

Customer Success Story:

Federal Government Agency Secures Email Exchange, Meets Data Security Standards & Compliance Requirements

Industry

- Federal Government

Customer Profile

- Responsible for the safety of civil aviation

Challenges

- Protecting sensitive information sent via email and/or email attachments
- Meeting data security standards and compliance requirements, including FISMA
- Finding a cost-effective solution that would fit within the budget and be easily and efficiently deployed

PKWARE® Solution

- SecureZIP® for Windows® desktop

Results

- Protected sensitive information exchanged via email using Lotus Notes
- Met compliance requirements (FISMA, OMB M-0408, and others)
- Maintained control of data by centrally-controlled encryption policies
- Integrated with current operating environment without requiring implementation of large infrastructure 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>

ESS-FG8-111208

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 U.S. commercial space transportation. The agency is divided into several individual offices.

Challenges & Requirements

An audit was performed within the agency to identify instances where Personally Identifiable Information (PII) may be exposed. 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 and email attachments. 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 encrypted information for purposes of audit and/or 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 agency needed a solution that would integrate with the application and also 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 agency 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

Competitive Landscape

The agency was already using WinZip® for desktop compression, but soon recognized that it was not a viable option for data security because it did not offer strong encryption or administrative

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

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 agency strong data file encryption that met their initial goal of implementing a security solution compatible with their Lotus Notes email application. The offices can now encrypt and securely exchange sensitive information via email and/or email attachments 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 agency 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 agency 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. It allows the agency to send sensitive data freely within the organization as it is protected from the originating source, in transit, and remains protected when it reaches its destination.

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>

ESS-FG8-111108

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