Paperclip

White Paper

eM4

Compliant Email Service

Contents

Overview 3

Adoption 2019 3

Why eM⁴? 4

The Compliance Landscape 5

Paperclip's Solution Approach 7

Simple Encryption Rules 8

On Premise (eM⁴ Relay Server) 9

SaaS 11

eM⁴ Cloud Client 12

The eM⁴ B2C (Business to Consumer) 14

Service Administration 16

Service Auditing 17

Proof of Delivery 18

Proof of Readability 19

Proof of Agreement 20

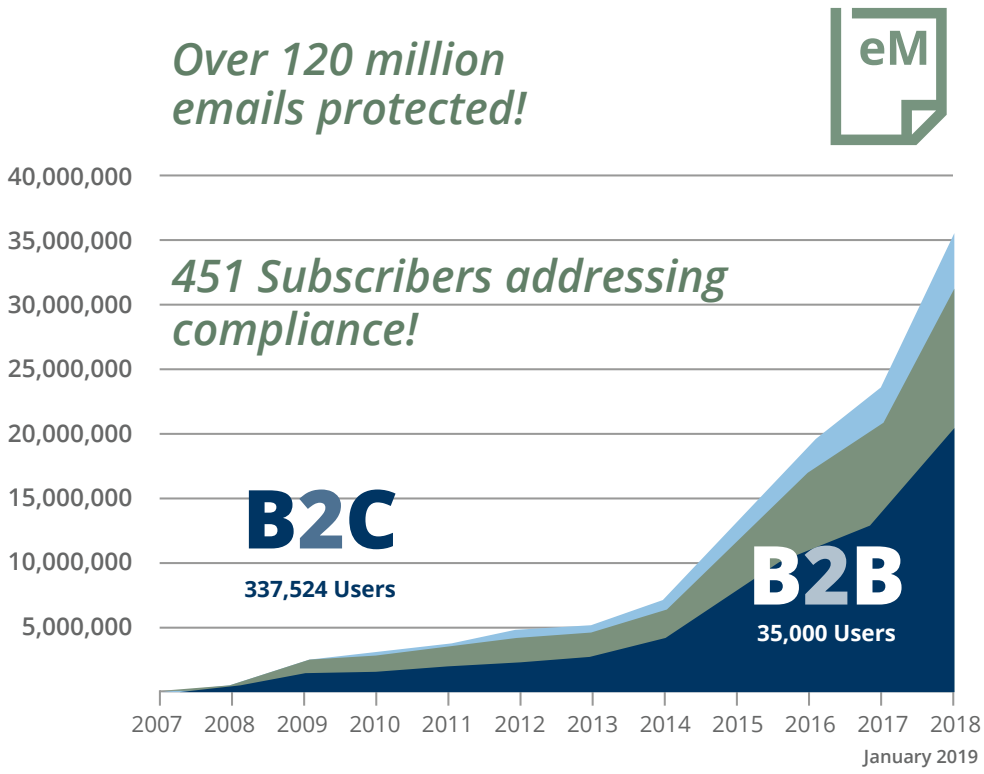
B2C Recall 22

Conclusion 22

The FTC Safeguard Rules require Financial, Insurance, Medical and Education professionals to protect their customer's private information or Non Public Information (NPI). Updated regulations like HIPAA 2013 and Consumer Financial Protection Bureau (CFPB) rules along with other Federal and State laws makes it very clear that all electronic communications among third parties must be safeguarded. This requires special handling of electronic information specific to Email on the public Internet. Email messages must be encrypted before releasing them on the Internet. Many organizations have deployed solutions securing their internal domain traffic but either send in clear text to their trading partners or share their proprietary interface. Trading partners cannot effectively use Email and meet compliance. Paperclip proposes a compliant Email service that can address interoperability, compliance, ease of use and necessary auditing.

Adoption 2019

Since 2007, eM⁴ Compliant Email Service has been widely adopted and proves that the industry advisors who designed the service got it right. We're excited about the future of eM⁴ and its evolution into a dynamic capture tool that meets the needs of efficiency while maintaining compliance. New services like eM⁴ Proof of Agreement, eM⁴ᶜ Cloud and eM⁴ˣᵒ CrossOver will continue eM⁴ Compliant Email as a leading solution solving today's challenges.

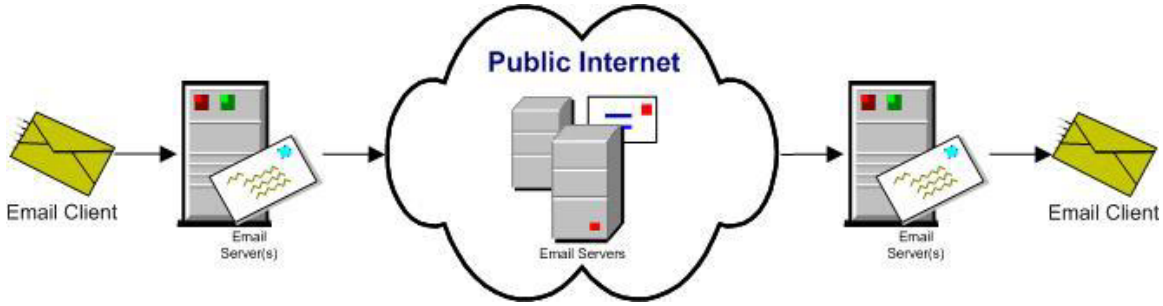


Since 2007, eM⁴ Compliant Email Service was intended to be more than just an encryption service. Paperclip recognized the utility of email as a communications tool capable of more value added to the business environment. Paperclip offers two enhancements. First: eM⁴ can be deployed as a cloud client, no software required to install. Second: eM⁴ Proof of Agreement (POA), and Electronic Signature (E- Sign) experience with no setup required, wallet authentication, click and sign and third-party archiving. POA supports many file types to include Microsoft Office, video, audio and many image types (i.e. PDF, TIF, PNG, JPEG, etc.).

To the end goal of Paperclip's Vision of "Authorized Data", POA is a great step forward. Users can replace attachments requiring wet signatures with POA which can be as simple as the email itself. Just put the content in the body of the email for E-Signing and upon return, store the email within your Paperclip VCF system or your choice of email repository/EDMS.

- No Login or Passwords Required
- B2B and B2C Functionality
- Simple Email Encryption Rules
- Three Deployment Options
- B2C Mailbox Portal Options
- B2C Large Attachment Support
- B2C Email Recall
- Proof of Delivery
- Proof of Readability
- Proof of Agreement / E-Signing
- Disinterested Third Party Audit (D3P)
- Annual Subscription - No tick charges
- B2B Cloud Client Store
- eM⁴ Actions, Outlook Add-In

The Internet has dramatically changed the way we conduct business today. The ability to deliver information, answer questions, and exchange ideas has benefited all who participate. One significant use of the Internet is electronic mail. The ability to replace a letter, fax or phone call with a simple electronic message has won the day. Storing and quickly retrieving these messages allows organizations to streamline communications processes. By today's business standards, Email has become a cornerstone of every business' operations.



