Privilege Management for Unix and Linux FIPS 140-2 Compliance Statement

Summary

When you need to protect Sensitive but Unclassified data with cryptography, you want to use a cryptographic module that meets the federal government (US and Canada) security standard FIPS 140-2, so that you can trust that the module is *tested* and *validated* by independent authorities. Products validated as conforming to FIPS 140-2 are accepted by the Federal agencies of both countries for the protection of sensitive information (United States) or Protected Information (Canada).

Definition

The **Federal Information Processing Standard (140-2) or FIPS**, specifies the security requirements that will be satisfied by a cryptographic module, providing four increasing, qualitative levels intended to cover a wide range of potential applications and environments. The areas covered, related to the secure design and implementation of a cryptographic module, include specification; ports and interfaces; roles, services, and authentication; finite state model; physical security; operational environment; cryptographic key management; electromagnetic interference/electromagnetic compatibility (EMI/EMC); self-tests; design assurance; and mitigation of other attacks.

This document details the FIPS 140-2 approved third-party cryptographic modules used in BeyondTrust Privilege Management for Unix and Linux.

> ***Note:*** *Cryptographic algorithms are only used if High Security is enforced.*

Third-Party Cryptographic Modules

Product Area	Encryption	Library	Manufacturer, Version
All data encryption and network communications	AES-128 AES-192 AES-256 3DES SHA-256	FIPS compliant OpenSSL	OpenSSL, 1.0.2a
Binary file checksum and Authentication HASH for REST services	MD5	Source built into the product	Derived from Open Source code originally written by Colin Plumb 1993