review the 3DS SDK Attestation of Validation, the "redline" version of the 3DS SDK ROV and the 3DS SDK Change Impact document for quality assurance purposes.

If the revision is deemed by the 3DS SDK Lab to be ineligible for Delta Evaluation, the 3DS SDK Lab returns the Vendor Change Analysis to the Vendor and works with the Vendor to consider what actions are necessary to address the 3DS SDK Lab's observations.

Following a successful PCI SSC quality assurance review of the change, PCI SSC will:

i. Amend the List of Validated 3DS SDKs on the Website accordingly with the new information; and
ii. Sign and return a copy of the 3DS SDK Attestation of Validation to both the Vendor and the 3DS SDK Lab. The expiry date of this newly listed 3DS SDK will be the same as that of the parent 3DS SDK.

For quality issues associated with any aspect of the submission, PCI SSC communicates those issues to the 3DS SDK Lab. PCI SSC reserves the right to reject any 3DS SDK Change Impact document if it determines that a change described therein and purported to be a Low Impact change by the 3DS SDK Lab or Vendor is ineligible for treatment as a Low Impact change.

5.1.3.4 High Impact Changes

Full Evaluation is required.

If changes to the 3DS SDK meet **any** of the following criteria, the 3DS SDK must undergo a full 3DS SDK Evaluation:

- Four or more high-level 3DS SDK Requirements are affected;
- Half or more of all 3DS SDK Requirements/sub-Requirements are affected;
- Half or more of the 3DS SDK's functionality is affected, or half or more of the 3DS SDK's code-base is changed;
- Addition of tested platform/operating system to include on the List of Validated 3DS SDKs; or
- The change is otherwise ineligible for treatment as a Low Impact change.

The 3DS SDK Lab will then submit a new 3DS SDK ROV (and if applicable, new Vendor Release Agreement) to PCI SSC for Acceptance. In this situation, the Vendor may first submit documentation of the change to the 3DS SDK Lab, who will determine whether the nature of the change impacts 3DS SDK security in accordance with current 3DS SDK Requirements.

5.2 Change Documentation

Administrative Change	No Impact Change	Low Impact Change	High Impact Change or New Application
▪ 3DS SDK Attestation of Validation ▪ 3DS SDK Change Impact document ▪ Vendor Release Agreement (one per Vendor) ▪ Fee	▪ 3DS SDK Attestation of Validation ▪ 3DS SDK Change Impact document ▪ Vendor Release Agreement (one per Vendor) ▪ Fee	▪ 3DS SDK Attestation of Validation ▪ 3DS SDK Change Impact document ▪ Report on Validation Redline ▪ Vendor Release Agreement (one per Vendor) ▪ Fee	▪ 3DS SDK Attestation of Validation ▪ Report on Validation ▪ Vendor Release Agreement (one per Vendor) ▪ Fee

***Note**: The 3DS SDK Change Impact document in Appendix B is mandatory for the 3DS SDK Lab for submitting Administrative, No Impact, and Low Impact changes to PCI SSC but may also be used by Vendors as a Vendor Change Analysis.*

5.3 Renewing Expiring Applications

As a 3DS SDK approaches its expiration date, PCI SSC will notify the Vendor of the pending expiration. The two options available for Vendor consideration are either new validation or expiry:

New Validation: If the Vendor wishes to renew the 3DS SDK validation, the Vendor must contact a 3DS SDK Lab to have the 3DS SDK fully re-evaluated against the then-current version of the PCI 3DS SDK Security Standard. Use of the Low/No Impact or Administrative Change process to achieve this goal is not permitted.

Expiry: In all other situations where the Vendor fails to resubmit the 3DS SDK for full Evaluation by the expiry date, PCI SSC will show the validation as expired.

5.4 Validation Maintenance Fees

If a listed 3DS SDK is revised, the Vendor is required to pay the applicable change fee to PCI SSC.

For any change affecting the listing of a Validated 3DS SDK, the applicable fee will be invoiced and must be received by PCI SSC for the changes to be Accepted and added to the List of Validated 3DS SDKs. Upon Acceptance, PCI SSC will sign and return a copy of the 3DS SDK Attestation of Validation to both the Vendor and the 3DS SDK Lab.

There is no PCI SSC fee associated with the processing of Annual Revalidations.

***Note:** The Vendor pays all 3DS SDK Evaluation-related fees directly to the 3DS SDK Lab (these fees are negotiated between the Vendor and the 3DS SDK Lab).*

PCI SSC will invoice the Vendor for all validation maintenance fees and the Vendor will pay these fees directly to PCI SSC.