In recent years, the United States Federal Government has passed new initiatives targeted at the way personal information must be handled on the public Internet. The major acts are Financial Services Modernization Act (GLB), Identity Theft Prevention Act of 2000, Health Insurance Portability and Accountability Act of 1996 (HIPAA 2013) and the Consumer Financial Protection Bureau (CFPB). These acts focus on different aspects of personal information, but all have the same mandate: protecting customer's personal information from unwarranted access and the accountability for its use. Some of the strongest rules concern maintaining a six year audit of those who had access to the protected information. Further, technology providers hosting third party NPI (HIPAA 2013) are liable to these same agencies and subject to penalties and fines.

eM^4 is annually audited by a third party for SOC2 Type 2 and HIPAA compliance and reports are available upon request. Paperclip has adopted the Cloud Security Alliance (CSA) security community as a corporate sponsor.

Non Public Information (NPI) is defined as personal information, which by itself or with other information could allow access to private assets or health information. Items listed below are a representation of NPI:

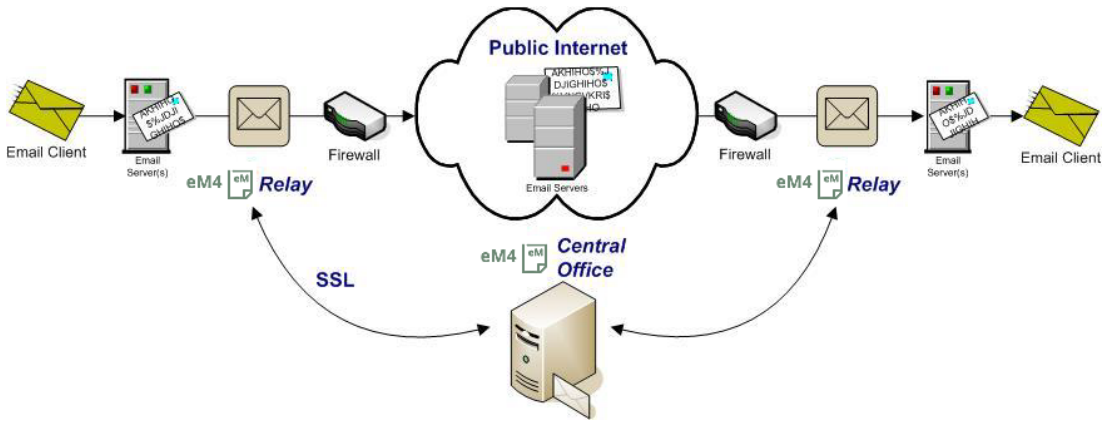
1. Social Security Number (9 digits)
2. Address
3. Demographic Information
4. Phone Number
5. Age
6. Date of Birth
7. Race
8. Sex /gender
9. Religion
10. Mother's maiden name
11. Driver's License Number
12. Passport Number (9 digits)
13. State identification card number
14. Personal identification numbers
15. Information commonly provided on an application for an insurance product or service.
16. Logon IDs and Account passwords
17. Digitized or other electronic signatures
18. Employer assigned employment identification number – AESC assigned ID (9 digits)
19. Unique electronic identification number or routing code
20. Government issued identification number
21. Bank Account Number
22. Debit Card Number (16 digits)
23. Credit Card Number (15-16 digits)
24. Payment History
25. Account Balance
26. Fund (investments) value/balance
27. Factors around customer's income or assets
28. Fact that person is a customer of a financial institution
29. Fact that the customer is or has obtained insurance policy Financial account number or credit card or debit card number
30. Information obtained when requesting or getting, collecting, or servicing a loan
31. Information from a consumer or credit report
32. Height or Weight
33. Other medical specifics such as blood type
34. Medical Conditions, Medical Diagnosis, Medical Test Results, Medications Used
35. Past, present, or future physical, mental, or behavioral health
36. Health care being provided
37. Health-related policy premiums
38. Health policy numbers
39. Biometric data, such as fingerprints, retina, iris images or DNA profile

Paperclip believes any chance to overcome the current market solution shortcomings and gain wide adoption is to change the paradigm. Twenty years ago, Paperclip's Internet eXpress was a new paradigm and its success today is measured with 500 plus customers (1,300+ nodes) exchanged over 70 million documents in 2018. Paperclip's approach is to climb outside of the box and integrate un-structured email to structured Internet eXpress (Project Crossover).

Starting with some simple user requirements, a proven encryption algorithm, a vendor service track record with our eye on the target, a new paradigm is created – eM^4 (called Email for – pronounced M4).

The new eM^4 approach resolves the many problems created in a diverse compliant industry:

- ✔ Encrypts Emails and their attachments, firewall to firewall
- ✔ Disinterested third party recording of Email transactions for auditing access
- ✔ Email infrastructure independent, multiple deployment options
- ✔ Ease of use accomplished - Subscriber's users don't have to learn something new
- ✔ Commodity pricing, affordable by organizations of any size



Emails do not pass through the Paperclip Central Office. The Central Office serves only to manage encryption keys, subscribers and collect auditing information.

The eM⁴Service has two deployment options, encryption enabled or disabled. These two options adhere to specific rules regarding how to encrypt Emails.

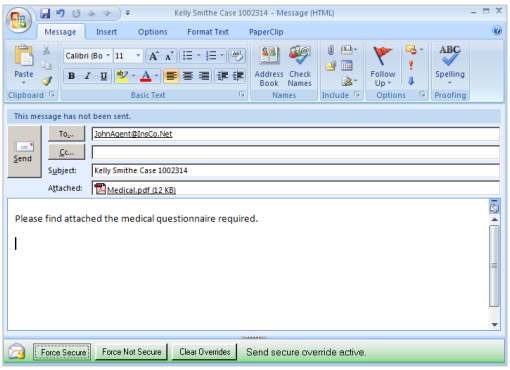
Encryption Enabled follows six rules as described below:

1. If an Email recipient's address domain is an eM⁴Subscriber.
2. If one or more Email recipients' address domains are eM⁴Subscribers, Email is encrypted to all recipients (Subscribers & Non Subscribers)
3. If the wild card Email address (flag@em4relay.smtp) appears as a recipient.
4. Microsoft Outlook Add-In Secure choice displaying a green ribbon.
5. If the wild card Email address (pass@em4relay.smtp) appears as a recipient, the Email will not be encrypted but audited as an exception.
6. Microsoft Outlook Add-In Force Not Secure choice displaying a red ribbon.

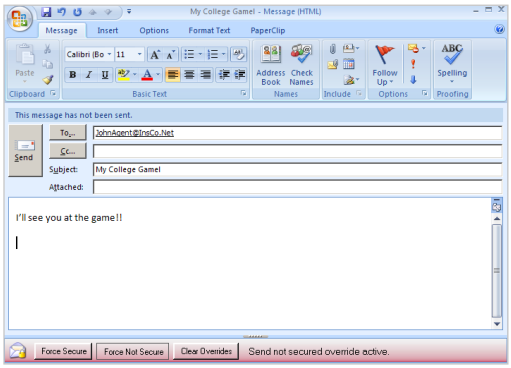
Encryption Disabled follows two rules described below:

1. If the wild card Email address (flag@em4relay.smtp) appears as a recipient then encrypt the Email to all recipients.
2. Microsoft Outlook Add-In Force Secure choice displaying a green ribbon.

