



## Time to Deliver:

Reducing Risk and Realizing Data Security  
With Wolters Kluwer Financial Services'  
Secure Document Exchange

## Abstract

Financial institutions have realized significant savings since the widespread adoption of electronic documents and Internet delivery tools. But inadequate security measures have made benefits of the electronic age come at the great cost of security breaches, negative publicity, and injured relations with customers. Facing new legislation, technology developments, and threats from all sides, financial institutions require content secured through the utmost redundancy, completely locked down system channels, and restricted access to content. This paper examines these essential requirements for a properly architected Internet delivery service. As such a solution, Wolters Kluwer Financial Services' SDX Secure Document Exchange serves as the exemplary model for this exploration.

## Overview

Numerous Internet document delivery offerings have emerged across the landscape of the financial services industry. Promoted with similar promises of efficiency and profitability, these competing products have created a serious challenge for financial institutions attempting to determine the best tool for their business. Large companies, which spend vast amounts of resources on shipping documents overnight, have been quick to implement Internet delivery solutions to realize time and cost savings.

However, many financial institutions continue to rely on other methods. Nearly half of the participants in a recent Wolters Kluwer Financial Services on-line poll responded that they continue to pay for overnight shipping of hard copies. Meanwhile, other busy professionals, in need of a fast solution, utilize the unpredictable practice of e-mailing documents. The disadvantages of these methods are clear; they ultimately pose vast financial inefficiencies and even greater security risks. That financial institutions continue risky practices is indicative of some shortcoming in the alternatives.

While Internet document transport services have undoubtedly delivered in terms of time and cost savings, financial institutions and technology providers have returned to the issue of security repeatedly. Between ever-increasing reports of data violations and identity theft, deficiencies in security measures have become the weakest link in organizations. Since the enactment of California's 2003 breach notification law, data breaches have been blazing across headlines. Security technology has come to mean serious business.

Hence, it is imperative that financial institutions carefully reevaluate their needs; assess available solutions; and choose the best technology to avoid the costly damages of insufficient security, negative publicity, and injured customer and stakeholder relations. Clearly, the optimal Internet document transport system needs to deliver the best available in security measures as well as time- and cost-saving benefits. Wolters Kluwer Financial Services' SDX Secure Document Exchange solution fulfills these requirements through highly redundant technology and a comprehensive methodology that helps ensure data security by:

- Leveraging usability to gain user acceptance and reliance on the system
- Locking down channels to secure the paths by which information flows
- Limiting access to document content according to organizational roles
- Locating messages and documents at all times
- Providing lasting value via scalable technology that accommodates legislative mandates

## Leveraging Usability

*“Security is usually a secondary goal. People do not generally sit down at their computers wanting to manage their security; rather, they want to send email, browse web pages, or download software, and they want security in place to protect them while they do those things.”<sup>1</sup>*

The practice of using unprotected e-mail programs for exchanging critical documents reveals the potent lure of immediacy and perceived simplicity. However, this behavior also shows that professionals desire electronic messaging tools that allow for quick and easy replies—a two-way messaging exchange based on a familiar platform. Hence, a solution that uses an easily recognized interface is more likely to gain trust and user acceptance. Unfortunately, most Internet delivery services overlook this need and provide for messages to travel in one direction only; recipients must initiate new messages for each communication instead of simply responding to senders via a reply button.

Unlike these limited offerings, SDX employs a familiar e-mail user interface and a true two-way communication channel between senders and intended recipients. With the ability to move messages conveniently in an easy-to-use environment, SDX encourages users to stay within the system and send documents securely instead of returning to insecure e-mail or other risky methods.

Independent validation of SDX by a third party also gains user confidence in the system. The Statement on Auditing Standards (SAS) No. 70 is a fundamental audit for an Internet delivery solution. While the audit report is a testament to a service’s control measures, the commonly perceived meaning of the audit is one of trust and security. Hence, as a SAS-70 certified service, SDX’s stated policies and procedures accurately reflect its architecture as its credentials reveal its reliability.

Providing additional functionality familiar to users also keeps them working within the SDX system, such as the ability to attach all file types. Furthermore, a secure SDX package can include multiple formats like Microsoft® Word, Portable Document Format (PDF), and Joint Photographic Experts Group (JPEG) to streamline the delivery process and preserve original data formatting. Without the hassles of conversion tools and the burden of managing multiple document versions, users can be more productive and less anxious over jeopardizing content integrity.

SDX seamlessly integrates into existing systems, at both the legacy and code level, to provide minimal work flow disruption and prevent collective organizational frustration. The solution easily

interfaces with existing e-mail systems to allow for the creation of rules—simple or complex—so confidential messages route through the secure SDX environment if they leave the company firewall. By adapting to the unique processes of each business it serves, SDX reduces user intervention to accomplish maximum security and timesaving enhancements. Therefore, staff can remain focused on accomplishing tasks and increasing the bottom line instead of attending to intrusive hardware or software security issues at their workstations.

