

email2 Technical White Paper

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

1. Introduction
2. Software + Service Architecture: Secure Messaging Clients
3. How do members and Private Email Networks (PENs) work together?
4. Technical Description of Features & Benefits

1. Introduction

What is email2?

email2 is a secure platform for enhancing electronic communications. It combines database messaging and permission-based document management concepts with Internet banking security protocols to give organizations the confidentiality compliance, and control they require. The protocol used by the email2 platform addresses the shortcomings of basic SMTP e-mail (encrypted or not), while remaining backward compatible with deployed infrastructure like Microsoft Outlook® and Exchange®, Blackberry® and PKI Certificates.

The email2 platform creates a Private Email Network, or PEN, for an organization. PENs are branded gated messaging communities exclusively reserved for approved, registered and authenticated members. A PEN could consist of a group as large as all the customers of a bank or as small as a Board of Directors. PENs are scalable solutions that provide absolute privacy and security, with a low-impact, seamless implementation.

In addition to security and privacy, the email2 platform extends the functionality of the whole electronic messaging system: members of a PEN can accurately track messages, send secure attachment-free video messages, control replying and forwarding permissions, manage attachments without any size restrictions, and more.

If you're looking for to get more productivity and security from your e-mail, preserve the relationships you've developed as well as comply with the latest rules and regulations, look no further. You deserve nothing less than a military-grade secure business communication solution that is built with ease of use in mind.

The email2 platform is a proven alternative to the many flavors of e-mail encryption solutions offered today. By replacing the SMTP protocol with a more up-to-date HTTP Protocol, the email2 platform offers not only offers security but a myriad of new productivity enhancements not possible before.

How does the email2 platform work?

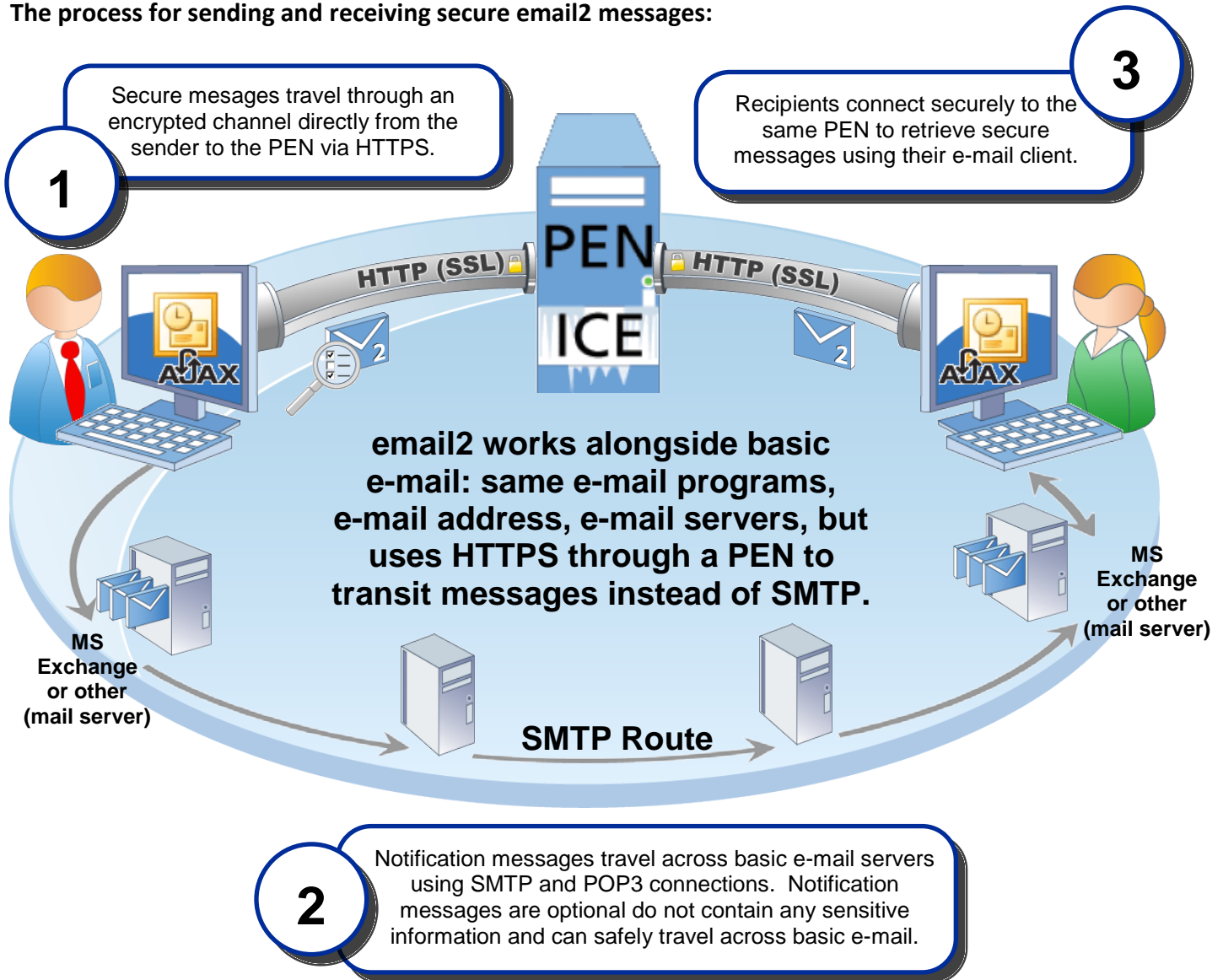
The email2 platform follows a 'Software + Service' model. Members securely connect to a Private Email Network (PEN) – either with the Outlook Toolbar, the Web Client, the Mobile Client for smart phones like Blackberry®, Palm®, iPhone® and Windows® Mobile devices or any other third party application connecting through the email2 published Application Programming Interface (API).

