Payment Card Industry

3-D Secure SDK (PCI 3DS SDK)

Template for Report on Validation

for use with PCI 3DS SDK Security Standard v1.1

Revision 1.0

February 2019

Document Changes

Date	Version	Description
February 2019	Revision 1.0	Initial release of template for submitting Reports on Validation for the PCI 3DS SDK Program. This document is intended for use with Version 1.1 of the *PCI 3DS Security Requirements and Assessment Procedures for EMV® 3-D Secure SDK* (PCI 3DS SDK Security Standard).

Table of Contents

Introduction to the PCI 3DS SDK Report on Validation (ROV) Template

This document, the *PCI 3-D Secure SDK Report on Validation Template* (hereafter referred to as the PCI 3DS SDK ROV Template), is required for completing a Report on Validation (ROV) for assessments against the *PCI 3DS Security Requirements and Assessment Procedures for EMV® 3-D Secure SDK,* v1.1 (PCI 3DS SDK Security Standard v1.1). This ROV Template provides reporting instructions and the template form for PCI 3DS SDK Labs to deliver a consistent level of reporting.

Note: Use of this Reporting Template is mandatory for all PCI 3DS SDK submissions.

When a PCI 3DS SDK Lab (Lab) performs an evaluation against the PCI 3DS SDK Security Standard, it must provide a detailed account of the results of the work performed. A PCI 3DS SDK evaluation involves thorough testing and assessment activities, from which the Lab will generate detailed work papers. These work papers hold comprehensive records of the assessment activities, including observations, results of system testing, configuration data, file lists, interview notes, documentation excerpts, references, screenshots, and other evidence collected during the evaluation. The ROV is a summary of evidence derived from the Lab's work papers to describe how the Lab performed the validation activities and how the resultant findings were reached. When completed, the ROV provides a comprehensive summary of testing activities performed and information collected during an evaluation against the PCI 3DS SDK Security Standard v1.1. The information contained in a ROV must provide enough detail and coverage to verify that the 3DS SDK is compliant with all PCI 3DS SDK Security Standard requirements.

This template should be used in conjunction with the following documents, available on the PCI SSC Website.

- PCI 3DS SDK Security Standard v1.1
- PCI 3DS SDK Program Guide
- PCI 3DS SDK Attestation of Compliance

Using the ROV Template

All sections and content contained in this ROV Template, including the introduction sections, must remain intact. The directions provided herein allow recipients of the report to understand the context of responses and conclusions made.

Tables have been included in this template to facilitate the reporting process. These tables may be modified to increase/decrease the number of rows or to change column width to ensure all information can be included. However, the Lab must not remove any details from the tables provided in this document. Additional appendices may be added if the Lab feels there is material relevant to the PCI 3DS SDK evaluation that does not fit within the current template format. Personalization, such as the addition of company logos, is acceptable.

ROV Template Structure

The ROV Template is organized into the following sections and appendices:

- Section 1: Contact Information and Report Date
- Section 2: 3DS SDK Information
- Section 3: 3DS SDK Diagrams
- Section 4: Evaluation Overview
- Section 5: Evaluation Results Summary
- Section 6: Findings and Observations
- Appendix A: Explanation of Non-Applicability
- Appendix B: Additional Information to Summary of Evaluation Findings

Completing the ROV

Sections 1–6 of the ROV Template **must** all be thoroughly and accurately completed. Sections 1–4 provide the context necessary for the reader to interpret the information contained in Sections 5 and 6. The appendices are used for the addition of supportive information as applicable (see the "Using Appendices" section for more information).

The ROV Template contains instructions to help ensure that Labs supply all required information for each section. All responses should be entered in the applicable location or table provided in the template. Responses should be specific, but efficient. Details provided should focus on the quality of detail, rather than lengthy, repeated text.

Completing the Findings and Observations Section

There are three main columns within the Findings and Observation section:

- 3DS SDK Security Requirements and Assessment Procedures
- Reporting Instructions
- Summary of Evaluation Findings

The first two columns are informational. The Summary of Evaluation Findings column is used to record the status of each requirement, and to document the Lab's responses to each reporting instruction. All responses must be supported by the documented findings and be consistent with other reporting documentation, such as the Attestation of Validation (AOV).

Summary of Evaluation Findings

Table 1 below provides an example of how the Findings and Observations section is structured. Within the Summary of Evaluation Findings column for each requirement, there is a choice of responses to indicate whether that requirement is "In Place," "Not Applicable (N/A)," or "Not in Place." Only one response must be selected for each requirement. To select a response, click on the applicable checkbox. Click once to mark with an "X." To remove a mark, click the box again.

Table 1: Example Requirement

Security Objective X: Objective Description				
3DS SDK Security Requirements and Assessment Procedures	**Reporting Instructions**	**Summary of Evaluation Findings**		
Requirement 1: Requirement Description				
1.1 Requirement Name Requirement text		**In Place** ☐	**N/A** ☐	**Not in Place** ☐
T.1.1.1 Assessment Procedure	Reporting Instruction	*<Report findings here>*		
	Reporting Instruction	*<Report findings here>*		
T.1.1.2 Assessment Procedure	Reporting Instruction	*<Report findings here>*		
	Reporting Instruction	*<Report findings here>*		

To determine the appropriate Summary of Evaluation Findings response for a given requirement, refer to Table 2 below.

Table 2: Response Selection for Example Requirement

Response	When to use this response	Example Requirement
In Place	When all expected testing has been performed, and all elements of the requirement have been met as stated.	In the Table 1 example, the Summary of Evaluation Findings for Requirement 1.1 is "In Place" if the results of Assessment Procedures T.1.1.1 and T.1.1.2 conclude that all aspects of the requirement are in place or are a combination of in place and not applicable.
Not in Place	Some or all elements of the requirement have not been met, or are in the process of being implemented, or require further testing before it will be known whether they are in place.	In the Table 1 example, the Summary of Evaluation Findings for Requirement 1.1 is "Not in Place" if the results of either T.1.1.1 or T.1.1.2 conclude that any aspect of the requirement is not in place.
N/A (Not Applicable)	The requirement does not apply to the 3DS SDK under evaluation. All "Not Applicable" responses require a detailed explanation of how it was determined that the requirement does not apply. (Refer to Appendix A.) A requirement is applicable if any aspect of the requirement applies to the software being evaluated. A "Not Applicable" designation in the Summary of Assessment Findings should not be used in this scenario.	In the Table 1 example, the Summary of Evaluation Findings for Requirement 1.1 is "Not Applicable" if all aspects of the requirement are concluded to be "not applicable" to the 3DS SDK under evaluation.

Understanding Reporting Instructions

In addition to specifying whether a requirement is "In Place," "N/A," or "Not in Place" under the Summary of Evaluation Findings column, the Lab must also document its findings for each assessment procedure. One or more reporting instructions are provided for each assessment procedure. Responses are required for all reporting instructions except where explicitly indicated within the instruction.

Responses should not repeat the requirement, assessment procedure, or the reporting instruction. As noted earlier, responses should be specific and efficient. The response should be focused on quality of detail provided, rather than unnecessary or repeated verbiage.

To provide consistency in how Labs document their findings, the Reporting Instructions use standardized terms. Those terms and the context in which they should be interpreted is provided in Table 3.

Table 3: Reporting Instruction Terms and Response Formats

Reporting Instruction Term	Example Usage	Description of Response
Describe	Describe the protections implemented to protect each data element against extraction or determination.	The response would include a detailed summary of the item or activity in question—for example, details of an implemented procedure or a method used to meet a security objective. The response should be of sufficient detail to provide the reader with a comprehensive understanding of the item or activity being described. For example, describing a procedure would include a summary of all the steps that are followed. Similarly, describing a security control or protection would include information about what is implemented, what it does, and how it meets its purpose.
Explain	Explain why the features are reasonable to prevent compromise of the 3DS SDK security.	The response would include a detailed rationale for the tester's action or finding—for example, to justify why a particular test was deemed appropriate or a particular control deemed sufficient to meet a requirement.
Identify	Identify the vendor materials, evidence, and source code files examined.	The response would be a brief overview or descriptive list of the applicable items—for example, the titles of documents that were examined, a list of vulnerabilities that were tested, or the names and job titles of individuals who were interviewed. ***Note:*** *Where the response includes identifying documents or individuals, the Lab may choose to enter the document name or interviewee name and job title in the Summary of Evaluation Findings column or enter the reference number that corresponds with the document/interviewee listed in the appropriate summary table in Section 4 of the ROV.*
Indicate	Indicate whether features are provided by the 3DS SDK to check that the 3DS Requestor App is installed from a trusted app store. (Yes/No)	The response would be either Yes or No. ***Note:*** *The applicability of some reporting instructions may be dependent on the response to an earlier instruction. For example, a response of "Yes" to a question about SDK functionality may result in further details being requested about that particular functionality. If applicable, the reporting instruction will direct the Lab to a subsequent instruction based on the Yes/No answer.*

While it is expected that a Lab will perform all Assessment Procedures identified for each requirement, it may also be possible for a requirement to be validated using different or additional assessment procedures. In such cases, the Lab should describe in the Summary of Evaluation Findings column why assessment procedures that differ from those identified in the PCI 3DS SDK Security Standard were used, and explain how those assessment procedures provide at least the same level of assurance as would have been achieved using the defined assessment procedures.

Sampling

Where appropriate, Labs may utilize sampling as part of the testing process. Samples must be representative of the total population. The sample size must be sufficiently large and diverse to provide assurance that the selected sample accurately reflects the overall population, and that any resultant findings based on a sample are an accurate representation of the whole. In all instances where the Lab's finding is based on a representative sample rather than the complete set of applicable items, the Lab should explicitly note this fact, identify the items chosen as samples for the testing, and explain the sampling methodology used.

If sampling is used, the Lab may either choose to utilize the Sampling section (Section 4) of the ROV Template or list out the items from the sample within the individual reporting instruction response. If sampling is not used, then the types of components that were tested must still be identified in Section 6, "Findings and Observations." This may be accomplished by either using Sample Set Reference numbers or by listing the tested items individually in the response.

Using Appendices

The ROV template includes two appendices for the addition of supportive information. Appendix A must be used if a finding of "N/A" (Not Applicable) has been selected for any given requirement to explain how it was determined that the related requirement is not applicable. Appendix B can be used to add extra information that supports the evaluation findings if that information is too large to include in the Summary of Evaluation Findings column. Extra appendices can be added if there is material relevant to the PCI 3DS SDK security assessment that does not fit within the current template format.

Appendix A: Explanation of Non-Applicability

If the "N/A" (Not Applicable) option is selected for any requirement, use Appendix A to explain why the requirement is not applicable. In the Findings and Observation section, document in the Summary of Evaluation Findings column for the applicable reporting instruction(s) that the explanation of non-applicability is detailed in Appendix A. Any information recorded in Appendix A should reference back to the applicable PCI 3DS SDK Security Requirement and Assessment Procedure.

Appendix B: Additional Information of Summary of Evaluation Findings

If information that supports the evaluation finding is too large to be included in the Summary of Evaluation Findings column, use Appendix B to add this information to the report. Examples of information that may be added in this Appendix include diagrams, flowcharts, or tables that support the Lab's findings. In the Findings and Observation section, document in the Summary of Evaluation Findings for the applicable reporting instruction that additional information has been included in Appendix B. Any information recorded in Appendix B should reference back to the applicable PCI 3DS SDK Security Requirement and Assessment Procedure.

Reporting Expectations

DO:	DO NOT:
▪ Complete all sections in the order specified, with concise detail. ▪ Read and understand the intent of each Requirement and Assessment Procedure. ▪ Provide a response for every Assessment Procedure. ▪ Provide sufficient detail and information to demonstrate a finding of "In Place" or "N/A." ▪ Describe *how* a Requirement was verified as the Reporting Instruction directs, not just that it *was* verified. ▪ Ensure the parts of the Assessment Procedure and Reporting Instruction are addressed. ▪ Ensure the response covers all applicable applications and/or system components, including third-party components. ▪ Perform an internal quality assurance review of the ROV for clarity, accuracy, and quality. ▪ Provide useful, meaningful diagrams, as directed.	▪ Do not report items in the "In Place" column unless they have been verified as being "In Place." ▪ Do not include forward-looking statements or project plans in the "In Place" column. ▪ Do not simply repeat or echo the Assessment Procedure in the response. ▪ Do not copy responses from one Assessment Procedure to another. ▪ Do not copy responses from previous evaluations. ▪ Do not include information irrelevant to the evaluation.

ROV Template for PCI 3DS SDK Report on Validation

1 Contact Information and Report Date

1.1 Contact information

PCI 3DS SDK Vendor	
▪ Company name:	
▪ Company address:	
▪ Company URL:	
▪ Company contact name:	
▪ Contact phone number:	
▪ Contact e-mail address:	
PCI 3DS SDK Lab	
▪ Company name:	
▪ Company address:	
▪ Company website:	
PCI 3DS SDK Lab Report Author	
▪ Report author(s) name(s):	
▪ Report author(s) phone number(s):	
▪ Report author(s) e-mail address(es):	

PCI 3DS SDK Lab Technical Reviewer	
▪ Technical reviewer(s) name(s):	
▪ Technical reviewer(s) phone number(s):	
▪ Technical reviewer(s) e-mail address(es):	
PCI 3DS SDK Lab Releasing Officer	
▪ Releasing officer name:	
▪ Releasing officer phone number:	
▪ Releasing e-mail address:	

1.2 Date and timeframe of evaluation

▪ Date of Report:	
▪ Timeframe of evaluation (start date to completion date):	
▪ Description of time spent performing evaluation—e.g., was all testing completed at PCI 3DS SDK Lab or was some testing performed remotely to the SDK Vendor location?	

1.3 Additional services provided by 3DS SDK Lab

PCI 3DS SDK Labs must be aware of and abide by all independence obligations including those described in the PCI Recognized Laboratory Agreement.

▪ Disclose all services offered to the SDK Vendor by the PCI 3DS SDK Lab, including but not limited to whether the SDK Vendor uses any security-related devices or applications developed or manufactured by the PCI 3DS SDK Lab, or to which the PCI 3DS SDK Lab owns the rights, or that the PCI 3DS SDK Lab has configured or manages:	
▪ Describe efforts made to ensure no conflict of interest resulted from the above-mentioned services provided by the PCI 3DS SDK Lab:	

2 3DS SDK Information

2.1 3DS SDK Identification

3DS SDK name and version number	
Identify 3DS SDK all applicable name(s) and version number(s) covered by this 3DS SDK evaluation.	
3DS SDK Name:	3DS SDK Version Number:
EMVCo issued 3DS SDK Reference Number:	Date of EMVCo Letter of Approval:

2.2 3DS SDK Tested Platforms

Operating systems tested			
Identify all operating system(s) on which the 3DS SDK was tested during this evaluation:			
☐ Android	☐ iOS	☐ Windows Mobile	☐ Other (please specify):

For each operating system tested, identify specific versions or service pack level, as applicable, and the underlying hardware platform that was used for the evaluation:

Details of platforms tested		
Operating System (e.g., Android, iOS, etc.)	**Specific version(s)** or service pack level, API levels, etc. as applicable:	**Description of hardware platform** (e.g., manufacturer and type of device)

2.3 Untested Platforms

Identify all operating system(s) and platforms that the 3DS SDK supports but that were **NOT** tested during this evaluation:

Note: *Only the specific operating systems and platforms on which the 3DS SDK was tested will be listed on the PCI SSC Website*

Platforms supported that were not tested			
Operating System (e.g., Android, iOS, etc.)	**Specific version(s)** or service pack level, API levels, etc. as applicable:	**Description of hardware platform** (e.g., manufacturer and type of device)	**Explanation why platforms weren't tested**

2.4 Third-Party Software Dependencies and Requirements

Identify and list all 3DS SDK dependencies, including software and hardware components, as applicable:

Dependencies			
Vendor	**Name of Product**	**Version of Product**	**Function of Product**

2.5 SDK Vendor's Versioning Methodology

Describe the SDK vendor's 3DS SDK versioning methodology:	
Describe the format of the version scheme, such as number of elements, number of digits used for each element, format of separators used between elements and character set used for each element (consisting of alphabetic, numeric and/or alphanumeric characters).	
Describe the hierarchy of the elements:	
Define what each element represents in the version scheme.	
If wildcards are used in the versioning methodology, describe how wildcards are used.	
Provide the name of the Tester who attests that the version methodology was reviewed to verify it to be consistent with the requirements in the *3DS SDK Program Guide v1.0*.	

Note: *If wildcarding is used, please refer to the PCI 3DS SDK Program Guide for information for wildcarding considerations and how they may affect the 3DS SDK's listing on the PCI website.*

3 3DS SDK Diagrams

3.1 3DS SDK Data-flow diagram

Provide a data-flow diagram that shows all inputs, outputs, and data flows of the 3DS SDK, including data flows involving sensitive 3DS SDK data elements. Ensure the diagram includes the following for each data flow:

- Identify the types of 3DS data involved (for example, consumer device data)
- Identify where the 3DS data exists
- Identify any protection mechanisms (for example, encryption, truncation, masking, etc.) applied to the 3DS data.
- Identify the functions involved in the transmission, processing or storage of 3DS data

<Insert data-flow diagram here>

3.2 SDK User Interface Diagram

Provide a diagram showing the path of any User Interface (UI) elements from the 3DS SDK to the hardware of the device upon which the 3DS SDK executes. Note any OS functions or other third-party features the 3DS SDK relies upon for the passing and render of UI elements.

<Insert 3DS SDK User Interface diagram here>

4 Evaluation Overview

4.1 3DS SDK Test Harness

A test harness is used to verify the 3DS SDK's compliance to the PCI 3DS SDK security objectives and requirements. The test harness could be developed by the 3DS SDK Vendor, PCI 3DS SDK Lab, or by another qualified third party. The 3DS SDK Vendor should work with its PCI 3DS SDK Lab to determine the tools and materials needed for the evaluation of a particular 3DS SDK.

The PCI 3DS SDK Lab must identify all tools and components used by the test harness. This will include reporting tools, logging tools and other tools used by the test harness.

Test Harness Overview		
Test harness provided by (check all that apply):		
☐ PCI 3DS SDK Lab	☐ SDK Vendor	☐ Other (please specify):

Test Harness Details – tools and components			
Tool/Component Provider	**Name of Tool/Component**	**Version of Tool/Component** (if applicable)	**Function of Tool/Component** (e.g., 3DS Requestor App, 3DS Server, ACS, DS, etc.)

4.2 Documentation Reviewed

Identify all reviewed documents			
Reference Number	**Document name** (including version, if applicable)	**Brief description of document purpose**	**Document date** (latest version date)
Doc-1			
Doc-2			
Doc-3			
Doc-4			
Doc-5			
Doc-6			
Doc-7			
Doc-8			
Doc-9			
Doc-10			

4.3 Individuals Interviewed

Identify all individuals interviewed.				
Reference Number	**Individual's Name**	**Role/Job Title**	**Organization**	**Summary of Topics Covered** (high-level summary only)
Int-1				
Int-2				
Int-3				
Int-4				
Int-5				
Int-6				
Int-7				
Int-8				
Int-9				
Int-10				

4.4 Sampling

Identify whether sampling was used:	
▪ Was sampling used during the evaluation?	☐ Yes ☐ No
If sampling was used:	
▪ Identify the name of the tester(s) who attests that all sample sets used for this evaluation are represented in the following table, "Identify and describe the sample sets used."	
▪ Describe the sampling process used for selecting sample sizes (for people, threats or vulnerabilities, data, etc.).	
If sampling was not used:	
▪ Identify the name of the tester(s) who attests that the total population of all items applicable for this evaluation were included in testing.	

