

Mail

Secure email for the SWIFT community



*The convenience
of email combined
with SWIFT's security
and reliability*

Benefits

- Secure, person-to-person exchange of messages and documents
- Easier compliance with IS security policies
- Minimised reputational risk
- Guaranteed delivery of sensitive documents and information
- Existing email infrastructure preserved
- No change to end user experience
- Cost effective, usage-based pricing

Executive summary

In the financial services industry, reputations are built on trust. One slip in terms of data security can result in massive damage to an institution's brand image. But this is an industry where documentation is crucial, whether in terms of business records, contract agreements, statements or guarantees, and those documents need to travel securely between parties.

Using a courier to deliver sensitive documents involves time and expense. With its speed, convenience and cost-effectiveness, email has established itself as the preferred medium for both business and personal communications. However, it is difficult to ensure the secure delivery of these sensitive items, especially in electronic formats.

SWIFT works to ensure the secure and efficient communication of sensitive information between organisations. Our IP-based network (SWIFTNet) provides an established standard for secure payments messaging. However, many institutions need to send longer documents, or those documents that are not supported by SWIFT messaging formats. Hence there was a demand among the SWIFT community for the same standards and security to be extended to email.

Mail provides a simple and cost-effective means for members of the SWIFT community to send emails containing sensitive information across SWIFTNet. There is no need for upfront investment in hardware, and because Mail works with the existing email interface, end users don't need any training.

Clearstream, DnB NOR, FirstRand Bank Ltd, HSBC, Nedbank, Standard Bank and SWIFT itself are among a growing community using Mail to communicate confidential information quickly, efficiently and securely between organisations. Mail expands the SWIFT user community further into the enterprise by extending accessibility to the desktop, and thus to a wider variety of users and uses.

By working together using Mail, each institution can continue to use its existing email technologies while safeguarding its reputation, and establishing a secure and low-cost network for communications across the financial community.

Sending sensitive data

Where financial matters are concerned, there will always need to be documentation – records need to be kept, contracts agreed, guarantees given and statements produced. But transmitting such sensitive information in a secure manner presents significant challenges. Items can get lost or delayed in the post; courier services might guarantee delivery, but they are expensive, and faxes can be intercepted.

From banks to brokers, insurers to corporates, financial institutions have extended communication across a growing number of channels, improving customer relationships and achieving more efficient processes as they go. In a world where almost every customer has access to a computer, channels such as the Internet provide a powerful communications interface that can allow better, faster communication between

.....
“The main issue we face is that whenever we transmit anything confidential, whether by fax or email, there is always a risk that it will go astray or be intercepted.”
.....

Colin Brooks, Deputy Head, HSBC Securities Services, Asia Pacific
.....

different offices, and between institutions and their customers.

Perhaps the strongest benefit of the Internet is that it is a public network, accessible across the world. No wonder then, that financial services organisations are among the many industries that have recognised its potential as a strategic business tool. The Internet has established a global user community, and businesses have embraced email, because large documents can be sent to multiple recipients at the touch of a button, without the time and expense involved in printing and delivering hard copies. As a result, business decisions can be made and communicated, in writing, within minutes.

But while channels such as email bring undoubted benefits, they are also accompanied by risk. Emails might be faster than ‘snail mail’, but they can also be lost or intercepted. Most of us have had a message go astray at some time – some are delayed due to server or network problems and turn up hours or days later, while others never arrive at their destinations at all.

At best, lost or delayed messages are a significant annoyance. At worst, they can spell disaster. When you are dealing with the paperwork that underpins a financial transaction, whether this is an application, contract or documentary support, a delayed message can mean the difference between a successful trade and a failed one – or between significant profits or losses.

The financial services community feels this risk keenly. In addition to the risks associated with delivery mishaps, this sector is more than any other a target for online fraud. Phishing, pharming, worms and Trojans are just some of a growing number of threats that face anybody sending sensitive information via the Internet, and of course, where a large volume of financial information is involved, fraudsters will try all the harder. “Email can

be collected, scanned, filtered and anybody can read or even change the content,” says Michael Jaeggi, head of department for product management and design of core products at Clearstream Banking. “This makes email communication an easy target for illegal interception.”

