

# **SECURE CONTENT EXCHANGE IN THE FINANCIAL SERVICES INDUSTRY**

## Table of Contents

Introduction .....	3
Background.....	3
Changing Information Needs Drive Security Requirements .....	3
Impact of Legislation .....	4
Embracing XML and Web Services .....	4
Content Security Trends .....	5
Characteristics of Secure Content Exchange.....	5
Supporting an Array of Technologies.....	7
Challenges in Using Proprietary Technology to Secure Content.....	8
Migration to XML and Web Services .....	9
XML and Web Services Security Challenges .....	9
Conclusion .....	10

## Introduction

The financial services industry is in the midst of massive revolution in how it manages information. In the past several decades, the storage and transmission of financial content has moved from being largely a manual task to being stored on monolithic computers that were accessed by a select few to being managed by a distributed network of computer systems that are accessed by many and transmit vital financial content around the globe at the speed of light. This evolution has not only impacted the “back office”. Millions of consumers are now electronically transacting with the financial services industry on a daily basis via the Internet.

The increased use of computing to manage financial content has also resulted in a radical change in how financial services institutions conduct their business. In an effort to harness this computing power to generate operational efficiencies, and create new business opportunities, many business processes have undergone significant modifications. New technologies have also evolved to meet the challenge of streamlining the flow of information. This increased digitalization of financial information has even given birth to legislation that has further altered the financial services landscape. As the financial service industry’s dependency on computing grows, so has the need for the secure exchange of this vital financial content.

## Background

With an ever-increasing reliance on the Internet to conduct business with partners and customers, it is crucial that the financial services industry have a high level of security for the content that is so critical to conducting its business. Three major challenges are driving the need for information security in the financial services industry:

- Organizations are relying on federated and loosely coupled, peer-to-peer, distributed, and store-and-forward networks to exchange mission critical content.
- Threats from inside an organization are becoming ever-increasing threats.
- Persistent content security mechanisms – security across time and space – are needed to comply with government and corporate regulations for electronic business.

In order to ensure the secure exchange of content, these issues must be addressed.

## Changing Information Needs Drive Security Requirements

As enterprise computing has evolved from monolithic systems to client/server to thin-client to distributed, peer-to-peer to modern grid computing, management of content has become more complex. Applications in the financial services arena continue to integrate and automate entire value-chains. They have also increased their reliance on information that is distributed in far-flung locations. The bottom-line: information management is more complicated than ever before. In particular, authority to access and act on information is being delegated to the nodes of the application using trust relationships to establish federated privileges. Add an increase in the amount, and type, of content being processed and stored over time, and you have a pronounced need for content security.

Financial services organizations are also continually searching for new ways to increase their competitive advantage. An example of this type of differentiating innovation is known as Straight Through Processing (STP). The banking and insurance industries have been focusing on STP to automate business processes and build systems that reduce the time from negotiating a trade to settling it to analyzing the results. The proper implementation of STP will depend on the ability to replace traditional modes of communication, like the telephone and fax, with a completely automated, closed loop information transmission system. This means disparate systems used by brokers,

clearing houses, and custodians need to be tied together in a seamless fashion. There also needs to be adequate security for this exchange of sensitive content.

## Impact of Legislation

Regulatory compliance is another important factor influencing the exchange of content over the Internet in the financial services industry. Recent legislation such as the Gramm-Leach-Bliley Financial Modernization Act, the amendments to SEC Books and Records, the USA Patriot Act, and the Health Insurance Portability and Accountability Act (HIPAA) are all driving forces in decision-making regarding how to effectively manage content.

The cost of compliance with these recent pieces of legislation is having a significant impact on the financial services industry. For example:

- According to TowerGroup, the brokerage industry will spend \$700 million on technology over the next two years to support the Patriot Act.
- Software compliance alone (with the Patriot Act) will cost firms the size of Merrill Lynch and Citigroup \$30 million each.<sup>1</sup>
- The United States' largest health insurance provider, Aetna Corporation, has already spent \$33 million on HIPAA compliance.<sup>2</sup>

The combination of this regulatory compliance with the increased use of the Internet to vend information to internal users, customers, and partners puts additional pressure on financial services organizations to ensure that important content is protected from malicious attack and/or theft.

