# PKWARE®

# Secure Government Computing Initiatives & SecureZIP

## Table of Contents

# Secure Government Computing Initiatives & SecureZIP

The United States Government has established several important regulatory requirements and guidelines for safeguarding sensitive information. These efforts have led to the formulation of a number of technology standards affecting the systems and software used by the Federal Government. These standards pertain to the software and hardware used for information processing, as well as the procedures for accessing these systems.

The Federal Information Security Management Act[1] (FISMA) is a key driver for the standards used by the Government. Enacted in 2002, FISMA requires heads of federal agencies to provide security protections inline with potential risks, if exposed. This law mandates that all information systems used by, or on behalf of, a federal agency must comply with Federal Information Processing Standards[2] (FIPS) established by the National Institute of Standards and Technology[3] (NIST). The NIST is a non-regulatory branch of the U.S. Department of Commerce. One role of the NIST is to develop the essential computer security standards needed to support FISMA and to certify compliance with these standards.

Key standards in effect today include:
• FIPS 140 – Standard for Hardware and Software Cryptographic Modules
• FIPS 201 – Standard for Personal Identity Verification (PIV)
• Federal Desktop Core Configuration (FDCC)

The strong security features of SecureZIP® provide the means to gain compliance with these Federal Government standards.

1 http://csrc.nist.gov/groups/SMA/fisma/index.html
2 http://www.itl.nist.gov/fipspubs/index.htm
3 http://www.nist.gov/index.html

## FIPS 140 and SecureZIP

FIPS 140 is a standard developed by the NIST that defines the requirements for cryptographic modules used within security systems for protecting sensitive but unclassified information.  Originally published in 1994 as version 140-1, it was revised in 2001 to the current 140-2 specification[4].

A cryptographic module consists of the hardware or software that implements approved security functions for cryptographic algorithms and key generation.  Several objectives of the FIPS 140 specification are to ensure that an approved cryptographic module is implemented correctly, is protected from unauthorized operation or use, and performs properly when operated in an approved mode.

To ensure these objectives are achieved by a cryptographic module, the NIST provides a rigorous validation process that each manufacturer of a cryptographic module must pass.  Validation testing is administered by independent validation test laboratories sanctioned by the NIST.   Once the validation testing is completed, the NIST reviews the test results and, if a cryptographic module is deemed acceptable, issues a certificate to the vendor confirming the validation.
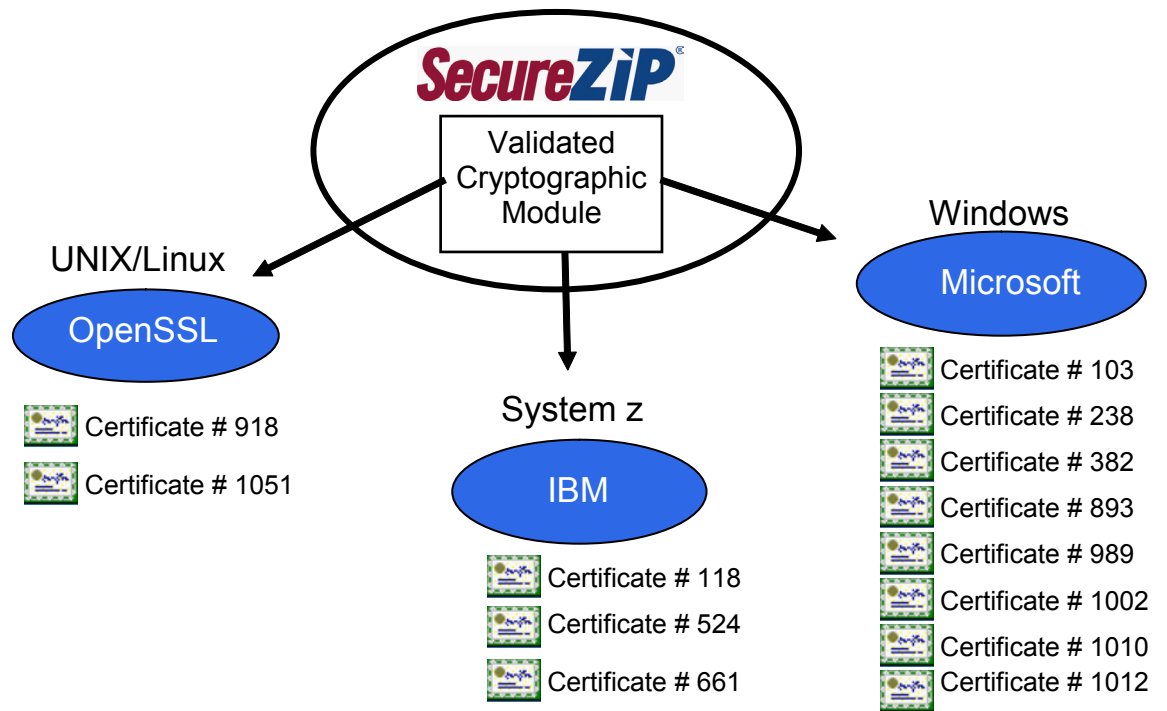
A list of validated cryptographic modules and their certificate numbers is maintained by the NIST.  This list can be reviewed on the NIST website at: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm.