If sampling is used, the following table may be used. Where a reporting instruction asks to identify a sample, the Lab may either list the sampled items individually in the response or refer to the sample Reference Number in this table (for example "Sample-1").

Identify and describe the sample sets used:			
Reference Number	**Sample Type/Description** (e.g., people, threats, vulnerabilities, data)	**List of all items in the sample**	**Rationale for each sample**
Sample-1			
Sample-2			
Sample-3			
Sample-4			
Sample-5			

5 Evaluation Results Summary

Conclusion on 3DS SDK Compliance

Compliance Status:	☐ Compliant ☐ Not Compliant

Security Objective 1: Protect the Integrity of the 3DS SDK

No.	PCI 3DS SDK Requirement	3DS SDK Lab Response	Notes
1.1	Security Checks	*Lab Response:*	
1.2	Installed from Approved Source	*Lab Response:*	
1.3	Run-Time Integrity	*Lab Response:*	
1.4	Protection against Reverse Engineering	*Lab Response:*	
1.5	Protections of 3DS SDK Reference Data	*Lab Response:*	

Security Objective 2: Protect Sensitive 3DS SDK Data Elements

No.	PCI 3DS SDK Requirement	3DS SDK Lab Response	Notes
2.1	Collection of Sensitive 3DS SDK Data Elements	*Lab Response:*	
2.2	Clearing of Sensitive 3DS SDK Data Elements	*Lab Response:*	
2.3	Use of Third-Party Services	*Lab Response:*	
2.4	Protection against Disclosure through Unintended Channels	*Lab Response:*	
2.5	Hardcoded 3DS SDK Data Elements	*Lab Response:*	
2.6	Run-Time Data Protection	*Lab Response:*	
2.7	UI Protection	*Lab Response:*	
2.8	HTML Rendering	*Lab Response:*	
2.9	Prevention of External Code or Script Execution	*Lab Response:*	

Security Objective 3: Use Cryptography Appropriately and Correctly

No.	PCI 3DS SDK Requirement	3DS SDK Lab Response	Notes
3.1	Approved Algorithms and Modes of Operation	*Lab Response:*	
3.2	Random Number Generator(s)	*Lab Response:*	
3.3	Random Number Entropy	*Lab Response:*	

Security Objective 4: Use Manage Risks and Vulnerabilities

No.	PCI 3DS SDK Requirement	3DS SDK Lab Response	Notes
4.1	Threat and Vulnerability Analysis	*Lab Response:*	
4.2	Development of Defensive Strategies and Mechanisms	*Lab Response:*	
4.3	Software Security Testing	*Lab Response:*	
4.4	Vulnerability Identification and Monitoring	*Lab Response:*	
4.5	Updates During Transaction Processing	*Lab Response:*	

Security Objective 5: Provide Guidance to Stakeholders

No.	PCI 3DS SDK Requirement	3DS SDK Lab Response	Notes
5.1	Availability of Stakeholder Guidance	*Lab Response:*	
5.2	Disclosure of Updates to Stakeholders	*Lab Response:*	
5.3	Frequency of Updates to Stakeholder Guidance	*Lab Response:*	

6 Findings and Observations

Security Objective 1: Protect the Integrity of the 3DS SDK				
3DS SDK Security Requirements and Assessment Procedures	**Reporting Instructions**	**Summary of Evaluation Findings**		
Requirement 1: Mechanisms are implemented to prevent unauthorized modification of the 3DS SDK, the functionality it provides and the sensitive 3DS SDK data elements it handles.				
1.1 Security Checks The 3DS SDK provides functionality to conduct device security checks (at a minimum, during initialization) and makes the results of those checks available to the 3DS Requestor App upon request as warning messages. Device security checks include, at minimum, determining whether: • The device is rooted or jailbroken • An emulator is being used to run the 3DS SDK • The 3DS SDK has been tampered with • A debugger is attached		**In Place** ☐	**N/A** ☐	**Not in Place** ☐
T.1.1.1 The tester shall examine vendor materials and other evidence to determine what features are provided by the 3DS SDK to provide security checks of the operating environment, and how any issues are escalated to the 3DS Requestor App. From this review, the tester shall determine what APIs are provided by the 3DS SDK for these purposes, the functions that are performed (and how often), and what error/warning messages are returned by the 3DS SDK. At a minimum, the SDK shall perform the checks upon initialization.	Identify the vendor materials and evidence examined that describe the features provided by the 3DS SDK to provide security checks of the operating environment.	*<Report findings here>*		
	Identify all APIs and functions provided by the 3DS SDK for the purposes of escalating issues to the 3DS Requestor App.	*<Report findings here>*		
	For each function identified, describe when and how often the function is performed.	*<Report findings here>*		
	Identify all possible error/warning messages that are returned by the 3DS SDK for the purposes of escalating issues to the 3DS Requestor App.	*<Report findings here>*		
	Describe how the tester confirmed the 3DS SDK performs security checks upon initialization.	*<Report findings here>*		

Security Objective 1: Protect the Integrity of the 3DS SDK		
3DS SDK Security Requirements and Assessment Procedures	**Reporting Instructions**	**Summary of Evaluation Findings**
T.1.1.2 Based on the information provided in T.1.1.1, the tester shall examine vendor evidence, including source code, to determine what methods are used to perform the environment validation, and what they are designed to detect. These checks must include the below, at a minimum: • Checking whether the device is rooted or jailbroken • Determining whether an emulator is being used to run the 3DS SDK • Validation of the integrity of the 3DS SDK, to determine whether it has been tampered with • Determining whether a debugger is attached or the device running the 3DS SDK is in a "developer" or "debug" mode	Identify the vendor materials, evidence, and the source code files examined that describe the methods used by the 3DS SDK to perform environment validation and the conditions those methods are designed to detect.	*<Report findings here>*
	Identify all security checks performed by the 3DS SDK. For each security check, describe all possible results/responses that can be returned and the conditions each result/response represents.	*<Report findings here>*
	Indicate whether the security checks identified include the minimum checks defined within the requirement. (Yes/No)	*<Report findings here>*
T.1.1.3 The tester shall also determine the platforms, operating systems, and specific versions of these supported by the 3DS SDK.	Identify all platforms (e.g., iPhone, Samsung, etc.), operating systems (e.g., iOS, Android, etc.) and versions supported by the 3DS SDK. ***Note**: The results of this testing may reference the information in Section 2 of the ROV Template, as long as that section includes all of the required information specified in this reporting instruction.*	*<Report findings here>*

Security Objective 1: Protect the Integrity of the 3DS SDK		
3DS SDK Security Requirements and Assessment Procedures	**Reporting Instructions**	**Summary of Evaluation Findings**
T.1.1.4 The tester shall test the 3DS SDK by attempting to execute the 3DS SDK on phones that have been rooted or jailbroken, and observe the response of the SDK to confirm that the 3DS SDK detects that the phone has been rooted or jailbroken. This test must include use of devices from at least two different manufacturers where the 3DS SDK or operating system supports it.	Identify all devices, operating systems, and versions used to test whether the 3DS SDK detects when the device has been rooted or jailbroken.	*<Report findings here>*
	Indicate whether devices from at least two different manufacturers were used to test the 3DS SDK. (Yes/No) *If "Yes," identify the devices used.* *If "No," explain why such testing is not supported.*	*<Report findings here>*
	Describe each test that was performed in an attempt to execute the 3DS SDK on devices that have been rooted or jailbroken and the response of the 3DS SDK to each test.	*<Report findings here>*
	Explain how the results of the tests performed confirm that the 3DS SDK detects when the device has been rooted or jailbroken.	*<Report findings here>*
T.1.1.5 The tester shall test the 3DS SDK by attempting to execute the 3DS SDK within an environment where raised privileges have been attained (i.e., the system has been rooted or jailbroken) with at least two readily available rooting or jailbreaking tools to confirm that the 3DS SDK detects such elevated privileges.	Indicate whether at least two readily available rooting/jailbreaking tools were used to test the 3DS SDK. (Yes/No) *If "Yes," identify which tools were used.* *If "No," explain why such testing is not supported.*	*<Report findings here>*
	Describe each test that was performed in support of this assessment procedure and the results of each test.	*<Report findings here>*
	Explain how the results of the tests confirm that the 3DS SDK detects when it is executed in an environment with raised elevated privileges.	*<Report findings here>*

Security Objective 1: Protect the Integrity of the 3DS SDK		
3DS SDK Security Requirements and Assessment Procedures	**Reporting Instructions**	**Summary of Evaluation Findings**
T.1.1.6 The tester shall test the 3DS SDK by attempting to execute the SDK within at least two different emulators and observe the response of the 3DS SDK to confirm that the 3DS SDK detects when an emulator is being used to run the 3DS SDK.	Indicate whether at least two different emulators were used to test the 3DS SDK. (Yes/No) *If "Yes," identify which tools were used.* *If "No," explain why such testing is not supported.*	*<Report findings here>*
	Describe each test that was performed in an attempt to execute the 3DS SDK within an emulator, and the response of the 3DS SDK each test.	*<Report findings here>*
	Explain how the results of the tests performed confirm the 3DS SDK detects when an emulator is being used to run the 3DS SDK.	*<Report findings here>*
T.1.1.7 The tester shall test the 3DS SDK by attempting to modify the 3DS SDK (for example: by modifying initialization files, runtime files, or cryptographic keys) and then execute this modified version to confirm the 3DS SDK detects when its code or execution has been tampered with. The modification must be specifically designed to attempt to bypass the integrity checking of the 3DS SDK.	Describe each test that was performed in an attempt to modify the 3DS SDK during execution and the results of each test. For each test, identify the specific sections of code, keys, files, etc. that were modified as part of the test.	*<Report findings here>*
	Describe how the tests performed were specifically designed to bypass the integrity checking of the 3DS SDK.	*<Report findings here>*
	Explain how the results of the tests performed confirm that the 3DS SDK detects when its code or execution have been tampered with.	*<Report findings here>*

Security Objective 1: Protect the Integrity of the 3DS SDK		
3DS SDK Security Requirements and Assessment Procedures	**Reporting Instructions**	**Summary of Evaluation Findings**
T.1.1.8 The tester shall test the 3DS SDK by attempting to execute the 3DS SDK in a system that allows for advanced control or insight into the execution of applications—e.g., such as running it in debug or developer mode to confirm the 3DS SDK detects this behavior.	Describe each test that was performed in an attempt to execute the 3DS SDK in a system that allows for advanced control or insight into the execution of the 3DS SDK and the results of each test.	*<Report findings here>*
	Describe how the test system/environment was configured to allow for advanced control or insight into the execution of applications.	*<Report findings here>*
	Explain how the results of the tests performed confirm that the 3DS SDK detects when it is executed in a system that allows for advanced control or insight into the execution of the 3DS SDK.	*<Report findings here>*
Additional assessor comments: *<Report findings here>*		

Security Objective 1: Protect the Integrity of the 3DS SDK				
3DS SDK Security Requirements and Assessment Procedures	**Reporting Instructions**	**Summary of Evaluation Findings**		
1.2 Installed from Approved Source The 3DS SDK conducts checks (at minimum, during initialization) to determine whether the embedding Requestor App was installed from a trusted app store (for example: Google Play, iTunes, and Microsoft App store, etc.), and makes that information available to the Access Control Server (ACS).		**In Place** ☐	**N/A** ☐	**Not in Place** ☐
T.1.2.1 The tester shall examine vendor materials and other evidence to confirm features are provided by the 3DS SDK to check that the Requestor App was installed by a trusted app store. This shall include confirming that action is taken by the 3DS SDK if the Requestor App fails this test.	Identify the vendor materials and evidence examined that confirm features are provided by the 3DS SDK to check that the Requestor App was installed by a trusted app store.	*<Report findings here>*		
	Describe all features provided by the 3DS SDK to perform these checks. For each feature, also describe the specific actions taken by the 3DS SDK if the 3DS Requestor App fails the check.	*<Report findings here>*		
T.1.2.2 Based on the information provided in T.1.2.1, the tester shall examine vendor materials and other evidence, including source code, to confirm the 3DS SDK verifies the Requestor App was not sideloaded or otherwise installed outside of the primary application distribution store of the operating system being used.	Identify the vendor materials, evidence, and the source code files examined that confirm the 3DS SDK verifies the 3DS Requestor App was not sideloaded or otherwise installed outside of the primary application distribution store of the operating system being used.	*<Report findings here>*		
	Describe how the 3DS SDK determines whether the 3DS Requestor App was “sideloaded” or otherwise installed outside of the primary application distribution store of the operating system being used.	*<Report findings here>*		

Security Objective 1: Protect the Integrity of the 3DS SDK		
3DS SDK Security Requirements and Assessment Procedures	**Reporting Instructions**	**Summary of Evaluation Findings**
T.1.2.3 The tester shall test the 3DS SDK by attempting to sideload an application and have it interface to the 3DS SDK as required by the 3DS SDK documentation for a valid Requestor Application. The tester shall observe the response of the SDK to confirm that normal 3DS transaction processing is not permitted/performed by the 3DS SDK.	Describe each test that was performed in an attempt to sideload an application and have it interface to the 3DS SDK and the response of the 3DS SDK to each test.	*<Report findings here>*
	Describe how the results of the tests performed confirm that normal 3DS SDK transaction processing is not permitted/performed by the 3DS SDK if the embedding 3DS Requestor Application has been sideloaded.	*<Report findings here>*
T.1.2.4 The tester shall examine publicly available information to determine what methods, if any, may exist to bypass the checks performed. Using this information, the tester shall test the 3DS SDK by attempting to perform such bypass using a sideloaded application to confirm that normal 3DS transaction processing is not permitted/performed by the 3DS SDK.	Describe how and the extent to which the tester searched for publicly available information on methods to bypass 3DS SDK security checks.	*<Report findings here>*
	Indicate whether any methods have been identified for bypassing the checks performed. (Yes/No) *If "Yes," complete the remaining reporting instructions for this assessment procedure.* *If "No," skip to T.1.2.5.*	*<Report findings here>*
	Describe the methods found for bypassing 3DS SDK security checks.	*<Report findings here>*
	Describe each test that was performed utilizing these methods in an attempt to bypass the security checks and the response of the 3DS SDK to each test.	*<Report findings here>*
	Describe how the results of the tests performed confirm that normal 3DS transaction processing is not permitted/performed by the 3DS SDK if checks to detect whether the 3DS Requestor Application has been sideloaded have been bypassed.	*<Report findings here>*
Additional assessor comments: *<Report findings here>*		

Security Objective 1: Protect the Integrity of the 3DS SDK				
3DS SDK Security Requirements and Assessment Procedures	**Reporting Instructions**	**Summary of Evaluation Findings**		
1.3 Run-Time Integrity The 3DS SDK performs run-time integrity checks to detect when its functionality has been modified. ***Note:*** *These checks shall go beyond the integrity checks performed during initialization as part of Requirement 1.1, "Security Checks."*		**In Place** ☐	**N/A** ☐	**Not in Place** ☐
T.1.3.1 The tester shall examine vendor materials and other evidence to confirm features are provided by the SDK to perform run-time integrity checks during execution, to verify that the security of the SDK cannot be compromised after the initialization phase by tampering with the execution code or parameters.	Identify the vendor materials and evidence examined that confirm features are provided by the 3DS SDK to perform run-time integrity checks during execution.	*<Report findings here>*		
	Describe all features provided by the 3DS SDK (beyond those identified in Requirement 1.1) to perform run-time integrity checks during execution.	*<Report findings here>*		
	Explain how the features prevent the security of the 3DS SDK from being compromised after the initialization phase by tampering with the execution code or parameters.	*<Report findings here>*		
T.1.3.2 Where these checks implement the use of a hash function to validate the integrity of the 3DS SDK executable, the tester shall examine vendor materials and other evidence to confirm that the hash function meets PCI requirements of strong cryptography, including applicable cryptography requirements in this standard.	Indicate whether the 3DS SDK implements the use of a hash function to validate the integrity of the 3DS SDK executable. (Yes/No) *If "Yes," complete the remaining reporting instructions for this assessment procedure.* *If "No," skip to T.1.3.2.*	*<Report findings here>*		
	Identify the vendor materials and other evidence examined that confirm hash functions used to validate the integrity of the 3DS SDK executable meet PCI requirements for strong cryptography and applicable cryptography requirements in this standard.	*<Report findings here>*		
	Identify all hash functions used to validate the integrity of the 3DS SDK executable.	*<Report findings here>*		

Security Objective 1: Protect the Integrity of the 3DS SDK		
3DS SDK Security Requirements and Assessment Procedures	**Reporting Instructions**	**Summary of Evaluation Findings**
	For each hash function identified: • Identify the cryptography requirements within this standard that are applicable to the hash function. • Describe how the hash function meets the applicable cryptography requirements within this standard as well as general PCI requirements for strong cryptography.	*<Report findings here>*
T.1.3.3 The tester shall confirm that these checks include tests to identify attacks that aim to perform interruption of code execution or flow, interception and modification of data elements as they are processed, or modification of responses from the SDK to the calling application.	Describe how the tester confirmed that the run-time integrity checks (as identified in T.1.3.1) include tests to identify attacks that aim to perform interruption of code execution or flow, interception and modification of data elements as they are processed, or modification of responses from the SDK to the calling application.	*<Report findings here>*
	For each feature provided by the 3DS SDK to perform run-time integrity checks (as identified in T.1.3.1), describe how the feature addresses attacks that attempt to perform interruption of code execution or flow, interception and modification of data elements as they are processed, or modification of responses from the SDK to the calling application.	*<Report findings here>*

Security Objective 1: Protect the Integrity of the 3DS SDK		
3DS SDK Security Requirements and Assessment Procedures	**Reporting Instructions**	**Summary of Evaluation Findings**
T.1.3.4 The tester shall determine where data values are stored (even temporarily) outside of the 3DS SDK code itself, or the memory space of the 3DS SDK provided by the device Operating System during execution – e.g., written to the device file system, stored in system functions such as a 'key store', etc., and confirm that features or methods are applied to protect these values.	Describe how the tester determined whether data values are stored (even temporarily) outside of the 3DS SDK code or the allocated memory space provided by the device operating system during execution.	*<Report findings here>*
	Identify all data values stored outside of the 3DS SDK code in reserved memory space provided by the operating system.	*<Report findings here>*
	For each data value identified, describe the features or methods applied by the 3DS SDK to protect these values.	*<Report findings here>*
T.1.3.5 The tester shall determine where other code, data, script, or features of the application are not included in the integrity check, and confirm that having these features out of scope does not affect the security of the SDK or 3DS transaction process.	Describe the process and rationale the tester used to determine whether other code, data, scripts, or features of the 3DS SDK are not included in the integrity check.	*<Report findings here>*
	Identify all other code, data, scripts, or features of the 3DS SDK that are not covered by the run-time integrity checks.	*<Report findings here>*
	For each item (code, data, scripts, or features) of the 3DS SDK not covered by the run-time integrity checks, explain why the exclusion of the item from the run-time integrity checks does not affect the security of the 3DS SDK or 3DS transaction process.	*<Report findings here>*
T.1.3.6 Based on the information provided in T.1.3.1 through T.1.3.5, the tester shall examine vendor materials and other evidence, including source code, to confirm that the claimed features are correctly implemented.	Identify the vendor materials, other evidence, and source code files examined that confirm the claimed features are correctly implemented.	*<Report findings here>*
	For each of the features identified in T.1.3.1 through T.1.3.5, describe the process and rationale the tester used to confirm the feature is implemented correctly.	*<Report findings here>*

