

Symmetric Key Management Annex v3.0.0 Requirements Mapping to NIST SP 800-53 Security Controls

Most of the requirements in the Symmetric Key Management Requirements Annex support the implementation of the security controls specified in the National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 5 (NIST SP 800-53). This appendix is provided for customers who must demonstrate implementation of a set of NIST SP 800-53 security controls as part of their Risk Management Framework (RMF) (formerly known as Certification and Accreditation (C&A)) process for a system incorporating Symmetric Pre-Shared Keys (PSKs) as part of the solution for applicable CP.

Note that the presence of a mapping between an Annex requirement and a NIST SP 800-53 security control does not necessarily indicate that the Annex requirement by itself is sufficient to satisfy the security control. Instead, a mapping indicates that the Annex requirement provides some degree of support to the application of the security control. Additional work outside the scope of this Annex may be required to effectively implement the security control on the target system.

Table 1 – Symmetric Key Management Annex v3.0.0 Requirements Mapping to NIST SP 800-53 Security Controls

Annex v3.0.0 Requirement	NIST SP 800-53 Revision 5 Security Controls
PSK GENERATIONAL, DISTRIBUTION, and INSTALLATION REQUIREMENTS	
PSK-GD-1	SA-4 (6), SC-12 (2)
PSK-GD-2	SC-12 (2)
PSK-GD-3	CM-6, SC-12 (2)
PSK-GD-4	SC-8 (1, 2), SC-12 (2), SC-13
PSK-GD-5	AC-3 (2), SC-8 (1, 2)
PSK-GD-6	SC-8 (1, 2), SC-12 (2)
PSK-GD-7	CM-6, SC-12 (2)
PSK-GD-8	IA-5 (1), SC-13
PSK-GD-9	IA-5 (1)
PSK-GD-10	IA-5 (1), SC-12 (2), SC-13
PSK-GD-11	SC-12 (2)
PSK-GD-12	SC-12 (2)
PSK-GD-13	IA-5 (6), SC-12 (2), SC-13
PSK-GD-14	AC-3 (2), SC-12 (2)
PSK-GD-15	IA-9, SC-12 (2), SC-13
PSK-GD-16	SC-12 (2), SC-13
Withdrawn	
PSK-GD-17	SC-12 (2)
PSK-GD-18	SC-12 (2)
PSK-GD-19	CP-9, SC-12 (1, 2), SC-28

PSK USAGE REQUIREMENTS	
PSK-U-1	CM-7, SA-4 (6, 9)
PSK-U-2	SC-12 (2), SC-28
PSK-U-3	AC-3 (2), SC-8 (1, 2), SC-12 (2)
PSK-U-4	IA-5
PSK-U-5	IA-9, SC-12 (2), SC-13
PSK-U-6	SA-8 (6), SC-12 (2)
PSK-U-7	IA-3 (1), SC-12 (3)
PSK-U-8	IA-3 (1), SC-12 (2, 3), SC-13
PSK REKEY REQUIREMENTS	
PSK-RK-1	SC-12 (2)
PSK-RK-2	SC-12 (2)
PSK COMPROMISE RECOVERY REQUIREMENTS	
PSK-CR-1	IR-4, SC-12 (2)
PSK-CR-2	IR-4, SC-12 (2)
PSK-CR-3	IR-4, SC-12 (2)
PSK-CR-4	IR-6, SI-4 (5)
PSK-CR-5	IR-6
PSK-CR-6	IR-4
PSK-CR-7	IR-4
PSK-CR-8	IR-4
PSK-CR-9	IR-4
KGS CONNECTIVITY REQUIREMENTS	
PSK-KC-1	SC-7, SC-12 (2)
PSK-KC-2	AC-4, SC-7, SC-12 (2)
PSK-KC-3	AC-4, SC-12 (2)
PSK-KC-4	AC-4, SC-12 (2)
KGS AUDIT REQUIREMENTS	
PSK-KA-1	AU-1, SC-12 (2)
PSK-KA-2	AU-6, PS-3
PSK TESTING REQUIREMENTS	
PSK-TR-1	SA-11, CM-3 (2), SC-12 (2)
ROLE-BASED PERSONNEL REQUIREMENTS	
PSK-RB-1	PS-3
PSK-RB-2	AC-5
PSK-RB-3	AC-5
PSK-RB-4	AT-3
PSK-RB-5	AC-3 (3), AC-5, IA-5, SC-12
PSK-RB-6	AC-5