Force Secure



Force Not Secure



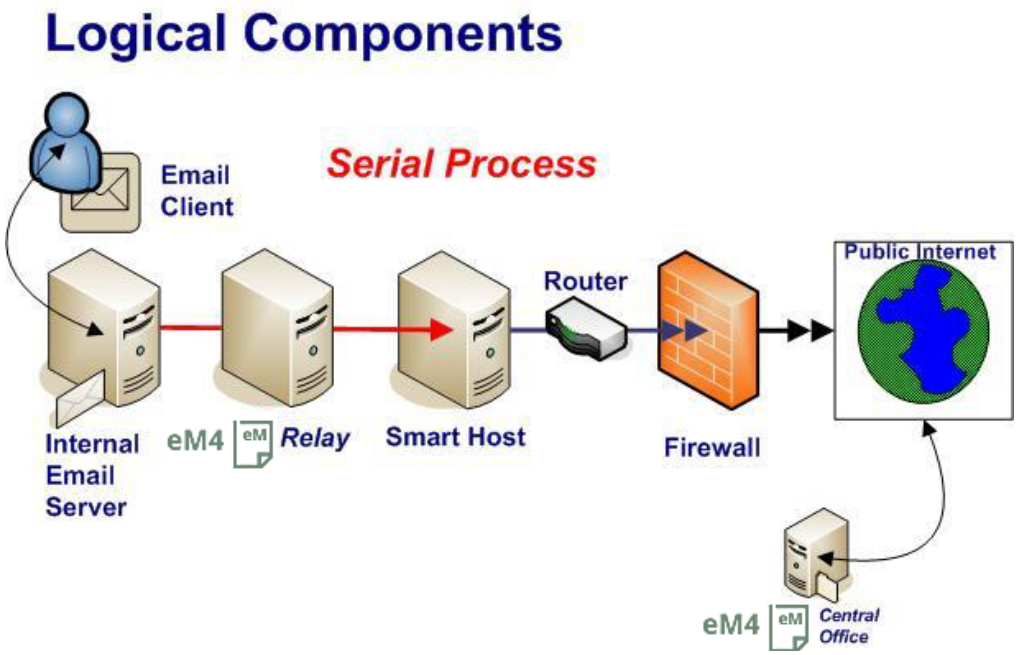
Note:

The Email addresses "flag@em4relay.smtp" and "pass@em4relay.smtp" can be supported with friendly names such as Secure and Not Secure supporting Email type ahead feature.

The receiver of a decrypted eM⁴Service Email will see appended to the bottom of the original Email a tag line – "Content protected by Paperclip eM⁴ Compliant Email System".

The eM⁴ Relay Server has two basic On-Premise configurations: Serial and Parallel. Serial configuration is the simplest configuration, requiring all Emails to pass through. In Parallel mode, eM⁴ Relay becomes a subsystem to your Email server. The host's Email rules decide what Emails are directed to the eM⁴ Relay for encrypting. Multiple eM⁴ Relays can be deployed to handle the largest traffic demands.

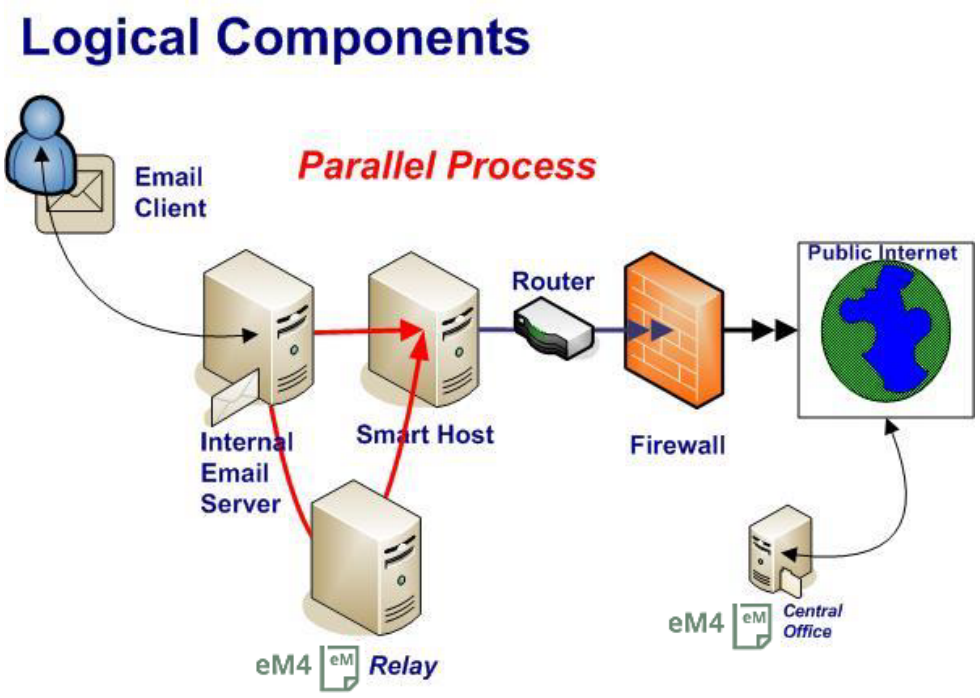
eM⁴ Relay installed as a "**Serial"** process maintains locally a list of compliant receivers' domains and Desktop subscribers maintained by the eM⁴ Central Office.



In **Serial** operations the Sending Email server delivers the Email to the eM⁴ Relay. eM⁴ Relay applies the Serial Rules and encrypts or not. eM⁴ Relay then delivers the Email to the Smart Host for delivery across the Internet directly to the receiving Email Server. Receiving Emails start at the Smart Host and are forwarded to eM⁴ Relay(s) for decrypting as necessary. eM⁴ Relay then releases the Email to the internal Email Server.

eM⁴ Relay deployed as a **"Parallel"** process to your Email Server allows your Email Server's rules engine to decide what Emails get encrypted going out. This method provides a centralized administration for more complex rules management leveraging existing resources. In this mode of operation, eM⁴ Relay adheres to the following rule:

1. All outgoing Email is encrypted.



In **Parallel** operations, the Sending Email Server decides what Emails are delivered to the eM⁴ Relay. eM⁴ Relay applies the Parallel Rules and encrypts all Emails. eM⁴ Relay then delivers the Email to the Smart Host for delivery across the Internet. Receiving Emails start at the Smart Host and are forwarded to the Internal Email Server. Internal Email Server rules identify it as an eM⁴ Relay encrypted Email and forward it on to the eM⁴Relay(s) for decrypting. eM⁴ Relay(s) then releases the Email back to the Internal Email Server

eM⁴ in the Cloud

The Cloud can take on different forms depending on the services engaged. One approach is to "forklift" your key servers including the eM⁴ Relay and co-locate them with a data center provider. Another approach is to replace your servers with data center provided applications or services. Paperclip's Cloud solution addresses both models.