Security Objective 1: Protect the Integrity of the 3DS SDK		
3DS SDK Security Requirements and Assessment Procedures	**Reporting Instructions**	**Summary of Evaluation Findings**
T.1.3.7 The tester shall test the 3DS SDK by attempting to modify the 3DS SDK prior to and during execution. Testing shall include attempts to modify the 3DS SDK code itself or values used by the code (for example, modifying configuration files, the runtime code, encryption keys, or keys or parameters stored temporarily in files or live memory during execution that could compromise the secure execution of the SDK.) The tester shall then observe the response of the 3DS SDK to confirm these modifications are detected. The changes must be made in such a way to attempt to avoid detection. Where the 3DS SDK code may be present in different locations (such as in the form of a pre-compiled file, as well as an ahead-of-time compilation that is ready to execute) the tester shall attempt to modify the 3DS SDK code in each location.	Describe each test that was performed in an attempt to modify the 3DS SDK prior to and during execution, and the response of the 3DS SDK to each test.	*<Report findings here>*
	Describe how the tests performed include attempts to modify the 3DS SDK code or values used by the code during execution.	*<Report findings here>*
	Describe how the tester identified all locations where the 3DS SDK is present, and how the tests performed account for these locations.	*<Report findings here>*
	Describe how the results of the tests performed confirm all attempts to modify 3DS SDK code or values during execution are detected.	*<Report findings here>*
T.1.3.8 The tester shall test the 3DS SDK by attempting to execute the 3DS SDK within an execution environment that allows for dynamic modification—such as a system that implements a hooking framework, a virtual machine (VM), or a device running a customized operating system to allow for such attacks to confirm that such modification attempts are detected by the 3DS SDK.	Describe each test that was performed in an attempt to execute the 3DS SDK within an execution environment that allows for dynamic and the results of each test.	*<Report findings here>*
	Describe how the execution environment where the tests were performed was configured to allow for dynamic modification.	*<Report findings here>*
	Explain how the results of the tests performed confirm that attempts to modify the 3DS SDK during execution are detected by the 3DS SDK.	*<Report findings here>*
Additional assessor comments: *<Report findings here>*		

Security Objective 1: Protect the Integrity of the 3DS SDK				
3DS SDK Security Requirements and Assessment Procedures	**Reporting Instructions**	**Summary of Evaluation Findings**		
1.4 Protection against Reverse Engineering The 3DS SDK binaries are protected from reverse engineering.		**In Place** ☐	**N/A** ☐	**Not in Place** ☐
T.1.4.1 The tester shall examine vendor materials and other evidence to confirm that features are provided by the 3DS SDK to protect the 3DS SDK and any data structures that may be stored in memory, the operating system file system, or other storage locations (such as an OS key store) from reverse engineering. ***Note**: This requirement is focused on the determination of the data flow and functions of the 3DS SDK, not necessarily the secrecy of the data.*	Identify the vendor materials and other evidence examined that confirm features are provided by the 3DS SDK to protect the 3DS SDK and any data structures that may be stored in memory, the operating system file system, and other storage locations from reverse engineering.	*<Report findings here>*		
	Describe each of the features implemented by the 3DS SDK to protect the 3DS SDK and any data structures stored in memory, the operating system file system, or other storage locations from reverse engineering.	*<Report findings here>*		
T.1.4.2 The tester shall determine where the SDK or data structures are not covered by these protections, and confirm this lack of protection does not affect the security of the SDK or 3DS operation.	Describe how the tester determined whether the 3DS SDK or any data structures are not covered by these protections.	*<Report findings here>*		
	Identify any aspects of the 3DS SDK or its data structures that are not covered by the protections identified in T.1.4.1.	*<Report findings here>*		
	For each item (code or data structures) found not to be covered by the protections identified in T.1.4.1, explain why the lack of protections does not affect the security of the 3DS SDK or 3DS operation.	*<Report findings here>*		
T.1.4.3 The tester shall determine all locations where functions provided by the 3DS SDK are executed. This will include the main processing environment of the device, but may also include other local execution environments (such as a Trusted Execution Environment or embedded security processor).	Identify all locations within the execution environment where functions provided by the 3DS SDK are executed.	*<Report findings here>*		
	Describe the process and rationale the tester used to identify these locations.	*<Report findings here>*		

Security Objective 1: Protect the Integrity of the 3DS SDK		
3DS SDK Security Requirements and Assessment Procedures	**Reporting Instructions**	**Summary of Evaluation Findings**
T.1.4.4 Where cryptography is implemented for the purposes of obfuscation and anti-tamper, the tester shall determine the locations and data protected by those methods. The tester shall also determine what protection is provided by the cryptography (confidentiality, integrity, or both) and what algorithms and modes of operation are used. The tester shall confirm that cryptography meets PCI requirements for strong cryptography, including applicable cryptography requirements in this standard, and that all keys used for these cryptographic operations are protected.	Describe the process the tester used to determine whether cryptography is implemented for the purposes of obfuscation and anti-tamper.	*<Report findings here>*
	Indicate whether the 3DS SDK implements cryptography for such purposes. (Yes/No) *If "Yes," complete the remaining reporting instructions for this assessment procedure.* *If "No," skip to T.1.4.5.*	*<Report findings here>*
	Identify all locations and data where cryptography has been implemented for the purposes of obfuscation and anti-tamper.	*<Report findings here>*
	Describe the process and rationale the tester used to determine the locations and data protected by cryptography.	*<Report findings here>*
	For each of the locations and data protected by cryptography: • Describe the protections provided by the cryptography (i.e., confidentiality, integrity, or both) and the modes of operation used. • Identify the cryptography requirements within this standard that are applicable to the cryptographic protections. • Describe how the cryptographic protections meet the applicable cryptography requirements within this standard as well as general PCI requirements for strong cryptography.	*<Report findings here>*
	Identify all keys used for these cryptographic operations. For each key, describe how the key is protected.	*<Report findings here>*

Security Objective 1: Protect the Integrity of the 3DS SDK		
3DS SDK Security Requirements and Assessment Procedures	**Reporting Instructions**	**Summary of Evaluation Findings**
T.1.4.5 Where protections are provided (partially or wholly) through code obfuscation, the tester shall perform the following:	Describe the process and rationale the tester used to determine whether protections are provided through code obfuscation.	*<Report findings here>*
	Indicate whether protections are provided (partially or in whole) through code obfuscation. (Yes/No) *If "Yes," complete the remaining reporting instructions for assessment procedures T.1.4.5 through T.1.4.5.4.* *If "No," skip to T.1.4.6.*	*<Report findings here>*
	Identify all 3DS SDK data structures protected through code obfuscation.	*<Report findings here>*
T.1.4.5.1 Examine vendor materials and other evidence, including application installation files where the protection methods have been applied, and compare these files to files where protections have not yet been applied to confirm the validity of the vendor attestations and documentation regarding the protection methods implemented. ***Note**: This test may require the 3DS SDK Vendor to provide both obfuscated and un-obfuscated binaries or source code to the 3DS SDK Lab to validate this requirement.*	Identify the vendor materials, other evidence, and the application installation files examined that confirm the validity of the vendor attestations regarding the protection methods implemented.	*<Report findings here>*
	Describe how the file-size comparisons confirm the protections provided (partially or wholly) through code obfuscation were implemented as attested by the vendor.	*<Report findings here>*

Security Objective 1: Protect the Integrity of the 3DS SDK		
3DS SDK Security Requirements and Assessment Procedures	**Reporting Instructions**	**Summary of Evaluation Findings**
T.1.4.5.2 Determine the comparative file sizes between unprotected and protected application samples, as well as the relative compression ratio of each file type when general purpose compression functions are applied to confirm that such analysis does not disclose any sensitive information about the 3DS SDK.	Describe how comparative file size between unprotected and protected application samples was determined.	*<Report findings here>*
	Describe how the relative compression ratio of each file type was determined and how the general-purpose compression functions were applied.	*<Report findings here>*
	Describe how the results of the above analysis confirm that sensitive information about the 3DS SDK is not disclosed by such methods.	*<Report findings here>*
T.1.4.5.3 Examine vendor materials and other evidence, and test the software by attempting to reverse engineer the code or extract details of the code execution (e.g., through extraction of ASCII strings, functional linking/interface tables such as PLT/GOT, etc.) to confirm such attempts do not result in the disclosure of any sensitive information about the 3DS SDK.	Identify the vendor materials and other evidence, including the source code files examined in support of this assessment procedure.	*<Report findings here>*
	Describe each test that was performed in an attempt to reverse engineer the 3DS SDK code and extract details of the code execution, and the results of each test.	*<Report findings here>*
	Describe how the results of the tests performed confirm such attempts to reverse engineer the code or extract details of the code execution do not result in the disclosure of any sensitive information about the 3DS SDK.	*<Report findings here>*
T.1.4.5.4 Analyze any areas of non-traditional execution where the obfuscation relies on virtualized/interpreted commands, non-deterministic operations, or other such techniques to confirm that the exploitation of such techniques does not result in the disclosure of any sensitive information about the 3DS SDK.	Describe the process and rationale the tester used to determine whether any areas of non-traditional execution are utilized and whether obfuscation relies on virtualized/interpreted commands, non-deterministic operations, or other such techniques.	*<Report findings here>*
	Describe how the tester confirmed that the exploitation of such techniques does not result in the disclosure of any sensitive information about the 3DS SDK.	*<Report findings here>*

Security Objective 1: Protect the Integrity of the 3DS SDK		
3DS SDK Security Requirements and Assessment Procedures	**Reporting Instructions**	**Summary of Evaluation Findings**
T.1.4.6 Where protections are provided by the operating environment, the tester shall perform the following:	Describe how the tester determined whether reverse engineering protections are provided by the operating system.	*<Report findings here>*
	Indicate whether reverse engineering protections are provided by the operating environment. (Yes/No) *If "Yes," complete the remaining reporting instructions for assessment procedures T.1.4.6 through T.1.4.6.2.* *If "No," skip to T.1.4.7.*	*<Report findings here>*
	Identify all 3DS SDK data structures protected from reverse engineering by features and functions provided by the operating environment.	*<Report findings here>*
T.1.4.6.1 Examine vendor materials and other evidence, including source code to confirm that such protections provide the required tamper-resistance features and that any elements of code or data that are not covered by these protections cannot be used to reverse engineer the code or disclose sensitive information about the 3DS SDK.	Identify the vendor materials, evidence, and the source code files examined that support the findings of this assessment procedure.	*<Report findings here>*
	Describe the process and rationale the tester used to: • Confirm protections provided by the operating environment against reverse engineering provide the required tamper resistance features. • Identify any elements of code or data not covered by these protections.	*<Report findings here>*
	Indicate whether elements of 3DS SDK code or data were found not to be covered by these protections. *If "Yes," complete the remaining reporting instructions for this assessment procedure.* *If "No," skip to T.1.4.6.2.*	*<Report findings here>*

Security Objective 1: Protect the Integrity of the 3DS SDK		
3DS SDK Security Requirements and Assessment Procedures	**Reporting Instructions**	**Summary of Evaluation Findings**
	Identify any elements of code or data that are not covered by these protections.	*<Report findings here>*
	For each of the elements of code or data identified, explain why the elements of code or data cannot be used to reverse engineer the code or disclose sensitive information about the 3DS SDK.	*<Report findings here>*
T.1.4.6.2 Test the 3DS SDK to confirm that the 3DS SDK will only execute on platforms which provide such integrated protections.	Describe each test that was performed to confirm that the 3DS SDK will only execute on platforms which provide the required and the results of each test.	*<Report findings here>*
	Describe how the results of the tests performed confirm that the 3DS SDK will only execute on platforms which provide such protections.	*<Report findings here>*
T.1.4.7 Where protections are provided by runtime methods or anti-debugging features, the tester shall perform the following:	Indicate whether reverse engineering protections are provided by run-time protections or anti-debugging features. (Yes/No) *If "Yes," complete the remaining reporting instructions for assessment procedures T.1.4.7 through T.1.4.7.3.* *If "No," skip to T.1.4.8.*	*<Report findings here>*
	Identify the elements of code or data protected by runtime methods or anti-debugging features.	*<Report findings here>*
T.1.4.7.1 Examine vendor materials and other evidence to confirm that such protections provide the required tamper-resistance features and that any elements of code or data that are not covered by these protections cannot be used to reverse engineer the code or disclose sensitive information about the 3DS SDK.	Identify the vendor materials and other evidence examined that support the findings of this assessment procedure.	*<Report findings here>*
	For each instance where elements of code or data are protected using run-time methods and anti-debugging features, describe how those protections provide the required tamper resistance features.	*<Report findings here>*

Security Objective 1: Protect the Integrity of the 3DS SDK		
3DS SDK Security Requirements and Assessment Procedures	**Reporting Instructions**	**Summary of Evaluation Findings**
	Identify all elements of code and data that are not covered by these protections.	*<Report findings here>*
	Explain why the elements of code and data not covered by these protections cannot be used to reverse engineer the code or disclose sensitive information about the 3DS SDK.	*<Report findings here>*
T.1.4.7.2 Confirm that the local software that provides these features is itself protected.	Describe the process and rationale the tester used to confirm that the local software that provides such features is itself protected.	*<Report findings here>*
	Identify and describe the mechanisms implemented to protect the local software.	*<Report findings here>*
T.1.4.7.3 Where any features require interaction with an external system (such as a cloud-based monitoring system), the tester shall confirm that mechanisms are in place to prevent disabling of the remote protections, such as through traffic or communications manipulation.	Indicate whether any protections and features were found that require interaction with an external system. (Yes/No) *If "Yes," complete the remaining reporting instructions for this assessment procedure.* *If "No," skip to T.1.4.8.*	*<Report findings here>*
	Describe the mechanisms in place to prevent disabling of the remote protections.	*<Report findings here>*
T.1.4.8 Where additional protections are provided by the application, the tester shall confirm that these protections apply across all supported platforms and operating systems (as assessed under Requirement 1.1, "Security Checks"), or that any gaps that exist in coverage of these protections do not increase the risk posed by those platforms.	Indicate whether additional reverse engineering protections are provided by the 3DS SDK. (Yes/No) *If "Yes," complete the remaining reporting instructions for this assessment procedure.* *If "No," skip to T.1.4.9.*	*<Report findings here>*
	Identify the additional reverse engineering protections provide by the application.	*<Report findings here>*

Security Objective 1: Protect the Integrity of the 3DS SDK		
3DS SDK Security Requirements and Assessment Procedures	**Reporting Instructions**	**Summary of Evaluation Findings**
	Indicate whether these protections apply across all supported platforms and operating systems. (Yes/No) *If "Yes," skip to T.1.4.9.* *If "No," complete the remaining reporting instructions for this assessment procedure.*	*<Report findings here>*
	Identify the platforms and operating systems not supported by these protections.	*<Report findings here>*
	For each of the platforms and operating systems not supported, explain why the gaps in coverage of these protections do not increase the risk posed by those platforms and operating systems.	*<Report findings here>*
T.1.4.9 Where device-specific features are relied upon, the tester shall attempt to execute the 3DS SDK on a system that either does not provide such features or has been modified to prevent the secure use of these features, and observe the operation of the 3DS SDK to confirm that the 3DS SDK does not execute when such features are absent or disabled.	Indicate whether device-specific features are relied upon for providing reverse engineering protections. (Yes/No) *If "Yes," complete the remaining reporting instructions for this assessment procedure.* *If "No," skip to Requirement 1.5.*	*<Report findings here>*
	Identify the device-specific features relied upon for reverse engineering protections.	*<Report findings here>*
	Describe how the tester confirmed that the 3DS SDK does not execute on platforms where such protections are absent or disabled.	*<Report findings here>*
Additional assessor comments: *<Report findings here>*		

Security Objective 1: Protect the Integrity of the 3DS SDK				
3DS SDK Security Requirements and Assessment Procedures	**Reporting Instructions**	**Summary of Evaluation Findings**		
1.5 Protection of 3DS SDK Reference Data 3DS SDK Reference Data is securely stored within the 3DS SDK code to prevent unauthorized modification.		**In Place** ☐	**N/A** ☐	**Not in Place** ☐
T.1.5.1 The tester shall examine vendor materials and other evidence to identify all 3DS SDK Reference Data used or required by the 3DS SDK, which must be protected against modification (see Table 2, "Sensitive 3DS SDK Data Elements").	Identify the vendor materials and other evidence examined that describe all 3DS SDK Reference Data used or required by the 3DS SDK.	*<Report findings here>*		
	Identify all instances of 3DS SDK Reference Data used or required by the 3DS SDK.	*<Report findings here>*		
T.1.5.2 The tester shall examine vendor materials and other evidence to confirm that features are provided by the 3DS SDK to protect each element of the 3DS SDK Reference Data listed above. Where there is any 3DS SDK Reference Data that is not covered by these protections, the tester shall confirm that the lack of protection does not affect the security of the 3DS SDK or 3DS transaction process.	Identify the vendor materials and other evidence examined that confirm features are provided by the 3DS SDK to protect all instances of 3DS SDK Reference Data.	*<Report findings here>*		
	Identify the features provided by the 3DS SDK to protect each instance of the 3DS SDK Reference Data identified.	*<Report findings here>*		
	Identify any instances of 3DS SDK Reference Data not covered by these protections, and for each explain why the lack of protection does not affect the security of the 3DS SDK or the 3DS transaction process.	*<Report findings here>*		
T.1.5.3 Where cryptography is implemented for the purposes of providing this protection, the tester shall confirm that the cryptographic protections include the protection of the integrity of the data. The tester shall also confirm that cryptography meets PCI requirements for strong cryptography, including applicable cryptography requirements in this standard, and that all keys used for these cryptographic operations are protected.	Indicate whether cryptography is implemented for the purposes of providing protection for 3DS SDK Reference Data. (Yes/No) *If "Yes," complete the remaining reporting instructions for this assessment procedure.* *If "No," skip to T.1.5.4.*	*<Report findings here>*		
	Identify all instances where cryptography is implemented for the purposes of providing protection for 3DS SDK Reference Data.	*<Report findings here>*		

Security Objective 1: Protect the Integrity of the 3DS SDK		
3DS SDK Security Requirements and Assessment Procedures	**Reporting Instructions**	**Summary of Evaluation Findings**
	Describe how the tester confirmed that the cryptographic protections include the protection of the data integrity.	*<Report findings here>*
	For each instance where cryptography was implemented to protect 3DS SDK Reference Data: • Identify the cryptography requirements within this standard that are applicable to the cryptographic protection. • Describe how the cryptographic protections meet the applicable cryptography requirements within this standard as well as general PCI requirements for strong cryptography.	*<Report findings here>*
	Identify the cryptographic keys used for the purposes of protecting 3DS SDK Reference Data. For each key identified, describe how the cryptographic key is protected.	*<Report findings here>*
T.1.5.4 Where obfuscation is implemented to provide the protections, the tester shall confirm that this obfuscation is covered under testing performed in Requirement 1.4, "Protection against Reverse Engineering."	Indicate whether obfuscation is implemented for the purposes of protecting 3DS SDK Reference Data. (Yes/No) *If "Yes," complete the remaining reporting instructions for this assessment procedure.* *If "No," skip to T.1.5.5.*	*<Report findings here>*
	Identify the protections provided and for each describe how these protections were covered under the testing performed in Requirement 1.4.	*<Report findings here>*