Connections between client applications and the Private Email Network (PEN) servers are direct and secure. Unlike basic e-mail, there are no intermediary routing SMTP servers and all connections use the HTTPS protocol (HTTP + SSL) with a minimum of 128-bit SSL encryption.

When a secure email2 message reaches the redundant PEN servers, it is server-side encrypted with our Patent Pending Interchangeable Crypto Engine (ICE) where the organization can interchange to their own cryptographic algorithm and Master Key certificate. By default, the email2 platform comes with an AES256-bit cryptographic engine. All content on the PEN server is encrypted using the unique PEN specific Master Key certificate (e2CAS certificate). Part of the PEN certification process involves that the client (your organization) enters a unique 'Master Key' that contributes to creating the PEN specific encryption certificate. Secure messages are stored encrypted for security, archiving and auditability purposes.

Once sent, the email2 platform sends a notification message to the intended recipient via basic e-mail (SMTP) (optional), but it contains no sensitive data about the content of the secure email2 message. When an intended recipient receives a notification message, he or she is able to trigger a seamless retrieval process during which the email2 message is securely transferred to the member. This architecture ensures that sensitive data is never exposed to the unsecured areas of the Internet.

The process for sending and receiving secure email2 messages:



1. On 'SEND', the Outlook Toolbar intercepts the command and re-routes the message via HTTPS securely to the PEN instead of SMTP. At this stage, only the line is encrypted, not the message itself. Once transferred securely to the PEN, the message content and attachments are server-side encrypted using a minimum of AES256-bit with your own Master Key as entered when your PEN is Certified.
2. The PEN then prepares a notification messages and send it back to Outlook using the same route, where this notification message is sent from the client's Outbox to the intended recipients via basic SMTP (optional).
3. Recipients receive the notification message alerting them of a new secure email2 message. If the recipients are already enabled using Outlook, the process is seamless: the Outlook Toolbar recognizes the notification message and sends a command to authenticate the member and decrypt the message and attachments, then transfers this content, along with the Delivery Slip metadata, using the same encrypted HTTPS route. For non-Outlook users, a convenient link is provided in the notification message to access the Secure Web Client where they can securely read and reply to all their secure email2 messages.

2. Software + Service Architecture: Secure Messaging Clients

Private Email Network (PEN Server platform)

A PEN is like a gated e-mail community available only to members that have been invited and completed the registration and authentication process. Members can belong to multiple PENs and select the most appropriate channel for a particular communication.

A Private Email Network (PEN) utilizes a secure and redundant server. Data and metadata backups are regular and handled with appropriate privacy and security. The PEN manages all secure messaging functions including message transport, encrypted database storage, archiving and tracking. When a member sends a secure email2 message, a direct and secure connection is opened between the sender's client (e.g. MS Outlook) and the PEN server. When a notification message is received, the member recipient uses the same client (e.g. MS Outlook, Web Client, or Handheld Mobile Web Client), to directly and securely connect to the PEN to retrieve the message, attachments, voice and video message, and associated metadata contained in the Delivery Slip.

Private Email Networks keep information private and secure. Information exchanged on a PEN can only be accessed by members of that same PEN with the correct credentials (e-mail address and password or more). Confidential information in secure email2 messages can only be viewed by the members that they are intended for.

Having a single, secure message repository enables your organization to enable e-mail compliance standards. In the case of a local disaster, secure email2 messages are unaffected because they are protected encrypted on a remote server: your PEN can be used as a full-featured disaster recovery tool. Members using the Outlook Toolbar can automatically download and locally store their messages (if enabled by the PEN Admin).

If using the Outlook Toolbar, secure email2 messages can be stored by Outlook into the traditional e-mail server repository (e.g. Exchange) as any other basic e-mail messages (optional, if enabled by the PEN Admin). This means that all company data is stored behind the company's firewall and any existing archiving or indexing e-mail systems will still work with secure messages. Although the email2 platform creates a second data store for all your secure email2 messages, it does not create a 'separate' data store: when sent or retrieved, all your secure email2 messages can be stored on your e-mail server as any other basic e-mail messages, ensuring your archiving and indexing infrastructure still works. If at any point a member stops using the PEN and uninstalls the Outlook Toolbar, these downloaded secure messages will behave as any other basic e-mail messages, without the added functionality of the PEN (e.g. Delivery Slip with tracking metadata, etc.). None of the company data is ever lost even if you stop using your PEN.

MS Outlook Toolbar

The Outlook Toolbar for Outlook 2003 / 2007 allows members of a PEN to manage their secure email2 messages alongside their basic e-mail messages seamlessly in the world's most widely used business e-mail client. With the Outlook Toolbar installed, a PEN member can use Outlook to seamlessly create, read and respond to secure email2 messages. Secure messages that are composed using the Outlook Toolbar can make use of all existing Outlook features, including Spell Check, Address Book, and Organizational Rules.