All 3DS SDK Program fees are posted on the Website. Program fees are non-refundable and are subject to change upon posting of revised fees on the Website.

5.5 Notification Following a Security Breach, Compromise, or Known or Suspected Vulnerability

In the event of a Security Issue (defined in the VRA) relating to a 3DS SDK, the VRA requires the applicable 3DS SDK Vendor to notify PCI SSC.

5.5.1 Notification and Timing

Notwithstanding any other legal obligations, pursuant to the VRA, the 3DS SDK Vendors are required to notify PCI SSC of all such Security Issues within the period of time specified in the VRA, including the related information pursuant to the VRA, and to provide follow-up information which may include (without limitation) an assessment of any impact (possible or actual) that the Security Issue has had or may or will have.

5.5.2 Notification Format

The Vendor‘s formal notification to PCI SSC must be in writing in accordance with the Vendor Release Agreement, and should be preceded by a phone call to the 3DS SDK Program Manager at +1 (781) 876-8855.

5.5.3 Notification Details

As part of the Vendor‘s initial notification to PCI SSC, the Vendor must supply the PCI SSC 3DS SDK Program Manager with the information required by the Vendor Release Agreement. At a minimum, this must include:

- The name, PCI SSC reference number, and any other relevant identifiers of the 3DS SDK;
- A description of the general nature of the Security Issue;
- The Vendor’s good-faith Evaluation, to its knowledge at the time, as to the scope and severity of the vulnerability or vulnerabilities associated with the Security Issue (using CVSS or other industry accepted standard scoring);
- Assurance that the Vendor is following its Incident Response and Vulnerability Handling Policies.

5.5.4 Actions following a Security Breach or Compromise

In the event of PCI SSC being made aware of a Security Issue related to a Validated 3DS SDK, PCI SSC may take the actions specified in the VRA and additionally, may:

- Notify Participating Payment Brands that a Security Issue has occurred.
- Request a copy of the latest version of the Vendor’s Vulnerability Handling Policies.
- Communicate with the Vendor about the Security Issue and, where possible, share information relating to the Security Issue.
- Support the Vendor‘s efforts to mitigate or prevent further Security Issues.
- Support the Vendor‘s efforts to correct any Security Issues.
- Work with the Vendor to communicate and cooperate with appropriate law enforcement agencies to help mitigate or prevent further Security Issues.

5.5.5 Withdrawal of Acceptance

PCI SSC reserves the right to suspend, withdraw, revoke, cancel, or place conditions upon its Acceptance of (and accordingly, remove from the List of Validated 3DS SDKs) any listed 3DS SDK in accordance with the VRA, in instances including, but not limited to, if PCI SSC reasonably determines that (a) the 3DS SDK does not offer sufficient protection against current threats and does not conform to 3DS SDK Requirements, or (b) the continued Acceptance of the 3DS SDK represents a significant and imminent security threat to its users, or (c) the 3DS SDK is subject to a Security Issue.

6 3DS SDK Evaluation Reporting Considerations

6.1 PCI 3DS SDK Security Standard Report Acceptance Process Overview

The 3DS SDK Lab performs the Evaluation in accordance with the PCI 3DS SDK Security Standard and produces a 3DS SDK ROV that is shared with the Vendor. When the 3DS SDK ROV has all items in place, the 3DS SDK Lab submits the 3DS SDK ROV and all other required materials to PCI SSC. If the 3DS SDK ROV does not have all items in place, the Vendor must address those items, and the 3DS SDK Lab must update the 3DS SDK ROV prior to submission to PCI SSC. For example, this may include updating user documentation or software. Once the 3DS SDK Lab is satisfied that all documented issues have been resolved by the Vendor, the 3DS SDK Lab submits the 3DS SDK ROV and all other required materials to PCI SSC.

Note: *All 3DS SDK ROVs and other materials must be submitted to PCI SSC in English or with certified English translation .*

Once PCI SSC receives the 3DS SDK ROV and all other required materials and applicable fees, PCI SSC reviews the 3DS SDK ROV from a quality assurance perspective, typically within 30 calendar days of payment of invoice, and determines whether it is acceptable. Subsequent iterations will also be responded to, typically within 30 calendar days of receipt. If the 3DS SDK ROV meets all applicable quality assurance requirements (as documented in the 3DS SDK Program Guide and related program materials), PCI SSC sends a countersigned 3DS SDK Attestation of Validation to both the Vendor and the 3DS SDK Lab and adds the 3DS SDK to the List of Validated 3DS SDKs.

