Payment Card Industry (PCI)

3-D Secure (PCI 3DS)

3DS Assessor Program Guide

Version 1.0

November 2017

Document Changes

Date	Version	Description
November 2017	1.0	This is the first release of the 3DS Assessor Program Guide.

Contents

1 Introduction

This Program Guide provides information to QSA Companies and QSA Employees participating in the 3DS Program as 3DS Assessor Companies or 3DS Assessor Employees. The requirements for QSA Companies and QSA Employees to participate in the 3DS Program are described in the 3DS Qualification Requirements on the Website, and capitalized terms used but not otherwise defined herein are defined in the 3DS Qualification Requirements.

The 3DS Assessor Program Guide and 3DS Qualification Requirements do not make any references to the EMV 3-D Secure Software Development Kit (SDK). Refer to the 3DS SDK Program Guide for information on the *PCI 3DS SDK Security Standard*.

2 Related Publications

This document should be reviewed in conjunction with other relevant PCI SSC publications, including but not limited to current publically available versions of the following, each available on the Website.

Document name	Description
Payment Card Industry (PCI) Qualification Requirements For 3DS Assessors (3DS Qualification Requirements)	Defines the baseline set of requirements that must be satisfied by 3DS Assessor Companies and 3DS Assessor Employees in order to perform compliance assessments against the PCI 3DS Core Security Standard.
Security Requirements and Assessment Procedures for EMV® 3-D Secure Core Components: ACS, DS, and 3DS Server (PCI 3DS Core Security Standard)	Lists the specific security requirements and assessment procedures used by 3DS assessors to validate 3DS Core Security compliance.
Payment Card Industry (PCI) Data Security Standard Requirements and Security Assessment Procedures (PCI DSS)	Lists the specific technical and operational security requirements and provides the assessment procedures used by assessors to validate PCI DSS compliance.
PCI DSS Qualification Requirements for Qualified Security Assessors (QSAs) (QSA Qualification Requirements)	Defines the baseline set of requirements that must be met by a QSA Company and Assessor-Employees in order to perform compliance assessments against the PCI DSS.
Payment Card Industry (PCI) Qualified Security Assessor Program Guide (QSA Program Guide)	Provides information pertinent to any role associated with the QSA Program.
PCI 3DS Report on Compliance Template for use with PCI 3DS Core Security Standard (3DS ROC)	Provides detail on how to document the findings of a PCI 3DS Assessment and includes the mandatory template for use in completing a 3DS Report on Compliance.
QSA Feedback Form	Gives the customer an opportunity to offer feedback regarding the QSA and the assessment process. https://www.pcisecuritystandards.org/assessors_and_solutions/qualified_security_assessors_feedback

3 Updates to Documents and Security Requirements

This Program Guide may be modified as necessary to align with updates to the *Security Requirements and Assessment Procedures for EMV® 3-D Secure Core Components: ACS, DS, and 3DS Server* (PCI 3DS Core Security Standard) and other PCI SSC Standards. Additionally, PCI SSC provides interim updates to the PCI community through a variety of means, including required QSA Employee training, e-mail bulletins and newsletters, frequently asked questions, and other communication methods.

PCI SSC reserves the right to change, amend, or withdraw security requirements, training, and/or other requirements at any time.

4 Terminology

For purposes of this Program Guide, the following terms shall have the meanings set forth below or in the documents referenced below. All such documents are available on the Website:

Term	Definition / Source / Document Reference
3DS Data Environment (3DE)	Refer to the PCI 3DS Core Security Standard
Participating Payment Brand	Refer to QSA Agreement.
PCI DSS	Refer to QSA Qualification Requirements.
PCI SSC	PCI Security Standards Council, LLC, which manages the PCI SSC Standards.
QSA Agreement	Appendix A to QSA Qualification Requirements.
QSA Company	Refer to QSA Qualification Requirements.
QSA Employee	Refer to QSA Qualification Requirements.

5 Roles and Responsibilities

Roles and responsibilities associated with various 3DS Program stakeholders include the following:

5.1 Participating Payment Brands

In relation to the PCI 3DS Core Security Standard, the Participating Payment Brands independently develop and enforce the various aspects of their respective programs related to compliance with PCI SSC Standards, including, but not limited to:

Note: *Contact details for the Participating Payment Brands can be found in FAQ #1142 on the Website.*

1. Determining requirements for validation to Part 1 and/or Part 2 of the PCI 3DS Core Security Standard.
2. Managing compliance and enforcement programs (requirements, mandates, or dates for compliance).
3. Establishing penalties and fees for non-compliance with applicable standards.
4. Establishing validation process requirements and who must validate.

