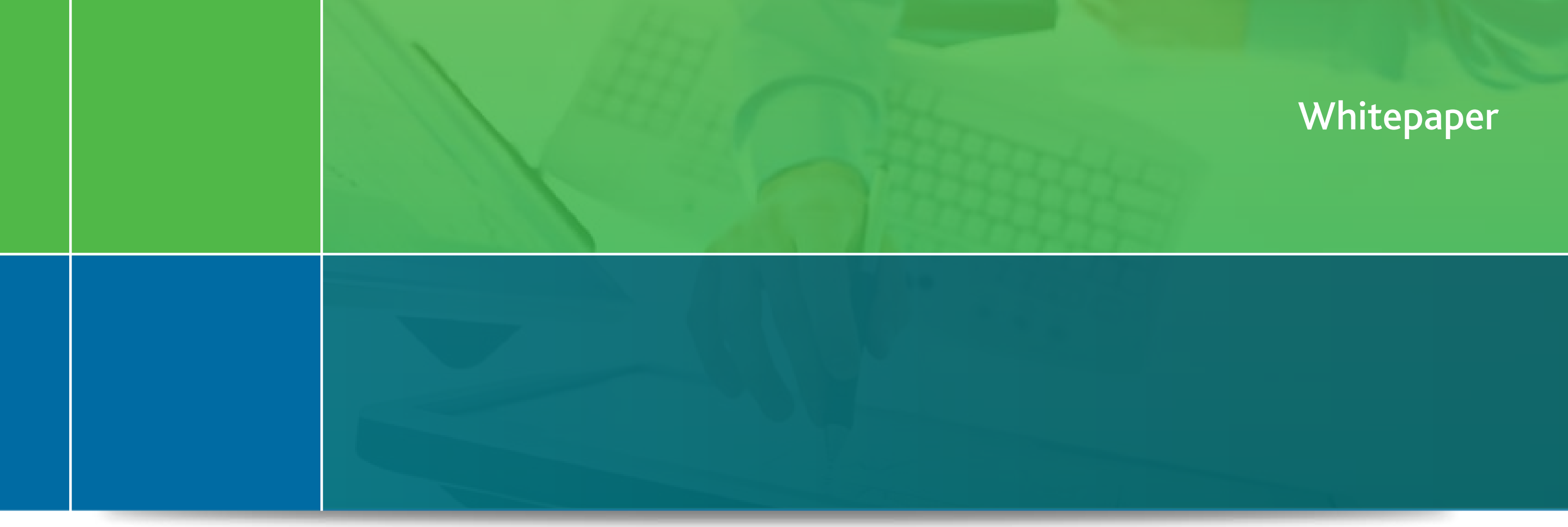

Whitepaper

Time to Deliver:
Reducing Risk and Realizing Data Security

By Dean Polsfut, Senior Product Manager, Wolters Kluwer Financial Services

Insurance companies have experienced considerable benefits since the widespread adoption of electronic documents and Internet delivery tools. But, taking advantage of all that electronic workflows have to offer comes with its own set of challenges. As more financial institutions move their business online, the risks associated with inadequate data security can result in security breaches, negative publicity and irreparable harm to your customers. To help avoid these pitfalls, this paper examines the essential requirements and best practices for implementing a properly architected Internet document delivery service.

Overview

Despite the proven time and cost savings associated with an Internet document delivery solution, the financial services sector has lagged behind other industries when it comes to implementation. A surprising number of insurance companies have been late adopters and continue to rely on other document delivery methods.

In fact, 78% of the participants in a Wolters Kluwer Financial Services online 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 and unsecure practice of emailing documents. The disadvantages of these methods are clear; they ultimately pose vast operational inefficiencies and even greater security risks. However, the fact that companies continue risky and/or expensive practices clearly indicates a shortcoming in the alternatives.

While Internet document delivery services undoubtedly deliver significant savings, insurance companies and technology providers still continue to voice concerns about security. Between ever increasing reports of data violations and identity theft, security deficiencies have become the weakest link in organizations. As a result, security technology has come to mean serious business.

Wolters Kluwer
Financial Services

Therefore, it is imperative that companies carefully reevaluate their needs, assess available solutions and choose the best technology to help them avoid the damages associated with insufficient security, negative publicity, and injured customer and stakeholder relations. The optimal Internet document delivery solution must deliver the best available in security as well as time and cost saving benefits. There are several key factors an insurer should consider when choosing an Internet document delivery provider, including:

- User-friendly and intuitive interface to grow user acceptance and reliance on the system
- Locking down channels to secure the paths by which information can travel
- Providing proof of acceptance through e-signature or e-consent and audit trails
- Limiting access to document content according to organizational roles
- Tracking messages and documents at all times
- Providing lasting value via scalable technology that accommodates legislative mandates
- Flexibility to be used in multiple ways and channels across the organization.