- **Comcast**
- **Verzion**
- **Optimum**
- **Time Warner Cable**
- **Cox Communications**
- **AT&T**

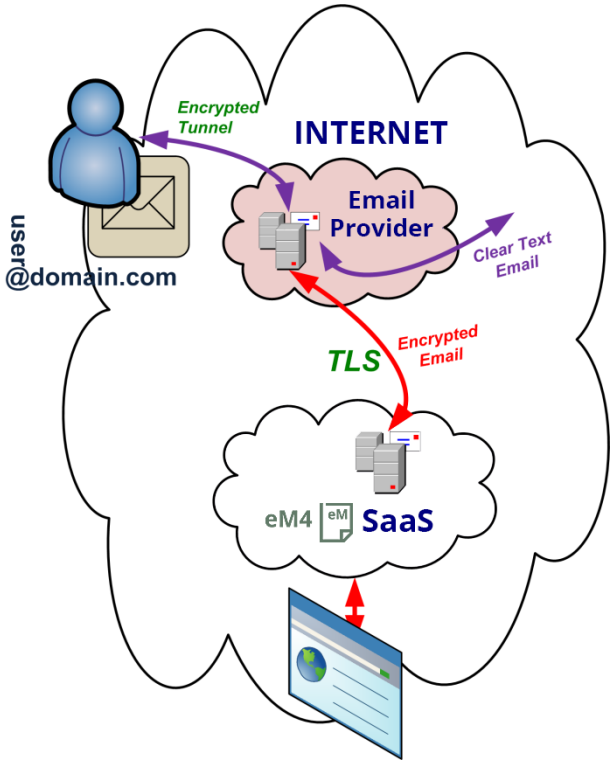
SaaS

3rd Party Private Cloud Services

Private Cloud Services are Email providers that host your email server dedicated to your organization. Many will also host the eM⁴ Relay Server but, for those who will not, Paperclip has Software as a Service (SaaS) eM⁴ˢ Relay Service. This service offers eM⁴ access where the private email provider connects to the SaaS eM⁴ˢ Relay Server via TLS. In this model, filtered emails can be directed to the eM⁴ˢ Relay Server.

Whether you're with a Private Hosting company or services such as Google Apps or Microsoft 365, the SaaS model seamlessly integrates.

The eM⁴ˢ Service is available as a Full Subscription. This provides access to all Auditing features and Non Subscriber support.

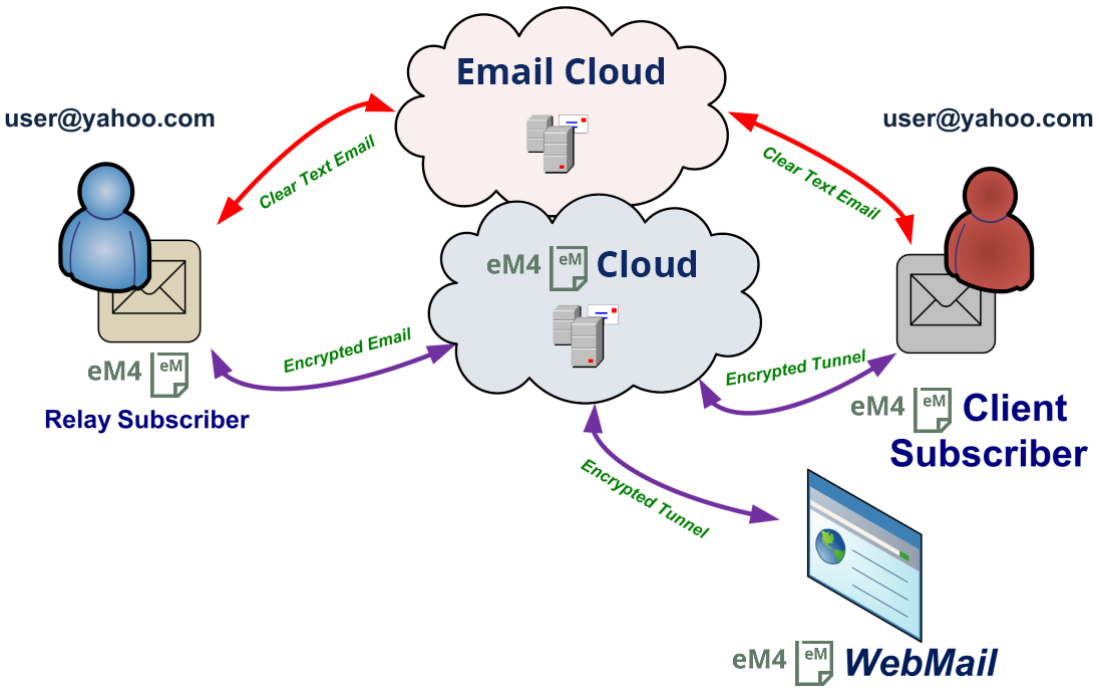


3rd Party Shared Cloud Service Providers

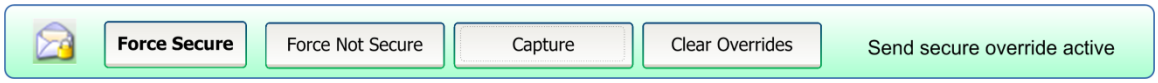
Email Cloud vendors today are considered closed systems and do not entertain integration with other third-party services. Some can provide webmail encryption services where all secured email require access via a browser with login and password. This "one too many" model and associated user experience has not been well accepted. Remember, eM⁴ was designed by your peers who wanted most of all, one mail client and no passwords.

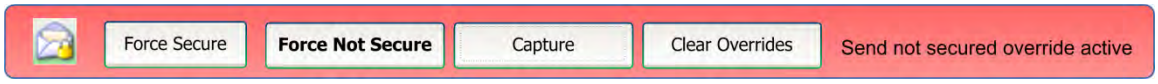
eM⁴ solution for this Cloud environment leverages the eM⁴ Cloud solution. The User uses the same Email Client used for the third-party Cloud provider and the User's proper Email address is maintained so no new addressing is required.

The user's Email address (user@yahoo.com) is leveraged by the eM⁴ Cloud. The new eM⁴ᶜ (Cloud) solution is designed to integrate with the user's Email Client as an eM⁴ Email Secure Account. This Account provides for secure tunnel transmission with the eM⁴ᶜ Servers where Email encryption and decryption are performed. In support of the Email Client Account configuration, Paperclip provides an install for Microsoft Outlook for easy setup. Email Client Accounts can be setup manually with configuration information found in the User's eM⁴ WebMail Mailbox. In addition, the User has access to their eM⁴ᶜ Mailbox where they can access eM⁴ sent and received Emails.