## Embracing XML and Web Services

Despite these compliance expenditures, and other pressures, financial services organizations are eagerly embracing the Internet to conduct business. For instance, banks are driving greater efficiency from the use of on-line services. In a survey by Celent Communications<sup>3</sup>, cost savings are ranked number one by participants in the list of overall benefits of having on-line banking services, with 26 percent. Customer retention is a close second at 23 percent, followed by the opportunity to cross-sell services at 19 percent. According to Grant Thornton, legislation like *Gramm-Leach-Bliley* is also driving community banks towards on-line services. In 2001, 75 percent reported offering on-line services – up from 55 percent in 2000.<sup>4</sup> Given their ability to seamlessly tie applications together on the back-end so that the necessary information can be vended on the front-end, Web Services and XML are being broadly adopted in the financial services industry as the enabler for conducting business on-line with customers and/or partners.

Web Services and XML are also helping financial services organizations streamline internal software integration. According to Gartner Group, “The use of standards-based messaging protocols, such as XML, can make new interface and integration development easier and more portable.”<sup>5</sup> As mentioned earlier, Straight Through Processing is a critical initiative of the financial services industry. To make STP a reality, the disparate financial services organizations involved need to agree on standard ways to exchange information that can be easily modified to address changing needs in a fluid environment. XML is a natural choice given these requirements. As such, financial services oriented XML variants, like FIXML, have been devised to address this need. FIXML was devised using an XML vocabulary coupled with the proprietary Financial Information eXchange (FIX) protocol,

<sup>1</sup> Bank Technology News, *Age of Tech's Transparency*, May 2003

<sup>2</sup> USA Today, *Health data mandate gives tech a boost*, June 8, 2003

<sup>3</sup> <http://www.celent.com/PressReleases/20011017/ROI.htm>

<sup>4</sup> Bank Technology News, *E-Mania Takes Community Banks by Storm*, May 2001

<sup>5</sup> Gartner Group, *Retail Branch Automation Technology: Perspective*, October 15, 2003

which is used for communicating securities information – it is estimated that the FIX protocol is used by up to 82% of all brokers to exchange information about quotes, trade orders, and other data.

Another example of the move to XML in financial services can be found with the Society for the Worldwide Interbank Financial Telecommunication (SWIFT). SWIFT is an industry-owned cooperative that provides the dominant form of financial messaging services used by banks, investment managers, and brokers/dealers worldwide to exchange information for such items as letters of credit, payments, and securities transactions. SWIFT has recognized the need to mitigate the inefficiencies brought about through the use of proprietary messaging technologies, and has been developing a new XML-based standard, referred to as ISO 15022XML, to eventually be used by its worldwide base of 7,000 banks to exchange critical financial information.

The retail banking industry is also making heavy use of XML and Web Services to gain efficiencies by tying internal front- and back-office systems together. As a replacement for legacy EDI systems, many financial institutions are looking to migrate their transactions to XML-based formats. This technology migration is being driven by EDI's slow, complex, and inflexible nature. Among other deficiencies, the use of EDI makes it difficult for financial institutions to keep up with customer demands for faster fund clearance, thus damaging important customer relationships. It also leads to higher costs for exception handling and other common transaction activities. According to Gartner Group, XML and Web Services are uniquely equipped to address these issues, "Web services will play a crucial part in developing the financial transactional part of the emerging XML-based business-to-business Internet. By 2006, more than 60 percent of worldwide fund clearances will use Web services (0.8 probability)."<sup>6</sup>

## Content Security Trends

There are inherent risks in exposing critical financial content to the outside world via the Internet. According to the Computer Security Institutes' (CSI) 2003 Computer Crime and Security Survey, computer crime and other information security breaches continue to be a major point of exposure. Theft of proprietary information resulted in the greatest financial damage – \$70+ million was lost in the trailing 12 months, with the average reported loss being approximately \$2.7 million. Furthermore, 36 percent of those surveyed cited their own internal systems as the source of attack. According to Chris Keating, CSI Director, "Fully 92 percent of respondents reported attacks. The 251 organizations that were able to quantify their losses reported a total of over \$200 million. Clearly, more must be done in terms of adherence to sound practices, deployment of sophisticated technologies, and most importantly adequate staffing and training of information security practitioners."<sup>7</sup>