Security Objective 1: Protect the Integrity of the 3DS SDK		
3DS SDK Security Requirements and Assessment Procedures	**Reporting Instructions**	**Summary of Evaluation Findings**
T.1.5.5 Where device-specific features are relied upon to provide the protections, the tester shall attempt to execute the 3DS SDK on a system that either does not provide such features or has been modified to prevent the secure use of these features to confirm that the 3DS SDK does not execute when such features are absent or disabled.	Indicate whether device specific features are relied upon for the purposes of protecting 3DS SDK Reference Data. (Yes/No) *If "Yes," complete the remaining reporting instructions for this assessment procedure.* *If "No," skip to T.1.5.6.*	*<Report findings here>*
	Describe how the 3DS SDK was evaluated and the details of the tests used by the tester to confirm that the 3DS SDK does not execute when such protections are absent or disabled.	*<Report findings here>*
T.1.5.6 The tester shall attempt to circumvent the features protecting the 3DS SDK Reference Data and modify this data in such a way that the modification is not detected by the 3DS SDK upon execution to confirm the 3DS SDK prohibits such modifications. This testing must consider the different types of protections applied and devices targeted by the SDK.	Describe how the tester attempted to circumvent the features protecting the 3DS SDK Reference Data.	*<Report findings here>*
	Describe how the attempts to circumvent protection features consider the different types of protections applied and the devices targeted by the 3DS SDK.	*<Report findings here>*
	Where such efforts to circumvent protections were successful, describe how the 3DS SDK Reference Data was attempted to be modified such that the modification could not be detected by the 3DS SDK.	*<Report findings here>*
	Describe how the results of the analysis and testing for this assessment procedure confirm that the 3DS SDK detects attempts to modify 3DS SDK Reference Data upon execution.	*<Report findings here>*
Additional assessor comments: *<Report findings here>*		

Security Objective 2: Protect Sensitive 3DS SDK Data Elements				
3DS SDK Security Requirements and Assessment Procedures	**Reporting Instructions**	**Summary of Evaluation Findings**		
Requirement 2: Sensitive 3DS SDK data elements are protected from unauthorized disclosure.				
2.1 Collection of Sensitive 3DS SDK Data Elements The 3DS SDK collects and retains only the sensitive 3DS SDK data elements absolutely necessary for the software to perform its intended purpose and functionality, and only for the duration necessary.		**In Place** ☐	**N/A** ☐	**Not in Place** ☐
T.2.1.1 The tester shall examine vendor materials and other evidence to determine all sensitive 3DS SDK data elements used or required by the 3DS SDK. Vendor evidence should account for the name of the data element collected, the duration for which the data element is retained, how the data element is stored (e.g., in memory only, in the OS file system, in an OS storage mechanism such as a key store, in a device mechanism such as a Trusted Execution Environment, etc.), and how the data element is securely deleted after storage.	Identify the vendor materials and other evidence examined that describe all sensitive 3DS SDK data elements used or required by the 3DS SDK.	*<Report findings here>*		
	For each sensitive 3DS SDK data element used or required by the 3DS SDK, describe the: • Name of the sensitive 3DS SDK data element. • Duration of time the data element is retained. • Location(s) where the data element is stored. • Method(s) used to securely delete the data element when retention is no longer required.	*<Report findings here>*		
T.2.1.2 The tester shall examine vendor evidence and other materials, including source code, to determine the functionality provided by the 3DS SDK and confirm that the functionality contained within the 3DS SDK correctly aligns with the vendor materials and evidence supplied and assessed in T.2.1.1.	Identify the vendor materials, evidence, and the source code files examined that describe all functionality provided by the 3DS SDK.	*<Report findings here>*		
	Describe the process and rationale the tester used to confirm the functionality provided within the 3DS SDK code correctly aligns with the vendor materials and evidence evaluated in T.2.1.1.	*<Report findings here>*		

Security Objective 1: Protect the Integrity of the 3DS SDK		
3DS SDK Security Requirements and Assessment Procedures	**Reporting Instructions**	**Summary of Evaluation Findings**
T.2.1.3 Given the output of T.2.1.1 and T.2.1.2, the tester shall reference Table 2 of the PCI 3DS SDK Security Standard, "Sensitive 3DS SDK Data Elements," to confirm that the list of sensitive 3DS SDK data elements identified in T.2.1.1 is exhaustive and correct given the functionality of the 3DS SDK under evaluation. Where sensitive 3DS SDK data elements are collected that are not required for the attested functionality, the tester shall note this as a non-compliance.	Describe how the output of T.2.1.1 and T.2.1.2 confirms that the sensitive 3DS SDK data elements identified in T.2.1.1 represent all data elements used or required by the 3DS SDK.	*<Report findings here>*
	Describe how the tester confirmed that the 3DS SDK does not collect any of the sensitive 3DS SDK data elements identified in Table 2 of the PCI 3DS SDK Security Standard, "Sensitive 3DS SDK Data Elements," it does not need for the attested functionality of the 3DS SDK under evaluation.	*<Report findings here>*
T.2.1.4 For each sensitive 3DS SDK data element identified in T.2.1.1, the tester shall determine whether the element is retained, and confirm that all sensitive 3DS SDK data elements that are retained are allowed to be retained, as noted in Table 2 of the PCI 3DS SDK Security Standard, "Sensitive 3DS SDK Data Elements."	Describe how the tester determined whether the sensitive 3DS SDK data elements identified in T.2.1.1 are retained.	*<Report findings here>*
	Identify all sensitive 3DS SDK data elements that are retained.	*<Report findings here>*
	Describe how the tester confirmed the each of the sensitive 3DS SDK data elements retained is permitted to be retained.	*<Report findings here>*

Security Objective 1: Protect the Integrity of the 3DS SDK		
3DS SDK Security Requirements and Assessment Procedures	**Reporting Instructions**	**Summary of Evaluation Findings**
T.2.1.5 The tester shall test the 3DS SDK by performing a series of 3DS operations, ensuring that these cover all functionality provided by the 3DS SDK, to confirm that all sensitive 3DS SDK data elements used by the 3DS SDK correctly and completely align with the sensitive 3DS SDK data elements identified in T.2.1.1. ***Note**: This testing must be performed against a 3DS test host/harness that emulates all required 3DS functionality and data elements, and allows for the monitoring of traffic to the 3DS SDK.*	Describe how the 3DS SDK was tested to confirm that all sensitive 3DS SDK data elements used by the 3DS SDK correctly and completely align with those identified in T.2.1.1, and the results of each test.	*<Report findings here>*
	Describe how the tester confirmed that the 3DS test host/harness emulates all 3DS SDK functionality and the tests performed cover all functionality provided by the 3DS SDK.	*<Report findings here>*
	Describe how the results of tests performed confirm that the sensitive 3DS SDK data elements used by the 3DS SDK do in fact align correctly and completely with the vendor materials and evidence evaluated in T.2.1.1.	*<Report findings here>*

Security Objective 1: Protect the Integrity of the 3DS SDK		
3DS SDK Security Requirements and Assessment Procedures	**Reporting Instructions**	**Summary of Evaluation Findings**
T.2.1.6 The tester shall test the 3DS SDK by performing a series of 3DS operations to determine how the sensitive 3DS SDK data elements are stored and retained, and confirm that the use and retention of sensitive 3DS SDK data elements correctly and completely aligns with the details provided in T.2.1.1. ***Note**: This testing may be achieved through operation of the 3DS SDK in a virtualized environment that allows for monitoring the memory and storage of the system during processing, through the use of tools to monitor the data elements during operation on a physical device, or other means that will allow for confirmation of the use the memory and storage space of the 3DS SDK operating environment. It is also noted that this testing may require assistance from the 3DS SDK Vendor to disable protections in the software that would otherwise prevent the use of these types of tools.*	Describe each test that was performed to determine how sensitive 3DS SDK data elements are stored and retained by the 3DS SDK, and the results of each test.	*<Report findings here>*
	Indicate whether it was necessary to disable protections in the 3DS SDK in order to perform the tests above. (Yes/No) *If "Yes," identify the protections that had to be disabled.*	*<Report findings here>*
	Based on the tests performed, describe how and the location where each of the sensitive 3DS SDK data elements used by the 3DS SDK is stored and retained.	*<Report findings here>*
	Describe how the tests performed confirm that the use and retention of sensitive 3DS SDK data elements by the 3DS SDK align correctly and completely with the details provided in T.2.1.1.	*<Report findings here>*
Additional assessor comments: *<Report findings here>*		

Security Objective 2: Protect Sensitive 3DS SDK Data Elements				
3DS SDK Security Requirements and Assessment Procedures	**Reporting Instructions**	**Summary of Evaluation Findings**		
2.2 Clearing of Sensitive 3DS SDK Data Elements Sensitive 3DS SDK data elements collected by the 3DS SDK in association with 3DS transactions are securely purged after 3DS transaction processing is complete and never retained, unless retention is explicitly permitted.		**In Place** ☐	**N/A** ☐	**Not in Place** ☐
T.2.2.1 Referencing the information produced in T.2.1.1, the tester shall examine vendor materials and other evidence, including source code, to confirm that each of the sensitive 3DS SDK data elements is securely deleted after use and that the methods used ensures that each sensitive 3DS SDK data element is rendered irretrievable to any subsequent process, component, functions, or applications after secure deletion.	Identify the vendor materials, evidence, and the source code files examined that describe how each sensitive 3DS SDK data element is securely deleted after use.	*<Report findings here>*		
	Describe the process and rationale the tester used to confirm that: • Sensitive 3DS SDK data elements are securely deleted when retention is no longer required. • Secure deletion methods ensure that each data element is rendered irretrievable to any subsequent process, component, function, or application.	*<Report findings here>*		
T.2.2.2 Where secure deletion is prevented by the nature of the 3DS SDK operating environment (e.g., through virtualized memory and garbage-collection processes), the tester shall examine vendor materials and other evidence to confirm that additional protections have been implemented beyond secure deletion of the data element, and that such protections are sufficient to be considered equal to industry best practice.	Describe how the tester determined whether secure deletion is prevented by the nature of the 3DS SDK operating environment.	*<Report findings here>*		
	Indicate whether secure deletion is prevented by the nature of the 3DS SDK operating environment. (Yes/No) *If "Yes," complete the remaining reporting instructions for this assessment procedure.* *If "No," skip to T.2.2.3.*	*<Report findings here>*		
	Identify the vendor materials and other evidence examined that describe the additional protections that have been implemented beyond secure deletion of the data element.	*<Report findings here>*		

Security Objective 2: Protect Sensitive 3DS SDK Data Elements		
3DS SDK Security Requirements and Assessment Procedures	**Reporting Instructions**	**Summary of Evaluation Findings**
	Describe each of the additional protections that have been implemented.	*<Report findings here>*
	Explain why the additional protections are sufficient to be considered equal to industry best practice.	*<Report findings here>*
T.2.2.3 Where additional protections or secure deletion methods are required to be implemented to compensate for lack of direct memory access in the 3DS SDK operating platform, the tester shall confirm that these methods are covered by the reverse-engineering protections tested under Requirement 1.4, "Protection against Reverse Engineering," and that any cryptography used is covered under the testing of Requirement 3.1, "Approved Algorithms and Modes of Operation."	Describe how the tester determined whether additional protections or secure deletion methods are required to be implemented to compensate for a lack of direct memory access in the 3DS SDK operating platform.	*<Report findings here>*
	Indicate whether the 3DS SDK has direct memory access to the 3DS SDK operating platform. (Yes/No) *If "Yes," skip to T.2.2.4.* *If "No," complete the remaining reporting instructions for this assessment procedure.*	*<Report findings here>*
	Identify all additional protections and secure deletion methods implemented to compensate for the lack of direct memory access in the 3DS SDK operating platform.	*<Report findings here>*
	Describe where the additional protections and secure deletion methods are covered by the reverse engineering protections tested under Requirement 1.4.	*<Report findings here>*
	Describe where any cryptography used by these additional protections and secure deletion methods are covered by the testing under Requirement 3.1.	*<Report findings here>*

Security Objective 1: Protect the Integrity of the 3DS SDK		
3DS SDK Security Requirements and Assessment Procedures	**Reporting Instructions**	**Summary of Evaluation Findings**
T.2.2.4 The tester shall test the 3DS SDK by performing a series of 3DS operations, ensuring that these cover all functionality provided by the 3DS SDK to confirm that each of the sensitive 3DS SDK data elements covered in T.2.1.1 is rendered irretrievable in accordance with the methods identified in T.2.2.1 through T.2.2.3. ***Note**: This testing must be performed against a 3DS test host/harness that provides all required 3DS functionality and data elements, and allows for the monitoring of traffic to the 3DS SDK. This testing may also require assistance from the 3DS SDK Vendor to disable protections in the software that would otherwise prevent the use of these types of tools.*	Describe each of the tests performed to determine whether the sensitive 3DS SDK data elements identified in T.2.1.1 are rendered irretrievable (in accordance with the methods identified in T.2.1.1 through T.2.2.3) and the results of each test.	*<Report findings here>*
	Indicate whether it was necessary to disable protections in the 3DS SDK in order to perform the tests above. (Yes/No) *If "Yes," identify the protections that had to be disabled.*	*<Report findings here>*
	Describe how the tester confirmed that the 3DS test host/harness provides all 3DS SDK functionality and the tests performed cover all functionality provided by the 3DS SDK.	*<Report findings here>*
	Describe how the results of the tests performed confirm that each of the sensitive 3DS SDK data elements covered in T.2.1.1 is rendered irretrievable in accordance with the methods identified in T.2.2.1 through T.2.2.3.	*<Report findings here>*
Additional assessor comments: *<Report findings here>*		

Security Objective 2: Protect Sensitive 3DS SDK Data Elements				
3DS SDK Security Requirements and Assessment Procedures	**Reporting Instructions**	**Summary of Evaluation Findings**		
2.3 Use of Third-Party Services The 3DS SDK uses third-party services and components only when and where it is documented and justified as part of the 3DS SDK architecture.		**In Place** ☐	**N/A** ☐	**Not in Place** ☐
T.2.3.1 The tester shall examine vendor materials and other evidence to confirm that the vendor maintains an inventory of all third-party services and components used by the 3DS SDK.	Indicate whether third-party services or components are used by the 3DS SDK. (Yes/No) *If "Yes," complete the remaining reporting instructions for this assessment procedure.* *If "No," skip to Requirement 2.4.*	*<Report findings here>*		
	Identify the vendor materials and other evidence examined that confirm the vendor maintains an inventory of all third-party services and components used by the 3DS SDK.	*<Report findings here>*		
	Describe each of the third-party party services and components used by the 3DS SDK.	*<Report findings here>*		
T.2.3.2 Referring to the information produced in T.2.1.1, the tester shall examine vendor materials and other evidence, including source code, to determine all sensitive 3DS SDK data elements that are passed to third-party components or services. ***Note**: Validation of this requirement must also consider whether the 3DS SDK has any advertising, machine learning, data collection, logging, tracking, or security features which rely on third-party components, features, or external services. This list of items is to be considered a minimum set and is not considered exhaustive of all potential third-party features which must be considered under this requirement.*	Identify the vendor materials, other evidence, and source code files examined that describe whether and how sensitive 3DS SDK data elements are passed to third-party components or services.	*<Report findings here>*		
	Identify all sensitive 3DS SDK data elements identified in T.2.1.1 that are passed to third-party components or services.	*<Report findings here>*		
	Describe the considerations the tester took into account when determining what sensitive 3DS SDK data elements are passed to third-party components or services.	*<Report findings here>*		

Security Objective 2: Protect Sensitive 3DS SDK Data Elements		
3DS SDK Security Requirements and Assessment Procedures	**Reporting Instructions**	**Summary of Evaluation Findings**
T.2.3.3 Where third-party services are used, interfaced with, or operated by the 3DS SDK, the tester shall examine vendor materials and other evidence to confirm the vendor provides reasonable and documented justifications for the use of each third-party system or components and that the vendor maintains processes for addressing vulnerabilities in those systems or components in accordance with Requirement 4.4, "Vulnerability Identification and Monitoring."	Identify the vendor materials and other evidence examined that confirm the vendor provides reasonable and documented justification for the use of third-party systems or components.	*<Report findings here>*
	For each of the third-party components and services used, interfaced with, or operated by the 3DS SDK (as identified in T.2.3.1), describe the vendor's rationale for its use and explain why this justification is considered reasonable.	*<Report findings here>*
	Describe the vendor's processes for addressing vulnerabilities in those third-party systems and components, and how they are maintained in accordance with Requirement 4.4.	*<Report findings here>*

Security Objective 1: Protect the Integrity of the 3DS SDK		
3DS SDK Security Requirements and Assessment Procedures	**Reporting Instructions**	**Summary of Evaluation Findings**
T.2.3.4 The tester shall test the 3DS SDK by performing a series of 3DS operations, ensuring that these cover all functionality provided by the 3DS SDK, to determine how any third-party components or services are utilized during this operation and which data elements are sent to third parties. The tester shall confirm this correctly and completely aligns with the vendor materials and evidence provided in T.2.3.1 and T.2.3.2. ***Note**: This testing must be performed against a 3DS test host/harness that provides all required 3DS functionality and data elements, and allows for the monitoring of traffic to the 3DS SDK. This testing may also be achieved through operation of the 3DS SDK in a virtualized environment that allows for monitoring the memory and storage of the system during processing, through the use of tools to monitor the data elements during operation on a physical device, or other means that will allow for confirmation of the use of third-party components and services. It is noted that this testing may require assistance from the 3DS SDK Vendor to disable protections in the software that would otherwise prevent the use of these types of tools.*	Describe each of the tests performed to determine how any third-party components or services are utilized during this operation and which data elements are sent to third parties, and the results of each test.	*<Report findings here>*
	Describe how the tester confirmed that the 3DS test host/harness provides all 3DS SDK functionality and the tests performed cover all functionality provided by the 3DS SDK.	*<Report findings here>*
	Describe how the results of the tests performed confirm that the use of third-party components and services by the 3DS SDK aligns correctly and completely with the details provided in T.2.3.1 and T.2.3.2.	*<Report findings here>*