Note*: It is common for submissions to require several iterations before the 3DS SDK is Accepted. Adequate QA review of the submission as part of the 3DS SDK Lab's internal QA process will help minimize the number of iterations required. Each iteration will be responded to typically within 30 days from the time that iteration was received in the Portal*

PCI SSC communicates any quality issues associated with 3DS SDK ROVs to the 3DS SDK Lab. It is the responsibility of the 3DS SDK Lab to resolve the issues with PCI SSC and/or the Vendor, as applicable. Such issues may be limited or more extensive; limited issues may simply require updating the 3DS SDK ROV to reflect adequate documentation to support the 3DS SDK Lab's decisions, whereas more extensive issues may require the 3DS SDK Lab to perform further testing, requiring the 3DS SDK Lab to notify the Vendor that re-testing is needed and to schedule that testing with the Vendor.

3DS SDK ROVs that have been returned to the 3DS SDK Lab for correction must be resubmitted to the PCI SSC within 30 days of the preceding submittal. If this is not possible, the 3DS SDK Lab must inform the PCI SSC of the timeline for response. Lack of response on 3DS SDK ROVs returned to the 3DS SDK Lab for correction may result in the submission being closed. Submissions that have been closed will not be reopened and must be resubmitted as if they are new 3DS SDK ROV submissions.

6.2 Delivery of the 3DS SDK ROV and Related Materials

All documents required in connection with the 3DS SDK Evaluation process must be submitted to PCI SSC by the 3DS SDK Lab, through a secure submissions web portal designated by PCI SSC (the "Portal"). PCI SSC staff pre-screen Portal submissions to ensure that all required documentation has been included and the basic submission requirements have been satisfied.

There must be consistency between the information in documents submitted for review via the Portal and the "Details" fields within the Portal. Common errors in submissions include inconsistent 3DS SDK names or contact information, incomplete or inconsistent documentation, insufficient explanation of 3DS SDK dependencies, and insufficient explanation of tested platforms/operating systems. Incomplete or inconsistent submissions may result in a significant delay in the processing of requests for listing and/or may not be Accepted for review by the PCI SSC.

6.2.1 Access to the Portal

Once an entity is qualified as a 3DS SDK Lab, PCI SSC will send login credentials and instructions for use of the Portal to the company's Primary Contact. Additional credentials can be requested by each 3DS SDK Lab's primary contact through PCI SSC's 3DS SDK Program Manager.

6.2.2 Listing Information

The listing on the List of Validated 3DS SDKs will contain, at minimum, the information specified below. Each characteristic is detailed in Appendix A, "Elements for the 3DS SDK Attestation of Validation and the List of Validated 3DS SDKs."

- 3DS SDK Vendor
- 3DS SDK Identifier
  - 3DS SDK Name
  - 3DS SDK Version Number
  - Application Type
  - Target Market, if applicable
  - Reference Number
  - Description Provided by Vendor
  - Tested Platforms/Operating Systems
  - Required dependencies
  - Validation Notes (PCI 3DS SDK Security Standard version)
  - Deployment Notes
  - Revalidation Date
  - Expiry Date
  - 3DS SDK Lab

Note: *All descriptions must be acceptable to PCI SSC, which reserves the right to modify any description at any time .*

7 Legal Terms and Conditions

Acceptance of a given 3DS SDK by the PCI Security Standards Council LLC (PCI SSC) only applies to the specific version (or eligible wildcard) of that 3DS SDK that was reviewed by a 3DS SDK Lab and subsequently accepted by PCI SSC (the Accepted Version). If any aspect of a 3DS SDK or version thereof is different from the Accepted Version—even if the different 3DS SDK or version (the Alternate Version) conforms to the basic product description of the Accepted Version—the Alternate Version should not be considered Accepted by PCI SSC, nor promoted as Accepted by PCI SSC.

No Vendor or other third party may refer to a 3DS SDK as "PCI Approved" or "PCI SSC Accepted," nor otherwise state or imply that PCI SSC has, in whole or part, approved any aspect of a Vendor or its 3DS SDKs, except that to the extent PCI SSC has actually issued an 3DS SDK Attestation of Validation with respect to the Approved Version of a 3DS SDK, such Approved Version may be referred to as PCI SSC Accepted or listed. All other references to PCI SSC's Acceptance or approval of a 3DS SDK or version thereof are strictly and actively prohibited by PCI SSC.

