PKWARE®

PKWARE Streamlines Data Exchange for City Government

TIME CONSUMING ENCRYPTION

In one of the country's largest cities, a government agency faced a series of challenges as it struggled to manage a rapidly increasing volume of secure data traffic.

The Office of the Chief Technology Officer (OCTO), the city government's central technology agency, is tasked with managing the city's technological infrastructure and providing support for other city departments. A key component of the OCTO's mission is managing data exchange between dozens of city and federal government organizations.

To meet federal standards for secure data exchange, the OCTO had relied on PGP encryption using a well-known encryption application. As the amount of data traffic grew year after year, however, data encryption became increasingly time-consuming. When encryption processing times began to cause the OCTO to miss its service commitments, the agency implemented a compression solution to reduce file sizes prior to encryption and transmission.

RETHINKING THE SOLUTION

Soon after, under pressure to curb costs and reduce complexity, the OCTO began searching for ways to consolidate technologies where possible. The agency's solution for data exchange came under scrutiny, as it employed one application to compress data and a second application to encrypt it. Licensing, maintaining, and training on multiple technologies was costly and added unnecesary complexity to each data exchange operation.

PAIN POINTS

INCREASING DATA EXCHANGE VOLUME

MISSED SERVICE COMMITMENTS

BUDGET PRESSURE

OVERLY COMPLEX PROCESSES

SOLUTION

ELIMINATION OF REDUNDANT TECHNOLOGY

SINGLE APPLICATION FOR COMPRESSION AND ENCRYPTION

INSTALLATIOM ON AGENCY MAINFRAME AND MULTIPLE SERVERS

100%
FISMA COMPLIANCE FOR PROTECTING DATA IN MOTION

PKWARE'S SMARTCRYPT

While evaluating alternatives to its current encryption process, the OCTO found that PKWARE's Smartcrypt solution would allow the agency to combine compression and encryption functionality in a single application. Smartcrypt's ability to support OpenPGP encryption (among other encryption standards) meant that the agency could maintain its current data security policies while improving performance and reducing costs.

After a thorough analysis of Smartcrypt's compression performance and persistent data encryption capabilities, the OCTO decided to move forward by replacing the existing compression and encryption applications with PKWARE's Smartcrypt. As a result, government entities across the city are now able to compress and encrypt large files using a single application.

Inspired by the success of OCTO's Smartcrypt implementation, another city agency, also using multiple encryption solutions, followed suit by evaluating and licensing Smartcrypt for Servers. The use of a standard encryption solution between their data center operation and that of the OCTO has further improved the city's data exchange capabilities.

LOOKING AHEAD

The unique capabilities of PKWARE's Smartcrypt enabled several of the city's IT departments to streamline their process for exchanging data while providing persistent protection for sensitive information. The Office of the Chief Technology Officer and other city agencies continue to save money while providing a high level of service and maintaining compliance with federal and local data security regulations.