## Locking Down Channels

*“The organizations most likely to report a breach are banks (20%), credit card companies (18%), governmental organizations (including state universities) (13%), and health care providers (9%).”<sup>2</sup>*

As the industry with the highest risk of breaches, financial services must protect data from outside and inside threats equally. Such measures require implementing the strongest security methodologies available and performing ongoing surveillance and system updates as needed. In the scope of a financial institution’s security strategy, redundancy is the key to realizing complete data lockdown. Secured channels present the first layer of redundancy by preventing outside intruders from gaining access to sensitive data.

## Channel Security

The security of a system’s channels is the main line of defense against attack by a number of external threats. Securing all paths by which information can travel provides sensitive data with the greatest amount of protection and significantly minimizes the opportunity for breaches to occur by accident, design, or malicious intent. Such channels include any portal designed into the system like routes to servers and pathways to heartbeat services, which provide mechanisms for monitoring the health and status of processes. Securing these gateways and monitoring access to them is a fundamental piece of a financial institution’s defense system.

While SDX provides highly secure channels, it also allows multiple safe access points for organizational flexibility and convenience. The system meets various security methodologies by supporting entry channels via Hypertext Transfer Protocol over Secure Socket Layer (HTTPS), Simple Mail Transfer Protocol via Secure Socket Layer (SMTPS), Transport Layer Security (TLS), and the Web Services (WS) model.

## Limiting Access

*“In a study of more than 1,000 identity theft arrests in the United States, Michigan State professor Judith Collins has discovered that perhaps as much as 70 percent of all identity theft starts with theft of personal data from a company by an employee.”<sup>3</sup>*

Before establishing a single test account or exchanging even one file with an Internet document delivery system, companies must consider the overwhelming evidence of internally generated security breaches. By severely limiting access to nonpublic information across the organization, financial institutions stand to reduce the risk of data leaks and the damage they deliver. Optimal access administration takes a variety of routes, from restricting organizational roles from the system to authenticating user identity and encrypting content.

As stated earlier, redundancy is the cornerstone of data security. With every wall of defense constructed, the organization creates a stronger shield to protect data—from outside as well as inside threats. In the past, Internet delivery tools possibly hand delivered sensitive data to ill-intentioned, profit-seeking employees by neglecting to restrict access to content within the organization. Unlike these misdirected offerings, SDX provides redundant, internal controls that allow financial institutions to limit access and protect data by:

- Helping eliminate the possibility of nonessential roles accessing data
- Requiring multiple authentication schemes to verify designated users
- Encrypting files to help ensure only intended recipients access them

## Eliminating Accessibility for Nonessential Roles

SDX helps financial institutions protect customer data by preventing areas and roles in the organization from accessing content sent through the system by registered users. Therefore, product help desks provide product support without the possibility of helping themselves to customer information. Moreover, limiting access to document content means that roles can be identified, or flagged, when special circumstances arise, such as separating document compliance functions from systems compliance approval.

## Requiring Multiple Authentication Schemes

The more control an organization needs over system access, the more authentication it will require from users. SDX provides flexible authentication schemes to make certain that those who have access to the system are indeed the person they claim to be. These user security requirements can include a password, personal identification number (PIN), or biometric data.

PINs are generally unique numeric values, or passwords, that accompany another form of authentication to gain system access. On the higher end of the scale, biometric authentications are more sophisticated and reliable devices. The use of biometric technologies generally refers to measuring and analyzing human body characteristics such as fingerprints, hand patterns, eye retinas and irises, facial patterns, and voice patterns to prove identity.

## Encrypting Files to Ensure Specific Access

High-level encryption secures SDX messages during transport to ensure that content is available only to the sender and recipient. The system's numerous encryption techniques minimize the risk of identity theft by keeping content under lock and key as it moves across the Internet, as well as the organization. Using industry standards, SDX employs encryption capabilities and server-side x509 v3 digital certificates for Public Key Infrastructure (PKI), Digital Rights Management (DRM), and tamper sealing.

Encryption enforces the integrity of messages and document package content. The SDX system uses the strongest encryption methods available like PKI, which manages digital keys and certificates to provide a network of reliable identities. DRM is a nonintrusive restriction management tool. SDX provides digital shredding capabilities, such as efficient handling of redundant file copies by encrypting them and destroying the encryption key after the retention period expires.

## Tamper Sealing

As the backbone of the entire organization, content requires the utmost in security measures. SDX features technology that ensures message and content integrity is never in question. Using industry-standard certificates, the system encrypts and maintains tamper-evident seals for all messages and secures them inside a digital vault.