Security Objective 1: Protect the Integrity of the 3DS SDK		
3DS SDK Security Requirements and Assessment Procedures	**Reporting Instructions**	**Summary of Evaluation Findings**
T.2.3.5 The tester shall test the 3DS SDK by performing a series of 3DS operations, ensuring that these cover all functionality provided by the 3DS SDK, and observe the traffic output from and received by the 3DS SDK to determine whether any of this traffic is external or extraneous to the 3DS test host to which the SDK is communicating, whether any sensitive 3DS SDK data elements are communicated through these channels, and if so, confirm that they correctly and completely align with the information provided in T.2.3.2.	Describe each of the tests performed to determine whether any traffic output from or received by the 3DS SDK is external or extraneous to the 3DS test host, and the results of each test.	*<Report findings here>*
	Describe how the tests performed cover all functionality provided by the 3DS SDK.	*<Report findings here>*
	Identify all sensitive 3DS SDK data elements communicated through these channels.	*<Report findings here>*
	Describe how the tests performed confirm that any sensitive 3DS SDK data elements found to be passed to third-party components or services align correctly and completely with those identified in T.2.3.2.	*<Report findings here>*
T.2.3.6 The tester shall determine the functionality provided by the 3DS SDK during testing and confirm that this correctly and completely aligns with the information provided in T.2.3.1 to T.2.3.4.	Describe how the results of the tests performed in T.2.3.5 confirm that the functionality found to be provided by the 3DS SDK aligns correctly and completely with the functionality identified in T.2.3.1 through T.2.3.4.	*<Report findings here>*
T.2.3.7 The tester shall examine vendor materials and other evidence to confirm that use of third-party services is only implemented where this is a reasonably justified and documented part of the 3DS SDK architecture.	Identify the vendor materials and other evidence examined where all uses of third-party services are documented and justified.	*<Report findings here>*
	Describe how the tester confirmed that third-party services are only implemented where their use has been documented and reasonably justified.	*<Report findings here>*
Additional assessor comments: *<Report findings here>*		

Security Objective 2: Protect Sensitive 3DS SDK Data Elements				
3DS SDK Security Requirements and Assessment Procedures	**Reporting Instructions**	**Summary of Evaluation Findings**		
2.4 Protection against Disclosure through Unintended Channels The 3DS SDK does not disclose sensitive 3DS SDK data elements through unintended channels.		**In Place** ☐	**N/A** ☐	**Not in Place** ☐
T.2.4.1 Referring to the information produced in T.2.1.1, the tester shall examine vendor materials and other evidence, including source code, to determine how each of the data elements is generated/input and displayed (if displayed).	Identify the vendor materials, other evidence, and source code files examined that describe how each of the sensitive 3DS SDK data elements identified in T.2.1.1 is generated, input, and displayed.	*<Report findings here>*		
	Describe how and where each of the 3DS SDK data elements in T.2.1.1 is generated, input, and displayed by the 3DS SDK.	*<Report findings here>*		
T.2.4.2 Referring to the information produced in T.2.1.1 and the details generated above, the tester shall confirm that for each sensitive 3DS SDK data element identified in T.2.1.1, the vendor has implemented protections to safeguard that data element against disclosure through unintended channels.	Describe the protections implemented by the vendor to safeguard each of the sensitive 3DS SDK data elements identified against disclosure through unintended channels.	*<Report findings here>*		
T.2.4.3 Where the sensitive 3DS SDK data element is input by the cardholder, the tester shall confirm that methods are implemented by the 3DS SDK to mitigate clickjacking, screen overlay, or other such input-stealing attacks.	Indicate whether any sensitive 3DS SDK data elements are input by the cardholder. (Yes/No) *If "Yes," complete the remaining reporting instructions for this assessment procedure.* *If "No," skip to T.2.4.4.*	*<Report findings here>*		
	Identify each of the sensitive 3DS SDK data elements input by the cardholder.	*<Report findings here>*		
	Describe the methods implemented by the 3DS SDK to mitigate input stealing attacks including "clickjacking" and screen overlay attacks.	*<Report findings here>*		

Security Objective 2: Protect Sensitive 3DS SDK Data Elements		
3DS SDK Security Requirements and Assessment Procedures	**Reporting Instructions**	**Summary of Evaluation Findings**
T.2.4.4 For all sensitive 3DS SDK data elements identified in T.2.1.1, the tester shall confirm that methods are implemented by the 3DS SDK to mitigate capture of each of these elements through use of shared resources such as memory or file systems.	For each of the sensitive 3DS SDK data elements identified in T.2.1.1, describe the methods implemented by the 3DS SDK to mitigate capture of the data element through the use of shared resources such as memory or shared file systems.	*<Report findings here>*
T.2.4.5 Referring to testing performed in Requirement 2.3, "Use of Third-Party Services," the tester shall confirm that methods are implemented to mitigate the capture or exposure of each sensitive 3DS SDK data element as it is passed between the 3DS SDK and any third-party services or components.	For each of the sensitive 3DS SDK data elements identified in T.2.3.2, describe the methods implemented by the 3DS SDK to mitigate capture or exposure of the data element as it is passed between the 3DS SDK and any third-party services or components.	*<Report findings here>*
T.2.4.6 Referring to the information produced in T.2.1.1, the tester shall examine vendor materials and other evidence, including source code, to confirm that only sensitive 3DS SDK data elements that are explicitly permitted to be hard-coded are stored in the source code.	Indicate whether sensitive 3DS SDK data elements are hard-coded in source code. (Yes/No) *If "Yes," complete the remaining reporting instructions for this assessment procedure.* *If "No," skip to T.2.4.7.*	*<Report findings here>*
	Identify all sensitive 3DS SDK data elements hard-coded into 3DS SDK source code.	*<Report findings here>*
	Identify the vendor materials, other evidence, and source code files examined that confirm that only sensitive 3DS SDK data elements that are explicitly permitted to be hardcoded are stored in the 3DS SDK source code.	*<Report findings here>*
	For each of the sensitive 3DS SDK data elements identified, describe where and how the tester confirmed it is permitted to be stored.	*<Report findings here>*

Security Objective 2: Protect Sensitive 3DS SDK Data Elements		
3DS SDK Security Requirements and Assessment Procedures	**Reporting Instructions**	**Summary of Evaluation Findings**
T.2.4.7 The tester shall examine source code to determine whether sensitive 3DS SDK data elements which are externally generated or provided are processed in a way that indicates they are static—for example, where they utilize a third-party service or component, covered under Requirement 2.3, "Use of Third-Party Services," which implements static values; or where the 3DS SDK processing clearly does not accommodate for the expected range of values which may be provided in any particular data element. In such cases, the tester shall confirm that these values are not static, and that any such attestations from the vendor are documented.	Indicate whether any sensitive 3DS SDK data elements are externally generated or provided. (Yes/No) *If "Yes," complete the remaining reporting instructions for this assessment procedure.* *If "No," skip to T.2.4.8.*	*<Report findings here>*
	Identify the source code files examined that describe where sensitive 3DS SDK data elements are externally generated or provided.	*<Report findings here>*
	Describe how the tester determined whether the 3DS SDK processes externally generated or provided data elements in a way that: • Indicates that the sensitive 3DS SDK data elements have static values, or • Does not accommodate for the expected range of values for a given sensitive 3DS SDK data element.	*<Report findings here>*
	Describe how the tester confirmed that: • Any sensitive 3DS SDK data elements that are externally generated or provided are in fact not static, and • Statements from the vendor attesting to the fact that these values are not static are documented.	*<Report findings here>*

Security Objective 1: Protect the Integrity of the 3DS SDK		
3DS SDK Security Requirements and Assessment Procedures	**Reporting Instructions**	**Summary of Evaluation Findings**
T.2.4.8 The tester shall examine vendor materials and other evidence, including source code, to identify all error, debugging, or other output functionality. Where such functionality is found, the tester shall confirm that the functionality does not result in the unintended disclosure or leakage of any sensitive 3DS SDK data elements.	Identify the vendor materials, evidence, and source code files examined that describe all error, debugging, or other output functionality.	*<Report findings here>*
	For each instance where such functionality is identified, describe the functionality and how the tester confirmed that the functionality does not result in the unintended disclosure or leakage of any sensitive 3DS SDK data elements.	*<Report findings here>*
T.2.4.9 The tester shall examine vendor materials and other evidence, including source code, to confirm that any functionality that results in the output of sensitive 3DS SDK data elements is intended. The tester is expected to cross reference any output functionality to the testing performed in Requirement 2.3, "Use of Third-Party Services," to validate that all communication of sensitive 3DS SDK data elements is intended.	Identify the vendor materials, evidence, and source code files examined that describe all 3DS SDK functionality that results in the output of sensitive 3DS SDK data elements.	*<Report findings here>*
	Identify all instances and locations where sensitive 3DS SDK data elements are output by the 3DS SDK.	*<Report findings here>*
	For each instance or location identified, describe how the tester confirmed that the output of each sensitive 3DS SDK data elements is intended.	*<Report findings here>*
	Describe how and where the testing in Requirement 2.3 was considered to validate that all communication of sensitive 3DS SDK data elements is intended.	*<Report findings here>*

Security Objective 1: Protect the Integrity of the 3DS SDK		
3DS SDK Security Requirements and Assessment Procedures	**Reporting Instructions**	**Summary of Evaluation Findings**
T.2.4.10 The tester shall test the 3DS SDK by performing a series of 3DS operations, ensuring that these cover all functionality provided by the 3DS SDK, and confirm that sensitive 3DS SDK data elements are not disclosed through unintended channels. ***Note**: This testing must be performed against a 3DS test host/harness that provides all required 3DS functionality and data elements, and allows for the use and monitoring of shared resources such as memory, keyboards and displays. The test harness must additionally allow for the capture of any error or debug data output from the 3DS SDK.*	Describe each of the tests performed to determine whether sensitive 3DS SDK data elements are disclosed through unintended channels. Describe the results of each test performed.	*<Report findings here>*
	Describe how the tester confirmed that the 3DS test host/harness provides all 3DS SDK functionality and the tests performed cover all functionality provided by the 3DS SDK.	*<Report findings here>*
	Describe how the results of the tests performed confirm that sensitive 3DS SDK data elements are not disclosed through unintended channels.	*<Report findings here>*
T.2.4.10.1 The tester shall test the 3DS SDK by attempting to capture or otherwise determine the values of sensitive 3DS SDK data elements generated, input, or processed by the 3DS SDK. The tester must attempt methods that include both on-device capture, as well as capture through monitoring of communication channels. Communication channel capture shall consider the application of traffic analysis to determine the sensitive 3DS SDK data elements communicated.	Describe each of the tests performed in an attempt to capture or otherwise determine the values of sensitive 3DS SDK data elements through the use of on-device capture methods as well as capture through the monitoring of communication channels. Describe the results of each test performed.	*<Report findings here>*
	Describe how the tests performed included attempts to capture sensitive 3DS SDK data elements using on-device methods as well as capture through the monitoring of communication channels.	*<Report findings here>*
	Describe how traffic analysis was utilized in the tests performed in attempts to capture sensitive 3DS SDK data elements during communications.	*<Report findings here>*
	Describe how the results of the tests performed confirm that sensitive 3DS SDK data elements are not disclosed through unintended channels.	*<Report findings here>*

Security Objective 1: Protect the Integrity of the 3DS SDK		
3DS SDK Security Requirements and Assessment Procedures	**Reporting Instructions**	**Summary of Evaluation Findings**
T.2.4.10.2 The tester shall attempt to capture or otherwise determine the values of sensitive 3DS SDK data elements generated, input, or processed by the 3DS SDK through capture and analysis of error codes or use of debugging/test features. The tester must attempt methods that utilize both normal and forced error flows of the processing, and determine whether any sensitive 3DS SDK data elements are leaked.	Describe each of the tests performed in an attempt to capture or otherwise determine the values of sensitive 3DS SDK data elements through capture and analysis of error codes or use of debugging test features. Describe the results of each test performed.	*<Report findings here>*
	Describe how the tests performed included attempts to analyze and capture of error codes and leveraged the use of debugging and test features.	*<Report findings here>*
	Describe how the tests performed utilized both normal and forced error flows to determine whether any sensitive 3DS SDK data elements are leaked.	*<Report findings here>*
	Describe how the results of the tests performed confirm that sensitive 3DS SDK data elements are not disclosed through unintended channels.	*<Report findings here>*
Additional assessor comments: *<Report findings here>*		

Security Objective 2: Protect Sensitive 3DS SDK Data Elements				
3DS SDK Security Requirements and Assessment Procedures	**Reporting Instructions**	**Summary of Evaluation Findings**		
2.5 Hardcoded 3DS SDK Data Elements Sensitive 3DS SDK data elements are not hardcoded in 3DS SDK code unless explicitly permitted.		**In Place** ☐	**N/A** ☐	**Not in Place** ☐
T.2.5.1 Referring to testing performed in Requirement 2.4, "Protection against Disclosure through Unintended Channels," the tester shall confirm that sensitive 3DS SDK data elements are not hardcoded in the 3DS SDK except where the vendor has maintained reasonable and documented justification for their use.	For each of the hardcoded sensitive 3DS SDK data elements identified in T.2.4.6, identify the specific vendor materials and other evidence where vendor justification for hardcoding sensitive 3DS SDK data elements in 3DS SDK code is documented.	*<Report findings here>*		
	For each of the hardcoded sensitive 3DS SDK data elements identified in T.2.4.6, describe the vendor's justification for hardcoding the sensitive 3DS SDK data element in code and explain why the vendor justification is considered reasonable.	*<Report findings here>*		
T.2.5.2 The tester shall test the 3DS SDK by performing a series of 3DS operations, ensuring that these cover all functionality provided by the 3DS SDK, and observe the use of sensitive 3DS SDK data elements across multiple operations and executions of the 3DS SDK. Where sensitive 3DS SDK data elements appear to have the same value or a limited range of values, the tester shall confirm that these values correctly and completely align with those values noted in T.2.5.1. ***Note**: This testing must be performed against a 3DS test host/harness that has been confirmed to provide all required 3DS functionality and data elements.*	Describe each of the tests performed to determine whether sensitive 3DS SDK data elements appear to have the same value or a limited range of values. Describe the results of each test performed.	*<Report findings here>*		
	Describe how the tester confirmed that the 3DS test host/harness provides all 3DS SDK functionality and the tests performed cover all functionality provided by the 3DS SDK.	*<Report findings here>*		
	Identify any sensitive 3DS SDK data elements that appear to have a static value or limited range of values. For each sensitive 3DS SDK data element identified, describe how the values observed align correctly and completely with the values identified in T.2.5.1.	*<Report findings here>*		
Additional assessor comments: *<Report findings here>*				

Security Objective 2: Protect Sensitive 3DS SDK Data Elements				
3DS SDK Security Requirements and Assessment Procedures	**Reporting Instructions**	**Summary of Evaluation Findings**		
2.6 Run-Time Data Protection The 3DS SDK implements run-time data protection techniques to protect the 3DS SDK instance from being accessed by unauthorized third-party applications and/or libraries.		**In Place** ☐	**N/A** ☐	**Not in Place** ☐
T.2.6.1 Referencing the sensitive 3DS SDK data elements identified in T.2.1.1 and the protection features determined through other testing, the tester shall confirm that protections against extraction or determination are provided for each sensitive 3DS SDK data element.	Describe the protections implemented by the 3DS SDK against extraction or determination for each sensitive 3DS SDK data element identified in T.2.1.1.	*<Report findings here>*		
T.2.6.2 The tester shall examine vendor materials and other evidence, including source code, and test the 3DS SDK to determine what sensitive 3DS SDK data elements may be most susceptible to side-channel attacks, such as cache timing or other attack methods, and to confirm that such attacks are not feasible given the implemented protections.	Identify the vendor materials, other evidence, and source code files examined to determine what sensitive 3DS SDK data elements may be most susceptible to side-channel attacks.	*<Report findings here>*		
	Describe each of the tests performed to identify the 3DS SDK data elements susceptible to side-channel attacks, and the results of each test.	*<Report findings here>*		
	Identify the sensitive 3DS SDK data elements most susceptible to side-channel attacks.	*<Report findings here>*		
	Describe the process and rationale the tester used to determine which sensitive 3DS SDK data elements are the most susceptible to side-channel attacks.	*<Report findings here>*		
	For each of the sensitive 3DS SDK data elements identified, describe the protections implemented to protect each data element from side-channel attacks.	*<Report findings here>*		

Security Objective 1: Protect the Integrity of the 3DS SDK		
3DS SDK Security Requirements and Assessment Procedures	**Reporting Instructions**	**Summary of Evaluation Findings**
T.2.6.3 The tester shall examine vendor materials and other evidence, including source code, and test the software to determine what sensitive 3DS SDK data elements may be most susceptible to exposure through code injection or code reuse attacks, and to confirm such attacks are not feasible given implemented protections.	Identify the vendor materials, evidence, and source code files examined to determine what sensitive 3DS SDK data elements may be susceptible to exposure through code injection or code reuse attacks.	*<Report findings here>*
	Describe each of the tests performed to identify the sensitive 3DS SDK data elements that are susceptible to exposure through code injection or code reuse attacks. Describe the results of each test performed.	*<Report findings here>*
	Identify the sensitive 3DS SDK data elements most susceptible to exposure through code injection or code reuse attacks.	*<Report findings here>*
	Describe the process and rationale the tester used to determine which sensitive 3DS SDK data elements are the most susceptible to exposure through code injection or code reuse attacks.	*<Report findings here>*
	Describe the protections implemented against code injection or code reuse attacks for each of the sensitive 3DS SDK data elements identified.	*<Report findings here>*
	Describe how the tester confirmed that code injection or code reuse attacks are not feasible given the protections implemented by the 3DS SDK.	*<Report findings here>*

Security Objective 1: Protect the Integrity of the 3DS SDK		
3DS SDK Security Requirements and Assessment Procedures	**Reporting Instructions**	**Summary of Evaluation Findings**
T.2.6.4 The tester shall examine vendor materials and other evidence, including source code, and test the 3DS SDK to determine what sensitive 3DS SDK data elements may be most susceptible to exposure through hooking methods (remote and local) and reverse-engineering attacks, and to confirm that such attacks are not feasible given other protections.	Identify the vendor materials, evidence, and source code files examined to determine what sensitive 3DS SDK data elements may be susceptible to exposure through hooking methods and reverse-engineering attacks.	*<Report findings here>*
	Describe each of the tests performed to identify the 3DS SDK data elements that are susceptible to exposure through hooking methods and reverse-engineering attacks. Describe the results of each test performed.	*<Report findings here>*
	Identify the sensitive 3DS SDK data elements most susceptible to exposure through hooking methods and reverse engineering attacks.	*<Report findings here>*
	Describe the process and rationale the tester used to determine which sensitive 3DS SDK data elements are the most susceptible to exposure through hooking methods and reverse-engineering attacks.	*<Report findings here>*
	Describe the protections implemented against hooking methods and reverse engineering attacks for each of the sensitive 3DS SDK data elements identified.	*<Report findings here>*
	Describe how the tester confirmed that hooking or reverse-engineering attacks are not feasible given the protections implemented by the 3DS SDK.	*<Report findings here>*

Security Objective 1: Protect the Integrity of the 3DS SDK		
3DS SDK Security Requirements and Assessment Procedures	**Reporting Instructions**	**Summary of Evaluation Findings**
T.2.6.5 The tester shall test the 3DS SDK by attempting to subvert any third-party components or services relied upon by the 3DS SDK to determine whether any sensitive 3DS SDK data elements are used by the 3DS SDK that are not already confirmed to be passed to that third-party component or service as per testing under Requirement 2.3, "Use of Third-Party Services". Where third-party components or services are known to receive sensitive 3DS SDK data elements, the tester shall attempt to extract the sensitive values from these services during operation of the 3DS SDK to confirm the sensitive 3DS SDK data elements are not exposed to extraction or determination through code injection, code reuse, reverse engineering, and the use of hooking (remote or local) methods.	Describe each of the tests performed to determine whether any sensitive 3DS SDK data elements are used by the 3DS SDK that are not already confirmed to be passed to the third-party component or service (as identified in T.2.3.2). Describe the results of each test performed.	*<Report findings here>*
	Describe how the tests performed include attempts to subvert any third-party components or services relied upon by the 3DS SDK.	*<Report findings here>*
	Describe how the tests performed include attempts to extract the sensitive data values from third-party services or components during 3DS SDK operation.	*<Report findings here>*
	Identify any sensitive 3DS SDK data elements discovered through the tests performed that have not already been confirmed to be passed to third-party components or services (as identified in T.2.3.2).	*<Report findings here>*
	For each of the sensitive 3DS SDK data elements known to be passed to third-party components or services (including those identified in this assessment procedure and those identified in T.2.3.2), describe how the tester confirmed that it is not exposed to extraction or determination through code injection, code reuse, reverse engineering, and the use of hooking methods.	*<Report findings here>*
Additional assessor comments: *<Report findings here>*		