Identity theft is also becoming an ever-increasing problem. The Federal Trade Commission received almost 120,000 complaints related to identity theft in 2002 – up from 85,000 in 2001. According to Ben Berry, supervisory special agent of the FBI's bank fraud squad, "With the advent of the Internet, there's so much information out there."<sup>8</sup>

## Characteristics of Secure Content Exchange

Information is the lifeblood of financial services. The need to securely exchange content has become more important than ever given the increased use of the Internet to vend and distribute content, and recent regulations that have altered how information is captured, distributed, and kept private. However, despite this, a large percentage of content remains unprotected within databases and file systems, is e-mailed without any sort of encryption, or is viewed and distributed by personnel

---

<sup>6</sup> Gartner Group, *Web Services Move Bank Payments Into 'Hyperdrive'*, August 7, 2002

<sup>7</sup> Computer Security Institute Press Release, "Cyber Attacks Continue, But Financial Losses Are Down" May 29, 2003

<sup>8</sup> Bank Technology News, *A New Breed of Criminals*, January, 2003

with insufficient access privileges. Financial services organizations, of all kinds, need to ensure that this critical component of their business is properly safeguarded. As such, secure content exchange should be characterized in the following way:

#### **Protocol Independence**

Many proprietary messaging frameworks and protocols are currently in use in the financial services industry to exchange content. As such, there must be broad security-related support for the associated range of messaging technologies, whether they are proprietary or standards-based, to ensure that transmitted content is kept secure.

#### **Encryption**

Much of the content in the financial services industry is private in nature. As a result, in order to protect the confidentiality of this content, it must be encrypted as it travels through numerous computer systems. By encrypting the content, only those with proper authorization can view a given piece of content.

#### **Persistent Security**

Content needs to be secured independent of time and location. Long-lived authentication ensures this by protecting information that is in-transit, stored in a database, or being processed by an application. Persistent security also involves guarding information in a mixed workflow environment – including e-mail, file transfers, EDI, mobile applications, and Web Services.

#### **Non-repudiation**

Preserving the integrity of content is also critical to securing content exchange. This is done, via non-repudiation, by ensuring that a transferred message has been sent and received by the parties claiming to have sent and received the message.

#### **Archiving**

By properly archiving transactions, it is possible to analyze security breaches, maximize operational performance, and maintain regulatory compliance.

#### **Policy Enforcement**

The ability to ensure that security policies are enforced is critical to enabling the secure exchange of content. The business logic describing a security policy must enforceable.

#### **Policy Update Monitoring**

There needs to be mechanisms in place to alert the proper personnel when a security policy is being modified. By doing this, changes to the security architecture can be audited to protect against “information leakage” resulting from insufficient policies, or inappropriate changes to security policies.

#### **Future Ready**

As important as it is to preserve investments in existing technology and infrastructure, it is equally important that systems be able to transition seamlessly to new technologies. By maintaining a high level of security as systems evolve to embrace advanced technologies, like XML and Web Services, financial services organizations can protect their mission critical content and develop a competitive advantage for the future.

## Supporting an Array of Technologies

Given that IT investments happen over time, secure content exchange must be viewed in the context of multiple technologies that have their own, distinct life cycles. Existing investments in proprietary “legacy” messaging frameworks, protocols, and associated infrastructure must be fully supported to ensure that there is unified security coverage and that existing investments are preserved as new technologies are adopted. The transition to open standards, like XML and Web Services, must occur seamlessly so that there is no disruption in service, or the security of exchanging content.

The following are some examples of popular messaging protocols, business frameworks, and security algorithms currently in use in the financial services industry:

### Business Transports Protocols:

<b>AS1</b>	The Internet Engineering Task Force (IETF) has developed this specifications for transporting EDI or XML documents over the Internet in a secure (digitally signed and encrypted), highly reliable manner. It secures data with S/MIME (Secure/Multipurpose Internet Mail Extensions) encryption over SMTP.
<b>AS2</b>	This “cousin” to AS1 makes use of the HTTP protocol to allow for much faster synchronous, “real time” transmission of data with immediate message delivery notices. It secures data with S/MIME over HTTP.
<b>eBXML</b>	Designed by United Nation’s CEFACT and OASIS to enable the exchange of electronic business data on a global scale using XML.
<b>Internet EDI</b>	Internet EDI (EDI/INT) supports the most secure data transfer standards, including AS1, AS2, PGP, S/MIME and Secure Sockets Layer (SSL). Digital certificates provide authentication, encryption and non-repudiation.

