



# Case Study: CMS Data-Sharing Project Highlights the Benefits of a Multiplatform Approach

9 November 2009

Jay Heiser, John Girard

Gartner RAS Core Research Note G00168944

The U.S. government agency responsible for healthcare payments needed a secure way to share sensitive data, most of it subject to regulatory requirements, with a disparate set of external partners. The success of its implementation offers valuable lessons for many other types of enterprises.

## Overview

The Centers for Medicare & Medicaid Services (CMS) implemented new cross-platform data security technology to meet public and regulatory demand for improved privacy protection. This government agency's experience offers valuable lessons for enterprises that need to protect sensitive data, particularly across heterogeneous extended computing environments.

## Key Findings

- Sharing data with a set of partners using a wide variety of system platforms, applications and data formats is practical only when the sharing organization uses a mechanism that is capable of translating that data into formats that the partners can readily use.
- The effective use of encryption and compression/decompression can improve data security and reduce the logistical and administrative burdens of data handling.
- Enterprises with large partner networks cannot expect all their partners to have compatible IT systems or comparable data-handling skill sets in place.

## Recommendations

- Enterprises planning to share encrypted data with partners that use platforms the enterprise does not have in-house must select a product vendor with the necessary expertise to address those partners' support needs.
- When very large datasets are to be moved, compression must be combined with encryption to reduce the logistical and administrative burdens of data handling and to avoid exceeding the storage limits of available media.
- If sensitive data cannot be monitored after it has been shared with a partner, the sending enterprise must establish a clear boundary of responsibility and liability with the receiving enterprises.

## What you need to know

Enterprises that share sensitive data with diverse networks of partners cannot expect to manage, or even fully understand, the varying systems, applications, data formats and skill levels their partners possess. Translating and securing the data so that it can be shared requires multiplatform technology and expertise.

## Case Study

### Introduction

The Centers for Medicare & Medicaid Services (CMS), the agency responsible for healthcare payments and financing for the United States government, maintains one of the largest collections of healthcare information in the world at its data centers in Baltimore, Maryland; Tulsa, Oklahoma; and Columbia, South Carolina. This highly sensitive data includes information related to various U.S. government healthcare programs, such as Medicare — which alone represents 1.2 billion separate claims annually — Medicaid and the Plan D prescription drug plan. The CMS exchanges data with hundreds of external entities, including other governmental bodies and research facilities, many of which have computing environments that may be incompatible with the CMS's mainframe systems.

Under increasing regulatory and public pressure, the CMS recognized that improved data security was an urgent requirement. The CMS's first attempt at implementing data encryption across its partner network proved unworkable because of interoperability issues, and the agency recognized that it needed simple, versatile file-handling technology that would facilitate data security but not place undue financial or administrative burdens on its partners. The solution CMS found — SecureZIP PartnerLink, a multiplatform encryption/compression product from Pkware — has both enhanced its data security and reduced the logistical and administrative burdens of transmitting vast amounts of data.

### The Challenge

The CMS has historically sent data to its huge network of external partners using mainframe tape cartridges. This practice, which required the shipment of more than 20,000 cartridges annually, has presented significant administrative and logistical burdens and security risks that the CMS increasingly recognized as unacceptable. The CMS has had significant reasons to implement stronger data security measures, including the fact that virtually all the data it houses and transmits is subject to rigorous regulatory requirements, including those of the

U.S. Health Insurance Portability and Accountability Act (HIPAA). The agency has received security directives from its parent agency, the Department of Health & Human Services, and the federal government's fiscal "watchdog" agency, the Office of Management and Budget. Moreover, the CMS, like many other entities, has faced increasing public concern about

security after a series of highly publicized data breaches, including the 2006 theft of more than 26 million individuals' personal information from the Department of Veterans Affairs systems.

In late 2006, in response to these concerns, the CMS purchased the IBM Encryption Facility for z/OS and informed its partners that no unencrypted data would be sent after 1 January 2007. However, this technology assumes a mainframe for decryption and has limited nonmainframe client alternatives, and CMS discovered that many, if not most, of its partners do not use mainframes — instead, they rely on tape cartridge readers connected to other systems that are not supported by IBM's decryption technology. When the mainframe-based system proved unworkable in its real-world partner environment, the CMS began evaluating other data protection technologies. The critical selection criteria were the need for:

- A multiplatform offering that could encrypt and decrypt very large sets of virtually any type of data (including fixed-block and variable-block) on virtually any system
- A file storage and retrieval format that could be read on any known computing platform
- Low cost or no cost for CMS's partners
- The ability to provide direct technical support to partner organizations using a huge variety of different platforms

The CMS also considered sending all data via telecommunications lines, completely stopping the mailing of mainframe cartridges. Many CMS partners that receive only small files did, in fact, make the transition to electronic receipt of data. However, careful study of the size of individual files revealed that many of them were far too large for this to be a viable overall solution. The use of physical media remained the only practical solution for the largest-volume files the agency needs to distribute.

## **Approach**

The CMS tasked Lockheed Martin, the outside contractor that manages its Baltimore data center, with surveying the marketplace to determine whether any available products could meet the agency's needs. Lockheed Martin identified several offerings that were advertised as multiplatform encryption products. These products were subjected to rigorous testing over several months before CMS selected Pkware's combined SecureZIP/PartnerLink encryption/decompression product offering.

Pkware's SecureZIP allows the CMS and its partners to encrypt, decrypt, compress and decompress data for storage and transmission, while PartnerLink enables the receipt of data across different computing platforms at no cost to CMS's partners. New partners can download the PartnerLink code and use it for data encryption and compression.