When the User wants to send an encrypted Email to an eM⁴ Subscriber or Non Subscriber, they simply select the eM⁴ᶜ Cloud Account as the sending account. Microsoft Outlook users have the option to install the Outlook Add-In for a simple visual selecting to send encrypted or not. If compliance requires all Emails to go secure, simply select the eM⁴ᶜ Cloud Account as your default Email account.





eM⁴ Emails sent to the user will arrive at the eM⁴ᶜ Cloud Servers, be decrypted, audited and securely delivered to the user's Email Client as clear text mail in their Inbox. Users requiring eM⁴ Emails to rest on their third party Cloud Servers can simply configure their Email Rules to forward eM⁴ Email to the same.

Service	*Relay*	*SaaS*	*Cloud*	*WebMail*
eM4 Subscriber	Serial Parallel ✓	✓	✓	
Non Subscriber				✓

B2C "Subscriber to Non-Subscribers"

- ✔ **No Logins**
- ✔ **No Passwords**
- ✔ **Decrypt Incoming Emails**
- ✔ **Reply To: Supported**
- ✔ **Revocation**
- ✔ **Audited**

The eM⁴Service can manage Non-Subscribers (NonSubs) via Paperclip's eM⁴ Webmail hosted by Paperclip. Subscribers have the option to deploy eM⁴ Webmail requiring receiver authentication.

Recipient Validation (RV) is the preferred method of authentication by Subscribers ensuring the person accessing the email is the correct person and still not require logins or passwords. RV method is designed to stop the notice from being hijacked and illegally used to view emails on the Paperclip Webmail servers. With no authentication required, the receiver can select the link and view the Email in a secure browser.

Users will receive their normal notice with a link to click on. This link will present a Captcha Code entry screen requiring the user to enter the Captcha Code. The page will refresh indicating a new email will arrive immediately with the link to open the email. Two principals are used to grant access to the Webmail, same location and same device. All validation data is recorded to the D3P audit. When Registration and Recipient Validation are used together, Two Factor authentication is achieved.

Choosing authentication will require receivers to create and maintain credentials. Non-Subscribers have the ability when registering to setup their eM⁴ Webmail account. Non-Subscribers will receive an Email with the appropriate link directing them back to the eM⁴ Service Webmail host.

Non-Subscribers will then have to login with their Email address or alias and authenticate with their password they registered with. The hosted eM⁴ Webmail Email will secure the Internet "pipe or tunnel" via SSL. Non-Subscribers will have the ability to save the Email and, if desired, "Reply to" the sender securely. Non-Subscriber Emails will remain within the hosted environment for thirty days after receipt then they will be purged.

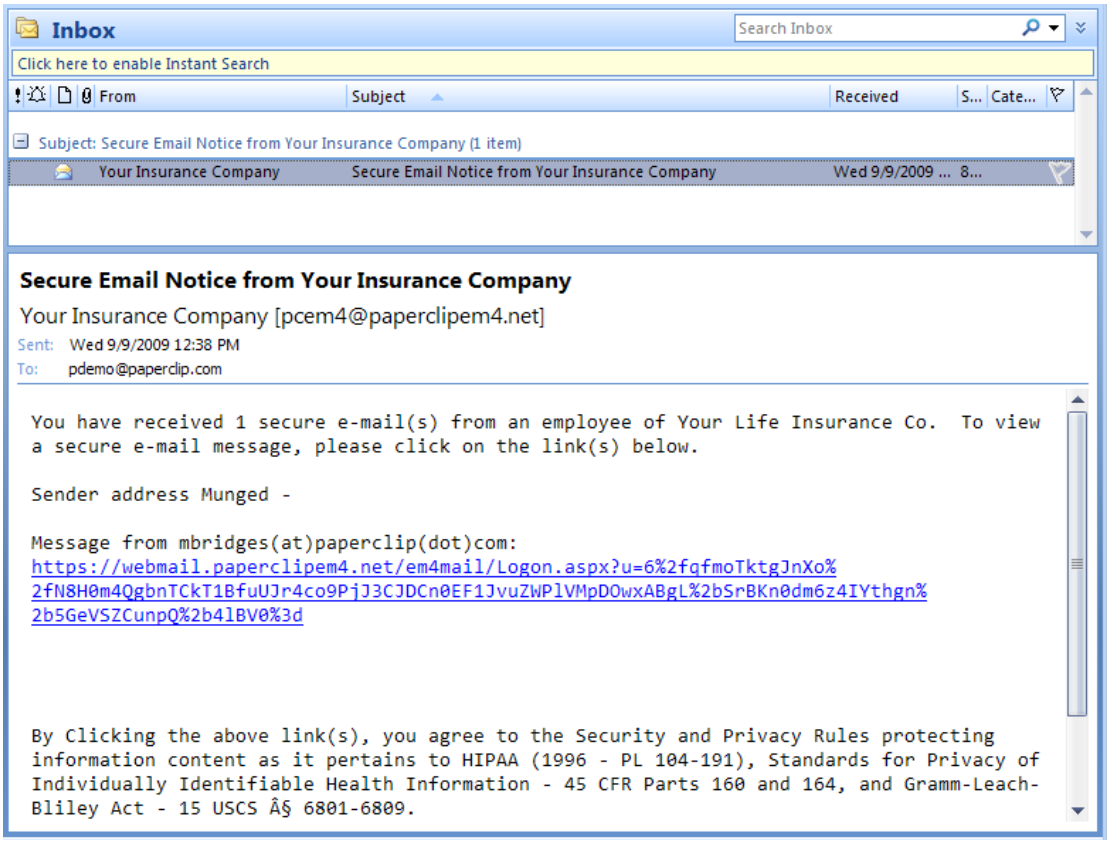
Non-Subscribers do not have access to eM⁴ Service portal. Non-Subscribers will be able to manage their own eM⁴ Webmail accounts as necessary (i.e., change password). Non-Subscribers have the option to freely initiate encrypted Emails to the sponsoring Subscriber at any time. There is no registration requirement and Non-Subscribers can have more than one sponsor.

Subscribers can control the content of the Email body with relevant compliance notices. In addition, they can brand their browser presentation with a custom banner or logo.