Leveraging Usability

The practice of using standard e-mail programs to send documents containing confidential information 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. Therefore, a secure solution that mimics an e-mail program and allows for easy sending and receiving is more likely to gain trust and user-acceptance.

Locking Down Channels

The risk of security breaches, especially those concerning sensitive personal data has never been higher. Insurers must protect data from both outside and inside threats. Responding to such risk demands the implementation of the strongest security methodologies available and performing ongoing surveillance and system updates as needed. In the scope of an insurer's security strategy, redundancy is the key to realizing complete data lockdown. Secured channels present the first of multiple layers to prevent outside intruders from gaining access to sensitive data.

Channel Security

Secure system channels are 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. These 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 an insurance companies' defense system.

Limiting Access

Before establishing a single test account or exchanging even one file with an Internet document delivery system, companies must address the ongoing problem of internally generated security breaches. By severely limiting access to non-public information across the organization, insurers stand to reduce the risk of data leaks and the damage they cause. 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. A good Internet document delivery solution provides redundant, internal controls that allow insurers to limit access and protect data by:

- Limiting access to sender and recipient
- Requiring multiple authentication schemes to verify designated users
- Encrypting files to help ensure only intended recipients can access them.

If accessibility for non-essential roles is eliminated, insurers can protect customer data by preventing access to content sent through the system by registered users. Therefore, product help desks can provide 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 circumstance 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 requires from users. An effective Internet document delivery solution provides flexible authentication schemes to ensure 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 other out-of-wallet data like mother's maiden name.

Encrypting Files to Ensure Specific Access

Industry standard encryption secures messages during transport to ensure content is available only to the sender and recipient. Applying numerous encryption techniques minimizes the risk of identity theft by keeping content under lock and key as it moves across the organization and the Internet. Encryption also enforces the integrity of messages and document package content. Digital shredding capabilities are another feature to consider. This includes the 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, customer content requires the utmost in security measures. Look for technology that encrypts and maintains tamper-evident seals for all messages and secures them inside a digital vault.

Location. Location. Location.

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 workflow management tools; they also are essential components of an overall security strategy.

Comprehensive Tracking

A comprehensive reporting interface allows for the creation of custom reports for secure messages sent, received, or pending delivery, e-signed, or printed, 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 use patterns. Audit trails help achieve multiple security-related objectives, such as individual accountability, reconstruction of events, intrusion detection, and ongoing system analysis.

Summary

Clearly, financial institutions must deal with more issues in the course of their 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.

However, as data leaks and identity theft continue to obliterate businesses, financial institutions must protect their customers with an Internet document delivery solution that offers the highest data security and performance possible. Added measures will increase the appeal of this offering, such as the intrinsic flexibility to cross technology platforms and bend with the needs of unique business models without breaking. But, while the time and cost savings associated with secure delivery are sizeable, maintaining the good relationships developed with customers and mitigating reputational risk are even more valuable.

Wolters Kluwer
Financial Services

Wolters Kluwer Financial Services is a comprehensive regulatory compliance and risk management business that helps financial organizations manage operational, compliance and financial risk and reporting, and improve efficiency and effectiveness across their enterprise. The organization's prominent brands include: FRSGlobal, ARC Logics® for Financial Services, PCi, Compliance Resource Network, Bankers Systems, VMP® Mortgage Solutions, AppOne®, GainsKeeper®, Capital Changes, NILS, AuthenticWeb™ and Uniform Forms™. Wolters Kluwer Financial Services supports its global customers with more than 30 offices in 20 countries and is a leading worldwide provider of compliance and risk management solutions for the financial services industry, serving more than 15,000 banking, insurance and securities customers across the globe. Wolters Kluwer Financial Services is part of Wolters Kluwer, a leading global information services and publishing company with annual revenues of (2011) €3.4 billion ($4.7 billion) and approximately 18,000 employees worldwide. Please visit our website for more information.

Wolters Kluwer Financial Services
130 Turner Street, Building 3, 4th Floor
Waltham, MA 02453
Phone: 781.907.6689

To learn more about
Secure Document Exchange,
please visit our website at
Insurance.WoltersKluwerFS.com,
or call us at 800.481.1522.