Security Objective 2: Protect Sensitive 3DS SDK Data Elements				
3DS SDK Security Requirements and Assessment Procedures	**Reporting Instructions**	**Summary of Evaluation Findings**		
2.7 UI Protection The user interface (UI) rendered by the 3DS SDK (both in Native and HTML modes) is isolated and secured such that user information (including authentication data) displayed and captured by the 3DS SDK is not accessible to any unauthorized process outside the 3DS SDK.		**In Place** ☐	**N/A** ☐	**Not in Place** ☐
T.2.7.1 The tester shall examine vendor materials and other evidence, including source code, to identify all OS functions or other third-party features the 3DS SDK relies upon for the passing and rendering of UI elements.	Identify the vendor materials, other evidence, and source code files examined that identify all OS functions or other third-party features the 3DS SDK relies upon for the passing and rendering of UI elements.	*<Report findings here>*		
	Describe each of the OS functions or other third-party features the 3DS SDK relies upon for passing and rendering UI elements.	*<Report findings here>*		
T.2.7.2 The tester shall examine vendor materials and other evidence, including source code, to confirm that security features are implemented to protect the UI against access by other applications.	Identify the vendor materials, other evidence, and source code files examined that identify the security features implemented to protect the UI against access by other applications.	*<Report findings here>*		
	Describe the security features implemented to protect the UI against access by other applications.	*<Report findings here>*		
T.2.7.3 The tester shall test the 3DS SDK by attempting to modify, capture, or otherwise undermine the security of the 3DS SDK UI to confirm that any user information captured and displayed by the 3DS SDK is not accessible to any unauthorized process outside of the 3DS SDK.	Describe each of the tests to determine whether any user information captured and displayed by the 3DS SDK is accessible to any unauthorized process outside of the 3DS SDK. Describe the results of each test performed.	*<Report findings here>*		
	Describe how the tests performed include attempts to modify, capture, or otherwise undermine the security of the 3DS SDK UI.	*<Report findings here>*		
	Describe how the results of the tests performed confirm that user information captured and displayed by the 3DS SDK is not accessible to any unauthorized process outside of the 3DS SDK.	*<Report findings here>*		

Security Objective 2: Protect Sensitive 3DS SDK Data Elements		
3DS SDK Security Requirements and Assessment Procedures	**Reporting Instructions**	**Summary of Evaluation Findings**
Additional assessor comments: *<Report findings here>*		

Security Objective 2: Protect Sensitive 3DS SDK Data Elements				
3DS SDK Security Requirements and Assessment Procedures	**Reporting Instructions**	**Summary of Evaluation Findings**		
2.8 HTML Rendering The 3DS SDK intercepts all external URL requests made by the HTML UI rendered (both during loading of the UI and on user action) and handles these requests within the 3DS SDK. Such requests are not passed to the device's operating system or the Internet.		**In Place** ☐	**N/A** ☐	**Not in Place** ☐
T.2.8.1 The tester shall examine vendor materials and other evidence, including source code, and the findings in T.2.7.1 to confirm that URL requests made by the UI in HTML mode are handled within the 3DS SDK itself and are not passed to the device's operating system or any other component (internal or external).	Identify the vendor materials, other evidence, and source code files examined that describe how URL requests made by the UI in HTML mode are handled by the 3DS SDK.	*<Report findings here>*		
	Describe how the vendor materials, other evidence, and source code examined confirm that URL requests made by the UI in HTML mode are handled within the 3DS SDK itself and not passed to the device's operating system or any other component (internal or external).	*<Report findings here>*		
T.2.8.2 The tester shall examine vendor materials and other evidence, including source code, to determine what web elements the 3DS SDK is configured to handle, and to confirm that these methods are created and used in a way that mitigates attacks and prevents references to external content that is not supplied by the Access Control Server (ACS).	Identify the vendor materials, other evidence, and source code files examined that identify the web elements the 3DS SDK is configured to handle.	*<Report findings here>*		
	Describe all web elements the 3DS SDK is configured to handle.	*<Report findings here>*		
	Describe how web elements are created and used in a way that mitigates attacks and prevents references to external content that is not supplied by the ACS.	*<Report findings here>*		

Security Objective 2: Protect Sensitive 3DS SDK Data Elements		
3DS SDK Security Requirements and Assessment Procedures	**Reporting Instructions**	**Summary of Evaluation Findings**
T.2.8.3 Using the information determined in T.2.8.2, the tester shall test the 3DS SDK by attempting to inject HTML references in ACS response(s), and observe the operation of the 3DS SDK to confirm that the UI processes running in HTML mode are handled by the 3DS SDK and are not passed to the device operating system or other component(s) (internal or external). ***Note**: This testing must be performed with a test host/harness that allows for such injection.*	Describe each of the tests performed to determine how UI processes running in HTML mode are handled by the 3DS SDK. Describe the results of each test performed.	*<Report findings here>*
	Describe how the tester confirmed the test host/harness supports the injection of HTML references into ACS responses.	*<Report findings here>*
	Describe how the tests performed include attempts to inject HTML references in ACS responses, and how monitoring of the 3DS SDK during execution was utilized.	*<Report findings here>*
	Describe how the results of the tests performed confirm that the UI processes running in HTML mode are handled by the 3DS SDK and are not passed to the device operating system or other component(s) (internal or external).	*<Report findings here>*
Additional assessor comments: *<Report findings here>*		

Security Objective 2: Protect Sensitive 3DS SDK Data Elements				
3DS SDK Security Requirements and Assessment Procedures	**Reporting Instructions**	**Summary of Evaluation Findings**		
2.9 Prevention of External Code or Script Execution The 3DS SDK prevents the injection and execution of any JavaScript code by the HTML UI or any other process outside the 3DS SDK.		**In Place** ☐	**N/A** ☐	**Not in Place** ☐
T.2.9.1 The tester shall examine vendor materials and other evidence to confirm that protections are provided by 3DS SDK to prevent the injection and execution of JavaScript into the UI (in HTML mode) or any other process outside of the 3DS SDK.	Identify the vendor materials and other evidence examined that identify the protections provided by the 3DS SDK to prevent the injection and execution of JavaScript into the UI or any other process outside of the 3DS SDK.	*<Report findings here>*		
	Describe the protections provided by the 3DS SDK to prevent the injection and execution of JavaScript into the UI in HTML mode or any other processes outside of the 3DS SDK.	*<Report findings here>*		
T.2.9.2 The tester shall examine vendor materials and other evidence, including source code, to confirm that the source code does not contain any JavaScript parsing or execution code, even if disabled, and that the functionality provided in the source code for preventing the injection and execution JavaScript into the UI or other processes outside of the 3DS SDK aligns with the details provided in T.2.9.1.	Identify the vendor materials, evidence, and source code files examined to determine whether functionality provided by the 3DS SDK for preventing the injection and execution of JavaScript into the UI or other processes outside of the 3DS SDK aligns with the detail in T.2.9.1.	*<Report findings here>*		
	Describe how the materials, evidence, and source code files were examined to confirm that the 3DS SDK does not contain any JavaScript parsing or execution code, even if disabled.	*<Report findings here>*		
	Describe how the protections defined within the 3DS SDK code were confirmed to align with the vendor materials and evidence identified in T.2.9.1.	*<Report findings here>*		

Security Objective 2: Protect Sensitive 3DS SDK Data Elements		
3DS SDK Security Requirements and Assessment Procedures	**Reporting Instructions**	**Summary of Evaluation Findings**
T.2.9.3 The tester shall test the 3DS SDK by attempting to inject JavaScript into the ACS response(s), and observe the response of the 3DS SDK to confirm that this is not executed by the 3DS SDK. ***Note**: This testing must use a test host/harness that allows for this modification of the ACS responses.*	Describe each of the tests performed to determine how the 3DS SDK responds to attempts to inject JavaScript into the ACS response(s). For each test performed, describe the results of each test.	*<Report findings here>*
	Describe how the tester confirmed the test host/harness supports the injection of JavaScript into ACS responses.	*<Report findings here>*
	Describe how the results of the tests performed confirm that attempts to inject JavaScript into the ACS response(s) are not executed by the 3DS SDK.	*<Report findings here>*
Additional assessor comments: *<Report findings here>*		

Security Objective 3: Use Cryptography Appropriately and Correctly				
3DS SDK Security Requirements and Assessment Procedures	**Reporting Instruction**	**Summary of Evaluation Findings**		
Requirement 3: The 3DS SDK only utilizes strong cryptography and it ensures that cryptographic methods are properly and appropriately implemented.				
3.1 Approved Algorithms and Modes of Operation Only approved cryptographic algorithms and methods are used. Approved cryptographic algorithms and methods are those specified within the *EMV® 3-D Secure SDK Specification*. Approved cryptographic algorithms and methods are also recognized by industry-accepted standards bodies—for example: NIST, ANSI, ISO, EMVCo, etc. Cryptographic algorithms and parameters that are known to be vulnerable are not used.		**In Place** ☐	**N/A** ☐	**Not in Place** ☐
T.3.1.1 The tester shall examine vendor materials and other evidence, including source code, to determine what cryptographic algorithms and methods are used and all cryptographic keys used in the system that are relied upon for the security of the 3DS SDK.	Identify the vendor materials, other evidence, and source code files examined that identify the cryptographic algorithms and methods used by the 3DS SDK, and cryptographic keys that are relied upon for the security of the 3DS SDK.	*<Report findings here>*		
	Describe cryptographic algorithms and methods used by the 3DS SDK.	*<Report findings here>*		
	Describe each of the cryptographic keys that are relied upon for the security of the 3DS SDK.	*<Report findings here>*		
T.3.1.2 The tester shall examine vendor materials and other evidence, including source code, to identify modes of operation available for each key, including determining how any additional values (such as initial vectors) may be generated for that mode of operation.	Identify the vendor materials, other evidence, and source code files examined that describe the modes of operation available for each cryptographic key identified in T.3.1.1.	*<Report findings here>*		
	For each cryptographic key identified in T.3.1.1: • Identify the modes of operation available. • Describe how any additional values (such as initial vectors) may be generated for each mode of operation.	*<Report findings here>*		

Security Objective 3: Use Cryptography Appropriately and Correctly		
3DS SDK Security Requirements and Assessment Procedures	**Reporting Instruction**	**Summary of Evaluation Findings**
T.3.1.3 Where the mode of operation may be open to exploitation—e.g., relocation or data analysis attacks on Electronic Code Book (ECB) mode—the tester shall confirm that this sort of attack is not feasible for this implementation. This testing must always be performed for keys that allow for ECB as a mode of operation.	Describe how the tester determined whether the modes of operation identified in T.3.1.2 may be open to exploitation.	*<Report findings here>*
	For each of the modes of operation identified in T.3.1.2: • Identify all exploitations (e.g., relocation or data analysis attacks on ECB mode) that the mode of operation could be open to. • Describe how the tester reached this determination.	*<Report findings here>*
	For each instance where a mode of operation is open to exploitation, describe how the tester confirmed that exploitation is not feasible for the implementation.	*<Report findings here>*
T.3.1.4 Where the mode of operation requires the use of another value, such as an Initialization Vector (IV) or counter, the tester shall confirm that the implementation ensures that this value is correct and secure.	Indicate whether any of the modes of operation identified in T.3.1.2 requires the use of another value, such as an IV or counter. (Yes/No) *If "Yes," complete the remaining reporting instructions for this assessment procedure.* *If "No," skip to T.3.1.5.*	*<Report findings here>*
	Identify the modes of operation identified in T.3.1.2 that require the use of another value, such as an IV or counter.	*<Report findings here>*
	For each mode of operation identified, describe how the tester confirmed that the implementation ensures that this value (e.g., IV or counter) is correct and secure.	*<Report findings here>*

Security Objective 2: Protect Sensitive 3DS SDK Data Elements		
3DS SDK Security Requirements and Assessment Procedures	**Reporting Instructions**	**Summary of Evaluation Findings**
T.3.1.5 The tester shall examine vendor materials and other evidence, including source code, to determine all key generation or key agreement processes that are used by the system, and to confirm that they ensure keys are generated with full entropy (e.g., a 128-bit key is generated with 128 bits of entropy input).	Identify the vendor materials, other evidence, and source code files examined that identify all key-generation or key-agreement processes used by the system.	*<Report findings here>*
	Describe each of the key generation or key agreement processes used by the system.	*<Report findings here>*
	For each key-generation or key-agreement process, describe how the tester confirmed that the process ensures the keys are generated with full entropy (e.g. a 128-bit key is generated with 128 bits of entropy input).	*<Report findings here>*
T.3.1.6 The tester shall confirm that no reversible key-calculation modes (such as key variants) are used to directly create new keys from an existing key. All key-generation functions must implement one-way functions or other irreversible key-generation processes.	For each key-generation function identified in T.3.1.5, describe how the tester confirmed that the function implements only irreversible key generation processes (such as one-way functions) and that reversible key calculation modes are not used.	*<Report findings here>*
T.3.1.7 The tester shall confirm that any key signature or fingerprint values returned by the system do not reveal any details about the key itself. Key checksum values (KCVs) must be limited to five bytes or less than half of the algorithm block size, whichever is smaller, and hash algorithms used for key fingerprints (on secret or private keys) must implement SHA256 or above.	Identify all instances where a key signature or fingerprint value could be returned by the system.	*<Report findings here>*
	For each instance identified, describe how the tester confirmed that the key signature or fingerprint values returned by the system do not reveal any details about the key itself.	*<Report findings here>*
	Describe how the tester confirmed that KCVs are limited to five bytes or less than half of the algorithm block size (whichever is smaller),	*<Report findings here>*
	Describe how the tester confirmed that hash algorithms used for key fingerprints (on secret or private keys) implement SHA256 or above.	*<Report findings here>*

Security Objective 2: Protect Sensitive 3DS SDK Data Elements		
3DS SDK Security Requirements and Assessment Procedures	**Reporting Instructions**	**Summary of Evaluation Findings**
T.3.1.8 The tester shall confirm that a cryptoperiod is defined for each key, and that update procedures are also defined to replace each key at the end of this cryptoperiod.	For each cryptographic key identified in T.3.1.1: • Identify the cryptoperiod defined. • Describe the update procedures used to replace the key at the end of the cryptoperiod.	*<Report findings here>*
T.3.1.9 The tester shall confirm that security is not provided to any key by a key of lesser strength—e.g., by encrypting a 256-bit AES key with a 128-bit AES key.	Describe how the tester confirmed that security is not provided to any of the keys identified in T.3.1.1 by a key of lesser strength.	*<Report findings here>*
T.3.1.10 For any public keys used by the system, the tester shall confirm that the authenticity of each public key is maintained. Use of public keys that are not signed or MAC'd or are maintained in self-signed certificates, is prohibited unless the authenticity of the key is ensured through use of a secure cryptographic module. Self-signed certificates that exist as part of the base platform on which the 3DS SDK is executed are excluded from this requirement.	Identify all public keys used by the system.	*<Report findings here>*
	For each pubic key identified, describe how the authenticity of the key is maintained.	*<Report findings here>*
	Describe how the tester confirmed that public keys that are not signed or MAC'd or that are maintained in self-signed certificates are not used unless the authenticity of the key is ensured through use of a secure cryptographic module.	*<Report findings here>*
T.3.1.11 The tester shall confirm that key purpose and integrity is ensured for all keys used in the system, preventing a key of one purpose (e.g., key encryption) from being replaced with a key of another purpose (e.g., general data encryption).	For each key identified in T.3.1.1, describe the purpose of that key and how the integrity of that key is ensured.	*<Report findings here>*
	Describe the methods used that prevent a key of one purpose from being replaced with a key of another purpose.	*<Report findings here>*

Security Objective 2: Protect Sensitive 3DS SDK Data Elements		
3DS SDK Security Requirements and Assessment Procedures	**Reporting Instructions**	**Summary of Evaluation Findings**
T.3.1.12 The tester shall confirm that each key has a single unique purpose, and that no keys are used for multiple purposes (such as both signing and encrypting data), and that keys used to encrypt Cardholder Verification Method (CVM) data are not used for any other operation (such as general-purpose data encryption, monitor message encryption, etc.).	Describe how the tester confirmed that no keys are used for multiple purposes (such as both signing and encrypting data).	*<Report findings here>*
	Describe how the tester confirmed that keys used to encrypt Cardholder Verification Method (CVM) data are not used for any other operation.	*<Report findings here>*
T.3.1.13 The tester shall confirm that keys used to validate the authenticity of a datagram are unique to each endpoint, so that a (H)MAC or signature generated at one end would always be different if generated by the other end point.	Describe how the tester confirmed that keys used to validate the authenticity of a datagram are unique to each endpoint (such that a (H)MAC or signature generated at one end would always be different if generated by the other end point).	*<Report findings here>*
Additional assessor comments: *<Report findings here>*		

Security Objective 3: Use Cryptography Appropriately and Correctly

3DS SDK Security Requirements and Assessment Procedures	Reporting Instruction	Summary of Evaluation Findings		
3.2 Random Number Generator(s) All random numbers used by the 3DS SDK are generated using only approved random number generation (RNG) algorithms or libraries. Approved RNG algorithms or libraries are those meeting industry standards for sufficient unpredictability (e.g., NIST Special Publication 800-22). ***Note**: Proof that RNG algorithms or libraries meet industry standards may include recognition by industry bodies, or evidence to show where those RNG algorithms or libraries were assessed to ensure that the random numbers generated are sufficiently unpredictable.*		**In Place** ☐	**N/A** ☐	**Not in Place** ☐
T.3.2.1 The tester shall examine vendor materials and other evidence, including source code, to determine the implementation of all random number generation functions used in the 3DS SDK implementation.	Identify vendor materials, other evidence, and source code files examined that describe the implementation of all random number generation functions used in the 3DS SDK implementation.	*<Report findings here>*		
	Describe all random number generation functions used in the 3DS SDK and how each is implemented.	*<Report findings here>*		
T.3.2.2 The tester shall examine vendor materials and other evidence, including source code, to determine all functions of the 3DS SDK that rely upon the on-device generation of random numbers. This should include uses such as random values required in secure communications channels (such as TLS).	Identify vendor materials, other evidence, and source code files examined that identify all functions of the 3DS SDK that rely upon the on-device generation of random numbers.	*<Report findings here>*		
	Describe all functions of the 3DS SDK that rely upon on-device generation of random numbers, including any that are used for securing communication channels (such as TLS).	*<Report findings here>*		

