FedRAMP Using Cryptographic Modules Policy

- **Release:** 25.11A
- **Published:** 2025-11-08
- **Designator:** UCM
- **Description:** Initial release of simplified 20x version of this existing FedRAMP policy.

Front Matter

Effective Date(s) & Overall Applicability

- **FedRAMP 20x**:
  - This release is effective **2025-11-01** for **20x**.
  - This policy applies to all FedRAMP 20x authorizations.
- **FedRAMP Rev5**:
  - This version does not apply to Rev5; the full Rev5 requirements related to this policy are documented in FedRAMP's Policy for Cryptographic Module Selection and Use.

Documentation Guidelines

The following FedRAMP documentation guidelines apply to this document:

- The capitalized key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in IETF RFC 2119.
- FedRAMP-specific terms defined in FRD-ALL (FedRAMP Definitions) are italicized throughout this document for reference.

Background & Authority

Purpose

This set of requirements and recommendations converts the existing FedRAMP Policy for Cryptographic Module Selection and Use (https://www.fedramp.gov/resources/documents/FedRAMP_Policy_for_Cryptographic_Module_Selection_v1.1.0.pdf) to the simpler FedRAMP 20x standard style and clarifies the implementation expectations for FedRAMP 20x.

The notable change from the default Rev5 Policy for Cryptographic Module Selection and Use is that the use of cryptographic modules (or update streams) validated under the NIST Cryptographic Module Validation Program are not explicitly required when cryptographic modules are used to protect federal customer data in cloud service offerings seeking FedRAMP authorization at the Moderate impact level. This acknowledges that not all Moderate impact federal customer data is considered “sensitive” and allows both cloud service providers and agency customers to make risk-based decisions about their use of Moderate impact services for agency use cases that do not include sensitive data.

FedRAMP recommends that cloud service providers seeking FedRAMP authorization at the Moderate impact level use such cryptographic modules whenever technically feasible and reasonable but acknowledges there may be sound reasons not to do so across the board at the Moderate impact level. As always, the reasoning and justification for such decisions must be documented by the cloud service provider.

Requirements

FRR-UCM

These requirements apply ALWAYS to ALL FedRAMP Authorized cloud services based on the current Effective Date(s) and Overall Applicability of this standard.

FRR-UCM-01

Applies to: Low, Moderate, High

> Providers MUST document the cryptographic modules used in each service (or groups of services that use the same modules) where cryptographic services are used to protect *federal customer data*, including whether these modules are validated under the NIST Cryptographic Module Validation Program or are update streams of such modules.

FRR-UCM-02

Applies to: Low, Moderate, High

> Providers SHOULD configure *agency* tenants by default to use cryptographic services that use cryptographic modules or update streams of cryptographic modules with active validations under the NIST Cryptographic Module Validation Program when such modules are available.

FRR-UCM-03

Applies to: Moderate

> Providers SHOULD use cryptographic modules or update streams of cryptographic modules with active validations under the NIST Cryptographic Module Validation Program when using cryptographic services to protect *federal customer data*.

FRR-UCM-04

Applies to: High

> Providers MUST use cryptographic modules or update streams of cryptographic modules with active validations under the NIST Cryptographic Module Validation Program when using cryptographic services to protect *federal customer data*.