

# email2 Security White Paper

---

Prerequisite reading:

- email2 Technical White Paper

The purpose of this white paper is to provide a comprehensive analysis of the security features of the email2 platform. This document is broken down into the following sub-items:

1. Increased end-to-end Transport Security & Privacy
2. Data-at-rest Security
3. Virus scan capabilities
4. Server level protection
5. Account authentication
6. Firewall Configuration
7. email2 Certification Authority (e2CAS) in a nutshell

## 1. Increased end-to-end Transport Security & Privacy

Security with the email2 platform is seamless and easy. Secure messages are all stored using AES encryption for data-at-rest on your Private Email Network (PEN) - not all over the internet on unprotected SMTP servers, like with basic e-mail (even if your e-mails are encrypted). AES is the only publicly available cipher certified for official government documents classed as 'Top Secret'. When secure messages are sent or received, they are transferred over a secure HTTPS connection (128-bit SSL, the same security used for online banking), instead of SMTP like e-mail encryption systems, ensuring that no one is able to intercept or tamper with the secure message content or attachments while they are in transit.

Exchanging messages and attachments over an HTTPS connection results in a much faster and more stable transaction. It gives each recipient the ability to reject or block messages without actually retrieving them onto their local e-mail server or computer. It eliminates current security flaws such as 'clear text' exchanges of usernames and passwords, and eliminates delivery failures typically encountered with basic or encrypted SMTP e-mail. Most e-mail security systems require a complicated exchange of public and private keys (PKI), but we take care of all the behind-the-scenes work to make the experience completely seamless for all your users. Sending secure and confidential messages is just as easy as sending a basic e-mail message. And of course, attachments are treated in exactly the same way. All of your data is completely safe and private within your Private Email Network (PEN).

The email2 platform uses at a minimum a 128-bit SSL transport encryption to ensure that all traffic to and from the Private Email Network (PEN) is secured. Instead of relying on the insecure SMTP, POP3 and IMAP4 protocols, your PEN uses encrypted HTTPS connections for all server calls and data transfers, from Outlook to Outlook without any technical changes on your part. HTTPS, (HTTP + SSL encryption), is the same secure connection technology used by online banking websites and e-

commerce trusted storefronts. We believe that SSL is currently the most effective way of transferring data securely across the internet, and the general consensus in the data security world supports this.

Three layers of protection with PKI encryption: the email2 platform uses a more robust delivery system, but still works with basic e-mail encryption. Combining the email2 platform with a PKI deployment means the following three layered security combination: through the Outlook Toolbar, messages and attachments are encrypted locally using the PKI infrastructure. Once encrypted, messages are sent through HTTPS to your PEN instead of the unreliable SMPT route. Messages are then AES encrypted a second time (effectively encrypting the PKI encrypted message) on your PEN with your corporate Master Key for at-rest storage. Messages are then requested by the recipient, decrypted from your PEN and transited through HTTPS, and finally locally decrypted using your PKI certificates.

Turn on the unique 'Super Secure' feature for even more security: ensure that no content is ever stored locally on any recipient computers, even if they are using Microsoft Outlook. Every secure message is securely re-downloaded (or re-retrieved) every time it is viewed by the recipient, and only stored locally for the time the message is being viewed. As soon as the recipient navigates away from the secure message (e.g. using Outlook by selecting a new message), the local content stored in their mail server such as MS Exchange is replaced back with the original Notification Message, which of course contains no confidential information. Recall the secure message and rest assure that no copy of it exists anywhere, unless of course a recipient printed a copy or saved the attachments locally. Note that with the 'Super Secure' feature turned on, your existing archiving e-mail systems will be archiving the Notification Messages instead of the actual content of the secure messages. If your company requires that secure messages be archived the same way basic e-mail messages are archived, simply turn off this feature.