The Outlook Toolbar appears in the default menu and toolbars section giving users the option to quickly choose between creating a new secure or basic e-mail message. This selection can also occur mid-way while composing your message: a Delivery Option pane is added to the right side of the message compose window that allows the sender to select the proper PEN, set forwarding, replying, and message tracking permissions as well as create Voice & Video

messages on demand. For sent and received messages, the Delivery Options becomes the Delivery Slip and provides real-time message metadata such as tracking information, attachment downloads and Voice & Video message playback.

Secure Innovative cross-platform Web & Mobile Clients

The Secure Web Client is a full featured AJAX web-based mail client that gives you access to all of your secure email² messages on a single Private Email Network (PEN). It is compatible with most major web browsers, including Firefox 2+, Microsoft Internet Explorer 6.0+, Safari 4.0+ and Chrome 0.2 beta+ on Windows PC, Mac or Linux.

The Secure Web Client allows authorized members of a Private Email Network (PEN) to read, reply, forward and create messages securely. It offers additional features and information about messages in the form of the Delivery Slip, which contains message tracking information, message permissions, streaming video messages, and more. The Web Client is specific to a Private Email Network (PEN), effectively creating a branded personal, private mailbox for each of your members. Only secure messages from that Private Email Network (PEN) can be acted upon in this interface: no basic e-mail messages, no spam, and virtually virus-free. Every PEN has a separate, branded web client interface.

The Web Client performs different functions for different users:

- Many members rely on the Web Client as their only portal to their Private Email Network (PEN). They receive notifications via basic e-mail and manage their secure messages through the Web Client. These members may be using an unsupported e-mail client, or they may simply feel that the Web Client is the easiest most accessible solution.
- Members that have the Outlook Toolbar installed but want to use specific Web Client features such as the Attachment Library allowing better management of their attachments (files) online.
- Members that have the Outlook Toolbar installed but want to access their secure messages securely from a different computer that does not have the Outlook Toolbar installed or configured.

Being browser based, the Web Client requires no installation on the local machine. The Web Client can easily extend itself to accommodate any new features as they are developed: the entire platform allows for the custom design and implementation of PEN-specific “modules” through our API. These modules can be productivity tools geared to a specific industry vertical.

Members accessing the Secure Web Client from a smart phone or other web enabled mobile device (like a Blackberry or an iPhone) are automatically directed to a mobile client. Create, read and reply to your secure messages on your BlackBerry, Windows Mobile and iPhone, or any other Smartphone device. The best part is that it uses the same secure access: all connections are still made over HTTPS (128-bit SSL encryption) and none of your private data is stored on the handheld device. Your information is protected, even if you lose your mobile device.

Mobile device access can quickly be enabled or disabled from the Web Client. Disabling mobile access after a handheld device has been lost or stolen adds additional protection by preventing access to the member’s account through the Mobile Client.

Powerful PEN Admin Console

For IT administrators, having the ability to fully control and manage the Private Email Network (PEN) across the entire organization is crucial. This is especially true for large enterprises with thousands of employees in multiple office locations and strict corporate policies to enforce. The PEN Admin Console allows IT administrators to set user configuration options and security authentication levels, and whether they want to enforce secure communications for all e-mail traffic. The web-based PEN Admin Console has a dashboard, bringing important statistics quickly and clearly. With a glance, Administrators can see the total number of members, or the total amount of storage for their PEN, along with a host of other statistics that can be quite useful when analyzing PEN usage. Additionally, all actions are recorded and logged to provide a clear audit trail for reporting purposes.

IT Administrators have the ability to:

- Set the proper security settings such as 'open' or 'closed' access environments, or by invitation only
- Design Member Packages on the fly establishing settings for members throughout their entire organization
- Control membership configuration options such as storage & bandwidth limitations
- Set who can invite new Members by enabling email2's unique 'Member Sponsorship' system that allows higher ranking members to sub-manage lower level members of the PEN
- Set and manage email2's unique 'Super Secure' option that forbids any clients (e.g. Outlook) or web browsers to store any information locally (even if using MS Exchange)
- Create grouped views by dragging a category into the grouping bar and export the member list into Microsoft Excel or Microsoft Word

Application Programming Interface (API)

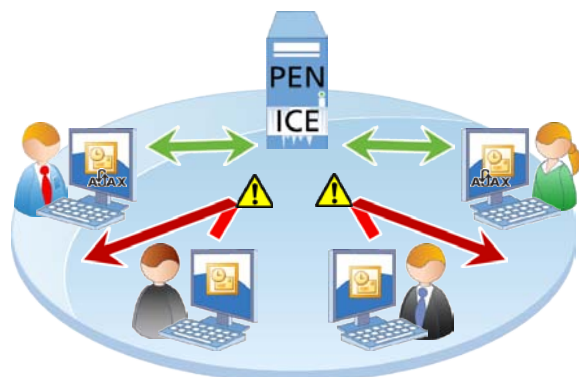
Our full featured developer API exposes commands to third party developers that wish to integrate the email2 platform with their applications, or even create standalone modules.

Build secure communication support into your web-app or just add a feature that you think is missing. We use a REST-like approach and accept custom formatted JSON requests. Integration with SAP, JD Edwards, Salesforce.com, ACCPAC are just a few examples of supported systems. For example, a Google Gadget was developed that allows a member to monitor the PEN inbox securely directly from their customized iGoogle start page. For each PEN a member belongs to, they can add a Google Gadget that checks and displays their secure messages. Clicking on a secure message link opens up the Web Client and logs the member in directly, if enabled.