Security Objective 2: Protect Sensitive 3DS SDK Data Elements		
3DS SDK Security Requirements and Assessment Procedures	**Reporting Instructions**	**Summary of Evaluation Findings**
T.3.2.3 The tester shall confirm that the 3DS SDK does not rely solely on any on-device random number generators and always uses an RNG provided by or within the 3DS SDK for the purposes of generating random values that are relied upon for the secure functionality of the 3DS SDK. The tester shall reference the random values required by the 3DS SDK listed in T.3.2.2. Where any values are generated without the use of the 3DS SDK RNG, the tester shall confirm the use of the RNG is prevented by the platform targeted by the 3DS SDK, and that the use of the on-platform RNG does not violate the security of the 3DS operations.	Describe how the tester confirmed that the 3DS SDK: • Does not rely solely on any on-device random number generators. • Always uses an RNG provided by or within the 3DS SDK for the purposes of generating random values that are relied upon for the secure functionality of the 3DS SDK.	*<Report findings here>*
	For all values generated without the use of the 3DS SDK RNG (per the functions identified in T.3.2.2), describe how the tester confirmed that: • Use of the 3DS SDK RNG is prevented by the platform. • Use of the on-platform RNG does not violate the security of the 3DS operations.	*<Report findings here>*
T.3.2.4 The tester shall confirm that values provided by the RNG are sufficiently random in accordance with Requirement 3.3, "Random Number Entropy."	Describe the process and rationale the tester used to confirm that values provided by the RNG are sufficiently random (in accordance with Requirement 3.3).	*<Report findings here>*
T.3.2.5 The tester shall examine vendor materials and other evidence to determine any requirements for the developer integrating the 3DS SDK to ensure that the random numbers are sufficiently random. The tester shall confirm that there is clear and sufficient guidance outlining these requirements made available to stakeholders in accordance with Requirement 5.1, "Availability of Stakeholder Guidance."	Identify vendor materials, other evidence, and source code files examined that describe requirements for generating sufficient entropy for random numbers.	*<Report findings here>*
	Indicate whether the 3DS SDK is reliant on the developers integrating the 3DS SDK to ensure that the random numbers are sufficiently random. (Yes/No) *If "Yes," complete the remaining reporting instructions for this assessment procedure.* *If "No," skip to T.3.3.1.*	*<Report findings here>*

Security Objective 2: Protect Sensitive 3DS SDK Data Elements		
3DS SDK Security Requirements and Assessment Procedures	**Reporting Instructions**	**Summary of Evaluation Findings**
	Describe the guidance outlining these requirements that is made available to stakeholders in accordance with Requirement 5.	*<Report findings here>*
	Describe how the tester confirmed that following the guidance ensures that the random numbers are sufficiently random.	*<Report findings here>*
Additional assessor comments: *<Report findings here>*		

Security Objective 3: Use Cryptography Appropriately and Correctly

3DS SDK Security Requirements and Assessment Procedures	Reporting Instruction	Summary of Evaluation Findings		
3.3 Random Number Entropy Random values have entropy that meets the minimum effective security strength requirements of the cryptographic primitives and keys that rely on them.		**In Place** ☐	**N/A** ☐	**Not in Place** ☐
T.3.3.1 The tester shall examine vendor materials and other evidence, including source code, and the results of testing performed in Requirement 3.2, "Random Number Generator(s)," to determine how the RNG within the 3DS SDK is implemented and how the entropy for the RNG is generated.	Identify the vendor materials, other evidence, and source code files examined that describe how the RNG within the 3DS SDK is implemented and how entropy for the RNG is generated.	*<Report findings here>*		
	For each of the RNG functions described in T.3.2.1, describe how the entropy is generated.	*<Report findings here>*		
T.3.3.2 Where the 3DS SDK relies upon an RNG that has been approved under the NIST Cryptographic Algorithm Validation Program (CAVP), the tester shall confirm from the approval and/or security policy of the RNG, whether the RNG requires the initial entropy to be seeded externally.	Indicate whether the 3DS SDK relies upon an RNG that has been approved under the NIST CAVP program. (Yes/No) *If "Yes," complete the remaining reporting instructions for this assessment procedure.* *If "No," skip to T.3.3.3.*	*<Report findings here>*		
	Identify the approval and/or security policy of the RNG examined.	*<Report findings here>*		
	Describe where the RNG requires the initial entropy to be seeded from, and whether this is external to the 3DS SDK.	*<Report findings here>*		
T.3.3.3 Where the 3DS SDK is required to generate entropy through use of its own RNG or a RNG that requires external seeding, the tester shall confirm that there is sufficient entropy generated—e.g., through confirmation that the entropy generation involves inputs that cannot be predicted within the domain of the random values produced by the RNG.	Describe how the 3DS SDK generates entropy—e.g., through use of its own RNG or an RNG that requires external seeding.	*<Report findings here>*		
	Describe how the tester confirmed there is sufficient entropy generated.	*<Report findings here>*		

Security Objective 3: Use Cryptography Appropriately and Correctly		
3DS SDK Security Requirements and Assessment Procedures	**Reporting Instruction**	**Summary of Evaluation Findings**
T.3.3.4 The tester shall confirm that the RNG is seeded with a random value of at least 256 bits for use during all operations.	Describe how the tester confirmed the RNG is seeded with a random value of at least 256 bits for use during all operations.	*<Report findings here>*
T.3.3.5 The tester shall obtain at least two sets of 64MB of random data from each of the RNG implementations used in the system, generated during separate installs and initial executions on the same device. This data may be supplied directly by the vendor, but the tester must detail the method used to generate this data, and justify why this sufficiently replicates the way in which the RNG will be used by the system after two similar installations. The tester shall combine the two sets of data and pass this 128MB of data through the NIST STS test program, and detail the results, indicating pass and fail results and how these demonstrate compliance to this requirement. In some situations, it is necessary to repeat such tests using additionally obtained data to confirm final results.	Identify the sets of 64MB of random data obtained. For each set of data, identify the RNG implementation from which it was generated.	*<Report findings here>*
	For each set of 64MB of random data, identify how the set of data was obtained (e.g., supplied directly by the vendor or generated by the tester).	*<Report findings here>*
	Describe the method used to generate this data and explain why this sufficiently replicates the way in which the RNG will be used by the system after two similar installations.	*<Report findings here>*
	Describe the results of combining the two sets of data and passing this 128MB of data through the NIST STS test program. Include pass and fail results and how these results demonstrate compliance to this requirement.	*<Report findings here>*
	Indicate whether the tester deemed it necessary to repeat such tests using additionally obtained data and describe these results.	*<Report findings here>*
Additional assessor comments: *<Report findings here>*		

Security Objective 4: Manage Risks and Vulnerabilities				
3DS SDK Security Requirements and Assessment Procedures	**Reporting Instructions**	**Summary of Evaluation Findings**		
Requirement 4: Risks and vulnerabilities affecting the 3DS SDK are minimized and addressed in a timely manner.				
4.1 Threat and Vulnerability Analysis Threats, attack scenarios and/or attack vectors applicable to the 3DS SDK are known, analyzed, documented, and described in terms of their exploitability, impact, and residual risk.		**In Place** ☐	**N/A** ☐	**Not in Place** ☐
T.4.1.1 The tester shall examine vendor materials and other evidence to confirm that a process is implemented by the 3DS SDK Vendor for identifying, documenting, and analyzing threats, vectors, and attack scenarios applicable to the 3DS SDK.	Identify the vendor materials and other evidence examined that confirm a process is implemented by the 3DS SDK vendor for identifying, documenting, and analyzing threats, vectors, and attack scenarios applicable to the 3DS SDK.	*<Report findings here>*		
	Describe the process implemented by the 3DS SDK vendor for identifying, documenting, and analyzing threats, vectors, and attack scenarios applicable to the 3DS SDK.	*<Report findings here>*		
T.4.1.2 The tester shall confirm that the process required is sufficiently detailed for it to be repeatable across different personnel and locations.	Describe methods and rationale used by the tester to confirm that the process is sufficiently detailed for it to be repeatable across different personnel and locations.	*<Report findings here>*		
T.4.1.3 The tester shall confirm that the process clearly outlines the individuals or teams responsible for determining and investigating new threats. It is acceptable if a group or job title is referenced, but the tester must ensure that there is a clear line of responsibility for this item.	Identify the individuals or teams outlined in the process as being responsible for determining and investigating new threats.	*<Report findings here>*		
	Explain how the tester confirmed there is a clear line of responsibility for this item.	*<Report findings here>*		

Security Objective 4: Manage Risks and Vulnerabilities		
3DS SDK Security Requirements and Assessment Procedures	**Reporting Instructions**	**Summary of Evaluation Findings**
T.4.1.4 The tester shall interview a sample of the personnel identified in T.4.1.3 and confirm that they are aware of the policy and procedure requirements for the analysis of new threats. The tester shall also examine vendor materials and other evidence produced by these interviewees to confirm that defined processes are being followed.	Identify the sample of individuals interviewed and explain how they demonstrated awareness of the policy and procedure requirements for the analysis of new threats.	*<Report findings here>*
	Describe the vendor materials and other evidence produced by these interviewees that confirms the defined processes are being followed.	*<Report findings here>*
T.4.1.5 The tester shall confirm from the evidence identified in T.4.1.1 that methods are defined and used for categorizing and ranking threats. The tester shall confirm that a documented methodology exists, which can be reasonably assumed to produce the same results each time it is enacted (assuming the same threat and threat environment). It is not a requirement that a public ranking method is used; it is acceptable for the vendor to implement its own method if this provides sufficient assurance and repeatability.	Describe the evidence identified in T.4.1.1 that confirms methods are defined and used for categorizing and ranking threats.	*<Report findings here>*
	Describe the documented methodology for categorizing and ranking threats, and how it can be reasonably assumed to produce the same results each time it is enacted (assuming the same threat and threat environment).	*<Report findings here>*
T.4.1.6 The tester shall interview a sample of the personnel identified in T.4.1.3 and confirm that they understand and can apply the categorizing and ranking methodology employed by the vendor.	Identify the sample of individuals interviewed and explain how they demonstrated understanding and that they can apply the categorizing and ranking methodology employed by the vendor.	*<Report findings here>*
T.4.1.7 For a sample of threats identified in T.4.1.4, the tester shall obtain the categorizing and ranking results for the sample and confirm that they align with the documented process.	Identify the sample of threats (from the vendor materials and other evidence examined in T.4.4.1) for which the categorizing and ranking results align with the documented process (described in T.4.1.5).	*<Report findings here>*
Additional assessor comments: *<Report findings here>*		

Security Objective 4: Manage Risks and Vulnerabilities				
3DS SDK Security Requirements and Assessment Procedures	**Reporting Instructions**	**Summary of Evaluation Findings**		
4.2 Development of Defensive Strategies and Mechanisms Defensive strategies and mechanisms to protect against attack vectors and/or attack scenarios are designed and implemented. Attack scenarios that are applicable to the 3DS SDK but are not specifically addressed are justified.		**In Place** ☐	**N/A** ☐	**Not in Place** ☐
T.4.2.1 The tester shall examine vendor materials and other evidence to confirm that there are clear, documented vendor policy and procedure statements regarding the remediation of identified vulnerabilities in the 3DS SDK. These statements must tie together with the identification and ranking process covered under Requirement 4.1, "Threat and Vulnerability Analysis."	Identify the vendor materials and other evidence examined that confirm there are clear, documented vendor policy and procedure statements regarding the remediation of identified vulnerabilities in the 3DS SDK.	*<Report findings here>*		
	Describe the policy and procedures for remediation of identified vulnerabilities in the 3DS SDK, and how these align with the identification and ranking process covered under Requirement 4.1.	*<Report findings here>*		
T.4.2.2 The tester shall determine whether the vendor explicitly allows for potential threats to remain un-addressed and, if so, the tester shall confirm that ranking/categorization levels are considered acceptable for this (as assessed in Requirement 4.1, "Threat and Vulnerability Analysis"), and that either this ranking process or another process explicitly involves a step to document and justify why it is acceptable to not address this vulnerability specifically.	Indicate whether the vendor explicitly allows potential threats to remain un-addressed. (Yes/No) *If Yes, complete the remaining reporting instructions for this assessment procedure.* *If No, skip to T.4.2.3.*	*<Report findings here>*		
	Explain how the ranking/categorization levels (as assessed in Requirement 4.1) are considered acceptable for allowing potential threats to remain un-addressed.	*<Report findings here>*		
	Describe the process (either the ranking process or another process) that explicitly involves a step to document and justify why it is acceptable to not address this vulnerability specifically.	*<Report findings here>*		
T.4.2.3 The tester shall interview personnel responsible for the implementation of defensive strategies and confirm that they know of and understand the policy and procedure requirements for this process.	Identify the sample of individuals interviewed and explain how the individuals demonstrated their knowledge and understanding of the policy and procedure requirements for this process.	*<Report findings here>*		

Security Objective 4: Manage Risks and Vulnerabilities		
3DS SDK Security Requirements and Assessment Procedures	**Reporting Instructions**	**Summary of Evaluation Findings**
T.4.2.4 Referencing the documented threats and vulnerabilities sampled in Requirement 4.1, "Threat and Vulnerability Analysis," the tester shall determine whether any vulnerabilities have been not specifically remediated and, if so, confirm that this is due to the correct and documented steps involved in the policy and procedures identified in T.4.2.1. Where all vulnerabilities have been addressed, the tester shall obtain more evidence to address this testing requirement. If vendor policy is to mitigate all threats and vulnerabilities, the tester shall require an increased sample size to confirm that each and every threat has been addressed.	For the documented threats and vulnerabilities sampled in Requirement 4.1, indicate whether they all have been remediated. *Complete the following Reporting Instructions as applicable.*	*<Report findings here>*
	• *If any of the documented threats and vulnerabilities (referenced in Requirement 4.1) have not been remediated:* Describe how the tester confirmed that the correct and documented steps involved in the policy and procedures identified in T.4.2.1 were followed.	*<Report findings here>*
	• *If all of the documented threats and vulnerabilities (referenced in Requirement 4.1) have been remediated and the vendor explicitly allows for potential threats to remain un-addressed:* Identify the additional evidence examined that confirms the correct and documented steps involved in the policy and procedures identified in T.4.2.1 were followed.	*<Report findings here>*
	• *If all of the documented threats and vulnerabilities (referenced in Requirement 4.1) have been remediated and the vendor policy is to mitigate all threats and vulnerabilities:* Identify the increased sample size that confirms that each and every threat has been addressed.	*<Report findings here>*
Additional assessor comments: *<Report findings here>*		

Security Objective 4: Manage Risks and Vulnerabilities				
3DS SDK Security Requirements and Assessment Procedures	**Reporting Instructions**	**Summary of Evaluation Findings**		
4.3 Software Security Testing Software security testing is an integral part of the 3DS SDK's life cycle, and is performed throughout the software life cycle to confirm that risks and attack scenarios are addressed, defensive mechanisms are implemented properly and the propagation of design flaws or vulnerabilities into production code is prevented.		**In Place** ☐	**N/A** ☐	**Not in Place** ☐
T.4.3.1 The tester shall examine vendor materials and other evidence to confirm that the vendor has written policy and procedures requiring internal security review and testing that accounts for the entire 3DS SDK code base, including detecting vulnerabilities in code developed by the vendor, as well as vulnerabilities in third-party, open source, or shared components or libraries.	Identify the vendor materials and other evidence examined that confirm the vendor has written policy and procedures that: • Require internal security review and testing that accounts for the entire 3DS SDK code base. • Include detecting vulnerabilities in code developed by the vendor, as well as vulnerabilities in third-party, open source, or shared components or libraries.	*<Report findings here>*		
T.4.3.2 The tester shall confirm that the process for testing of internal code involves both manual and automated means.	Describe how the tester confirmed the process includes both manual and automated means.	*<Report findings here>*		
T.4.3.3 The tester shall confirm that the process clearly outlines the individuals or teams responsible for this testing. It is acceptable if a group or job title is referenced, but the tester must ensure that there is a clear line of responsibility for this item.	Identify the individuals or teams outlined in the process as being responsible for the testing.	*<Report findings here>*		
	Explain how the tester confirmed there is a clear line of responsibility for this item.	*<Report findings here>*		
T.4.3.4 The tester shall confirm that the process includes ensuring that the processes for identification and mitigation of threats are correctly performed prior to the release of any production code.	Describe how the process ensures threats are correctly identified and mitigated prior to the release of any production code.	*<Report findings here>*		
T.4.3.5 The tester shall confirm that the process includes ensuring that any test, debug, or other code that is intended only for internal use is removed prior to release to production.	Describe how the process ensures that any test, debug, or other code that is intended only for internal use is removed prior to release to production.	*<Report findings here>*		

Security Objective 4: Manage Risks and Vulnerabilities		
3DS SDK Security Requirements and Assessment Procedures	**Reporting Instructions**	**Summary of Evaluation Findings**
T.4.3.6 Referencing threats sampled in the tests for Requirement 4.1, "Threat and Vulnerability Analysis," the tester shall examine vendor materials and other evidence, interview personnel, and test the 3DS SDK to confirm that threats identified and noted as required to be mitigated were addressed before the 3DS SDK was released.	Identify the vendor materials and other evidence examined that confirm that threats identified and noted as required to be mitigated (as referenced in Requirement 4.1) were addressed before the 3DS SDK was released.	*<Report findings here>*
	Identify the personnel interviewed who confirmed that the threats identified and noted as required to be mitigated (as referenced in Requirement 4.1) were addressed before the 3DS SDK was released.	*<Report findings here>*
	Describe the testing performed, the results of each test, and the rationale used by the tester to confirm that threats identified and noted as required to be mitigated (as referenced in Requirement 4.1) were addressed before the 3DS SDK was released.	*<Report findings here>*
Additional assessor comments: *<Report findings here>*		

Security Objective 4: Manage Risks and Vulnerabilities

3DS SDK Security Requirements and Assessment Procedures	Reporting Instructions	Summary of Evaluation Findings		
4.4 Vulnerability Identification and Monitoring The 3DS SDK and its components are monitored for vulnerabilities. In addition to their own processes, 3DS SDK Vendors provide mechanisms to enable third parties to report vulnerabilities. Information on identified vulnerabilities is maintained. Vulnerabilities are addressed and software updates are made available to all stakeholders in a timely manner. All exceptions are documented and justified. The reoccurrence of previously addressed vulnerabilities is tracked and minimized.		**In Place** ☐	**N/A** ☐	**Not in Place** ☐
T.4.4.1 The tester shall examine vendor materials and other evidence to confirm that there is a documented release policy for the 3DS SDK, and that this ensures the processes outlined in previous 4.x requirements are followed before the SDK is released to production.	Identify the vendor materials and other evidence examined that confirm: • There is a documented release policy for the 3DS SDK, • The policy ensures the processes outlined in the previous 4.x requirements are followed before the SDK is released to production.	*<Report findings here>*		
T.4.4.2 The tester shall confirm that the release policy clearly outlines the acceptable period of time after which patches are made available for the different rankings of vulnerabilities as defined in previous 4.x requirements.	Describe the acceptable period(s) of time clearly outlined in the release policy after which patches are made available.	*<Report findings here>*		
T.4.4.3 The tester shall examine vendor materials and other evidence, and interview personnel to confirm that the vendor has an explicit procedure in place for the acceptance and processing of new vulnerabilities through external communications. Although not mandated, this requirement can be met by a properly administered bug bounty program. It does require that reported vulnerabilities are formally registered and processed according to the documented process previously assessed in the 4.x requirements.	Identify the vendor materials and other evidence examined that confirm the vendor has an explicit procedure in place for the acceptance and processing of new vulnerabilities through external communications.	*<Report findings here>*		
	Describe the procedure for acceptance and processing of new vulnerabilities through external communications.	*<Report findings here>*		
	Identify the personnel interviewed who confirmed that the procedure for acceptance and processing of new vulnerabilities through external communications is followed.	*<Report findings here>*		