PCI SSC Acceptance signifies that (i) a 3DS SDK Lab has determined that the Accepted Version of a 3DS SDK complies with the PCI 3DS SDK Security Standard and therefore implements certain security and operational characteristics important to the achievement of PCI SSC's goals; and (ii) the corresponding 3DS SDK ROV has successfully completed AQM review.

Acceptance does not under any circumstances include or imply any endorsement or warranty by PCI SSC or any Participating Payment Brand regarding the 3DS SDK Vendor or the functionality, quality, or performance of the 3DS SDK or any other product or service. PCI SSC does not warrant any products or services provided by third parties. PCI SSC Acceptance does not, under any circumstances, include or imply any product warranties from PCI SSC, including, without limitation, any implied warranties of merchantability, fitness for purpose or non-infringement, all of which are expressly disclaimed by PCI SSC. All rights and remedies regarding products and services that have been Accepted by PCI SSC, shall be provided, if at all, by the party providing such products or services, and not by PCI SSC or any Participating Payment Brand.

Appendix A: Elements for the 3DS SDK Attestation of Validation and List of Validated 3DS SDKs

A.1 3DS SDK Vendor

This entry denotes the **3DS SDK Vendor** for the Validated 3DS SDK.

A.2 3DS SDK Identifier

The **3DS SDK Identifier** is used to denote relevant information for each Validated 3DS SDK, consisting of the following fields (fields are explained in detail below):

- 3DS SDK Name
- 3DS SDK Version #
- Target Market, if applicable
- PCI SSC Assigned Reference Number

Example of an 3DS SDK Identifier:

Component	Description
3DS SDK Name	Acme Payment 600
3DS SDK Version #	PCI 4.53.x
Target Market	(None noted)
Reference #	09-01.00111.001

3DS SDK Identifier: Detail

- **3DS SDK Name**

  3DS SDK Name is provided by the Vendor and is the name by which the 3DS SDK is sold. The 3DS SDK Name cannot contain any variable characters.

  The PCI SSC's various Program names and/or acronyms (e.g., PCI DSS, PCI 3DS SDK Security Standard, PTS, etc.) are strictly prohibited from use in Vendor 3DS SDK Names. PCI SSC reserves the right to reject any 3DS SDK of which any such Program name or acronym is a part.

- **3DS SDK Version #**

  3DS SDK Version # represents the 3DS SDK version reviewed in the 3DS SDK Evaluation. The format of the version number:

  – Is set by the Vendor;

  – May consist of alphanumeric characters and;

  – Must be consistent with the Vendor's versioning methodology for this product.

- **Reference Number**

  PCI SSC assigns the Reference Number once the 3DS SDK is posted to the Website; this number is unique per Vendor and will remain the same for the life of the 3DS SDK's listing.

  An example reference number is 08-XX.XXXXX.XXX.AAA, consisting of the following:

Field	Format
Year of listing	2 digits + hyphen
3DS SDK Type (see above)	2 digits + period
Vendor #	5 digits + period (assigned alphabetically initially, then as received)
Vendor App #	3 digits + period (assigned as received)
Minor change reference	3 alpha characters (assigned as received)

A.3 Description Provided by Vendor

This section allows for the submission of a description of the 3DS SDK that is to be used in the List of Validated 3DS SDKs, should the 3DS SDK ROV be Accepted. This must be a factual description of the 3DS SDK functionality and, optionally, the target market. The description must not:

- Contradict any PCI SSC program or requirement—e.g., the 3DS SDK must not claim to store sensitive authentication data after authorization.
- Make misleading claims about the 3DS SDK—e.g., that usage of the 3DS SDK reduces the scope of a PCI DSS Evaluation.
- Claim the 3DS SDK is valid under another PCI SSC program or standard.

PCI SSC recommends keeping the description concise and including only pertinent information about the 3DS SDK.

All descriptions must be acceptable to PCI SSC, which reserves the right to modify any description at any time.

A.4 Tested Platforms/Operating Systems

Identify the specific operating system type and version and any other platform components on which the 3DS SDK was tested.

Only the specific operating systems and platforms on which the 3DS SDK was tested will be listed on the Website.

A.5 Evaluation Notes

Evaluation Notes are used by PCI SSC to denote what standard, and the specific version thereof, was used to assess the compliance of a Validated 3DS SDK. Please see table under Expiry Date below for examples.

