Read Me First

Instructions and Guidance for RFC2 on the PCI Key Management Operations (KMO) Security Requirements v1.0

PCI Security Standards Council®

Table of Contents

PCI Key Management Operations(KMO) RFC

Introduction

First and foremost, the PCI Security Standards Council (PCI SSC) would like to thank you for taking the time to review **the RFC2 draft of PCI Key Management Operations (KMO) Security Requirements v1.0.**

Your review and feedback are fundamental to the ongoing evolution of our standards and programs. The following slides provide instructions and guidance that will assist you during your review.

Before You Begin

- **Please read these instructions and guidance in their entirety.**
- Plan your reviews ahead of time and ensure your feedback is submitted before the RFC period closes **at 11:59pm Eastern Time on 9 January 2026**.
- For more information refer to:

  What to Know Before Participating in a PCI SSC Request for Comment

  PCI SSC RFC Process Guide

Purpose & Scope

The PCI SSC is planning a new standard that addresses key management operations across multiple other PCI standards. This new standard is the PCI KMO standard.

As part of the planned revision effort, the PCI SSC is conducting a Request for Comment (RFC) period to solicit general feedback on the following document:

- *PCI Key Management Operations Security and Test Requirements*

This RFC is on the second draft of this the new PCI KMO standard. An initial RFC has been previously performed in the June/July period of 2025, and this second RFC is on the updates made to the KMO standard based on the RFC1 feedback.

Feedback received during this RFC period will be reviewed and considered prior to the release of the PCI KMO standard.

Note: *Revisions to existing standards and programs typically include RFCs on draft content. Refer to the RFC Process Guide for more information.*

RFC Timeline

- The RFC period will run from **24th November 2025 to 9th January 2026.**
  - Additional time is provided for this RFC as it extends over the end of year period
- Submit your feedback **before 11:59pm Eastern Time on 9th Jan 2026**.
- Late feedback **will not** be accepted.

> ***Note:*** *PCI SSC can only accept feedback that is received via the Portal during the RFC period. Late feedback and feedback submitted via any other channel will not be accepted.*

PCI KMO RFC Focus Areas

The PCI KMO standard is intended to be referenced by other PCI standards and programs ("calling standard/program"). Examples of how this may work is provided in the "Example PCI KMO Implementations" and "Applicability Matrix" sections of the standard.

The goal for the v1 release of PCI KMO is to address the key management operational requirements currently contained in the PCI PIN standard and Domain 5 of the PCI P2PE standard. Additional key management aspects to align with other PCI standards may be considered for future PCI KMO revisions.

At this point, a version of the Program Guide for the PCI KMO standard has not been finalized. However, this deck contains slides that provide an outline of some of the intended program aspects to assist with the RFC2 review.

Example areas of the PCI KMO standard that PCI SSC is soliciting input on include:

- Are the current requirements clearly and correctly stated?
- Are the current requirements sufficiently verifiable?
- Are any requirements missing, given the focus of PCI KMO on PCI PIN and PCI P2PE Domain 5?
- Are any requirements overly onerous or incorrectly addressing extant risk?

Overview of Proposed PCI KMO Program

PCI Security Standards Council®

The PCI KMO Program

- The PCI KMO standard will be associated with its own program
  - This will be a listing program, with its own associated PCI KMO assessors
- The PCI KMO program is still under development
- The contents of these slides provides details on the current intention and direction of the PCI KMO program
  - Details may change prior to PCI KMO release
- The re-assessment period of PCI KMO listings is planned to be set to 3 years
  - This aligns with PCI P2PE, but is 1 year longer than the current PCI PIN program
  - The PCI PIN program would be updated to align with this period for PCI KMO
  - An annual checkpoint-style assessment would be implemented to accommodate for the increased time between on-site assessments
- Full details of the PCI KMO listing elements are yet to be developed, but will include all existing elements of the PCI P2PE and PCI PIN listing programs, with potential additions to be considered

PCI Security Standards Council®

PCI KMO / PCI PIN / PCI P2PE

- The PCI KMO Program is intended to align and interact with the PCI PIN and PCI P2PE Programs
- A period of overlap will exist between the release of the PCI KMO Standard and Program, and any deprecation of existing PCI PIN or PCI P2PE key management requirements
  - This overlap period is yet to be determined but is likely to be no less than 1 year
- Although the PCI KMO requirements are intended to eventually replace the PCI PIN requirements, it is expected that the PCI PIN program will continue to exist
  - After the overlap period this will reference the PCI KMO standard rather than the PCI PIN standard
- Both the PCI P2PE Standard and Program will continue to exist, which will include the aspects of the PCI P2PE Standard that address items not covered by PCI KMO

Listing Component Types

- PCI KMO is expected to have the following listing component types upon launch
- These are intended to include all PCI P2PE key management listing component types, with additions for PIN processing, signing and remote key distribution entities
- The table below is a copy of 'Table 2' within the RFC2 version of the PCI KMO standard