Contact your Reseller to obtain a developer documentation kit that includes several Case Studies.

3. How do members and Private Email Networks (PENs) work together?

Companies or organizations that implement a branded Private Email Network (PEN) have full control over the administration and management of the network. When the PEN is created, the organization designates an administrative account (PEN Admin). The PEN Admin creates member packages, sets membership levels and invitation policies. PEN Admins can also choose to explicitly set up each new member account, can grant invitation privileges to certain members, or can make the PEN open access for all current members to invite new members. The published API can be used to automatically provision member accounts or create new secure email2 messages through another program like a web service or Active Directory (LDAP).



PEN = Members Only!

When a membership is created, an invitation message is generated and sent to the new member's current e-mail address. The invitation contains information about the PEN protocol and a secure link to complete the registration and authentication process. Registration requires verifying your name and selecting a password (Quick Authentication). The full Authentication requires each member to validate they in fact own the e-mail address to be registered by entering a validation code.

Once the membership is confirmed, the member is informed of a new secure email2 message by a notification message sent to his or her existing e-mail address via basic e-mail. Outlook Toolbar users will have the secure message automatically pulled into their inbox like any other e-mail message, but using HTTPS instead of POP3 or IMAP. Members who do not use the Toolbar will see a secure link in the notification message that will direct them to the Web Client to view and respond securely.

4. Technical Description of Features & Benefits

Increased End-to-End Transport Security & Privacy

Security with the email2 platform is seamless and easy. Secure email2 messages are all stored using at a minimum AES256bit encryption for data-at-rest storage 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'. It ensures that your data is not tampered with (edited) over time, and is automatically archived for an unlimited amount of time. Since the secure messages stay encrypted from creation to retrieval, it is impractical to change its content during the transaction (message body & attachments), ensuring tamper-proof transactions.

All connections made through the email2 platform are done via the secure HTTPS protocol instead of SMTP like e-mail encryption systems, ensuring that no one is able to intercept or tamper with the message content or attachments while they are in transit. Instead of relying on the unsecure SMTP, POP3 and IMAP4 protocols, your PEN uses encrypted HTTPS connections for all server calls and database 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 and believed to be currently the most effective way of transferring data securely across the internet. Secure email2 messages are only decrypted when a valid retrieval request has been received, at which point a copy of the secure message transferred across the same HTTPS connection to the authorized recipient(s). At no point in this model is the data ever stored or transferred in a non-secure manner.

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: attachments are broken down into 4MB files, stored encrypted on the PEN server. All of your data is completely safe and private within your Private Email Network (PEN).

Three layers of protection with PKI encryption: the email2 platform uses a more robust delivery system, but still works with PKI keys or Digital certificates. 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 SMTP route. Messages are then server-side encrypted a second time (effectively encrypting the PKI encrypted message) on your PEN with your corporate Master Key for secure at-rest storage. Secure messages are then requested by the recipient, decrypted from your PEN and transited through HTTPS, and finally locally decrypted using your PKI certificate deployment.

Turn on the unique 'Super Secure' feature of the email2 platform 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 another 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 policies require that secure messages be archived the same way basic e-mail messages are archived, use the email2 API to export all data to your local store instead, or simply turn off the Super Secure feature.

Private Email Network (PEN): a Controlled, Centralized Secure Message & Attachments Repository

Secure the line, not just the message: the email2 platform takes secure messaging to a new level, giving you ownership of a secure communication path from sender to recipient through your own, fully branded, Private Email Network (also referred to as a PEN). Every message is secure, trackable and auditable allowing you to prove who read your communication and what they did with it, AND it still works with your current message encryption system for additional security.

A Private E-mail Network (PEN) is a way for individuals or organizations to retain control of the information that they send over e-mail without adopting a whole new system of communication. Using an email2 Private E-mail Network (PEN) doesn't mean that you have to replace any technology currently in place: you keep using the same e-mail address, the same e-mail program (Outlook, Exchange) and in fact, you still need to host your e-mail domain either internally or externally as you do today. The email2 platform does not replace or interfere with any infrastructure in place: it acts as a secure message gateway by bringing a more reliable protocol to your existing e-mail infrastructure.

Most other secure e-mail solutions available work by encrypting the message being sent – for instance by using PKI (Public and Private Keys). The problem is that once those secure messages leave your mail server, they are still sent over an unsecured and unreliable SMTP network. Copies of your messages can be left on servers that neither you nor your recipient control or they can just become lost in cyberspace.

When your PEN is certified, the PEN Admin or client is asked to enter securely a unique 'Master Key' that will contribute to creating the encryption certificate (e2CAS certificate) that will be used to encrypt all messages and attachments securely on the PEN. For more information, please refer to the document 'email2 Security Whitepaper'.