Security Objective 4: Manage Risks and Vulnerabilities		
3DS SDK Security Requirements and Assessment Procedures	**Reporting Instructions**	**Summary of Evaluation Findings**
T.4.4.4 The tester shall examine vendor materials and other evidence, and interview personnel to confirm that there is a public-facing procedure for the reporting of vulnerabilities in the 3DS SDK. This procedure must implement methods to ensure the confidentiality of the vulnerability as it is reported. For example, a process that requires the reporting of a vulnerability to a shared "info@[company]" e-mail address, without additional encryption, would be non-compliant to this requirement. ***Note**: Use of a specific web portal secured with TLS (using acceptable ciphersuites), and/or e-mails secured with strong cryptography are examples of acceptable methods to secure the confidentiality of vulnerability reporting.*	Identify the vendor materials and other evidence examined that confirm: • There is a public-facing procedure for the reporting of vulnerabilities in the 3DS SDK. • The procedure implements methods to ensure the confidentiality of the vulnerability as it is reported	*<Report findings here>*
	Describe the public-facing procedure for reporting of vulnerabilities in the 3DS SDK, including the methods for ensuring the confidentiality of the vulnerability as it is reported.	*<Report findings here>*
	Identify the personnel interviewed who confirm that the procedure for reporting of vulnerabilities in the 3DS SDK, including the methods to ensure the confidentiality of the vulnerability as it is reported, are followed.	*<Report findings here>*
T.4.4.5 The tester shall examine vendor materials and other evidence, and interview personnel to confirm that, where any such third-party vulnerability reports have been accepted and processed, the process appears correct—e.g., through validation of any special e-mail address or portal that is to be used for public vulnerability reporting.	Indicate whether any such third-party vulnerability reports have been accepted and processed by the vendor. (Yes/No) *If Yes, complete the remaining reporting instructions for this assessment procedure.* *If No, skip to T.4.4.6*	*<Report findings here>*
	For all instances where third-party vulnerability reports have been accepted and processed, describe the vendor materials and other evidence examined that confirm the process appears correct.	*<Report findings here>*
	For all instances where third-party vulnerability reports have been accepted and processed, identify the personnel interviewed who confirm that the process was correct.	*<Report findings here>*

Security Objective 4: Manage Risks and Vulnerabilities		
3DS SDK Security Requirements and Assessment Procedures	**Reporting Instructions**	**Summary of Evaluation Findings**
T.4.4.6 The tester shall examine vendor materials and other evidence to confirm that there is a process to validate that new releases have not re-introduced older vulnerabilities. This may involve the process being updated to specifically check for vulnerabilities as they are discovered, or ensuring that older and un-patched software components and libraries are removed from the development environment as they are updated.	Identify the vendor materials and other evidence examined that confirm there is a process to validate that new releases have not re-introduced older vulnerabilities.	*<Report findings here>*
	Describe the vendor's process for validating that new releases have not re-introduced older vulnerabilities.	*<Report findings here>*
T.4.4.7 The tester shall examine vendor materials and other evidence, and interview personnel to confirm that the process as documented is understood and followed. Where previously sampled vulnerabilities identified the need for an update to internal libraries or components, the tester shall confirm through these interviews and evidence that these have been correctly updated and the older, unpatched versions have been removed.	Describe the vendor materials and other evidence examined that confirms the documented process is followed. Where previously sampled vulnerabilities identified the need for an update to internal libraries or components, describe how the evidence confirms that these have been correctly updated and the older, unpatched versions have been removed.	*<Report findings here>*
	Identify the personnel interviewed who confirm that the documented process is understood and followed. Where previously sampled vulnerabilities identified the need for an update to internal libraries or components, describe how these interviews confirmed that these have been correctly updated and the older, unpatched versions have been removed.	*<Report findings here>*

Security Objective 4: Manage Risks and Vulnerabilities		
3DS SDK Security Requirements and Assessment Procedures	**Reporting Instructions**	**Summary of Evaluation Findings**
T.4.4.8 Where not covered under previous requirements, the tester shall examine vendor materials and other evidence, and interview personnel to confirm that any decisions not to address vulnerabilities are reasonably justified and documented.	Describe the vendor materials and other evidence examined that confirm that any decisions not to address vulnerabilities are reasonably justified and documented.	*<Report findings here>*
	Identify the personnel interviewed who confirm any decisions not to address vulnerabilities are reasonably justified and documented.	*<Report findings here>*
Additional assessor comments: *<Report findings here>*		

Security Objective 4: Manage Risks and Vulnerabilities

3DS SDK Security Requirements and Assessment Procedures	Reporting Instructions	Summary of Evaluation Findings		
4.5 Updates During Transaction Processing The 3DS SDK Vendor does not enable updates or changes to 3DS SDK functionality to be pushed to the 3DS SDK during 3DS transaction processing.		**In Place** ☐	**N/A** ☐	**Not in Place** ☐
T.4.5.1 The tester shall examine vendor materials and other evidence to confirm that the 3DS SDK does not accept updates during 3DS transaction processing.	Describe the vendor materials and other evidence examined that confirm the 3DS SDK does not accept updates during 3DS transaction processing.	*<Report findings here>*		
T.4.5.2 The tester shall examine vendor materials and other evidence, including source code, to confirm that methods are implemented to prevent the SDK from being updated during 3DS transaction processing.	Describe the vendor materials and other evidence examined, including source code, that confirm methods are implemented to prevent the SDK from being updated during 3DS transaction processing.	*<Report findings here>*		
	Describe the methods implemented to prevent the SDK from being updated during 3DS transaction processing.	*<Report findings here>*		
T.4.5.3 Where the operating systems and platforms targeted by the 3DS SDK do not allow for the applications to prevent or delay updates themselves, the tester shall confirm that other protections have been put in place by the vendor to mitigate interruption of the 3DS transaction process during updates.	For each operating system and platform tested, indicate whether the operating system and platform allow for the applications to prevent or delay updates themselves. (Yes/No) *If Yes for any operating system/platform, complete the remaining reporting instructions for this assessment procedure for that operating system/platform.* *If No for all operating systems/platforms, skip to T.4.5.4.*	*<Report findings here>*		
	Describe how the tester confirmed that other protections have been put in place by the vendor to mitigate interruption of the 3DS transaction process during updates.	*<Report findings here>*		

Security Objective 4: Manage Risks and Vulnerabilities		
3DS SDK Security Requirements and Assessment Procedures	**Reporting Instructions**	**Summary of Evaluation Findings**
T.4.5.4 The tester shall test the 3DS SDK by performing a series of 3DS transactions within a test host/harness that allows for updates to be pushed to the 3DS SDK, to confirm that the 3DS SDK does not accept updates during the transaction processing, and that the outcome of this testing aligns with the vendor materials and evidence provided in T.4.5.1 through T.4.5.3.	Describe each of the tests performed to determine how the 3DS SDK responds to attempts to push updates to the 3DS SDK during 3DS transaction processing. Describe the results of each test performed.	*<Report findings here>*
	Describe how the tester confirmed that the test host/harness allows for updates to the pushed to the 3DS SDK.	*<Report findings here>*
	Describe how the results of the tests performed confirm that the 3DS SDK does not accept updates during the transaction processing,	*<Report findings here>*
	Describe how the outcome of this testing aligns with the information specified in the vendor materials and evidence provided in T.4.5.1 through T.4.5.3.	*<Report findings here>*
Additional assessor comments: *<Report findings here>*		

Security Objective 5: Provide Guidance to Stakeholders

3DS SDK Security Requirements and Assessment Procedures	Reporting Instructions	Evaluation Findings		
Requirement 5: The 3DS SDK Vendor provides written security guidance to stakeholders.				
5.1 Availability of Stakeholder Guidance The 3DS SDK Vendor creates, maintains, and makes available guidance to all stakeholders on the appropriate and secure implementation, configuration, and use of the 3DS SDK as well as all APIs provided by the 3DS SDK.		**In Place** ☐	**N/A** ☐	**Not in Place** ☐
T.5.1.1 The tester shall examine vendor materials and other evidence to confirm that the 3DS SDK Vendor maintains detailed security guidance for the secure implementation of the 3DS SDK, as determined in previous testing within this standard, and that such guidance contains all references required for a secure implementation and configuration of the 3DS SDK.	Describe the vendor materials and other evidence examined that confirm the 3DS SDK vendor maintains detailed security guidance for the secure implementation of the 3DS SDK.	*<Report findings here>*		
	Describe how the tester confirmed the guidance contains all references required for a secure implementation and configuration of the 3DS SDK.	*<Report findings here>*		
T.5.1.2 The tester shall confirm that vendor security guidance is made available to all software developers who will be integrating the 3DS SDK into their applications. The tester shall also confirm there are no specific legal, distribution, or other requirements that appear to prevent the distribution of the security guidance to developers who require this guidance—e.g., a data classification that prevents the document from being distributed to other entities.	Describe how the tester confirmed that vendor security guidance is made available to all software developers who will be integrating the 3DS SDK into their applications.	*<Report findings here>*		
	Describe how the tester confirmed there are no specific legal, distribution, or other requirements that appear to prevent the distribution of the security guidance to developers who require this guidance.	*<Report findings here>*		

Security Objective 5: Provide Guidance to Stakeholders		
3DS SDK Security Requirements and Assessment Procedures	**Reporting Instructions**	**Evaluation Findings**
T.5.1.3 The tester shall confirm that the security guidance identifies all configurable security-related options and parameters of the 3DS SDK, and provides guidance on how to properly configure and secure these options and parameters.	Identify all configurable security-related options and parameters of the 3DS SDK that are included in the security guidance.	*<Report findings here>*
	For each option and parameter, describe how the tester confirmed that following the guidance results in the option and parameters being properly configured and secured.	*<Report findings here>*
T.5.1.4 For all scenarios where the 3DS SDK receives or generates sensitive 3DS SDK data elements, the tester shall confirm that the security guidance specifically notes how these are to be transmitted to/from the 3DS SDK in a secure manner. The tester shall reference testing performed under Requirement 1 to confirm the correct guidance for all sensitive 3DS SDK data elements used.	Indicate whether the 3DS SDK accepts and receives sensitive 3DS SDK data elements. (Yes/No) *If Yes, complete the remaining reporting instructions for this assessment procedure.* *If No, skip to T.5.1.5.*	*<Report findings here>*
	Identify all instances where the 3DS SDK accepts and receives sensitive 3DS SDK data elements.	*<Report findings here>*
	Describe the specific notes within the security guidance that address how sensitive 3DS SDK data elements are to be received and provided to the 3DS SDK in a secure manner. Include references to testing performed under Requirement 1, as applicable.	*<Report findings here>*
T.5.1.5 Where the 3DS SDK requires entropy input from the application for the purposes of seeding the random number generator, the tester shall confirm that the security guidance includes examples of methods on how to successfully generate entropy on the end system, and how much entropy is required for the secure operation of the 3DS SDK.	Indicate whether the 3DS SDK requires entropy input from the application for the purposes of seeding the random number generator. (Yes/No) *If Yes, complete the remaining reporting instructions for this assessment procedure.* *If No, skip to T.5.1.6.*	*<Report findings here>*
	Identify and describe the methods included in the security guidance on how to successfully generate entropy on the end-system.	*<Report findings here>*

Security Objective 5: Provide Guidance to Stakeholders		
3DS SDK Security Requirements and Assessment Procedures	**Reporting Instructions**	**Evaluation Findings**
	Identify how much entropy is required for the secure operation of the 3DS SDK, as defined in the security guidance.	*<Report findings here>*
T.5.1.6 The tester shall confirm that the vendor has a documented policy and procedure for the generation of the security guidance prior to release of the 3DS SDK.	Describe how the tester confirmed the vendor has a documented policy and procedure for the generation of the security guidance prior to release of the 3DS SDK.	*<Report findings here>*
T.5.1.7 The tester shall confirm that an individual or group is assigned the clear responsibility for the maintenance and update of the security guidance. The tester shall interview a sample of these individuals and confirm they understand the requirements for the security guidance, and that they are aware of their responsibility for managing this information.	Identify the individual or group assigned responsibility for the maintenance and update of the security guidance.	*<Report findings here>*
	Identify the individuals interviewed who confirmed that they understand the requirements for the security guidance, and that they are aware of their responsibility for managing this information.	*<Report findings here>*
Additional assessor comments: *<Report findings here>*		

Security Objective 5: Provide Guidance to Stakeholders				
3DS SDK Security Requirements and Assessment Procedures	**Reporting Instructions**	**Evaluation Findings**		
5.2 Disclosure of Updates to Stakeholders Upon any changes and/or updates to the 3DS SDK, the 3DS SDK Vendor provides all stakeholders with a clear and unambiguous indication that updates were made, and makes available detailed information regarding the specific changes made, the functionalities that are affected and the potential security impacts associated with those changes (for example, release notes). The relationship between the updated software and detailed information about the updates should be clear.		**In Place** ☐	**N/A** ☐	**Not in Place** ☐
T.5.2.1 The tester shall examine vendor materials and other evidence to confirm that procedures exist to clearly communicate changes to the 3DS SDK security guidance to relevant stakeholders. This process must require the initiation of contact regarding the change from the 3DS SDK Vendor; it is not considered acceptable to post changes on a website or other location that requires the stakeholder to initiate a process to check whether changes have been made. A process involving e-mails to the stakeholders to inform them of updates is considered an acceptable example of initiation.	Identify the vendor materials and other evidence examined that confirm procedures are defined to clearly communicate changes to the 3DS SDK security guidance to the relevant stakeholders.	*<Report findings here>*		
	Describe the procedures for clearly communicating changes to the 3DS SDK security guidance to relevant stakeholders.	*<Report findings here>*		
	Describe how the 3DS SDK vendor notifies and informs stakeholders of changes to the 3DS SDK.	*<Report findings here>*		
T.5.2.2 The tester shall examine vendor materials and other evidence to confirm that the procedures for updating the security guidance requires or includes the production of details indicating exactly what has changed in this new version. This may be in the form of release notes or a marked-up version of the document. A full trace of changes must be possible from the first release of the security guidance through the most current version.	Describe how details indicating exactly what has changed in the new version are produced as part of the procedures for updating the security guidance.	*<Report findings here>*		
	Describe how the process ensures a full trace of changes is possible from the first release of the security guidance through to the most current version.	*<Report findings here>*		

Security Objective 5: Provide Guidance to Stakeholders		
3DS SDK Security Requirements and Assessment Procedures	**Reporting Instructions**	**Evaluation Findings**
T.5.2.3 The tester shall confirm that the change notice also includes any impacts to the functionality and/or security of the 3DS SDK, as applicable. This should include any new requirements that are conveyed to the application integrating the 3DS SDK—e.g., new APIs that must be called, or changes to the way in which entropy must be collected and passed to the 3DS SDK.	Describe how the change notice includes descriptions of all impacts to 3DS SDK functionality and security.	*<Report findings here>*
	Describe how the tester confirmed this process includes new requirements for the application integrating the 3DS SDK.	*<Report findings here>*
T.5.2.4 The tester shall confirm that the process for informing and distributing the security guidance also ensures the distribution of the change details.	Describe how the tester confirmed that the process for informing and distributing the security guidance also ensures the distribution of the change details.	*<Report findings here>*
Additional assessor comments: *<Report findings here>*		

Security Objective 5: Provide Guidance to Stakeholders

3DS SDK Security Requirements and Assessment Procedures	Reporting Instructions	Evaluation Findings		
5.3 Frequency of Updates to Stakeholder Guidance The 3DS SDK Vendor updates security guidance whenever changes warrant updates. The criteria for determining whether updates are necessary are clearly defined by the vendor and are reasonable. At a minimum, security guidance is reviewed at least annually, and updates made whenever new or changes to functionality, security features, APIs, or configurable settings are introduced.		**In Place** ☐	**N/A** ☐	**Not in Place** ☐
T.5.3.1 The tester shall examine vendor materials and other evidence to confirm that the vendor has a documented policy and procedure to identify when updates to the security guidance are necessary.	Identify the vendor materials and other evidence examined that confirm the vendor maintains a documented policy and procedure for identifying when updates to the security guidance are necessary.	*<Report findings here>*		
	Describe the vendor's procedure for identifying when updates to the security guidance are necessary.	*<Report findings here>*		
T.5.3.2 The tester shall examine vendor materials and other evidence to confirm that the vendor has a documented policy and procedure requiring regular reviews of the security guidance. At a minimum, there must be a procedure to review the 3DS SDK and confirm any updates required at least annually.	Describe the vendor's policy and procedure requiring regular reviews of the security guidance.	*<Report findings here>*		
	Describe the vendor's procedure and frequency for reviewing the 3DS SDK to confirm if any updates are required.	*<Report findings here>*		
T.5.3.3 Where possible, the tester shall obtain previous versions of the security guidance and confirm that they have been updated and published in accordance with the vendor policy and procedure.	Identify previous versions of the security guidance examined that confirm they have been updated and published in accordance with the vendor policy and procedure. If previous versions of the security guidance are not available, describe how the assessor confirmed that security guidance is updated and published in accordance with the vendor policy and procedure.	*<Report findings here>*		

Security Objective 5: Provide Guidance to Stakeholders		
3DS SDK Security Requirements and Assessment Procedures	**Reporting Instructions**	**Evaluation Findings**
T.5.3.4 The tester shall interview a sample of the personnel responsible for updating the security guidance to confirm that they understand the policy and procedures for this, as well as their responsibility for maintaining and updating this document.	Identify the sample of individuals interviewed who confirmed they understand the policy and procedures for updating the security guidance, as well as their responsibility for maintaining and updating this document.	*<Report findings here>*
T.5.3.5 The tester shall confirm that the vendor policy and procedures require updates to the security guidance when new or changes to functionality, security features, APIs or configurable settings are introduced.	Describe how the vendor policy and procedures require updates to the security guidance when new or changes to functionality, security features, APIs, or configurable settings are introduced.	*<Report findings here>*
T.5.3.6 The tester shall interview a sample of the personnel responsible for updating the security guidance to confirm that they understand that the security guidance must be updated when new or changes to functionality, security features, APIs or configurable settings are introduced.	Identify the sample of individuals interviewed who confirmed they understand that the security guidance must be updated when new or changes to functionality, security features, APIs, or configurable settings are introduced.	*<Report findings here>*
Additional assessor comments: *<Report findings here>*		

Appendix A: Explanation of Non-Applicability

If the "N/A" (Not Applicable) column is selected for any requirement in the Summary of Evaluation Findings column, use this Appendix to explain why the related requirement is not applicable.

Requirement	Reason Requirement is Not Applicable
Example:	
1.1	The requirement does not apply to the 3DS SDK because…

Appendix B: Additional Information to Summary of Evaluation Findings

If the evaluation finding information cannot be included in the Summary of Evaluation Findings column, use this Appendix to include the additional information. Record in the Summary of Evaluation Finding that additional information is recorded in Appendix B.

Requirement	Assessment Procedure	Additional Information
Example:		
1.1	T.1.1.1	A table of all error/warning messages returned by the 3DS SDK to the 3DS Requestor App is attached to this ROV.