## 2. Data-at-rest Security: e2CAS

The email2 platform use a "Master Key" provided by the PEN Admin or client owner of the PEN in order to customize the encryption process and create a PEN specific certificate with the extension .e2cas. e2CAS is the email2 Certification Authority Server that is responsible for certifying all email2 PENs, whether hosted by email2, the reseller or hosted internally on the customer's own servers. Only someone with the original e2CAS encryption certificate and or Master Key has the ability to "unlock" stored data. Because of this, it is important to store the .e2CAS certicate for your organization's Private Email Network (PEN) in a safe place, and to keep a backup. You have the option of changing your e2CAS certificate by requesting a re-certification of your PEN.

All data stored on the Private Email Network (PEN) is encrypted immediately upon arrival and is only decrypted when requested by an authorized party. This means that once a secure message is sent, it is effectively "locked" until a valid recipient requests it from the PEN server. This process is automatic, seamless and incredibly secure. In addition to keeping your data secure through its own technologies, your PEN does not interfere with your existing encryption and protection software. You can continue to use any encryption such as PKI, archiving or filtering software that you currently have in place.

### 3. Virus scan capabilities

Your PEN does not interfere with your existing virus scanners and security programs. The secure processes can be seamlessly integrated with existing third-party virus scanners. Accessing your PEN using the Web Client means that all secure messages you receive and attachments that you download will be monitored by the virus scanning programs that you currently use to monitor your browsing.

The experience with the Outlook Toolbar is even more tightly integrated. Because secure messages exist in Outlook the same as basic e-mail messages, all of your existing virus scanning, spam filtering and archiving software will continue to operate just as it did before. email2 "plays nice" with your existing virus software, and does not interfere with the processes and workflows that you've already set up.

An additional security benefit of the email2 platform with reference to virus scanning capabilities is that the Outlook Toolbar allows members to keep attachments on the PEN and download them on-demand. Basic e-mail often downloads attachments with the message, meaning that harmful files can end up on users' computers through no fault of their own. With your PEN, attachments remain encrypted on the PEN until a user specifically requests them by clicking the download link. This adds a level of security and control that is often simply unavailable when using basic e-mail.

### 4. Server level protection

The email2 platform is offered On-demand (SaaS) or 'Host it Yourself' when the entire PEN application is installed and maintained on your own servers, behind your firewall.

email2 licenses several high security, redundant server environments from award-winning international data hosting providers recognized for their security, reliability and redundancy. email2 has an exclusive lease on all the physical servers utilized preventing outside data contamination. email2 ensures that all data remains entirely portable and can be moved to a different hosting provider at a moment's notice. The following steps are taken to ensure the safety and security of your encrypted data:

- Daily incremental backups with a weekly full backup.
- Up-to-date hardware and software firewalls.
- 100% Network Uptime Guarantee.
- Full server redundancy.
- Real-world physical protection of all machines containing private data.

### 5. Member and PEN authentication

The email2 platform uses a mutual trust system in order to validate the identities of all parties that are communicating with one another. Private Email Networks (PENs) are exclusive networks, to which only approved people can belong. An organization can limit a PEN to a specific domain (e.g. @sys-national.com) or even a specific list of e-mail addresses.

The Outlook Toolbar uses a proprietary system in order to ensure that a user legitimately owns the e-mail address that he or she is attempting to send / receive secure messages with. A message notification contains a unique identification key that links it to a specific basic e-mail account. If a user does not legitimately own the basic e-mail account, the secure message will not be retrieved. The Outlook Toolbar is able to detect 'spoofed' basic e-mail accounts, preventing spammers from impersonating legitimate recipients.

When an invalid user tries to read secure messages that do not belong to him or her, the messages are never decrypted or transmitted. When an invalid user tries to fraudulently send a secure message, the recipient will be alerted and warned of the suspected identity fraud.

The Web Client can only be accessed using a previously registered password, and all data is passed and received using HTTPS connections, preventing hackers from "sniffing" the password as it is sent to the Private Email Network (PEN).

Your PEN can also function seamlessly with existing identity-based security systems, such as PGP or other PKI implementations. PENs can also employ a number of optional security extensions:

- PENs can be set to require a user's password every time a secure message is received on a new computer.
- Messages can be protected with individually mutually trusted passwords.
- Messages can be set to remote-view only (Outlook local store disabled), preventing local copies from being saved on the hard drive (used for super security requirements).