Backward Compatibility: Seamless Microsoft Outlook Integration

There is no need to reconfigure your e-mail server, e-mail address or change your ISP (e.g. MX records) to start using your PEN. We designed it to be a client-side solution via a desktop client, the Outlook Toolbar, easily deployed without requiring Administrative rights. Send secure messages through your branded PEN directly within MS Outlook without requiring your e-mail server's interaction: your PEN works with all mail servers including Microsoft Exchange® and Zimbra®, without needing any integration changes or complicated configurations. And because secure messages and attachments are sent through your PEN instead of through your e-mail server, your e-mail system will no longer be bogged down with viruses and spam. All your existing investment in e-mail archiving, compliance, workflow and management remain intact and continue to work with your PEN: there is nothing to change or replace.

The email2 platform does not require any changes of e-mail address or e-mail client and can be used with all e-mail systems currently in use: It has been designed so that it will not conflict with other e-mail applications, even other security applications. If enabled, members are able to send basic e-mail messages because the email2 platform does not affect any part of basic e-mail. Alternatively, a special PEN set-up can force a specific member's computer to only send

secure email2 messages over a specified PEN. When a member sends a secure message, the confidential portion of the message bypasses the regular basic e-mail workflow and servers, instead using the secure PEN workflow. Basic e-mail messages still behave exactly as they did before and there is NOTHING to configure on the company's network, hardware or e-mail server. The email2 platform stops its integration at the client level (e.g. Outlook) and does not interfere with your existing applications, back-up systems or firewalls: it only requires port 80 and standard SSL port 443 to function properly.

email2's desktop client provides convenient ways for you to send and receive secure & critical messages and attachments through the most widely used e-mail application: Microsoft Outlook. With the Outlook Toolbar, you now have great flexibility and control when exchanging secure messages over your Private Email Network (PEN). The Outlook Toolbar provides added flexibility by conforming to the way users work within Outlook yet takes advantage of all the security and tracking capabilities of the email2 platform.

The Outlook integration is seamless: secure messages appear in Outlook alongside basic e-mail messages. They can be read, replied to, archived, or deleted, just as basic e-mail. However, they are still transferred using the security of your PEN, and you gain access to all the extra information and features provided only for secure email2 messages available through the Delivery Slip. There is no need to navigate to a separate browser, no need for complex encryption keys or cumbersome passwords. You are also able to send files of any size without limitations that are otherwise imposed by traditional e-mail or force users to use secure FTP.

There is no need to reconfigure your e-mail servers because it is a client-side solution: the Outlook Toolbar bolts on to Microsoft Outlook allowing secure messages to be managed alongside basic e-mail messages, all within an interface that is familiar to the user. Universal to all Private E-mail Networks (PENs), the Outlook Toolbar allows PEN members to create, read and organize secure messages directly from Outlook. All e-mail client features, like contact lists and spellchecker, remain intact. PEN members with the Outlook Toolbar installed receive secure messages directly into their e-mail client just like basic e-mail messages.

The Outlook Toolbar does not require Administrative rights on a computer to be installed; members can install it by themselves (in under 2 minutes). Although the email2 platform still works with e-mail encryption technologies, by default it does not require complicated encryption programs or keys, making it a seamless experience for members. No special software is required on the corporation's servers (no integration with Microsoft Exchange required: as secured messages are sent or received, they are stored, by Outlook, into the local mail store as any other basic e-mail messages). Members keep using the same e-mail address and standard firewall ports are utilized.

The Outlook Toolbar also installs the Delivery Slip in Outlook, which means that whenever a secure message is selected, you have access to more information (message metadata) and actions than you do for basic e-mail messages. The Delivery Slip contains information such as message tracking information, message permissions, streaming video messages, and more, directly in Outlook.

The Outlook Toolbar is a lightweight COM Add-in for Microsoft Outlook 2003 and 2007. Support for other e-mail clients is possible and some are currently under development. The minimum Outlook Toolbar system requirements are:

- MS Windows XP SP2 and above, or MS Windows Vista
- MS .NET Framework 2.0 and above (installed automatically)
- MS Office 2003 or 2007

- Macromedia Flash and a webcam (optional, used with video messaging)

Proactive Message Summary: unique 'Delivery Slip' (Patent Pending)

The unique Delivery Slip contains pertinent information regarding the message details, attachments, message tracking results, video messages and policies applied to the current secure message. It is a window to the secure message where the recipient can access information about the sender, the recipients, what actions have been performed on the message – message retrieved, forwarded, replied, deleted or recalled, etc.

The Delivery Slip is a collection of metadata related to a specific secure message. In the Secure Web Client, a delivery slip for any given message can be viewed by clicking on a message in the Web Client inbox. If you are using the Outlook Toolbar, the Delivery Slip is visible beside the secure message in your standard e-mail client inbox. The Delivery Slip provides pertinent data about the message at hand: you can determine whether you want to download attachments, or even the secure message itself (with auto-retrieve off). Delivery Slips provide secure identity verification, so you know that no one has "spoofed" an e-mail account and sent a forged or altered email to you. Because there is sender transparency, personal accountability ensures a reduction in spam, phishing and malicious software.

Among other benefits, the Delivery Slip allows users to:

- Find out if the PEN used is Certified Secure by the e2CAS Authority
- Find out who the secure message is from, and who it was sent to
- Review the filename, size and type of any attachments before they are downloaded locally
- Review tracking for all recipients involved, when the message was retrieved, replied to, forwarded, recalled, even printed or deleted
- Review the special policies applied to the secure message such as replying and forwarding permissions, as well as if the tracking is on or off and if it is shared with every recipient

Real time Message and Attachment Tracking

Guaranteed delivery, and allows you to confirm it. Track your secure messages on any platform -- Outlook, Web Client and mobile phones -- with absolute accuracy. When was a message opened? Who was it forwarded to? Did the recipient print it? These actions and more can be recorded automatically for any message sent on your Private Email Network (PEN).

