Federal Information Processing Standard (FIPS) Publication 140-2

Microsoft certifies that its cryptographic modules comply with the US Federal Information Processing Standard (FIPS).

Microsoft and FIPS

The National Institute of Standards and Technology (NIST) publishes a list of vendors and their cryptographic modules validated for FIPS 140-2. Rather than validate individual components and products, Microsoft certifies the underlying cryptographic modules used in Microsoft products, including Microsoft business cloud services, with each new release of the Windows operating system. This enables customers to configure and use those services in a way that helps meet their information encryption and compliance requirements.

When a new version of Windows and Windows Server is in development, a new certification project is started to validate compliance with FIPS 140-2. In fact, Microsoft has maintained a FIPS 140 validation program for every major release of the Windows operating system and Windows Server since the inception of the standard in 2001.

Validations and certifications

Validated Microsoft business cloud services include Azure, Azure Government, Dynamics 365, Dynamics 365 Government, Office 365, Office 365 U.S. Government, Office 365 U.S. Government Defense, Windows, Windows Server.

Certification goes into effect when Microsoft receives validation from NIST; it does not expire.

- How Microsoft products and cryptographic modules comply with FIPS 140
  Learn more
- Microsoft FIPS 140 Validated Cryptographic Modules
  Learn more
- Validations in process
  Learn more

How to implement

- **FIPS 140 Validation**
  Get information on how Microsoft products and cryptographic modules comply with FPS 140-2.
  Learn more
- **About Azure Key Vault**
  Get general information and implementation guidance about Azure keys, secrets, and certificates.
  Learn more
- **SQL Server 2012 and FIPS 140**
  Get instructions for using SQL Server 2012 in the FIPS 140-2-compliant mode.
  Learn more

About FIPS

The Federal Information Processing Standard (FIPS) Publication 140-2, *Security Requirements for Cryptographic Modules*, is a US government standard that defines minimum security requirements for cryptographic modules in products and systems, as defined in Section 5131 of the Information Technology Management Reform Act of 1996.

Testing against the FIPS 140 standard is maintained by the Cryptographic Module Validation Program, a joint effort of the US National Institute of Standards and Technology (NIST) and the Communications Security Establishment of Canada. The current version of the standard, FIPS 140-2, has security requirements covering 11 areas related to the design and implementation of a cryptographic module. Each module has its own security policy—a precise specification of the security rules under which it will

operate—and employs approved cryptographic algorithms, cryptographic key management, and authentication techniques. For each area, a cryptographic module receives a security level rating—1 to 4, from lowest to highest—depending on the requirements met.

Validation against the FIPS 140-2 standard is required for all US federal government agencies that use cryptography-based security systems—hardware, firmware, software, or a combination—to protect sensitive but unclassified information stored digitally. (Note, however, that any business can take advantage of the FIPS 140-2 mode of operation if they desire.) Some agencies also require that the modules procured for secret systems meet the FIPS 140-2 requirements.

Frequently asked questions

What is the relationship between FIPS 140-2 and the Common Criteria?

These are two separate security standards with different, but complementary, purposes:

- FIPS 140-2 is a standard designed specifically for validating product modules that implement cryptography rather than the products that use them—for example, Azure is not FIPS compliant. However, cryptographic modules that are implemented within a service can be certified as meeting the requirements for hash strength, key management, and the like.
- The Common Criteria are a set of guidelines and specifications for evaluating security functions in IT products and include a path to certification. In many cases, Common Criteria evaluations will rely on FIPS 140-2 validations to provide assurance that cryptographic functionality is implemented properly. (Windows and Windows Server have received an official certification of their compliance with Common Criteria from an independent auditor.)

There are so many modules listed on the NIST website for each release. How do I know which one applies to my agency?

If you are required to use only cryptographic modules validated through FIPS 140-2, you simply need to verify that the version you use appears on the validation list. Microsoft strives to validate all releases of its cryptographic modules, because each module provides a different set of cryptographic algorithms.

What does "When operated in FIPS mode" mean on a certificate?

This caveat identifies required configuration and security rules that must be followed to use the cryptographic module in a way that is consistent with its FIPS 140-2 security policy. The security rules are defined in the security policy for each module, and you can find links to each security policy on the Cryptographic Module Validation Program list of validated modules.

Are applications validated through FIPS 140-2?

No. Only low-level cryptographic modules are validated.

Can I use Microsoft adherence to FIPS 140-2 in my agency's certification process?

An agency does not need to be certified. To comply with FIPS 140-2, your system must be configured to run in a FIPS mode of operation, which means that you must ensure that a cryptographic module uses only FIPS-approved security methods. Microsoft business cloud services and Windows Server enable organizations to configure them to use FIPS mode. You'll find information about the FIPS 140 mode of operation in FIPS 140 Validation.

Additional resources

- Encryption in the Microsoft Cloud
- Microsoft Online Services Terms