TLS

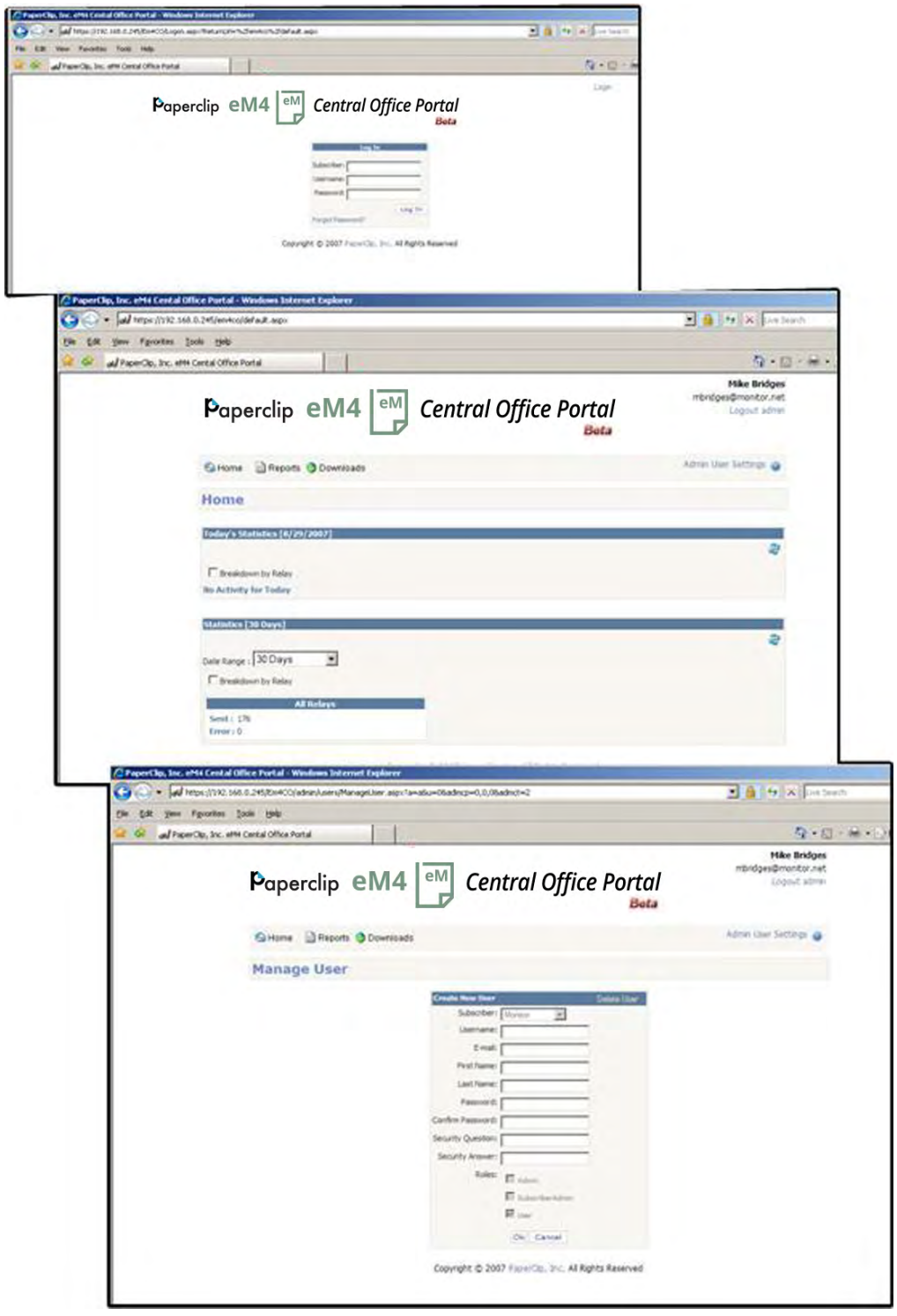
Transport Layer Security is an encryption method whereby the connection between the mail servers is encrypted, otherwise known as a secure tunnel. Paperclip utilizes Opportunistic TLS when delivering Webmail Notices to Non- Subscribers. This method will secure the tunnel to the receiving mail server and the notice is secure from outside criminal activities. Receiving mail servers not configured to support TLS will force a connection downgrade to unsecure. Most email cloud providers (Microsoft, Google, Yahoo, etc.) enable TLS on their servers; therefore, notices sent to these providers travel through an encrypted tunnel.

eM⁴ Clear Text Email Notice



eM⁴ Clear Text Email Notice

Subscriber administrators have access to the eM⁴Service portal via a browser. The portal provides user functions for analyzing Subscriber's metadata (Auditing), sender and Email revocation and reporting.



eM⁴ Auditing captures and maintains information regarding Email transactions and administration. Auditing starts with the data collected every time a request is made to encrypt or decrypt. Sender's eM⁴ Relay connects (SSL) to the eM⁴ Central Office (eM⁴ CO) and updates the eM⁴ CO in an asynchronous manner. The initial Sender's request message file includes:

- **eM⁴ Client Metrics**
- **eM⁴ Transaction ID**
- **3DES Session Key**
- **Sender Email address**
- **Receiver(s) Email address**
- **Request Date/Time Stamps**
- **Subject Line**
- **Attachment Names**

Receiver's eM⁴ Relay connects to the eM⁴ CO (SSL) and completes the data record, closing the transaction. eM⁴ Relay connects to the eM⁴ CO in an asynchronous manner to update. This update passes the following metadata recorded by the eM⁴ CO:

- **eM⁴ Client Metrics**
- **eM⁴ Transaction ID**
- **Sender Email address**
- **Receiver Email address**
- **Request Date/Time Stamps**

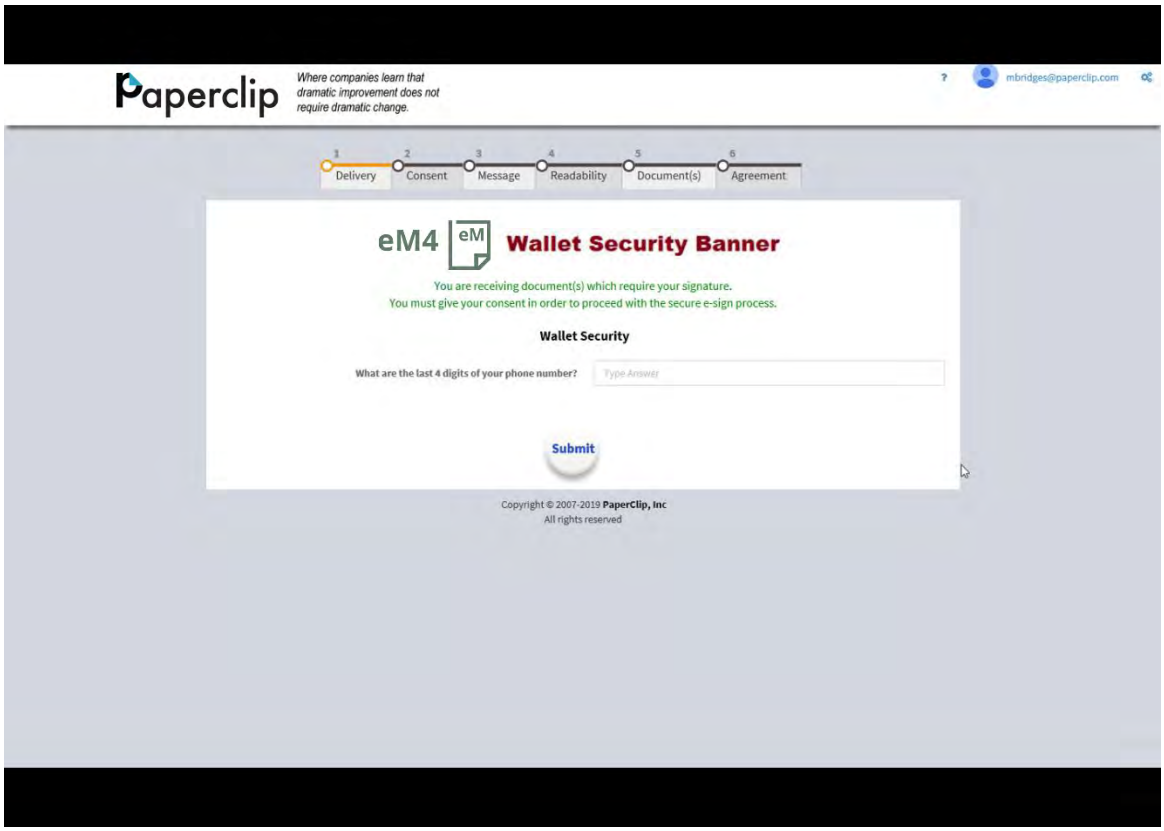
Non-Subscriber's eM⁴ Add-In or eM⁴ Webmail connects to the eM⁴ CO (SSL) and updates the transaction data in an asynchronous manner. This update passes the following metadata recorded by the eM⁴ CO:

- **eM⁴ Add-In Metrics**
- **eM⁴ Transaction ID**
- **Sender Email address**
- **Receiver Email address**
- **Request Date/Time Stamps**

Auditing allows for the isolation of an eM⁴ transaction and all associated events. Filter on Email senders or receivers drilling deeper with date and time ranges as needed. Auditing reports or data can be exported to Subscribers for continued reconciliation.

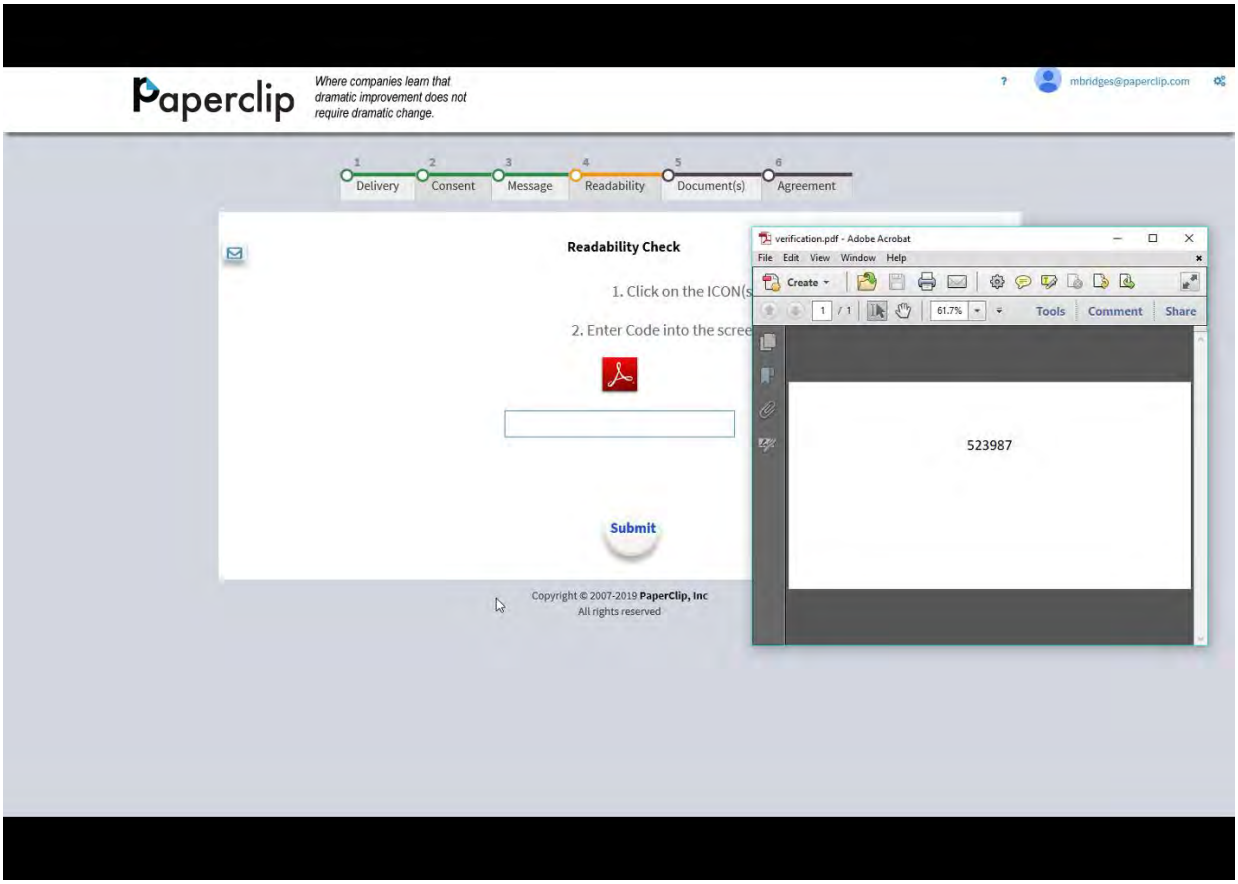
Proof of Delivery provides the means where document providers can send a secure email with attachments to a receiver where compliance requires a confirmation that the person did receive the mail and documents (e.g., Voice Signature, Disclosures, etc.).

Receiver clicks on the link provided and authenticate by answering a combination of simple questions of shared personal information (last four of SSN, Birth Date, etc.).



Outlook Add-In provides the ability for Ad-Hoc questions and answers. Create a question using the Add-In and re-use it from a drop-down list, then provide the answer(s) to the questions and submit. Receiver, when receiving the mail, will be asked to answer the questions and upon success, the mail and attachments are presented.

