What standards are covered by SNMP4J (i.e., RFCs, FIPS 140-2)?

IETF RFC Compliance

SNMP4J / SNMP4J-Agent implements the following IETF RFCs:

RFC #	Title	Coverage	Versions (SNMP4J)
3410	Introduction and Applicability Statements for Internet Standard Management Framework	✅	⭐
3411	An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks	✅	⭐
3412	Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)	✅	⭐
3413	Simple Network Management Protocol Applications	✅	⭐
3414	User Based Security Model (USM) for SNMPv3	✅	⭐
3415	View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)	✅	⭐
3416	Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)	✅	⭐
3417	Transport Mappings for the Simple Network Management Protocol (SNMP)	UDP and TCP only	⭐
3418	Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)	✅	⭐
3584	Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework	✅	⭐
3826	The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model	✅	⭐
4088	Uniform Resource Identifier (URI) Scheme for the Simple Network Management Protocol (SNMP)	✅	>= 2.2
5343	Simple Network Management Protocol (SNMP) Context EngineID Discovery	✅	>= 2
6353	Transport Layer Security (TLS) Transport Model for the Simple Network Management Protocol (SNMP)	✅ TLS 1.0, 1.2 ✅ DTLS	>= 2 (TLS 1.2 with Java SE 8 or later) >= 3.0
5590	Transport Subsystem for the Simple Network Management Protocol (SNMP)	✅	>= 2
5591	Transport Security Model for the Simple Network Management Protocol (SNMP)	✅	>= 2 CRL, OSCP revocation checking >= 3.6.0
5592	Secure Shell Transport Model for the Simple Network Management Protocol (SNMP)	⛔	
7630	HMAC-SHA-2 Authentication Protocols in the User-based Security Model (USM) for SNMPv3	✅	>= 2.4
draft-reeder-snmpv3-usm-3desede-00	Extension to the User-Based Security Model (USM) to Support Triple-DES EDE in "Outside" CBC Mode	✅	⭐
draft-blumenthal-aes-usm-04	The AES Cipher Algorithm in the SNMP's User-based Security Model	✅ (AES 192 + 256)	⭐

SNMP4J-AgentX implements the follow IETF RFCs:

RFC #	Title	Coverage	Versions
2741	Agent Extensibility (AgentX) Protocol Version 1	✅ (TCP only)	⭐
2742	Definitions of Managed Objects for Extensible SNMP Agents	✅	⭐

FIPS 140-2 Compliance

SNMP4J uses standard JCE hashing and encryption algorithms as provided through the Java Cryptography Extension (JCE) as listed in the table below. Thus, by using a FIPS 140-2 certified JCE provider, SNMP4J becomes FIPS 140-2 compliant:

Message Digest / Cipher Suite Name	SNMP4J Class Name	SNMPv3 Protocol	Protocol Type
SHA-1	AuthSHA	SHA	Authentication
MD5	AuthMD5	MD5	Authentication
DES/CBC/NoPadding	PrivDES	DES	Privacy
AES/CFB/NoPadding	PrivAES128 PrivAES192 PrivAES256 PrivAES192With3DESKeyExtension PrivAES256With3DESKeyExtension	AES 128 AES 192 AES 256 (nonstandard) (nonstandard)	Privacy
DESede/CBC/NoPadding	Priv3DES	3DES	Privacy