A.6 Deployment Notes

Deployment Notes are used by PCI SSC to denote the scenarios in which Validated 3DS SDKs are recommended for use. Assigned deployment notes are determined by the Vendor's active participation in annual revalidation, whether or not the particular version of the 3DS SDK is still being supported by the Vendor, or by the 3DS SDK's Expiration Date (noted below).

Validated 3DS SDKs are denoted with one of the following Deployment Notes:

- **Acceptable for New Deployments:** All newly Accepted Validated 3DS SDKs are initially put into this state and will maintain this state until such time that either (i) annual revalidation requirements are not maintained by the Vendor causing an early administrative expiry; or (ii) the Validated 3DS SDK expires as a matter of course based on the version of the PCI 3DS SDK Security Standard under which it was validated.
- **Acceptable only for Pre-Existing Deployments:** This deployment note is assigned to Validated 3DS SDKs where either (i) annual revalidation requirements are not maintained by the Vendor causing an early administrative expiry; or (ii) the Validated 3DS SDK expires as a matter of course based on the version of the PCI 3DS SDK Security Standard under which it was validated. Questions about continued use of Validated 3DS SDKs that have expired should be referred to the Participating Payment Brand.

These deployment notes are used by PCI SSC to note the status of a Validated 3DS SDK in relation to its Expiry Date. See table under "Expiry Date" below for examples.

Please refer to specific Participating Payment Brand requirements for usage of Validated 3DS SDKs.

A.7 Revalidation Date

The **Revalidation Date** is used by PCI SSC to indicate when the Vendor's annual 3DS SDK Attestation of Validation is due. The Annual Revalidation is part of the 3DS SDK Attestation of Validation form.

A.8 Expiry Date

The **Expiry Date** for a Validated 3DS SDK is the date by which the Vendor must have the 3DS SDK re-evaluated against the current 3DS SDK Requirements in order to maintain the acceptance. The Expiry Date is related to the Deployment Notes, noted above.

Participating Payment Brands have their own compliance programs for the usage of Validated 3DS SDKs. Questions on how using a 3DS SDK listed as Acceptable only for Pre-Existing Deployments affects PCI DSS compliance must be addressed to the merchant's acquirer and/or the Participating Payment Brands involved.

Validation Notes	Expiry Date	Deployment Notes	Annual Revalidation Required
Validated According to PCI 3DS SDK Security Standard vX			

A.9 3DS SDK Lab

This entry denotes the name of the 3DS SDK Lab that performed the Evaluation and determined that the 3DS SDK is compliant with PCI 3DS SDK Security Standard.

Appendix B: 3DS SDK Change Impact

Administrative, No Impact (if a validated wildcard versioning methodology is not used), and Low Impact changes to Validated 3DS SDKs must be disclosed in this 3DS SDK Change Impact document. Note that all High Impact changes require a full 3DS SDK Evaluation.

A 3DS SDK Lab must complete each section of this document, and all required documents based on the type of change (see "Required Documents" section below). The 3DS SDK Lab is required to submit this 3DS SDK Change Impact along with supporting documentation to PCI SSC for review.

Always refer to the applicable 3DS SDK Program Guide for information on 3DS SDK changes.

3DS SDK Details				
Name of 3DS SDK		Application Version		
Validation PCI 3DS SDK Security Standard		Validated Listing Reference #		
Submission Date				
Type of Change (please check)	☐ Administrative	☐ No Impact	☐ Low Impact	☐ High Impact

3DS SDK Vendor Contact Information			
Contact Name		Title/Role	
Contact E-mail		Contact Phone	

3DS SDK Lab Contact Information			
Contact Name		Title/Role	
Contact E-mail		Contact Phone	

3DS SDK Lab QA Contact Information			
Contact Name		Title/Role	
Contact E-mail		Contact Phone	

Change Revision			
Revised Company Name (if applicable)			
Revised Application Name (if applicable)		Revised Application Version	

Required Documents (indicated with an "x")					
Type of Change	**3DS SDK Attestation of Validation (AOV)**	**3DS SDK Change Impact**	**Red-lined ROV**	**Report on Validation (ROV)**	**Vendor Release Agreement (VRA)**
Administrative Change	X	X			*
No Impact Change	X	X			*
Low Impact Change	X	X	X		*
High Impact Change	X			X	*

* If applicable

3DS SDK Change Impact Details

For **each** change, provide the following information. Any that impact 3DS SDK Requirements must be reflected in the Redline 3DS SDK ROV submitted. Use additional pages if needed.