### Application Transport Protocols:

<b>FTP/S</b>	An SSL-enabled equivalent of the File Transfer Protocol (FTP) that supports the use of X.509 digital certificates.
<b>HTTP/S</b>	HTTP/S (Hypertext Transfer Protocol over Secure Socket Layer, or HTTP over SSL) is a Web protocol developed by Netscape. HTTPS supports the use of X.509 digital certificates from the server so that, if necessary, a user can authenticate the sender.
<b>Message Queues</b>	A transport conduit for carrying messages using a store-and-forward delivery model that guarantees the arrival of messages which have been onto a specific destination “queue”.
<b>SMTP</b>	Simple Mail Transfer Protocol (SMTP) is the Internet’s standard host-to-host mail transport protocol.

### Content Security Protocols:

<b>PGP/MIME &amp; OpenPGP</b>	Both use MIME to structure their messages and move signed/secure messages over the Internet. They are based on PGP (Pretty Good Privacy).
<b>S/MIME</b>	Secure Multipurpose Mail Extensions (S/MIME) is an e-mail security protocol. It was designed to prevent the interception and forgery of e-mail by using encryption and digital signatures. S/MIME builds security on top of the MIME protocol and is based on technology originally developed by RSA Data Security, Inc.
<b>Web Services Security (WS-Security)</b>	A specification that proposes a standard set of SOAP extensions that can be used when building secure Web services to implement integrity and confidentiality.

It is reasonable to assume that a typical financial services organization will have several of these messaging technologies in use in their organization – plus, many others. Secure content exchange must provide ‘blanket coverage’ to this universe of messaging technologies so that there is no ‘weak link’ in the chain.

## Challenges in Using Proprietary Technology to Secure Content

As a particular technology sector matures, it is a normal occurrence to initially have a multitude of competing proprietary solutions develop until open standards evolve and become ubiquitous. As the table above depicts, the appearance of multiple proprietary solutions has definitely occurred within the financial services industry. Several security challenges arise from the proliferation of numerous messaging protocols in use in today’s financial services industry:

### **Complexity**

Non-standard protocols require that custom scripts be developed to facilitate cross-system communication. If several protocols are in use, considerable code needs to be generated. The more complex the code base, the more difficult it is to defend against malicious attack and the more likely crucial information will be unknowingly exposed to unauthorized access.

### **Cost**

Incremental costs can result from a number of sources when proprietary technology is in use. Additional programmer expenses are incurred from the generation of custom code. Also, large amounts of custom code can lead to security breaches that can become very costly given the sensitivity and financial nature of the content involved. Many proprietary security technologies, like PGP, also require expensive recurring license fees as part of their usage.

### **Maintenance**

The aforementioned custom code requires maintenance as security, and business, conditions change. Also, the greater the mix of proprietary messaging protocols in use, the more difficult it is to provide adequate security as the level, and type, of security attacks increases.

### **Interoperability-related Security Gaps**

Tying two, or more, proprietary messaging technologies together can result in unforeseen security gaps as financial services organizations exchange content with partners and customers. Security flaws in proprietary APIs, required for cross-protocol communication, can result in unwarranted access to valuable content.

### **Lack of Adaptability**

As new technologies and standards emerge, it is often difficult to migrate existing investments in proprietary code and infrastructure. This forces an organization to either chose to stay with old, non-secure technologies or scrap significant existing investments in order to take advantage of the latest advances.

## **Migration to XML and Web Services**

The use of XML and Web Services technologies makes it easier for applications to communicate with each other in a transparent nature. Through Web Services, integration is enabled as the applications access one another as a 'service'. The communication of content between applications is unrelated to the underlying proprietary nature of the applications. The result is relatively seamless application integration.