Your PEN lets you track your delivery of your secure message just like couriers and logistics companies. It provides truly accurate message tracking because all messages are stored on a central, mutually trusted server. Because an entire conversation is stored on a single mirrored server, all requests for retrieval, replies, and forwards are tracked. Additionally, the server tracks when the message has been printed and the attachments have been downloaded. Only the centralized server structure of a PEN can provide accurate message tracking data. Secure messages are tracked both when they are received and when they are opened, providing the most accurate data possible. Additional tracking information is available for video messages and attachments. Because the PEN tracking information is so accurate, it can be used by organizations to aid in compliance with regulatory requirements, (e.g. SOX, HIPAA, and others): this means that a PEN can track all activity that's happening on it, with 100% accuracy.

Through the Delivery Slip, the tracking feature displays a list of message participants, and whether or not they have (for messages and attachments):

- Reviewed the Delivery Slip
- Retrieved the message (read)
- Replied to the message, (and to whom – available only to the sender)
- Forwarded the message, (and to whom – available only to the sender)
- Printed the message though the Web Client
- Deleted the message permanently though the Web Client
- Recalled the message

Each of these actions is recorded every time they occur with a date stamp and IP address. For example, a recipient may first retrieve your message from Outlook at work, then re-read the message from the Web Client at home, and finally forward it to another member (if enabled) on their Smartphone: each action is recorded and available to the sender for increased accountability and control over their content. This information can be shared with other participants through the Delivery Slip, or kept private. Message and attachment tracking increases accountability and effectively recreates the workflow of registered snail mail, but electronically. Administrators can even generate audit reports with tracking data for multiple messages, which will aid in compliance with difficult regulatory requirements - such as those found in Sarbanes-Oxley (SOX), HIPAA, etc.

Pre-emptive Policy Quality Control: Keyword filtering, Black & White listing

The email2 platform uses a centralized, mutually trusted Private Email Network (PEN) to ensure that policies are always upheld. Your PEN works with existing policy systems, such as Information Rights Management (IRM) and Digital Rights Management (DRM), meaning prior corporate investments are utilized. It allows the sender to control a message for its entire life cycle on the PEN. The unique PEN architecture empowers the sender to limit reply and forward permissions on the PEN, set an expiration date for a message, even recall a message at any point, even if previously read. If enabled, members have the ability to explicitly allow or disallow the forwarding and/or replying of their secure messages on their PEN. All actions taken on a message (e.g. replies and forwards) are always handled by the same Private Email Network (PEN). Because there is only one server in this model, permissions can be attached to the message and are then interpreted by the PEN.

It is important to note that this model cannot prevent the spread of information. If someone is intent on forwarding information, it can be copied and pasted into a new basic e-mail or secure message. Even if the copy and paste functionality is disabled, users can still print, take a screenshot or photograph their monitor, or verbally share the data. From a fiduciary standpoint, however, best efforts have been made to control the flow of data by using a PEN. Delivery options only restrict what can be done for a specific secure message residing on your PEN, therefore reducing liability issues.

Pre-emptive policy control allows keyword filtering of all messages and black & white listing of all recipients before the message is sent (as set by the Administrator of the PEN). Policy control takes place dynamically – on ‘SEND’ before the message is transferred to the server. This is drastically different, (and more effective), than solutions which rely on ad-hoc parsing or outgoing message filters. Black listing allows to completely block e-mail address or e-mail domains before they can even be invited or registered with the PEN, and White listing allows the PEN Admin to ensure that specific e-mail addresses or e-mail domains are always using the PEN when exchanging e-mail messages.

True message Recall

E-mail has sped up our workflows, but its irrevocable nature means that highly visible mistakes are often made. You can now fully and 'truly' recall your secure messages and all attachments, even if the message has already been opened. All attachments are automatically recalled and deleted.

Ever tried the 'wishful thinking' recall feature of MS Outlook? This message recall feature is different due to the underlying architecture of the platform: permission based database messaging means that you can recall the read permission at any point during the life cycle of the conversation, with no special conditions.

Gigabyte File Attachments

Everyone is accustomed to sending files as e-mail attachments, however e-mail content is getting big, and it will continue to get bigger. Documents, spreadsheets, presentations and most other forms of information now in use, now employ rich multimedia content. When you're dealing with large files, you know from experience that your e-mails are getting bounced, quarantined and are saturating both your and your recipient's inbox: basic e-mail was never intended for this use.