Whatever the logic of machines and security processes, the people who use them are only human. They might be incredibly smart, but they can also make mistakes. Most people would swear that they would never respond to a bogus email purporting to be from their bank or another financial institution and asking for sensitive information – but in phishing attacks, emails such as these are sent out on a massive scale – why wouldn’t they be, since email is such a cheap (or often, in the case of Internet mail, free) and fast medium? Even if less than one per cent of recipients respond, that adds up to a massive return for the sender, in the form of identity theft and other fraudulent gains.

Reputations at stake

Many firms are working to secure their email communications, but choosing a secure email system is growing more complex – there are so many in operation that most are used according to one-to-one agreements between parties. This adds cost as well as complexity, since many of these applications entail

investment in servers and network technologies.

“There are encryption packages on the market, but there is no standard package,” says Colin Brooks, deputy head of HSBC Securities, Asia Pacific.

“Every institution pretty much chooses its own preferred option. If we have 100 clients, the chances are that we’ll be using ten or twenty different packages on a bilateral basis to encrypt the data we send them – otherwise, the client might ask us to send the information via email, saying they’re willing to take the chance of it being intercepted or misdirected.”

The problem is that, even if clients are willing to take that chance, there is a far greater risk entailed for the bank. “We can explain the risks to the client and make sure they acknowledge that we’ve alerted them to these,” explains Brooks. “But if we send information and it gets intercepted and used fraudulently, the newspapers are not going to be concerned with the fact that the client accepted the risks. Particularly in the Internet age, if data is lost electronically, it does serious harm to your brand.”

A community response

The fact that most companies have internal policies on email usage tells us that financial institutions are taking these issues seriously. Recent research by Forrester found that, in 2006, almost 50 percent of organisations were planning to deploy some form of email security, for reasons that were as much to do with compliance as to do with combating spam and malicious attacks.

But secure email is only part of what financial institutions need – they also need to reduce the complexity of using security solutions across the industry by introducing a product that every institution

.....
“In this industry, institutions can spend billions of dollars on building their brand. The publicity following any sort of breach would focus on how data was intercepted because it was sent in an insecure environment. That’s a serious reputational risk for any financial institution.”
.....

Colin Brooks, Deputy Head,
HSBC Securities Services, Asia Pacific
.....

.....
“By reducing the number of delivery channels and service providers you’re using, you’re simplifying the infrastructure, improving resilience and enabling better solutions.”
.....

Finn Otto Hansen, Head of Clearing and Settlement Strategies, DnB NOR
.....

can work with. “It would ease communication to have a protected solution within the financial community, which could be used for transmitting several types of document, to send reports or to transmit messages containing sensitive data,” says Jaeggi. One community was quick to recognise this. SWIFT works for the benefit of the financial services industry, providing common standards for financial transactions around the world. A global community of financial institutions is connected to our IP-based financial messaging network, SWIFTNet, which currently connects over 8,000 institutions in 205 countries, and is a trusted medium for the majority of the world’s interbank messages. This community saw the need for a simple and reliable answer to the problem of sending sensitive documents via email, and it asked SWIFT to develop a solution. The result was Mail.

“The battle to convert email into a reliable and trustworthy business tool continues to drain the resources of organisations and tax the ingenuity of solution providers,” says Keith Vallance of SWIFT. “Mail delivers a simple, compelling alternative to the challenge of making Internet email fit for business by offering a secure, dependable communication channel for financial organisations and their partners.”

Mail

Mail lets users access the SWIFT network from their desktops, so that simply by using their usual email application, they can direct sensitive messages across SWIFTNet, avoiding the perils of the public Internet. It can be used by any organisation connected to SWIFTNet, and its growing user community includes Clearstream, DnB NOR, FirstRand Bank Ltd, HSBC, Nedbank, Standard Bank and SWIFT itself. For many institutions, Mail has proven to be the ideal medium for a range of sensitive documents.

“SWIFT provided an early response to the demand for this type of application,” says Finn Otto Hansen, head of clearing and settlement strategies at DnB NOR. “When we made our decision to connect to Mail, we were looking at all aspects of our connectivity. We wanted to reduce the number of delivery channels we used.”