5.2 PCI Security Standards Council

PCI SSC is the standards body that maintains the PCI SSC Standards and supporting programs and documentation. In relation to the 3DS Program, PCI SSC:

1. Maintains the PCI SSC Standards and related validation requirements, programs and supporting documentation.
2. Provides training for and qualifies 3DS Assessors to perform PCI 3DS Assessments.
3. Lists 3DS Assessor Companies and 3DS Assessor Employees on the Website.
4. Maintains a 3DS Quality Management (AQM) program as part of its QSA Company AQM program.

5.3 3DS Assessor Companies

A 3DS Assessor Company is an organization that has been qualified as a 3DS Assessor Company by PCI SSC and has been added to the 3DS Assessor List.

3DS Assessor Companies and their 3DS Assessor Employees' responsibilities in connection with the 3DS Program include, but are not limited to, the following:

- Adhering to the QSA Qualification Requirements and the QSA Program Guide.
- Maintaining knowledge of and ensuring adherence to current and relevant PCI 3DS Core Security Standard guidance and instructions located in the Document Library section of the Website.
- Performing PCI 3DS Assessments in accordance with the PCI 3DS Core Security Standard, including but not limited to:
  - Validating and confirming 3DS Data Environment (3DE) scope as defined by the assessed entity.
  - Selecting employees, facilities, systems, and system components accurately representing the assessed environment if sampling is employed.

- Being on-site at assessed entity during the PCI 3DS Assessment.
- Evaluating compensating controls as applicable.
- Providing an opinion about whether the assessed entity meets PCI 3DS Core Security Standard.
- Effectively using the *PCI 3DS ROC Template for use with PCI 3DS Core Security Standard* to produce 3DS Reports on Compliance (3DS ROCs).
- Validating and attesting as to an entity's PCI 3DS Core Security Standard compliance status.
- Maintaining documents, work papers, and interview notes that were collected during the PCI 3DS Assessment and used to validate the findings.
- Applying and maintaining independent judgement in all PCI 3DS Assessment decisions.
- Conducting follow-up assessments, as needed.
- Stating whether or not the assessed entity has achieved compliance with the PCI 3DS Core Security Standard.

PCI SSC does not approve 3DS ROCs from a technical perspective, but performs QA reviews on 3DS ROCs to ensure that the documentation of testing procedures performed is sufficient to support the results of the PCI 3DS Assessment. See Section 8, "Assessor Quality Management Program," for additional information.

5.4 Customers

The role of PCI 3DS Assessment customers (merchants, service providers, financial institutions, etc.—collectively, "Customers") in connection with the 3DS Program includes the following:

- Understanding compliance and validation requirements of the current PCI 3DS Core Security Standard.
- Maintaining compliance with the PCI 3DS Core Security Standard at all times.
- Defining 3DS Data Environment scope per guidance provided in PCI 3DS Core Security Standard.
- Selecting a 3DS Assessor Company (from the 3DS Assessor List) to conduct their PCI 3DS Assessment, as applicable.
- Providing sufficient documentation to the 3DS Assessor Employee to support the PCI 3DS Assessment.
- Providing related attestation (e.g., proper scoping and network segmentation).
- Remediating any issues of non-compliance as required.
- Submitting the completed 3DS Report on Compliance to their Participating Payment Brands, as directed by the Participating Payment Brands.
- Providing feedback on 3DS Assessor Employee performance in accordance with the *3DS Assessor Feedback Form* on the Website.
- Notifying their acquirer and/or Participating Payment Brands if they suspect or discover a cardholder data breach.

6 3DS Assessor Qualification Process

In an effort to help ensure that each 3DS Assessor Company and 3DS Assessor Employee possesses the requisite knowledge, skills, experience, and capacity to perform PCI 3DS Assessments in a proficient manner and in accordance with industry expectations, each company and individual desiring to perform PCI 3DS Assessments must be qualified by PCI SSC as a 3DS Assessor Company or 3DS Assessor Employee, and then must maintain that qualification in "good standing" in accordance with the 3DS Qualification Requirements.

Note: *The QSA certification is a prerequisite for becoming a 3DS Assessor Employee.*

Only those 3DS Assessors qualified by PCI SSC are recognized by PCI SSC to perform PCI 3DS Assessments. All qualified 3DS Assessor Companies will be listed on the Website and added to the Website's search tool.

Each QSA Company entering the 3DS Program is required to submit a signed copy of the 3DS Assessor Addendum (Appendix A of the 3DS Qualification Requirements). Each 3DS Assessor Company must have at least one qualified 3DS Assessor. An application (Appendix B of the 3DS Qualification Requirements) must be submitted for each 3DS Assessor Employee to be qualified.