Indicate which 3DS SDK Requirements are impacted by the change:													
☐ 1	☐ 2	☐ 3	☐ 4	☐ 5	☐ 6	☐ 7	☐ 8	☐ 9	☐ 10	☐ 11	☐ 12	☐ 13	☐ 14

If any 3DS SDK Requirements were excluded from the Evaluation, provide a description of the testing performed to validate that excluded 3DS SDK Requirements **are not** impacted (for example, comparing code, Vendor Change Analysis, details from developer interviews, details from functionality testing, etc.):

Change Number	Detailed description of the change	Description of why the change is necessary	Description of how CHD is impacted	Description of how the change impacts 3DS SDK

Appendix C: 3DS SDK Software Versioning Methodology

Vendors are required to document and follow a software versioning methodology as part of their 3DS SDK development lifecycle. Additionally, Vendors must communicate the versioning methodology to their customers and resellers. Customers and resellers require this information to understand which version of the 3DS SDK they are using and the types of changes that have been made to each version of the 3DS SDK. 3DS SDK Labs are required to verify that the Vendor is adhering to the documented versioning methodology as part of the 3DS SDK Evaluation.

Note: *If a separate version-numbering scheme is maintained internally by the Vendor, a method to accurately map the internal version numbers to the publicly listed version number(s) must be documented and maintained by the Vendor.*

C.1 Version Number Format

The format of the 3DS SDK version number is set by the Vendor and may be comprised of several elements. The versioning methodology must fully describe the format of the 3DS SDK version number including the following:

- The format of the version scheme, including:
  - Number of elements
  - Numbers of digits used for each element
  - Format of separators used between elements
  - Character set used for each element (consisting of alphabetic, numeric, and/or alphanumeric characters)
- The hierarchy of the elements
  - Definition of what each element represents in the version scheme
  - Type of change: major, minor, maintenance release, wildcard, etc.
- The definition of elements that indicate any use of wildcards
- The specific details of how wildcards are used in the versioning methodology

C.2 Version Number Usage

All changes to the 3DS SDK must result in a new version number. However, whether this affects the version number listed on the Website depends on the nature of the change and the Vendor's published versioning methodology (see Section C.3, "Wildcards," below). All changes that impact security functionality and/or any 3DS SDK Requirements must result in a change to the version number listed on the Website; wildcards are not permitted for changes impacting security functionality and/or any 3DS SDK Requirements.

The Vendor must document how elements of the application version number are used to identify:

- Types of changes made to the 3DS SDK—e.g., major release, minor release, maintenance release, wildcard, etc.
- Changes that have no impact on the functionality of the 3DS SDK or its dependencies

- Changes that have impact on the 3DS SDK functionality but no impact on security or 3DS SDK Requirements
- Changes that impact any security functionality or 3DS SDK Requirement

Elements of the version number used for non-security-impacting changes must never be used for security-impacting changes.

If the Vendor uses a versioning scheme that involves mapping of internal version numbers to external, published version numbers, all security-impacting changes must result in an update to the external, published version number.

Vendors must ensure traceability between 3DS SDK changes and version numbers such that a customer or reseller may determine which changes are included in the specific version of the 3DS SDK they are running.

C.3 Wildcards

A "wildcard" element is a variable character that may be substituted for a defined subset of possible characters in an application versioning scheme. In the context of 3DS SDK, wildcards can optionally be used to represent non-security-impacting changes between each version represented by the wildcard element. A wildcard is the only variable element of the Vendor's version scheme. Use of a wildcard element in the versioning scheme is optional and is not required in order for the 3DS SDK to be validated. The use of wildcard elements is permitted subject to the following:

a. Wildcard elements may only be used for No Impact changes, which have no impact on security and/or any 3DS SDK Requirements.
b. The use of wildcard elements is limited to the rightmost (least significant) portion of the version number. For example, 1.1.x represents acceptable usage. A version methodology that includes a wildcard element followed by a non-wildcard element is not permitted. For example, 1.x.1 and 1.1.y.1 represent usage that is not permitted.
c. All security-impacting changes must result in a change to the non-wildcard portion of the application version number and will therefore result in an update to the version number listed on the Website.
d. Wildcard elements must not precede version elements that could represent security-impacting changes; version elements reflecting a security-impacting change must appear "to the left of" the first wildcard element.
e. All wildcard usage must be pre-defined and documented in the Vendor's versioning methodology.
f. All wildcard usage must be consistent with that validated by the 3DS SDK Lab as part of the 3DS SDK Evaluation.