Many of the validated cryptographic modules are not packaged as free-standing software products but must be integrated as components into other products or applications that provide security services using the capabilities of the module.  SecureZIP is a software product that provides security services in this manner.   When operated in FIPS Mode, SecureZIP will ensure that only FIPS 140 validated cryptographic modules are used for encryption processing.  This approach provides a high degree of flexibility for customers needing to meet FIPS compliance on major computing platforms by utilizing the best available FIPS validated modules.

---

[4] Draft work has been underway since 2007 towards the 140-3 specification that will eventually replace the 140-2 version

An illustration of the SecureZIP approach for using FIPS validated cryptographic modules across multiple computing platforms is shown below:



## Ensuring Software is FIPS 140 Compliant

As stated by the NIST, "When selecting a module from a vendor, verify that the application or product that is being offered is either a validated cryptographic module itself…or the application or product uses an embedded validated cryptographic module. Ask the vendor to supply a signed letter stating their application…incorporates a validated module…and reference the modules validation certificate number."[5]

If the vendor of the cryptographic module is known, the Module Validation List published by the NIST can be checked directly:
http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm.

If the vendor's module appears in this list, it is a validated module.  However, there are far more security products that may use a cryptographic module than there are modules that may appear in the validated list.  Hence, the stipulation in the guidance that a vendor must provide a letter of attestation regarding the FIPS-140 certified cryptographic source integrated into their products.

PKWARE provides a signed Letter of Attestation identifying each validated cryptographic module incorporated by SecureZIP, as well as the validation certificate number, which allows for quick validation of whether or not the module appears on the NIST validated vendor list.  Quick lookup is available at: http://csrc.nist.gov/groups/STM/cmvp/