## Location, Location, Location

*"Users are less likely to attempt to circumvent security policy if they know that their actions will be recorded in an audit log." <sup>4</sup>*

While securing packages with encryption technology is essential to preventing security breaches, it is equally important to know the whereabouts of document packages before, during, and after transmission. Tracking features, reporting functionality, and audit trails are not only excellent work flow management tools; they are also essential components of an overall security strategy. Given the likelihood of internally originated data breaches, it is crucial to put controls in place to deter potential leaks, as well as detect and detail any suspicious activity. From a security perspective, such strategy is another example of the SDX system's protective redundancy measures because completely locking down channels, content, and access already resists outside threats.

## Comprehensive Tracking

To provide the greatest utility for financial institutions and their many branches and business partners, users on both sides of the SDX two-way communication channel can produce detailed reports on their activity and, under direction and system permission, the activity of others. The system's comprehensive reporting interface allows the creation of custom reports for secure messages sent, received, or pending delivery with size of package and more.

Audit trails are essential to producing a record of system activity that, when used with other tools and procedures, can help detect performance issues and suspicious patterns of use. Audit trails help to achieve multiple security-related objectives, such as individual accountability, reconstruction of events, intrusion detection, and ongoing system analysis.

## Lasting Value

*"...Many experts believe that electronic fraud, especially account hijacking, will have the effect of slowing the growth of online banking and commerce."*<sup>5</sup>

Clearly, the financial services industry must deal with more issues in the course of its operational life than security threats. Areas of business growth require constant attention, as do ongoing procedural and technology refinements as well as regulatory and legal issues. These factors require great time and talent while necessitating tools that can adapt to changing times.

SDX accommodates future needs through the extensive capacity of its implementation formats. Architected on the server side to provide maximum scalability and redundancy, SDX gives financial institutions the convenience of using their preferred delivery system as their business grows. Moreover, the solution accommodates changes quickly and efficiently to ensure the highest level of data protection, as well as the most up-to-date technology, is secured.

The SDX system also meets the needs of critical compliance issues to help financial services meet the ongoing requirements of legislative mandates. Designed to accommodate the increasing need for specialized handling of electronic information, SDX seamlessly coexists with corporate archive and e-mail systems already in place. This means the delivery system can adapt to changes without bypassing existing security policies or compliance content inspection. SDX helps to ensure compliance with multitudes of data handling directives required by Sarbanes-Oxley, NASD 3010, HIPAA regulations, and SEC 17 a-4, which requires financial institutions to preserve electronic records in non-rewritable and non-erasable format.

Wolters Kluwer Financial Services provides for user registration needs as organizations grow. The SDX support team can contact potential recipients from a client-provided database and educate them on the features and benefits of the system. Alternatively, clients can elect to use a variety of intuitive built-in mechanisms to register and authenticate recipients. An on-line registration by invitation allows secure, fast, and simple growth of the user base. SDX also features a "self-sign-up" process whereby authorized users or "approvers" can approve and deny new users to the system. The solution also provides the ability to add a large number of users in a batch mode.

## Summary

SDX helps financial institutions through a variety of approaches. As a tool for ensuring data safety and accuracy, the system is a virtual change agent in an industry currently besieged by internal and external security threats. As an innovative system, SDX provides a new approach to limiting access to data. As a seamlessly integrated, scalable solution, it helps financial institutions meet the requirements of abundant legislative mandates. Finally, as a smart decision with lasting value, SDX helps financial institutions streamline organizational processes, save resources, and keep busy professionals away from the snares of insecure document delivery methods.

As data leaks continue to hit newsstands, the time has come for an Internet document transport service to deliver the highest data security and performance capabilities possible. Added measures will increase the value of this offering, such as providing the intrinsic flexibility to cross technology platforms and bend with the needs of unique business models without breaking. To be sure, human error and malicious intent are, to some extent, independent variables in the data security equation. Their impact on sensitive customer information is controllable in part, however, through the implementation of a highly redundant and reliable system like Wolters Kluwer Financial Services' SDX solution.

<sup>1</sup> Usability of Security: A Case Study; Alma Whitten and J. D. Tygar; Computer Science Department, School of Computer Science; Carnegie Mellon University, 1998.

<sup>2</sup> The National Survey on Data Security Breach Notification; White & Case, LLP and Ponemon Institute, LLC; August 25, 2005.

<sup>3</sup> Study: ID theft usually an inside job; <http://msnbc.msn.com/id/5015565>.

<sup>4</sup> Special Publication 800-12; National Institute of Standards and Technology; an Agency of the U.S. Commerce Department's Technology Administration.

<sup>5</sup> Putting an End to Account-Hijacking Identity Theft; Federal Deposit Insurance Corporation; Dec. 14, 2004.