

Case Study:

Federal Regulatory Agency Must Meet
Government's Encryption Standard

Securing sensitive data and enforcing corporate security policy

This Federal Regulatory Agency, with more than 3,000 employees, is charged with protecting the nation's public health, safety, and environment, as well as promoting and securing the common defense.

In its daily work, the Agency handles and protects various types of sensitive information, which is exchanged both internally and externally. When information such as Official Use Only documents leave the Agency's perimeter — transmitted to satellite offices, partners, and consultants — the data must be secured. In fact, its security must meet the standards of the Federal Information Security Management Act.

The Act requires all federal agencies to put in place an agency-wide program to secure sensitive information, as well as the information systems that support the Agency's operations and assets.

In addition, many federal agencies whose documents are "sensitive but unclassified" are limited in the acquisition of IT applications. The government mandates that federal agencies may purchase only security products with encryption technology that comply with Federal Information Processing Standard 140-2, (FIPS 140-2) published by the National Institute of Standards and Technology.

The Need

The Agency was tasked with finding an encryption solution that would meet FIPS 140-2 requirements. The Agency had been using WinZIP® technology, but WinZIP could not provide the strength or type of encryption required. Also, in keeping with the FIPS 140-2 mandate, the Agency was in the process of implementing a Public Key Infrastructure (PKI) to secure its data using X.509 standard digital certificates. WinZIP fell short on that count, too. Designed for consumer use — not for enterprises with serious security needs — WinZIP is based only on password encryption, not PKI.

Moreover, WinZIP does not enable administrators to control how the product is being used. The Agency could neither prevent users from encrypting files nor control how files were encrypted.

The Search

Federal agencies are required to evaluate at least three IT solutions before purchasing an application. Therefore, the Agency contracted with a consultant to help assess possible solutions. The consultant investigated PGP®, Sigaba®, File Assurity®, Tumbleweed®, and SecureZIP®.

Here is the Agency's assessment in overview: "The competitors quickly disqualified themselves because they could not meet the FIPS 140-2 requirement. SecureZIP provided a win-win solution, offering more than FIPS 140-2. With PKWARE's long history of providing enterprise file management solutions, we realized early on that if SecureZIP were chosen, it would do double-duty, replacing WinZIP in compressing files and replacing PGP in securing files."

Only SecureZIP met the need The Agency chose SecureZIP® for these reasons.

- **FIPS 140-2 compliance.** Most importantly for the Agency, SecureZIP was the only product that included FIPS 140-2-compliant encryption technology by leveraging the RSA® BSAFE® library.
- **Supports Public Key Infrastructures.** SecureZIP supports this infrastructure; WinZIP does not, and the Agency was intent on using PKI.
- **X.509 digital certificates.** SecureZIP was the only solution that could work effortlessly with these certificates. PGP is a proprietary technology that does not fully support the X.509 industry standard.
- **Centralized encryption policies.** Security only works if it can be easily enforced. The great advantage of SecureZIP is that an enterprise can set security protocols, so they automatically become part of the workflow. In some cases, users are unaware that files are being secured because SecureZIP works "in the background," encrypting and decrypting files, without requiring any user interaction. Therefore, the Agency viewed these Policy Manager capabilities within SecureZIP as a decided advantage.

Using Policy Manager, administrators could centrally control encryption standards, configuring and securing protocols. Every time an Agency employee or affiliate created a SecureZIP file, the user was locked into encrypting the file according to the Agency's settings. This is the control that was lacking with WinZIP.

- **Minimal learning curve.** Because both SecureZIP and WinZIP are based on the .ZIP standard, they are virtually identical in their use; therefore, the transition was quick and easy.
- **The advantage of compression.** SecureZIP serves the dual purpose of encryption and compression. The Agency had become accustomed to the efficiency of compressed files using WinZIP. Accepting a solution without compression would be an operational step backward.

The Rollout

"SecureZIP essentially killed two birds with one stone. First, it replaced WinZIP as a file compression utility. Second, SecureZIP met our stringent needs for data security and eliminated our concern about people misusing encryption capabilities," reports the Agency's Security Architect. "Its ease of deployment truly lived up to its advertising. SecureZIP operates exactly as WinZIP, and we were already familiar with that application. We never needed the help offered by PKWARE's Support Team.

"The Policy Manager is a terrific addition to the security process. It gives us the confidence that data is being secured the way we intended. That gives us great peace of mind."

And that, after all, is the ultimate goal in securing data.

For more information, visit www.pkware.com

United States

648 N. Plankinton Ave., Suite 220
Milwaukee, WI 53203
1.888.4.PKWARE

UK/EMEA

Crown House
72 Hammersmith Road
London W14 8TH
United Kingdom
ph: +44 (0) 207 470 2420
fax: +44 (0) 207 470 2421

APAC

Cerulean Tower 15F
26-1 Sakuragaoka-cho, Shibuya-ku
Tokyo 150-8512 Japan
+81.3.5456.5599

© 2008 PKWARE, Inc. All rights reserved. PKWARE, PKZIP, SecureZIP, and SecureZIP Mail Gateway are trademarks or registered trademarks in the U.S.A. and other countries. Any other trademarks are used for identification purposes only and remain the property of their respective owners.