

Federal Government Agency #8

Industry

- United States Government

Customer Profile

- Established in 1958
- Responsible for the safety of civil aviation

Challenges

- Securely exchanging email with external contacts
- Deploying a solution that would meet a host of compliance requirements
- Finding a cost-effective solution that would fit within the budget and be easily and efficiently deployed

PKWARE® Solution

- SecureZIP® for Windows® desktop

Results

- Ability to use encryption to securely exchange email using Lotus Notes
- Compliance with FISMA, OMB M-0408, and other initiatives
- Policy manager function allows administrators to define how users apply encryption
- Cost-effective solution fit well into the current operating environment without requiring implementation of large changes

Out of respect for our clients' privacy, names have been omitted from customer success stories. Many of our clients are happy to discuss their experience with PKWARE products. If you are interested in learning more information about a particular customer success story, please contact us at <http://www.pkware.com/contactus>

Customer Background

Our client is a Federal Government agency responsible for the safety of civil aviation. The agency maintains various responsibilities, including: regulation of civil aviation to promote safety; development of civil aeronautics; research and development of the National Airspace System; and regulation of US commercial space transportation. The agency is divided into several individual offices.

Challenges & Requirements

An audit was performed to identify instances where Personally Identifiable Information (PII) may be exposed throughout various federal agencies. Upon learning about the audit, two offices within our client agency took a proactive stance and concluded that they needed additional security around information that is exchanged daily via email. They began searching for a solution that would allow them to encrypt sensitive information exchanged via email and, if possible, a solution that would also allow them to access any and all information that was encrypted for purposes of data recovery.

The agency uses Lotus Notes for desktop email communication. While encryption capabilities are built into the program for secure exchange between Lotus Notes users, the offices needed a solution that would integrate with the application and allow for secure external email exchange. In addition, with office employees located across the country, it was imperative that the solution be quick to deploy and easy to integrate within the daily workflow.

When searching for a security solution, the offices needed to ensure the solution would meet the requirements outlined in their statement of work for encryption software. These requirements included:

- Compliance with Federal Information Security Management Act (FISMA) of 2002 for mandatory use of FIPS 140-2 compliant technology
- Compliance with Information Technology Management Reform Act of 1996, Public Law 104-106 to use Validated Cryptographic Modules
- Compliance with OMB Memo M-0408, Maximizing Use of SmartBuy and Avoiding Duplication of Agency Activities with the President's 24 E-Gov Initiatives GSA Advantage purchase

The agency was already using WinZip® for desktop compression, but the offices recognized that it was not a viable option for data security because it did not offer strong encryption or administrative policy support for contingency keys. WinZip also could not meet several of the compliance requirements, specifically FIPS-140.

The Solution - SecureZIP for Windows desktop

Strong encryption for secure email exchange. SecureZIP offered the offices strong data file

encryption that met their initial goal of a security solution that is compatible with their Lotus Notes email application. The offices can now encrypt and securely exchange information with all external endpoints.

Access data for audit/recovery purposes. Contingency key functionality ensures that data can be accessed at any time, even if a passphrase used for encryption is lost or stolen. The offices can recover any data encrypted using SecureZIP, which is especially important in the instance of an agency audit.

Centrally control encryption capabilities. Policy manager, another capability of SecureZIP, grants the offices the ability to 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. Using policy manager, administrators can centrally control encryption standards, configuring and securing protocols. Every time an employee or affiliate creates a SecureZIP file, the user is locked into encrypting the file according to the agency’s settings.

Fast and easy deployment. SecureZIP also provides a solution that is easy to use and deploy within the current work environment. Because both SecureZIP and WinZip are based on the .ZIP standard invented by PKWARE, they are virtually identical in their use, so the transition was quick and easy. Realizing that WinZip could not remain as the standard for compression, SecureZIP now serves the dual purpose of encryption and compression.

Out of respect for our clients’ privacy, names have been omitted from customer success stories. Many of our clients are happy to discuss their experience with PKWARE products. If you are interested in learning more information about a particular customer success story, please contact us at <http://www.pkware.com/contactus>

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

UK/EMEA
Siena Court
The Broadway
Maidenhead, Berkshire, SL61NJ
+44(0)162.850.9019

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