Component Type	Description
Decryption Management Component Provider (DMCP)	An entity that manages the decryption environment that can support a P2PE solution
PIN Processing Service (PPS)	An entity that performed PIN verification and/or PIN translation services (that is not the card Issuer).
Key Injection Facility (KIF)	An entity that performs cryptographic key services including, but not limited to, key generation, conveyance, and/or key loading.
Key Loading Component Provider (KLCP)	An entity that manages the cryptographic key loading.
Key Management Component Provider (KMCP)	An entity that manages cryptographic key generation and key conveyance.
Certification/Registration Authorities (CA/RA)	An entity that signs public keys such as X.509 or other non-X.509 certificates for use in connection with the remote distribution of symmetric keys using asymmetric techniques. A Registration Authority (RA) performs registration services on behalf of a CA to vet requests for certificates that will be issued by the CA.
Key Distribution Component Provider (KDCP)	An entity that performs cryptographic key services including, but not limited to, key generation, conveyance, and/or (remote) key loading (using symmetric and/or asymmetric techniques)
Signing Service Component Provider (SSCP)	An entity that signs software or data packages (such as firmware, applications, configuration files, etc.) so that they can be authenticated by other systems.
HSM-as-a-Service	An entity that manages HSMs for use by multiple tenants.

Note: The names and details of listing component types may be subject to change prior to release of the PCI KMO Standard and Program

PCI PIN/P2PE/KMO Comparison Summary

	PCI PIN	PCI P2PE (KM)	PCI KMO*
Assessor individual type	QPA	P2PE Assessor (QSA or QPA prerequisite)	KM QSA (Prerequisites and qualifications TBD)
Assessor company type	QPA Company	P2PE Assessor Company	KMO Assessor Company
Cryptographic key types	PIN keys	Non-PIN account data keys POI application signing keys	PIN keys Non-PIN account data keys POI application signing keys** MPoC A&M keys** [More to be added over time]
Reassessment period	2 years	3 years	3 years
Annual self-validation?	No	Yes	Yes
Listing program?	Yes	Yes	Yes
Listing component types	N/A	Key Injection Facility (KIF) Key Loading (KLCP) Key Management (KMCP) Cert/Reg Authorities (CA/RA) Decryption (DMCP)	KIF, KLCP, KMCP, CA/RA, DMCP + HSM Service (HaaS) + PIN Processing Service (PPS) + Key Distribution (KDCP) + Signing Service (SSCP)

Notes: * Proposal only, all aspects yet to be finalised
** Details and support TBD

PCI Security Standards Council®

RFC Feedback Instructions

Accessing the RFC Document

Note: *Only your company's primary contact may log into the portal and download the RFC documents. If you do not know who your company's primary contact is, please contact RFC@pcisecuritystandards.org for assistance.*

- Log in to the PCI SSC Portal with your username and password: https://programs.pcissc.org/
  - *If you don't know your password, click "Forgot your password" to create a new password. If you do not have a username, please contact RFC@pcisecuritystandards.org for assistance.*
- Click on **PCI Key Management Operations (KMO) Security Requirements v1.0 RFC2**
- Accept the Non-Disclosure Agreement (NDA).
- Click to download the RFC document.

Entering Your Feedback

1. In the *Document* field, choose one of the following options from the drop-down:
    - PCI Key Management Operations (KMO) Security Requirements v1.0 RFC2

2. In the *Section* field, select or specify the appropriate document section that is the subject of your feedback (as applicable).

3. Specify the *Page Number* containing the content to which your feedback refers.

4. Select the appropriate *Category* of feedback from the drop-down menu.

5. Specify your *Comments* and provide a *Suggested Solution* for each item of feedback.

Note: *Further details describing the subject of your feedback should be specified in the Comments and/or Suggested Solution field(s).*

Maximizing Your Feedback

- In the Comment field, explain the reason for your feedback.
- In the Suggested Solution field, include a recommendation to address your feedback.
- Be as detailed as possible with your comments and suggested solutions.
- Feel free to leave either the Comment or Suggested Solution fields blank. It is not necessary to duplicate the same information in both fields.
- <u>Do not</u> submit the same feedback item more than once.
- <u>Do not</u> include company sensitive information and remember to keep your comments professional and collaborative.
- Consolidate all feedback for your company since each company can only provide 50 feedback entries.
- Please contact RFC@pcisecuritystandards.org with any questions or concerns.

Other Feedback Reminders

- Ensure your work is saved after each entry and before you exit the portal, select “Save Draft Comments.”
- You can come back later to finish entering feedback; you do not need to enter all feedback in the same session.
- When all your feedback is complete, select “Submit Feedback” and then select “Ok” to confirm your submission is complete.
- Once you select “Ok,” <u>you will not be able to edit your feedback</u>.
- A confirmation email will be sent after you submit your feedback.
- All feedback received will be reviewed and considered by PCI SSC.

After Submitting Your Feedback

- All RFC feedback will be reviewed and considered by PCI SSC.
- Your feedback, including your organization's name, and how PCI SSC actioned your feedback will be made available for review by RFC participants through the PCI SSC Portal.
- Refer to the PCI SSC RFC Process Guide for more information.

Thank You!

PCI Security Standards Council®