PKWARE | SMARTCRYPT

FIPS 140-2 COMPLIANT ENCRYPTION

WHAT IS FIPS 140-2?

FIPS 140-2 is the current version of the Federal Information Processing Standardization 140 (FIPS 140) publication, which specifies requirements for cryptography modules.

The National Institute of Standards and Technology (NIST) issues the FIPS 140 series to define the requirements that United States government systems and IT products should meet.

FIPS 140-2 requires all federal government agencies and departments that use cryptographic-based security to meet specific standards related to encryption strength and capabilities.

HOW DO FIPS 140-2 STANDARDS AFFECT MY ORGANIZATION?

FIPS 140-2 requirements apply to all government agencies that use encryption to protect sensitive data.

In addition, organizations that do business with government agencies or department must meet FIPS 140-2 security requirements when exchanging sensitive data.

Many other organizations must now meet these same standards, as FIPS 140-2 compliance is becoming an accepted best practice outside of the government sector and outside of the United States.

FIPS VALIDATION	CERT NUMBER	FIPS LEVEL
Windows 2000	103	140-1
Windows XP	238	140-1
Windows XP w/SP3	989	140-2
Windows Vista	893, 1002	140-2
Windows 7	1330	140-2
Windows 8	1894	140-2
Windows 10	2606, 2937	140-2
Windows Server 2003	382, 1012	140-2
Windows Server 2008	1010	140-2
Windows Server 2008 R2	1337	140-2
Windows Server 2012	1894	140-2
Windows 2016	2937	140-2
UNIX/Linux	918, 1747	140-2
Java JRE	1502, 2057	140-2
Android	1502, 2057, 1747	140-2
iOS 6	1963	140-2
iOS 7	2021	140-2
iOS 8	2396	140-2
iOS 9	2594, 2609	140-2
iOS X	2015, 2408, 2597, 2832	140-2
z900, z800	118	140-2
z196, z114, zEC12, zBC12	1505	140-2
z990, z890, z9EC, z9BC, z10EC, z10BC	524, 661, 1505	140-2

HOW CAN SMARTCRYPT HELP ORGANIZATIONS MEET FIPS 140-2 STANDARDS?

Smartcrypt fully addresses the standards outlined in FIPS 140-2 by strongly encrypting the data itself. PKWARE's own FIPS mode setting ensures only FIPS 140-2 validated cryptography is used and eliminates the need for disruptive operating system FIPS policy settings.

Smartcrypt keeps data secure:

- At rest and in motion
- At its origin and destination

Smartcrypt offers government agencies the ability to use validated cryptographic modules for protecting data when run in FIPS mode. Data remains protected even if placed on removable media that is lost or stolen during transit.

FIPS 140-2 COMPLIANT ENCRYPTION AND BEYOND

In addition to meeting the security standards outlined in FIPS 140-2, Smartcrypt helps solve several other data security issues that government agencies face today.

Please visit our website for case studies that show how government agencies such as CMS are solving their data security challenges, and to learn more about how Smartcrypt can help solve specific government data security issues.

PKWARE®

www.PKWARE.com

PKWARE provides a data-centric audit and protection platform that automates policy-driven discovery, classification, and encryption wherever sensitive data is used, shared, or stored.

CORPORATE HEADQUARTERS
201 E. Pittsburgh Ave.
Suite 400
Milwaukee, WI 53204

+ 1 866 583 1795

EMEA HEADQUARTERS
79 College Road
Suite 221
Harrow HA1 1BD

+ 44 (0) 203 367 2249