The cross-platform Pkware product uses a variety of encryption standards, including the

Advanced Encryption Standard, and public-key methodology for authentication. All CMS partners — including all individuals receiving CMS data — sign an agreement detailing how data will be used, what it will be used for, how long it will be held and what steps will be taken to dispose of it. All recipients receive configuration files and public keys from CMS, which allows them to verify that the data is coming from CMS. A critical Pkware advantage is the ability to archive, retrieve and convert any type of mainframe data, including binary, fixed-block and variable-block. Formats held in the zip archive are not corrupted during transit, even when data passes across systems that use different binary word lengths and different endian bit orientations. This feature was particularly helpful, because many CMS partners use different processing platforms.

The CMS implementation team — which included individuals with deep expertise in government IT deployments — had some reservations about using an off-the-shelf product. It had been their experience that products seldom met all customer needs and usually had to be customized at customer expense. Moreover, testing was typically done in a test environment with test data. For this reason, the CMS team requested a 90-day period prior to the actual purchase to continue testing the product in a production environment, and Pkware agreed. This extended "live test" period allowed it to observe all the potential problems that the CMS's users might have, and verify that the Pkware product could meet operational needs and that Pkware service could live up to CMS requirements.

Pkware was also able to build CMS-requested new features into its offering with only a few months' turnaround time. This customization was done without any additional cost to CMS. The CMS reports that Pkware was, in general, extremely responsive and effective in implementing the custom features that the agency required, and that Pkware's support, particularly for CMS's external partners, was outstanding. Partner support by Pkware and Lockheed Martin was crucial, because implementation and interoperability issues (mostly related to file conversion formats) emerged at many of the receiving partner sites, because of highly disparate platforms and skill sets.

One problem that emerged during testing and implementation was the difficulty of determining all the parameters used to generate data formats and encryption formats. The translation of character sets to different formats — particularly binary files in variable-block formats — required technical expertise and understanding of formats that many of the partners did not have. Pkware worked with CMS and Lockheed Martin to develop a simplified set of parameters to be used for the various file formats.

The different systems and varying skill sets of the many CMS partners required a considerable amount of "hand-holding" that CMS was not equipped to provide. Lacking experience and access to platforms, CMS does not have the ability to support every computer and operating system used by data recipients. The CMS found that deep expertise and close engagement by the vendor and the agency's contractor were crucial to the success of this implementation. The CMS implementation team developed a standard procedure for every new partner. The process began with a conference call with CMS and Pkware, during which the vendor asked about the platform being used, the amount of data being sent and other issues, and the partner could

ask any questions about the product and its implementation. In many cases, this was all the preparation the partner needed. Most partners were then able to have the technology up and running within hours.

The Pkware implementation has delivered an additional benefit that was not originally central for the CMS: a significant reduction in the administrative and logistical burdens of handling the huge amounts of data sent to and received from its partners. A compression rate of approximately 80% (a ratio of 5:1) has dramatically reduced the number of mainframe tape cartridges that must be used. Data can now also be easily placed on DVD or, in an increasing number of cases, transmitted via the Internet. This reverses the issues of the z/OS encryption approach that the CMS previously attempted to deploy, which had significantly increased the number of cartridges used.

## Results

- The Pkware encryption/compression technology the CMS implemented across its partner network has significantly improved data security, helping the agency to meet its crucial regulatory compliance mandates for privacy protection.
- The offering's compression functionality significantly reduced the burdens of transmitting large numbers of tape cartridges and enabled the CMS and its partners to use alternative media, including DVDs and online transfers over the Internet.

- Huge amounts of highly sensitive information are being rapidly shared with hundreds of different recipients, enabling all of them to safely meet their business goals and make effective use of this medical data.

## **Critical Success Factors**

One of the key factors the CMS has identified in the success of this project is the deep commitment by the product vendor. The extreme heterogeneity of the CMS partner network's extended computing environment created many interoperability challenges that the CMS team had neither the time nor the expertise to address, but Pkware had already encountered virtually all these issues in previous engagements. The partners' IT organizations and other stakeholders brought widely varying degrees of sophistication and expertise to the project, and the vendor was able to provide them with the necessary hand-holding for successful implementation. The development of a repeatable standard procedure for introducing partners to the technology and its uses was also extremely helpful. Pkware's ability to support this project through its engineering support staff was essential in securely sharing data with so many different partners and platforms.

The relative simplicity of Pkware's approach to generating encrypted file archives was sufficient for the task. The fact that Pkware's technology is widely known and could already be read on major platforms using simple executable tools was essential to the project's success.

## **Lessons Learned**

The CMS had already recognized that it was virtually impossible to manage — or even understand — the range of systems, applications and data formats used by the partners in its huge and constantly changing extended network. This crucial fact was underscored still further

by the experience of implementing the Pkware SecureZIP/PartnerLink offering. The prolonged engagement of the vendor provided the CMS with the depth of expertise necessary to bridge both platform gaps and differences in skill sets. The CMS recognized that clear delineation of responsibility for the data, for access key management and for the transfer of liability when data left the CMS must all be considered basic requirements of doing business with the agency. Without these conditions in place, the program and the responsible personnel would be exposed to potential fines and violations. With these conditions in place, the program can expand without incrementally increasing exposure risks.

*© 2009 Gartner, Inc. and/or its Affiliates. All Rights Reserved. Reproduction and distribution of this publication in any form without prior written permission is forbidden. The information contained herein has been obtained from sources believed to be reliable. Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. Although Gartner's research may discuss legal issues related to the information technology business, Gartner does not provide legal advice or services and its research should not be construed or used as such. Gartner shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretations thereof. The opinions expressed herein are subject to change without notice.*