Additionally, for businesses that need to comply with all the latest rules and regulations and confidentiality standards, sending attachments through basic e-mail is largely forbidden. You can now quickly and easily send large files (tested up to 20GB / 20,000MB) that would bring a traditional e-mail system to its knees. Since all communications are made using the HTTPS protocol, (instead of SMTP/POP3/IMAP4), large files can easily be sent and downloaded at high speeds (up to 10x faster with email2's accelerator technology), from Outlook to Outlook, without requiring the user to log in to a secure FTP server or a browser based application. We eliminate all the problems people have with basic e-mail as a file transferring tool. Consider the following benefits:

- Works directly in Outlook: e-mail large attachments within Outlook without dealing with size and security limitations.
- No attachment size limits: send and receive large attachments with no problem & eliminate large e-mail storage issues from your e-mail server: you don't have to download attachments every time you download your e-mail messages (pull approach).
- No more FTP and secure FTP headaches: large attachments can be uploaded faster using more efficient protocols: eliminate FTP problems while meeting user needs and security requirements.
- Security Compliance: enforced HTTPS (128 bit SSL encryption) connections and AES server encryption keep your attachments safe during transfer and storage.
- Track attachments and view specific metadata, just like secure messages: used in CPA/Accounting, Law, Architecture, Construction, & Engineering, Military & Defense and the Healthcare industries.
- The Attachment Library tab lets you manage, re-download and re-attach files that are already stored on the PEN: when you forward an attachment, you don't need to upload it again (you are only forwarding the permissions to the attachment).
- From an IT management perspective, you are effectively reducing storage bloat on your Exchange servers and thus reducing IT costs and overhead.

Secure Attachment Library

Users no longer have to struggle with e-mail's limitations such as attachment size restrictions, inbox storage quotas, and lack of security: the Attachment Library is a new way to work with your e-mail attachments. Every time you send or receive a secure message with an attachment, that attachment is automatically added to your secure, searchable Attachment Library. It is accessible from the Web Client by clicking on the "Attachments Library" tab (can be labeled differently based on your PEN and Member Package). Resend large files without waiting for them to upload again. You can do a quick search of your attachments when you're looking for that important document. Monitor tracking data for attachments that you own, even recall or delete older attachments that are just taking up space. Use the Web client to easily find and act on all secure messages: gone are the days of sorting through countless messages in your inbox to find an attachment.

The Attachment Library provides a web-based secure and permission-based online storage for sharing files internally and externally. Files that are exchanged via your Private Email Network (PEN) from your vendors, partners, and/or clients can be stored in the Attachment Library for later access, instant 'permission' transfer without any additional upload time. For example, if you have a large file that you regularly send to different stakeholders, you can just upload it once and resend it any time you want, rather than uploading that same file each time you want to send it to different stakeholders.

Permissions-Based User Access Control: Each file is protected by an authorized access list of your external guests and internal users with different permission levels. Therefore, you have full control of who has access to your files. Deleting the file from your Attachment Library automatically delete's for the entire audience you had previously shared the file with, even if that file was forwarded by one of your original recipients.

Attachment-free Secure Video Messaging

Send voice and video messages using the integrated attachment-free video messaging– but without using attachments (web cam required). No more mucking around with codecs and third-party software. You can stream video directly onto your Private Email Network, record it securely, and have your recipients watch the video message using the same streaming, permission-based technology (for example, a message from doctor to patient pertaining to a file or issue – creating brand/doctor loyalty).

Simply press the record button in the 'Video Message' section of the Deliver Options and it will automatically start streaming the video directly to the Private Email Network's media server. When your recipient receives the video message, all he or she needs to do is click the Play button to begin watching it.

You probably already have your own ideas, but here are a few reasons why we think video messaging is great:

- Sometimes it's easier to get your point across with intonation and hand gestures. You can't do this with text e-mails - but you can with video messages.
- If you're not a very fast typer, you can send detailed messages faster than ever before.
- Face to face messages are always more effective in marketing campaigns. You can now make a personal connection with your clients and prospects.
- During new membership setup, the video message component can be utilized to welcome new members, provide "how to" assistance, and as a marketing tool such as a personal message from the company CEO discussing the Private Email Network as a component of the company's security initiatives.

The video recorder is a standard flash component that works with plug-and-play web cameras with little to no configuration. Playing and recording videos only requires the Adobe Flash plug-in, which is already present on most computers, or quick to install if it is missing. No downloads or special players required using Macromedia Streaming Server RTMPE.

Attachment Management & Virus Control: Pull VS Push paradigm

When using your PEN, messages are not 'pushed' to users. That is, users are not sent e-mail messages without their consent. The actual secure messages are sent to your Private Email Network (PEN), and the recipients must actively retrieve messages from the PEN itself. This is considered a 'pull' structure, in which users personally select which content to download to their local environments, resulting in a significant virus reduction.

Pull structures are generally considered superior, but due to the constraints imposed by the original design of basic e-mail, it is impossible for basic e-mail messaging to adopt a pull methodology. Users are subjected to spam, viruses, large (often unwanted) attachments and a number of other headaches associated with push systems. The email2 platform offers a pull structure through your PEN without invalidating basic e-mail.

PEN attachments, unlike basic e-mail attachments, are automatically added to an online 'Attachment Library', specific to each PEN member. This means members can download attachments when they want to (on-demand – permission-based). This is especially useful for dealing with large files: the large file can be left on the company PEN until needed and can be forwarded without the need to re-upload the file. This saves bandwidth, storage and time when dealing with large files. Basic e-mail attachments are pushed to users along with e-mail messages, which can cause message bottlenecks and waste bandwidth and storage by duplicating the attachment by the number of recipients, or unwanted attachments. The PEN pull VS push process for attachments also adds a degree of protection: users do not have to download suspect files that might damage their computers.