Private Email Networks (PENs) are validated using SSL certificates from the email2 Certification Authority Server (e2CAS). When a member connects to a Private Email Network (PEN), the Outlook Toolbar (or the member's web browser) queries the Certification Authority in order to ensure that the PEN is who it claims to be.

## 6. Firewall Configuration

The email2 platform does NOT require special firewall configuration. It relies on standard protocols (HTTP and HTTPS), which nearly all firewalls are configured to leave open by default. HTTP and HTTPS (HTTP+SSL) are the same technologies used by online banking websites and secure checkouts on e-commerce sites. email2 only requires port 80 and standard SSL port 443 to function properly. However, since these are the standard ports for internet usage, this is most likely already the case. Using alternative ports is an option, but there are numerous disadvantages to changing the default email2 ports. In nearly all cases, we recommend using the default HTTP and HTTPS ports. Finally, use of the email2 platform does not conflict with other services that are using port 80 and port 443.

## 7. email2 Certification Authority (e2CAS) in a nutshell

The email2 Certification Authority (e2CAS) is an entity independent of any Private Email Networks (PENs), clients, or other interested parties. The job of the email2 Certification Authority is twofold: to

provide PENs with certificates that can be used to verify identity and validity, and to digitally sign encryption methods to be used by the PEN Interchangeable Crypto Engine (ICE). The email2 Certification Authority ensures that PENs and encryption methods are legitimate and that they behave as they are reported to. Its purpose is to prevent mischievous or intentionally malicious people from taking advantage of members by hosting unsafe PENs or providing potentially harmful encryption methods. Authorized administrative users are able to submit encryption methods, which can be manually inspected for malicious code, digitally signed and then returned for use with a specific PEN. The email2 Certification Authority protects against 'phishing PENs' (bogus websites that exist only to illicitly gather user information) by issuing security certificates to PENs that investigation has determined to be legitimate and trustworthy. During the 'PEN discovery' process, members using the Outlook Toolbar are able to see whether or not a PEN holds a security certificate, and integrate this information into the decision making process of whether or not to allow communication with the PEN.

The email2 Certification Authority (e2CAS) is responsible for the validation and provision of all new Private Email Networks (PEN) deployed. As customers have a choice of hosting their PEN with email2, their qualified email2 Reseller or host it internally behind their own firewall, e2CAS is responsible for preserving the integrity of the service for all PEN members, no matter which particular PEN they use.

Since the Outlook Toolbar is multi-PEN capable, e2CAS validates the authenticity of any given PEN they get in contact with. When a PEN is provisioned for a new customer, such as a law firm or financial broker, their information is submitted to e2CAS where a validation process is initiated (payment, if needed, is also processed at this stage). During this time the PEN exists in a 'Trial mode', where only specific domains are allowed to exchange secure messages on that PEN for testing purposes. After successfully completing the validation procedure an X.509 certificate is generated for the new PEN, which is submitted automatically to the corresponding PEN Server. The validation process ensures that the company or organization requesting certification is really who they say they are, reducing possibilities for phishing tricks.

The PEN Admin receives via a secure message (for security reasons) a copy of this new e2CAS certificate. Only the PEN Admin has access to this certificate on the PEN Server, allowing a high level isolation and confidentiality of the messages and attachments of this PEN.

At an end-user level, all PEN notification messages contain an encrypted security access key (email2 signature – hidden to the user) that specifies to the PEN client (e.g. the Outlook Toolbar) where the PEN server is located, and checks with the e2CAS the validity of the PEN storing the message before the PEN Server is contacted. Upon successful validation of the PEN, the normal workflow is initiated. If this is the first time an end-user communicates with a specific PEN, the activation process is initiated displaying the Activation and Certificate Window. If a PEN is not certified, the end-user is notified at every transaction (e.g. receive, send) and can opt to either 'Establish a Secure Connection' or 'Block' the PEN, the latter forbidding all and any communications with the PEN (reduction is virus distribution and spam).