Refer to Section 3.2 of the 3DS Qualification Requirements for details on qualifying as a 3DS Assessor.

6.1 3DS Assessor Employee Requalification

Each 3DS Assessor Employee must requalify on an annual basis. Requalification requires proof of training successfully completed, and payment of annual training fees.

The annual requalification date is based upon the 3DS Assessor Employee's *previous qualification date*. *For example, a one-year requalification for a certification with a current qualification date of 15 March 2016 will be changed to 15 March 2017 upon successful completion regardless of whether the requalification was completed on 29 February 2016 or 25 March 2016.*

Note: *Negative feedback from Customers (merchants, service providers, etc.), PCI SSC, Participating Payment Brands, or others may impact the 3DS Assessor Employee's eligibility for requalification.*

6.1.1 Requalification Timeframe

In an effort to help ensure adequate time to complete requalification requirements, 3DS Assessor Employees should note:

- Registration for requalification training must be completed (and approved, where applicable) prior to the 3DS Assessor Employee's expiration date. A candidate who is not registered prior to their expiry date must re-enroll as a new candidate.
- A two-week grace period is provided beyond the candidate's expiry date in order to complete requalification training; however candidates will not be certified during this time and will not be recertified until the requalification exam is completed and passed.
- Access to the course and requalification exam will be granted only after payment is processed, and candidates will have access to the exam at most four weeks prior and two weeks past their expiration date.
- If a candidate is enrolled for requalification training and fails to take the training within the defined period, payment will be forfeited in full and the individual will need to reapply to the 3DS Program as a new candidate.

7 PCI 3DS Assessment Process

To demonstrate compliance with the PCI 3DS Core Security Standard, Customers may be required to have PCI 3DS Assessments conducted as required by the applicable Participating Payment Brand.

Note: *Customers should consult with their Participating Payment Brands to confirm what PCI 3DS validation is applicable.*

PCI 3DS Assessments are required to be conducted in accordance with the PCI 3DS Core Security Standard, which contains requirements, testing procedures, and guidance to help ensure that the intent of each requirement is understood.

PCI 3DS Assessments are required to be conducted by a 3DS Assessor Company, through its QSA Employees who are also qualified as 3DS Assessor Employees.

7.1 Documenting a PCI 3DS Assessment

The 3DS Assessor will document the results of the PCI 3DS Assessment in a 3DS ROC. Each 3DS ROC must accurately represent the assessed environment and the security controls evaluated by the 3DS Assessor.

For each PCI 3DS Assessment, the resulting 3DS ROC must follow the most current 3DS ROC Template available on the Website. The 3DS ROC must be accompanied by a 3DS Attestation of Compliance (AOC) in the form then available in the Documents Library on the Website (3DS AOC). A duly authorized officer of the 3DS Assessor Company must sign the 3DS AOC, which summarizes whether the entity that was assessed is or is not in compliance with the PCI 3DS Core Security Standard, and any related findings.

By signing the 3DS AOC, the assessed entity is attesting that the information provided in the 3DS AOC and accompanying 3DS ROC is true and accurate. The date on the 3DS AOC cannot predate the 3DS ROC.

The 3DS AOC is submitted to the requesting entity/entities according to applicable Participating Payment Brand rules.

7.2 PCI 3DS Assessment Evidence Retention

As per Section 4.5 “Evidence (Assessment Workpaper) Retention” of the QSA Qualification Requirements, QSA Companies are expected to gather evidence to support the contents of each 3DS ROC. The QSA Company must secure and maintain, for a minimum of three (3) years, digital and/or hard copies of case logs, audit results, workpapers, e-mails, interview notes, and any technical information—e.g., screenshots, configuration settings—that were created and/or obtained during the PCI 3DS Assessment. This information must be available upon request by PCI SSC and its affiliates. The QSA Company must also provide a copy of the evidence-retention policy and procedures to PCI SSC upon request.

8 Assessor Quality Management Program

The QSA Company's existing internal quality assurance program and quality assurance manual must be extended to include and cover PCI 3DS Assessments and address applicable requirements specified in the 3DS Qualification Requirements and PCI 3DS Core Security Standard. As part of PCI SSC Assessor Quality Management (AQM) program audits of QSA Companies, PCI SSC performs a holistic review of the QSA Company's internal documentation required by the QSA Qualification Requirements ("QSA Audits"). For 3DS Assessor Companies, these audits and the AQM Program generally will also cover 3DS ROCs. Refer to the QSA Program Guide and QSA Qualification Requirements for applicable information regarding AQM, the QSA Audit process, remediation and revocation.