



Secure E-Signature

Secure e-signature is the first truly secure way to easily and quickly sign and exchange digitally approved documents without relying on complex deployments.





Secure E-Signature

Electronic-signature functionality is rapidly becoming an essential aspect of any digital enterprise. Moreover, users increasingly expect the process to be fast, simple, and secure. While many products offer fast and simple e-signature capabilities and others offer full security, only Secure Messaging provides all three without the added cost and burden of additional security software. And because it is built right into Secure Messaging, there's no extra cost and nothing to implement. You can simply start using it. It's that easy—and that secure.



Background

The advent of electronic signatures has significantly sped up the process of getting required signatures on documents and dramatically reduced much of the cost since documents can now simply be signed and exchanged digitally. In most e-signature products available today, the required signatory just electronically signs the document using whichever means specific to that product and delivers the file back, often via email.

Secure Messaging's e-signature feature offers the best available combination of speed, simplicity, and security.

The problem with this basic exchange is protecting the security of the files. While numerous tools and solutions for effectively creating e-signatures have been developed, because of legislation now in place in many countries, enterprises and organizations require a solution that not only makes it fast and easy to electronically sign files, but that can also guarantee the security of the information during transmission between the parties involved (without reverting to sealed envelopes and couriers).

The secure e-signature feature in Secure Messaging does just that. It is the first truly secure way to easily and quickly sign and exchange digitally approved documents without the need for an added layer of encryption security software or hardware.

What is an e-signature?

An e-signature replaces an actual, physical hand-written signature to indicate that a person adopts the intentions recorded in the document being signed. Usually this is done using letters, characters, numbers, or other symbols in digital form incorporated in, attached to, or associated with an electronic document.



Secure E-Signature



Problem Solved

Given the massive benefits of developing a legitimately viable “click to acknowledge” marketplace, many countries have passed various laws to encourage the adoption of e-signatures as valid. The E-SIGN Act in the U.S., for example, is meant to “facilitate and promote commerce and governmental transactions by validating and authorizing the use of electronic records and electronic signatures.” In most cases, the laws stipulate that any electronically signed document must be securely protected throughout the exchange.

Until now, no one has been able to offer true stand-alone secure file-exchange capability to protect the signed documents without adding additional steps or software or hardware. You either had to compromise on security in favor of ease-of-use and lower implementation costs, or shell out for the added cost and weight of full encryption capability.

With Secure Messaging’s e-signature feature, there are no compromises required and no additional costs or steps to ensure security. You can seamlessly and securely sign and exchange a full range of document types simply by typing your name and clicking a button—all from within your email program and in a matter of seconds.



Who Needs Secure E-Signature?

The short answer is everybody. Whether it’s signing and exchanging contracts, medical records, or financial information, businesses and organizations of just about any size need to exchange signed documents. And by the very nature of the intent of a signature, that information is usually important, sensitive, confidential—or all three.

You need Secure Messaging’s e-signature solution because it is a simple “click to acknowledge” process that is secure and easy for anybody to understand and use. It supports major document formats, including PDFs and Microsoft Office files, as well as most common image formats (JPG, PNG, etc.), with few restrictions on file size transfers. Whether you are a lawyer, engineer, or doctor, from complex agreements to digital blueprints to x-rays, you can obtain required signatures literally in seconds.

“Using a pen to sign a physical receipt or contract is fast becoming obsolete. Enterprises’ efforts to digitize transactional processes are driving the transition to electronic signatures, an undertaking now eased by the software-as-a-service (SaaS) delivery model.”

Forrester Research



Secure E-Signature



Advantages

Secure e-signature offers the best available combination of speed and simplicity alongside security, traceability, and non-repudiation.

- **Secure**
Unlike other products that send plain text links in which anyone intercepting the basic (unsecured) email can e-sign the document, because it is integrated into Secure Messaging, the secure e-signature feature requires every user to be authenticated before they can access or e-sign the document. As well, all messages and their contents are cryptographically hashed and delivered via secure cloud (rather than over basic unsecured mail), providing more robust security even than PKI-based solutions, and without you or your users needing any additional hardware or software. Plus, the e-signature documents and associated hashed versions are stored encrypted in your Secure Messaging portal.
- **Easy to use**
You don't require an online tutorial to start using the secure e-signature feature. Much like you would with an email, you simply attach the file to be signed from the secure e-signature upload area of the Delivery Slip and click **Send Secure**. There's no need to design a complicated agreement with special fields or move between various programs to create and securely deliver the file; every document gets an e-signature certificate page appended to the end for easy reference and is presented to required signatories for signing right in their email window.
- **Simple to sign**
With the simple click-to-acknowledge process, required signatories to a document only need to click on the attachment in their email, type their name into the e-signature certificate field, and then click to acknowledge their signature. Secure Messaging then automatically informs the sender that the recipient has signed (via a desktop and mobile alert notification). Done.
- **Branded to you**
Because the Secure Messaging portal is private-labelled and branded to your organization, at no point during the exchange will anyone think they are dealing with anyone but you. The absence of documents having to go through 3rd-party solution providers will not only allay users' fears that process is not secure, but it will bolster your brand and authority as an organization that knows how to effectively and securely conduct business in a digital economy.



