etherFAX and Security

Security is a clear differentiator when comparing other outsourced fax services to etherFAX. etherFAX incorporates a multi-level encryption/security system known as a "defense-in-depth" approach. It is a layering tactic, conceived by the National Security Agency (NSA), as a comprehensive approach to information and electronic security.

In addition, all fax transactions are processed in a secure and encrypted database utilizing the same standards. Lastly any images/content in the etherFAX system only persists for the life of the transmission and is then destroyed with all data being zeroed; ensuring etherFAX meets all regulatory compliance requirements.

We start with a secure communication channel over HTTPS that secures the "pipe" between the etherFAX client/customer and the back-end services hosted by etherFAX. Once a secure channel has been established, each customer is authenticated using his or her account, user name, and password. Lastly, the etherFAX web service model further encrypts and protects the communication on a "message level" even though the HTTPS channel is already arguably secure.

Many products and services in the market completely disregard security when it comes to communication with the back end services. Forwarding faxes as e-mail attachments, poorly designed communication systems, or even deploying T.38 right at the customer premise all contribute to poor (or NO) security at all. Think of it this way; HTTPS using certificates is only using "a" public/private key-pair system for communication where this base key is the basis for communication between all systems. With message level security, a new key is derived using a challenge/response mechanism that creates a key that is unique to each session with the etherFAX back-end system. Once the channel/pipe is secure using HTTPS, the etherFAX web service protocol then further protects (doubly encrypts) information on the message level within an already secure channel.

Some ask why we've implemented this level of security for fax. The simple answer is that we know security and implementing models like these with modern day tools (web services, SOAP, XML, .NET communications foundation, etc.) is actually not that complicated or foreign to us. Customers who use fax are used to a relatively secure medium, but are wary of Internet based solutions. We decided early on that we did not want to have security (or lack thereof) be a factor in NOT choosing an outsourced communication solution.

For more information contact Sales at 877-384-9866 or sales@etherFAX.net