“SWIFT already has a good reputation within the financial services business,” adds Colin Brooks. “It has established connectivity and a reputation for reliability. The wide SWIFT connectivity that already exists within the industry can be used to make Mail the standard, uniform encryption package that everybody can use.” John Sagegg, securities services project management at Nordea, adds: “Generally, SWIFT is of great strategic importance to us on the security side, and we’re looking forward to being able to send documents such as contracts, reports and invoices securely via email when we implement Mail in the fourth quarter of 2007.”

In addition to the trust that SWIFT engenders among financial firms, Mail uses the existing email infrastructure, removing the need for investment in new hardware and network equipment.

Simple and effective

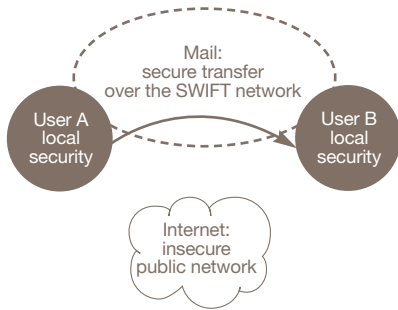
Unlike Mail, standard encryption packages often entail messages travelling through an indeterminate number of stages to reach their final destination, with no control over the route they might take. Internet connectivity is potentially vulnerable, and as evidenced in the aftermath of the Taiwan earthquake in December 2006, it is not always possible for a damaged network to reroute Internet traffic so it reaches its destination. As a point-to-point service, Mail delivers mails quickly over the SWIFT network, using the existing email infrastructure while avoiding the public Internet.

As long as the institution has SWIFT-supplied interface software (Alliance Gateway or Alliance Starter Set), it can use Mail with its existing email infrastructure. Once it has been installed and the email system configured to carry mail with the ‘.swift’ addition to email addresses, there is no need for individual set-up – or for training – with each end user.

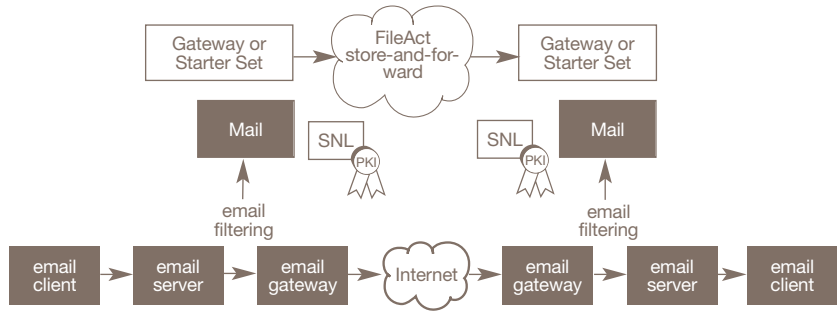
“For the end user, there isn’t a new front end at all,” says Jane Cole, head of solutions at FirstRand Bank Ltd. “The front end is effectively their normal email inbox, and that’s a big positive. This means that users already know how to use it – the only training you have to do is to tell people to put ‘.swift’ at the end of the email address, then the message will automatically be rerouted via Mail rather than across the public Internet.”

As the Mail community grows, companies at different stages of implementation agree on its simplicity. “We understand what is expected both from ourselves and from SWIFT,” says Nordea’s Sagegg. “We expect the implementation to be simple, straightforward and easy, and we think we will easily be able to tailor Mail to our internal email and Internet usage policies.”

In Cole’s experience, this expectation is justified: “It was very simple to implement,” she says. “The documentation we got from SWIFT was comprehensive, so we knew what to expect throughout the process, and any questions we had were answered within the space of a phone call.”



Mail seals the secure passage of emails between organisations



How Mail carries sensitive documents through the system

How does it work?

Mail is easy to install and to use, but how does it work? In simple terms, it acts as a gateway for sensitive emails (those with '.swift' added to the address), taking them onto a secure delivery route as they pass through the organisation's email system.

Instead of messages being sent through the normal email gateway via the Internet, where they become vulnerable, they are directed through the secure Mail application. Here, they are wrapped in a FileAct envelope and passed safely over the network. All encryption is handled at line level, and any files attached to the message are signed with Mail public key infrastructure (PKI) to ensure their integrity and security.

The diagram above shows how Mail works with the email filtering system at both the sender's and the receiver's end, to reroute emails via and provide them with a secure passage between SWIFT users.

“Users can start using Mail immediately, because all they have to know is to add ‘.swift’ to the addressee’s e-mail address. The solution can be used from the standard mail client.”