Secure E-Signature

- **Nothing to implement**

Unlike most products and services out there that require the download of special software in order for you to create and electronically sign documents, using the secure e-signature feature in Secure Messaging only requires that you can connect to the Internet through a browser. There's no need for complex workflows.
- **Integrated right into your email client**

The secure e-signature feature is a click away in the Delivery Slip that integrates right into your email client. From Outlook with Office 365 to Google Apps for Work and your mobile apps, ease of use is assured for both internal and external recipients.
- **Full mobile functionality**

It's simple to obtain an e-signature using the Secure Messaging mobile app or via a device browser. Unlike other products, users don't need to download the file and open it in a separate program (e.g., a PDF), or wait until they can get back to their desktop to sign. Because the file is stored securely in the cloud, users can sign time-sensitive documents on the spot from anywhere. The e-signature feature is fully supported on all mobile devices, including iOS, Android, Windows Mobile, and Blackberry 10. As well, for even greater protection for e-signed and other exchanged documents, Secure Messaging supports fingerprint authentication on iOS devices.
- **Compliant with data jurisdiction by storing documents in your region**

Unlike many services that store e-signed documents unencrypted in a public cloud, the Secure Messaging e-signature feature allows your organization to choose where your data is hosted (to help ensure data jurisdiction compliance), and all documents are always stored at rest using AES256bit encryption. For enterprise deployments, our dedicated cloud service also allows custom encryption salt and custom hashing of e-signature documents.
- **Enhanced e-discovery**

For most regulated industries or any organization that needs to archive electronic communications, managing the storage and retrieval of communications is onerous and often costly given that it often requires third-party archival services. Plus, PKI-encrypted messages may become difficult or impossible to retrieve if the encryption key is lost. With Secure Messaging, every e-signature document is MD5-hashed for later comparison and validation of the original e-signed document. Hashed documents are stored indefinitely on the Secure Messaging portal (and original e-signed documents can be stored decrypted into your existing third-party archive) regardless of the data retention policies set in place for your portal, ensuring auditability at any time.



Secure E-Signature

- **Dedicated cloud service**

Unlike other products with a generic authority to validate the authenticity of e-signed documents, the Secure Messaging e-signature feature creates a unique authority as part of the Secure Messaging portal you get as a client. The path from your message to your space in the cloud on our servers is dedicated.
- **Non-repudiable**

One of the major stumbling blocks for other products trying to offer full security is the ability to guarantee non-repudiation (where the signatory cannot claim they didn't sign the document subsequent to signing it). Unlike other products that simply send a basic (insecure) email with a link to e-sign documents, because the secure e-signature feature is built right into Secure Messaging, every user is automatically authenticated. Plus, it tracks when they logged in, when the document was viewed or downloaded, and when and where the document was signed. This data is then added to the signature on the e-signature certificate page that is appended to the original file.
- **Ensures legislative compliance**

Because Secure Messaging protects the security of the documents throughout the process and ensures the validity of the authorization provided, this makes any documents signed and exchanged using the secure e-signature feature fully compliant with existing legislation in technology neutral countries such as the U.S., UK, Canada, and Australia, just to name a few. This includes (but is not limited to) acts in the U.S. such as E-SIGN, GLBA, HIPAA (and HITECH); PIPEDA in Canada;; and the Electronic Transactions Act in Australia.
- **Integrates with your SSO**

Whereas many other products require you (and everyone in your organization using that product) to create a new identity with their service, the Secure Messaging system seamlessly integrates with your existing SSO deployment (whether SAML 2.0 or OAuth 2.0). Plus, using your own federation service for authentication adds additional reputation to verifying the authenticity of every user action without requiring the use of complex keys. (Available with the Enterprise Dedicated Cloud service.)
- **Integrates into other apps**

Because the Secure Messaging API is available as a rest-like API, developers can easily embed secure messaging features such as secure e-signature into other business solutions such as CRMs, EMRs (electronic medical records) or any third-party application with Web API capabilities.
- **Total message control**

With Secure Messaging, along with the capability to restrict users from forwarding files, you can easily recall a sensitive document sent to the wrong recipient.



Secure E-Signature

- **Real-time activity alerts & timeline insights**

With the secure e-signature feature integrated right into Secure Messaging, you also get our famous real-time notification alerts. You can be notified of every point along the transaction, such as when a required signatory reviews or signs the file you have sent them. As well, you can opt at any time to click into an overall timeline snapshot of all activity on a file. This makes it simple to send out targeted reminders to only the required signatories who need prompting.
- **Securely exchange and sign large files**

With the secure large file exchange capabilities in Secure Messaging, you can easily get large files validated without having to rely on external, unsafe file-exchange programs or worry about email file-size restrictions in place. Required signatories can simply preview and sign the document right in the email window, regardless of its size.
- **Reduced software costs**

Unlike other complicated products that charge upwards of \$20 a month per user, your Secure Messaging subscription already includes the secure e-signature feature. Plus, you can realize significant other savings through the additional features available in the Secure Messaging Suite, such as secure file sharing and secure bulk send e-campaigns, which can further reduce your need for additional software or subscriptions.
- **Reduced courier costs**

The savings for some organizations are dramatic. Imagine having to obtain signatures on a file from thousands of clients or customers and the costs of having to mail out those documents and arrange for their return. With Secure Messaging, it's now the click of a button.
- **Instant verification**

Along with the benefit of reduced courier costs, the secure e-signature feature reduces the time it takes to get documents signed and verified to literally seconds—basically, as long as it takes required signatories to open a message and type their name. Plus, all participants are immediately notified of any activity during the process and all transmissions are trackable and date-stamped.

Sample file to be signed in the secure e-signature preview window