100% Spam, Virus and Phishing Control

Your Private Email Network is the "gated community" of the e-mail world. Members are approved by your organization, and can be banned from the community at the first sign of abuse. Message throttling prevents inappropriate use of the system to send large volumes of e-mail (unsolicited e-mails). Attachments can be scanned at the server level to catch viruses before they even get to a recipient's computer, limiting the possibility of viruses entering the system. Self executable viruses are not able to infect the PEN and propagate themselves because files are stored broken into parts on the PEN, resulting in an overall more secure global network.

Your PEN also eliminates unwanted 'spam' e-mail and messages: limit communication to a specific user groups. The Delivery Slip allows members to check incoming attachment for viruses before retrieving the attachment to their local computer. Allowing recipients to manually retrieve messages once the Delivery Slip has been reviewed substantially reduces the probability of getting infected by a virus. Additionally, users are guaranteed to retrieve messages from the proper sender / organization, resulting in a 'phishing' reduction.

With basic e-mail, anyone that can guess your e-mail address can contact you, with or without your consent. Once a spammer has your e-mail address, they can contact you from as many different e-mail addresses as they like, as often as they like. There have been major advances in the area of spam filtering, but large amounts of spam messages still manage to get through every day, wasting your time and hurting your productivity. Since Private Email Networks are only available to verified members, they are a tool for organizations to control the flow of spam into their network. Since sender identity is always known, there is built-in accountability and an implied trust for all messages being

received. Spam does not exist in messages sent via the PEN because spammers do not have access to this exclusive gated e-mail community.

Instead of trying to filter basic e-mail spam, the email2 platform focuses on fixing the system that lets spam happen in the first place. With your PEN, spammers lose before they even begin. Anyone that does not belong to a PEN is blocked from sending messages to a PEN's members. Private Email Networks are exclusive and controlled: PEN members that are engaging in abusive behaviors, such as spamming, can be immediately removed by the PEN Administrator. PEN Administrators decide who is and isn't a member of the PEN, which means that spammers get left out in the cold.

If your organization receives an enormous amount of basic e-mail messages on a daily basis, such as a government organization, you may want to consider simply 'ignoring' basic e-mail and focus exclusively on secure email2 messages. Using the Secure Web Client, basic e-mail messages are not present, therefore 100% spam-free.

Member Package Management

Member Identity verification is performed when a user registers with a Private Email Network (PEN) and becomes a member. E-mail address ownership is confirmed by a challenge during registration that requires an activation code (optional). Depending on how the member registers, this activation code may be provided transparently. In other cases, it will be provided in an e-mail message. If a member sends a secure message to an individual that is not using the PEN, the recipient will receive an invitation via basic e-mail to register with the specific branded PEN and then retrieve the message securely. This can be disabled by a PEN Admin for situations where the PEN is "closed" and new members must be explicitly authorized by the PEN Admin.

Every member of your PEN is automatically assigned a Member Package that dictates their level of functions within your PEN. Each member's Package can be upgraded/downgraded at a later time by the PEN Admin or assigned automatically via the email2 API. While the email2 platform does not allow deletion of members from the PEN (for auditability purposes), members that do not require access to your PEN can be set as 'Disabled' preventing them from accessing your PEN.

Member definitions:

- **'Active Members'** role can create new secure email messages (e.g. new message with attachments and personal video messages) and invite new members to the PEN.
- **'Guest Members'** role can only read/reply to a secure email2 message initiated by an Active Member.
- **'Enabled Members'** are registered members that have access to your PEN.
- **'Disabled Members'** are registered members that do not have access to your PEN, and do not count as a user for billing purposes.

Every single function of the email2 platform is driven through the Member Packages. Design your own specific Member Packages to allow your clients to only use the Secure Web Client, rename the tabs to reflect how your organization works, restrict video messaging, who can invite new members, and more.

E-mail Aliases Management

E-mail aliases are often created within an organization so that multiple version of an e-mail address can reroute all traffic to a final e-mail account. The email2 platform supports e-mail aliases and allows each member of a PEN to define as many e-mail aliases as necessary. E-mail aliases only count as a Guest email2 license and is this unique feature is included with any PEN.

E-mail Aliases can be self configured by each Member under the 'Tools' section of the Web Client, or administered by the PEN Admin on behalf of the Member. Before adding an e-mail aliases for a member, ensure that the user has access to the basic e-mail account for the e-mail address as they will need to manually confirm ownership of the e-mail account.

Enhance Visual Branding, Enable Compliance & Adopt a Green IT Policy

Every aspect of the email2 platform is entirely brandable. The Outlook Toolbar, Web Client and Mobile Client can follow your company's strict branding guidelines in order to reinforce your brand image. By extending invitations to your PEN to your client base, you are in the process extending your brand into their local computers. Invitations sent to new Members can also be customized to reflect your branding and properly explain what is expected of the new Member and why your organization is now using a secure method to communicate confidential information with them. Custom messaging at the login screen of the Web Client can be quickly inserted just the same.

The email2 platform re-creates the full business process of traditional registered snail mail, but electronically, (and therefore paperless). All attachments are stored encrypted, certified and available for later retrieval in their original condition. Every transaction is verifiable and protected from tampering, providing a defensible chain of custody for compliance and litigation. Distributing information to large groups such as employee statements of client invoices and statements incur a significant reduction of fuel consumption and paper reduction over paper-based mail delivery.

Enhance your corporate Green Image through reduction in fuel consumption (used by couriers) and paper consumption. This allows your organization to qualify for an Energy Star rating from the EPA or carbon credits.