Michael Jaeggi, Head of Department for Product Management and Design of Core Products, Clearstream Banking

Mail uses your regular email application, such as Outlook or Lotus Notes, so sending secure messages and documents is as easy as sending any other email:

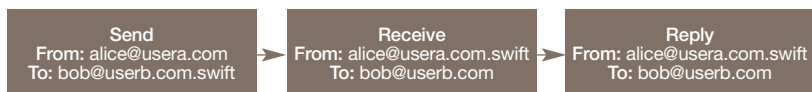
1. By adding '.swift' to the end of the recipient's email address (e.g. bob@userb.com.swift), the sender directs the message to the Mail application
2. The message is carried across the SWIFT network where it is wrapped in a secure FileAct wrapper and any attachments signed
3. The message arrives in the recipient's inbox, with the '.swift' tag added to the sender's email address (e.g. alice@usera.com.swift) – so that by clicking the 'reply' button, the recipient automatically sends any response through mail.

Because the majority of financial institutions are connected to SWIFT, this means that they can easily implement Mail to ensure cost-efficient email security.

“Using SWIFT, you know that the message is going to be delivered,” says Cole. “That’s a major benefit.”

“Our expectations of Mail were clear. We knew what to expect during the implementation, and following that, in terms of the way the product worked. All those expectations were met.”

Jane Cole, Head of Solutions, FirstRand Bank Ltd



.....
"You only have to have one solution to communicate securely by email with anybody on the SWIFT network, instead of having to have multiple party-to-party solutions in place."

Rob Green, Head of Payments,
FirstRand Bank Ltd
.....

Extending the benefits

Mail extends the benefits of the SWIFT network deeper into the enterprise, enabling users to send emails over from their desktops with no need for expensive outlay on new technology. Its clarity, ease of implementation and the lack of training required for end users make Mail perhaps the simplest secure email product available for the financial services industry.

"The difference with Mail is that it's pervasive – every person in the world who is connected to SWIFT can potentially send and receive mail in an encrypted format. This makes it a lot more powerful than other secure email solutions, which tend to be used on the basis of individual agreements," says Rob Green, head of payments at FirstRand Bank Ltd. "The level of connectivity that Mail provides automatically opens up the entire worldwide communication base of a bank, enabling it to send normal email messages in a secure fashion."

This potential to extend one secure email application across the entire SWIFT network opens up a world of uses, as Cole points out: "For example, in the trade environment, copies or images of documents are still sometimes sent by

.....
"Mail is a vastly superior product that helps organisations quickly and easily to avoid potential damage to their reputation – it's difficult to put a dollar value on that."

Colin Brooks, Deputy Head,
HSBC Securities Services,
Asia Pacific
.....

email in the event of queries. Mail can make sure users enjoy that convenience while keeping the documents secure."

As well as ensuring the secure delivery of emails and sensitive documents, Mail can be configured to comply with internal communications policies – emails pass through the organisation's email security and are protected by the same firewalls as the company's Internet system, before being securely routed through the SWIFT network.

Mail out of the box

Because Mail can reach all levels of the organisation, its uses are limited only by the thinking of the institutions using it. Here are some examples:

- Contracts – the physical hard copy that goes between banks and legal teams via courier can be handled digitally and sent via email
- Service level agreements
- Guarantees and standby letters of credit – these can sometimes be too long for the trade message structures that handle them. Where appropriate, they can be sent by email
- Loan documentation between financial institutions
- Requests for information and responses to these
- Confirmations and affirmations
- Management information system reports
- Terms and conditions
- Interbank reporting, such as details of non-STP (straight-through processing) charges.

"Many areas of the financial services industry, from treasury to the custodial

business, have a significant amount of faxes and hard copies floating around that could be automated, digitised and dealt with via Mail," says Green.

"Look at the things you're sending by fax, email or courier today, that you're a little uncomfortable with. All of this can be sent via Mail. The list is endless, and it's driven by the creativity that you have, and where you see the potential to use it. A lot of banks haven't yet asked themselves where they should look to introduce Mail throughout the organisation, to users and departments who will see value in using it.

For example, there's a lot of exchange in the domestic market between banks, for unpaid cheques, requests for reports and so on, which is sent via ordinary email or as physical hard copy. That is a natural candidate to be able to use Mail."