Financial services organizations are rushing to embrace XML and Web Services as a standards-based way to exchange content internally, and with customers and partners. According to a report from the TowerGroup entitled *The Networked Financial Institution: Connections for a Successful Business Strategy* "The lack of common platforms and protocols is a significant barrier to realizing the vision of the networked financial services institution. Web services adoption can be expected to drive momentum in the financial services industry as technology providers move toward true standardization."<sup>9</sup>

The use of standards-based technologies, like XML and Web Services, can lead to previously unforeseen system integration efficiencies, both internally and externally, and other new business opportunities. For instance, prior to the use of XML and Web services, if a commercial bank wanted to resell insurance it would have to invest heavily in IT infrastructure and reach agreement with the insurance company on the type(s) of proprietary communications protocol(s) to be used, the appropriate data format, and the intermediary VPN or EDI network to be deployed. Once agreement was reached, someone would have to maintain this extensive communications system at considerable expense. The use of XML and Web Services renders many of these decisions, and expenses, moot. To further quantify the point, according to Celent Communications, significant cost savings can be expected in the insurance industry as XML adoption increases, "If embraced universally throughout the US insurance industry, the use of standards could save the industry over US\$250 million in technology costs annually."<sup>10</sup>

## **XML and Web Services Security Challenges**

Although many of the security challenges posed by the use of proprietary technologies are solved through the use of XML and Web Services, several new issues related to the secure exchange of content are created. XML's greatest strength and weakness is that it describes a great deal about the content that's represented in a document. On one hand, this feature simplifies programming and facilitates interoperability among systems and disparate applications. On the other hand, XML's openness makes it easy for those interested in breaching security to see where crucial content 'lives'. The exposed nature of XML elevates security issues from the TCP/IP stack to the application layer of the OSI model.

---

<sup>9</sup> [http://about.reuters.com/newsreleases/art\\_27-8-2002\\_id1055.asp](http://about.reuters.com/newsreleases/art_27-8-2002_id1055.asp)

<sup>10</sup> Celent Communications, LLC., *ACORD XML Standards in US Insurance Industry*

When using XML, there is a need for content-awareness as well as context-awareness. Authentication, authorization, confidentiality and auditing cannot be provided (or retro-fitted) at the lower layers of the OSI stack. As more information moves between applications that are not in the immediate control of the originator, it becomes essential to guarantee that only the intended recipients are given appropriate access privileges to the information – wherever it resides. Assurances need to be made that information is not only tamper-proof and confidential during transit but also upon arrival, in-storage, and during processing.

Security is further complicated when one considers that XML and Web Services-based systems must interact with existing proprietary messaging systems. After all, it is not reasonable to assume that organizations will 'flip a switch' on their 'legacy' systems and transition entirely to state-of-the-art systems. There will, undoubtedly, be a lengthy period of co-existence where financial services organizations will need to preserve their considerable investments in existing systems as they gradually migrate to standards-based XML and Web Services systems. As such, financial services organizations will need a security architecture that will accommodate both new and existing systems, and provide adequate security for content exchange between systems, internally and externally.

## Conclusion

The financial services industry is experiencing an explosion in the use of computing and the Internet to manage, distribute, and vend information to partners and customers. This has resulted in increased efficiencies and expanded business opportunities for those financial services organizations willing to embrace change, but it has also brought new challenges in how to protect vital content that is widely exposed through the increased use of global networks and the Internet. Add the need to comply with recent privacy-related legislation plus radical changes in business processes to gain competitive advantage, and there exists an information management challenge of monumental proportions. Technologies like XML and Web Services will help a great deal in addressing these challenges, as they become the lingua franca of the financial services industry. However, the security needs exposed through the use of these new technologies, in conjunction with existing methodologies, need to be addressed if financial services organizations are to be successful.

With this in mind, Forum Systems has developed Presidio™ to address these complex security challenges that are facing the financial services industry. Presidio is an integrated, appliance-based solution that provides secure content exchange for both legacy messaging technologies, as well as XML and Web Services. Through its use, financial services organizations, of all kinds, can securely preserve their investments in existing messaging infrastructure and at the same time take advantage of the benefits enabled by XML and Web Services. For more information on Presidio, please see the Forum Systems website at [www.forumsys.com](http://www.forumsys.com)