---

5 http://csrc.nist.gov/groups/STM/cmvp/validation.html

validation.html.  This allows retrieval of a validation certificate for a module; the lookup function provided by the NIST appears as shown below:
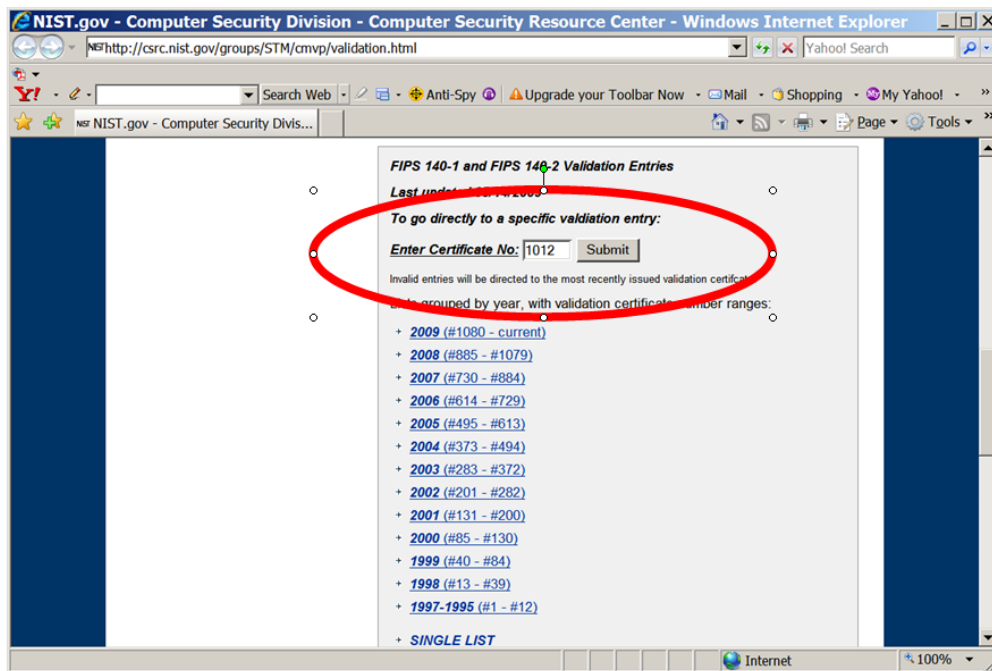


## FIPS 201 and SecureZIP

FIPS 201  is the NIST standard for Personal Identity Verification (PIV).  This standard was defined in support of the Presidential Directive from the Department of Homeland Security (HSPD-12 ).   The objective of HSPD-12 is to enhance security, increase government efficiency, reduce identity fraud, and protect personal privacy.  This directive set the policy for a common identification standard for federal employees and contractors, and, in conjunction with OMB M-05-24 , requires federal agencies to issue identity credentials meeting the FIPS 201 specification.

FIPS 201 defines the architecture and technical requirements for a PIV system.  This system provides the means for verifying the identity of an individual seeking physical access to federally-controlled government facilities or electronic access to federally-controlled government information systems.  It defines both physical and operational requirements for identity credentials.

Identity credentials in use today most often take the form of a Smart Card, sometimes labeled a "common access" card or CAC card .  A Smart Card is a plastic card usually the size and shape of a common credit card.  Each card includes an embedded processing chip used to store the electronic credentials of the authorized card holder; the chip interfaces with card readers used to read and validate the contained credentials.

The U.S. Government has issued over 13 million smart cards.   Identity credentials are not limited to Smart Cards--other form factors such as USB tokens or Biometric devices (e.g., fingerprint capture) may be used as well.  These devices provide a secure, tamper-proof, and portable means for storing identity information.

Compliance with FIPS 201 requires that identity device manufacturers adhere to the specification and, just as with FIPS 140, must pass certification.  Approved products are listed on the GSA FIPS 201 Approved Products List available at:

http://fips201ep.cio.gov/apl.php

PKWARE is not a vendor or manufacturer of either Smart Card or USB token technology and, therefore, neither PKWARE nor SecureZIP will appear in the Approved Products List.  SecureZIP does interoperate with Smart Card and USB token identity credentials from leading vendors on Windows® operating systems.   PKWARE routinely performs compatibility testing with products from the following approved vendors:

- ActivIdentity®
- Gemalto
- RSA® Security, Inc.
- SafeNet®, Inc.
- VeriSign®, Inc.

The encryption and digital signing capabilities of SecureZIP can be used with digital certificates that are stored on FIPS 201 compliant devices from each of these vendors.  Integration with these vendors' products is accomplished using the certificate services provided by the underlying Microsoft® Windows operating system.  These services provide a standard access method for all Windows application programs, such as SecureZIP, that make use of certificates.  SecureZIP is designed to look for digital certificates, specifically private keys used for data decryption or digital signing, in the Windows Certificate Store managed by the Windows certificate services.  This mechanism provides a flexible means for interoperability since each vendor provides access to certificates stored on their device through the Windows services; the application programs need not even be aware of which vendor's product is in use.