Cost benefits

Because of its versatility and ease of implementation across the SWIFT network, Mail can create significant savings from a variety of perspectives:

Spend

SWIFT connectivity reaches across the financial services industry, and Mail reaches deeper into the organisation, offering a comprehensive, standard means of secure email communication with no outlay on hardware. The small per-message charge has recently been reduced by 50 per cent, and the system needs very little in terms of ongoing maintenance.

Simplicity

Mail reaches end users throughout the organisation without adding complexity. Once it is configured to comply with internal email and Internet usage regulations, it simply works with the existing email system and firewall. Encryption and security measures take place within the SWIFT system, so there is no installation at the desktop, and it can be managed easily on a central basis.

Resources

End users don't need training to start using Mail – it works with their usual email application, and the only thing they need to remember is to add '.swift' to the end of the email address. The need to devote IT resources is also minimised, as Mail is easy to implement and avoids the complexity that can arise from maintaining multiple email solutions.

Risk

Mail minimises risk from several perspectives:

- There is no significant upfront investment
- Its ease of use with familiar email programs means there is no risk of rejection by end users
- It safeguards brands and reputations by simplifying secure communication and reducing the risk associated with sending documents by email

A growing community

The simplicity of Mail can be deceptive in terms of the multiple ongoing benefits it delivers to ever more levels of a growing community. The community is widely established across the financial services industry, and Mail adds a further dimension by giving users access to the network for sending emails from their desktops.

Mail is already established as the secure email solution for a growing number of major financial firms, where it has proven to be an exceptionally simple, efficient and cost effective way to ensure the secure delivery of sensitive documents. But the full extent and impact of the benefits that it can deliver across the financial services industry will not become clear until Mail is extended and widely used across the SWIFT community.

"Mail has proven to be an effective technical solution," says Cole. "It's now up to us as financial institutions, and other users beyond that, to adopt Mail, and to start engaging with each other to see how further business benefits emerge. Industry players such as stock exchanges, banks, and other institutions need to discuss amongst themselves whether they send information by fax or by Mail. This is not something that can be driven by any single organisation worldwide. It will require input and effort from everybody within their own countries to get this up and running on a global scale."

This ethos is characteristic of the SWIFT community, says Paul Shetler, Senior Manager, Product Innovation at SWIFT: "The SWIFT community has been growing for over 30 years, and is built on cooperative action and mutual trust. Mail has been developed to extend that level of trust further, within and between the

.....
"We are working to encourage our counterparties, and even our competitors, to use the service. It follows the SWIFT ethos, which is to provide services and solve problems for the financial community – I think Mail will make a big contribution to this."
.....

Colin Brooks, Deputy Head, HSBC Securities Services, Asia Pacific
.....

financial organisations of that community. It increases the versatility of the SWIFT network by providing a single tool for simple and secure email communication between financial organisations, and across a growing array of roles within them."

SWIFT members know that in order to ensure that level of protection throughout the SWIFT network, all of them need to consider connecting with each other via Mail.

Once this is achieved, the financial services industry will benefit from a common level of protection and the ease of having to manage only one point of connection to that shared environment.

Jaeggi looks forward to the benefits of a more widespread Mail community: "Once the majority of SWIFT member banks are using Mail, it will become a medium for communication with our customer base, with no need to set up bilateral exchanges. The infrastructure is already in place when the SWIFT member decides to participate," he says. "We will be proposing to our customers that they use Mail as the preferred medium for exchanging sensitive information."

Looking ahead, Brooks adds that Mail has significant potential: "Beyond the uses we currently have for Mail, the possible breadth of its uses is enormous, across every aspect of financial services. "

In the future, says Brooks, Mail could extend beyond the immediate financial services community towards other sectors that it deals with. "For example, we run a corporate trust and loan agency business, and one aspect of that is that we have to move quite a lot of legal documents around, exchanging them with solicitors and law firms. If those industries were to become SWIFT-enabled, like the financial

services industry, then Mail could benefit communications in these businesses too."

For the SWIFT community, Mail offers a fast, simple and low-cost solution to the problems inherent in sending sensitive information between organisations. By working together using Mail, each institution can continue to use its existing email technologies while safeguarding its reputation and working towards an industry standard for secure communications.

For more information please contact your SWIFT account manager or visit www.swift.com