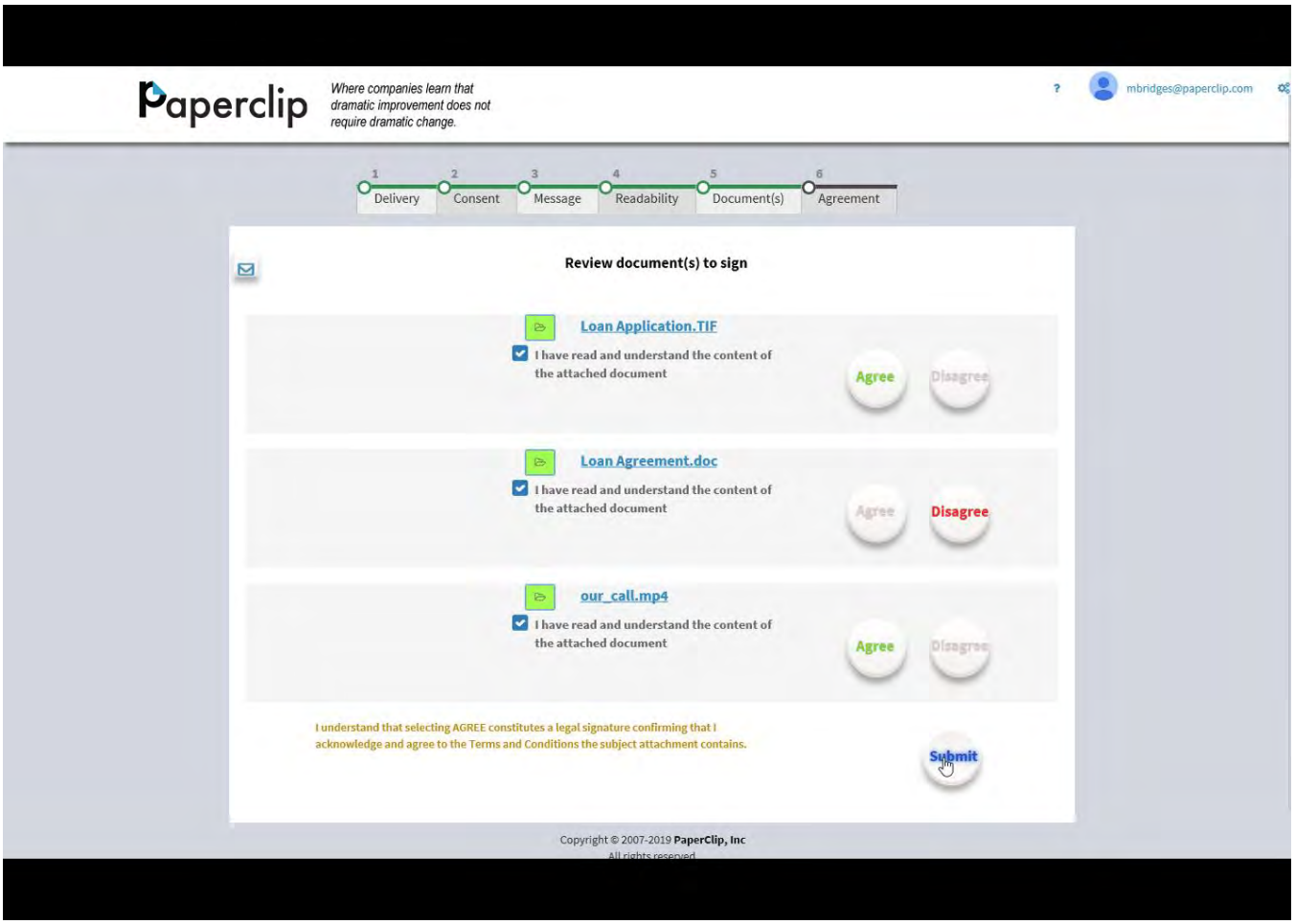
Proof of Readability ensures that the attachment sent to the receiver can be opened and read. A PDF attachment would open a PDF file containing a number. The user is required to type that number into the screen. If they match, the event, POR is recorded in the auditing portal and the process moves to the next event.



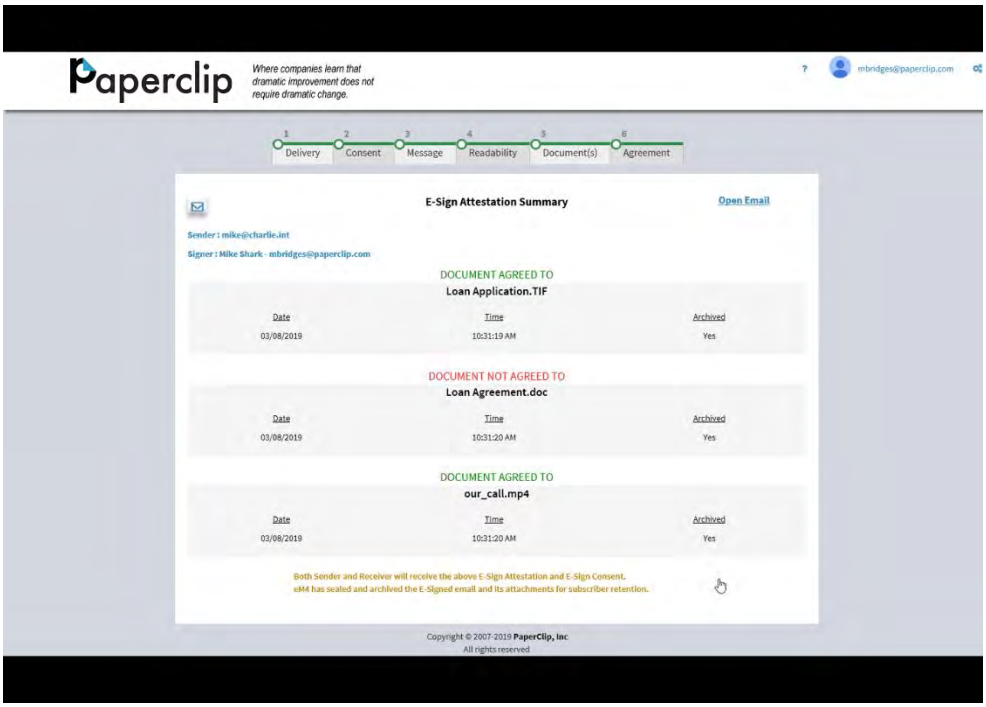
POR supports the following file formats:

PDF	TIFF	BMP	GIF	JPG	PNG
DOC	DOCX	XLS	XLSX	PPT	PPTX
AVI	MP3	MP4	WAV	WMV	WMF

Proof of Agreement (POA) is the E-Signing event that is equivalent to a handwritten signature. Paperclip implemented a simple “Click & Sign” mechanism to avoid the pitfalls of other schemes that require signing document setup and preparations, installing client-side software or browser requirements/ limitations. The Case Law today judges the process, not the type of signature (i.e., Ink, facsimile or location). The measure is, “did the signer know this is an electronic signing event” executing a contract or authorizing an approval.



At the end of the E-Signing process the Attestation Document is created confirming required information representing the signing event. The email and attestation are returned to the participants (Sender, Receivers, Carbon Copy) for filing as their original copy.



The email, attachments and attestation attachment are then encrypted (AES 256) Hashed (SHA-2) and archived by Paperclip for three years as the D3P. At the end of three years, with 30 days' notice, Paperclip will purge the same.

eM⁴ RECALL and RECALL ALL will delete the email from the receiver's mailbox. When the receiver clicks on the Notice Email the return browser will explain the email was Recalled by the sender, no further action required. To recall an email, sender can send the same mail subject line and append to the end "em⁴-recall". A second option of Recall All will delete all emails in the receiver's mailbox from you (em⁴-Recallall). Sender will receive a confirmation of recall and if the email was opened or not before the recall was executed.

Conclusion

The need to encrypt Emails and their attachments across the public Internet protecting NPI is an undisputed requirement. Current deployed market solutions suffer from industry interoperability, deviate and burden trading partners' workflow and require many IT resources not available to all. It's time to climb out of the box.

Paperclip's new paradigm meets compliance, is easy to use and adds the opportunity to reduce paper as original documents signed and agreed to by all parties.

This new paradigm or eM⁴ Service can scale from one to thousands of users. It makes industry compliance affordable and uniform. It's simple.