Customers may select the FIPS 201 validated identity credential product that best meets their requirements.  SecureZIP interoperability with identity credentials leverages investments made in these devices and helps meet compliance objectives.  With SecureZIP, FIPS 201 validated identity credentials can be used to protect sensitive files and emails.  Combined with PKWARE's enterprise policy capabilities to lock encryption settings, the risk of data compromise is significantly reduced.

## FDCC and SecureZIP

FDCC stands for the Federal Desktop Core Configuration  that defines a standard desktop configuration for computers.  Use of a standard desktop configuration is mandated by OMB M-08-22  (and by the earlier OMB M-07-11 ).  This mandate directs federal agencies to adopt the FDCC standard defined by the NIST.  It is intended primarily to cover desktop and laptop computers and provides a single configuration that reduces the cost and complexity of managing and securing government desktop systems.  FDCC is currently not applicable to special purpose computers or to computers used as servers.

Working directly with Microsoft, the NIST, NSA, DISA, and the U.S. Air Force defined the recommended secure configuration settings that could be uniformly installed to provide a single image for all desktops.  Once installed, specific tools are required to ensure desktop settings remain as set by the FDCC specification.

In effect since February of 2008, the FDCC is only applicable for computers running Windows XP and Windows Vista.  Implementing FDCC does not require a special version of Windows XP or Windows Vista®; it utilizes the same versions of these operating platforms that are available from Microsoft to businesses and the general public.  An FDCC compliant desktop is achieved by applying specific configuration settings to Windows.

Many of the settings are configured to ensure that by default, features or functions that may leave a machine open to compromise are either disabled or are otherwise enabled to an approved state. Functions or services that may pose a risk, such as Telnet, are disabled to avoid leaving open unnecessary attack vectors.

Other settings help to regulate appropriate use of a machine, such as regulating who can install device drivers or increase the priority of a process running on the machine. Under FDCC guidelines, these functions can only be performed by an administrator. Still, other settings enforce security policy elements such as minimum password length and required use of password complexity. In total, the specification defines over 600 settings that have been identified as required for compliance.

The FDCC guidelines do not provide specific settings for all software applications that may be required on a government computer. However, they do require that all software that will run on a government computer operate correctly on FDCC configured desktops.

PKWARE is committed to ensuring that SecureZIP supports FDCC compliance requirements for government users. Using approved images of FDCC compliant versions of Windows XP and Windows Vista, PKWARE's Quality Assurance Laboratory has certified the operation of SecureZIP on these platforms. These test platforms are those provided by the NIST for vendors to use in order to validate the operation of their products under the FDCC configuration. In support of the FDCC mandate, PKWARE has confirmed that SecureZIP operates correctly on FDCC configured desktops.

## Conclusion

Security is now an inherent part of information technology. With minimal tolerance for data compromise, it is critical for businesses and government agencies to ensure data is protected wherever it is, wherever it goes, and however it gets there. Information must be protected from the concerted efforts of hackers and thieves, as well as from the unintentional exposure by employees through carelessness, misuse, or lack of training.

SecureZIP by PKWARE provides the only cross-platform ZIP solution that meets data protection standards for Federal Government computing. ZIP has been the leading format for compressed data storage and transfer for over 20 years. PKWARE continues to lead the way in providing easy-to-use file compression and security for data in transit and at rest, across all major computing platforms.

## About PKWARE

PKWARE, Inc., the largest global software company providing ZIP solutions, is the creator and continuing innovator of the ZIP standard. PKWARE products are used to ensure the security and portability of data internally, as well as with partners, across all major platforms. Hundreds of global organizations in financial services, banking, retail, healthcare, government, and manufacturing use PKWARE services daily. PKWARE products provide unmatched scalability, ease of use and deployment, making them the most cost-effective means of securing data and complying with industry regulations. PKWARE, a privately held company, is based in Milwaukee, WI with additional offices in New York, the United Kingdom and Japan.

**United States**
648 N. Plankinton Ave., Suite 220
Milwaukee, WI 53203
1.888.4.PKWARE
www.pkware.com

**UK/EMEA**
Crown House
72 Hammersmith Road
London W14 8TH
United Kingdom

**PKWARE**®