

## **How to send a S/FAX over IP** – by *Stefan Engelbert, Director Zest Promotions Limited, Pembroke, Malta*

What are the dilemmas the modern business community is facing? Electronic document exchange became very easy accessible. Legal and technical standards in business document exchange are still not on a solid ground yet.

In old days you just wrote and signed a letter, posted it and thanks to your signature your document was legally binding. Nowadays most businesses can not afford to use snail mail for their time and money critical business correspondence.

The next evolution step after postage was FAX. FAX keeps the look and feel of your document and arrives on the recipient's desk in a matter of minutes. Unfortunately the law in most countries does not accept a FAX as a legal relevant Document. Furthermore everybody knows the low quality and resolution of FAX transmitted documents.

With the next evolution step some disadvantages of FAX had been removed. Nearly everybody today can be reached via email. The introduction of the S/Mime standard removed one of the last remaining weak points of email. S/Mime allows you to digitally sign your correspondence. But while snail mail and FAX preserved the look and integrity of your original documents with the introduction of e-mail nobody knows the look of his email at the recipient's end. But what happens if an architect wants to send a design to a customer? Most likely the customer will not have CAD software available to display the drawings! Furthermore did you ever think about what happens with the email once it arrives to its recipient? An email is unprotected and can be copied and printed without any limits. For example it is close to impossible to do a digital rights management (DRM) of your documents sent via email.

There is one other big problem that email is currently facing. SPAM! Long underestimated and just seen as an unwelcome noise it became a real threat to email communication. Along with this threat a number of SPAM filters were developed. Most SPAM Filters currently on the market are just content sorter. They sort HAM and SPAM after accepting the mail. But due to the large amount of SPAM nobody really bothers to review all emails which were classified as SPAM. This results in bad habits of deleting SPAM fully automatic. You as a sender would not get notified that your email got deleted as SPAM. That would work only if the recipient uses a SPAM Filter on protocol level which rejects SPAM with the reason of rejection before accepting it. Such Anti SPAM SMTP Proxies are very rare on the market.

The ideal solution for modern document exchange would incorporate all advantages of Letter, FAX and S/Mime. Such a solution would incorporate the features listed below and could be called S/FAX over IP.

- Keep look and integrity of your original documents.
- Should use existing transport infrastructure such as SMTP.
- Must meet legal requirements like Digital Signatures.
- Should encrypt content to avoid 3<sup>rd</sup> parties reading it .
- Has to allow Digital Rights Management (DRM) of the transmitted documents.
- Recipient must not need any new Software or Hardware.
- Bypass SPAM Filter due to content encryption.

This next evolution step has already taken place silently with the introduction of PDF. Everybody knows the Portable Document Format which can be read on virtually every Computer Platform nowadays.

### **Why PDF?**

Portable Document Format (PDF) has long been the de-facto standard for exchanging platform-independent, printable documents. This format is truly omnipresent - virtually every document downloadable from the Web is a PDF. A PDF Reader on your computer is as much a necessity nowadays as a browser or Microsoft Word.

So here comes the novel idea: S/FAX over IP will generate secure email in the PDF format instead of S/MIME. Such email will be based on passwords and digital certificates, and free of all the shortcomings of Letter, FAX and S/MIME mentioned above.

What makes PDF a great media for transporting secure mail?

- PDF is printable - your document will come out the same no matter what printer or platform you print it on.
- PDF is platform-independent. Your email will never again look like gibberish due to encoding incompatibilities - all the fonts necessary to display the message are embedded in the document.
- PDF is free. PDF Reader, are available at no cost.
- PDF supports file attachments. A PDF document can contain binary embeddings of arbitrary size and contents (called File Attachment annotations) that can be extracted and saved to disk at a click of a button.
- And last, but not least, PDF is secure. That's really what makes this whole idea work. We will take a close look at PDFs security features next.
- Secure, signed PDF are allowed to be used for electronic case filing in US

This PDF Document was generated for free by the Aloaha PDF Suite

If you want to learn how to make your own PDF Documents visit:

**<http://www.aloaha.com>**

## PDF Security Overview

Security is built into PDF format in the form of password-based encryption, permission flags, and digital signatures. All of that is beneficial for secure mail, especially password protection.

When a secure PDF is created, the document author can opt to supply two secret strings: the Owner and User passwords. Applying these two passwords to the document using an algorithm described in PDF specifications produces a secure document. The author may optionally embed a set of permission flags in the document that would prevent a user from performing certain operations with the document, such as printing, copying/pasting, modifying and form filling.

A secure PDF's content is encrypted with the RC4 algorithm, a stream cipher invented by Ron Rivest of RSA Security. Either a 40-bit or 128-bit key can be used. An encryption key is derived from the user password alone. The owner password is used to encrypt the user password and also to protect the immutability of the document's permission flags. An encrypted copy of the user password is embedded in a secure PDF for validation purposes.

To open an encrypted document, the viewer must specify either the user or owner password. Specifying the valid user password enables a user to view the document, but also makes him subject to the permission flags associated with the document. For example, a user may not be able to modify or print the document. Specifying the valid owner password gives the user full control over the document: not only can he view it, but he can also change or remove its security settings.

In addition to encryption and permission flags, PDF also allows a document to be digitally signed. A digital signature protects a document's integrity and provides proof of the signer's identity. PDF uses the same digital signature format, known as PKCS#7, as S/MIME, and it is also based on certificates. Digital signing of PDF documents nowadays is a legal requirement for business relevant documents in most industrial countries.

## Implementing S/FAX over IP

Let's go back to S/FAX over IP. Since the new reincarnation of the secure FAX implementation is digital signature based, the sender and recipient do not need to agree on a password.

Whenever a secure message needs to be sent, S/FAX over IP generates a secure PDF document containing order information including buyer's name, address, phone, and credit card number. The document is encrypted using the client's password, signed with the sender's digital signature and sent to the client as an attachment via email. Any mailing component can be used for that.

Upon receipt of the message, the client opens the file attachment. Acrobat Reader comes up verifies automatically the integrity of the document and digital signature. Note that the client is free to use any email software at all, and on any platform, including free Web-based email systems like hotmail.com -- a luxury the S/MIME approach could not afford him.

As an additional amenity, digital rights management can be applied with ease. The PDF can be encrypted with two different passwords. One password allows the client to view the PDF document on screen only, the other gives him full control over the document, including printing and copying/pasting privileges.

One affordable tool to implement S/FAX over IP is the **Aloaha PDF Suite**. The Aloaha PDF Suite allows you to generate a digitally signed PDF Document from every windows application and send it via SMTP or MAPI.

This PDF Document was generated for free by the Aloaha PDF Suite  
If you want to learn how to make your own PDF Documents visit:  
**<http://www.aloaha.com>**