



WEBINAR AMPLIFIER

Migrate PGP Encryption to the Cloud with Ease

Sarah Happé
Director of Client Engagement, Echoworx

Chris Peel
VP of Customer Engineering, Echoworx

Table of Contents

Introduction	3
Challenges of running PGP on-premises	3
Identifying critical business needs for PGP	4
Migrating PGP to Echoworx: Key management essentials	4
Comprehensive overview of boundary encryption process	5
Setting up your digital signatures	7
Ongoing feature additions for optimized key management	8
Transitioning to the Echoworx cloud: A straightforward approach	9
Navigating test and configuration phases	9
Baseline testing and fallback delivery	10
Key steps of platform branding and testing	11
Key migration for enhanced encryption security	11
Final steps for enabling PGP encryption in Echoworx	13
Echoworx migration process overview	17
PGP migration made easy with Echoworx	18

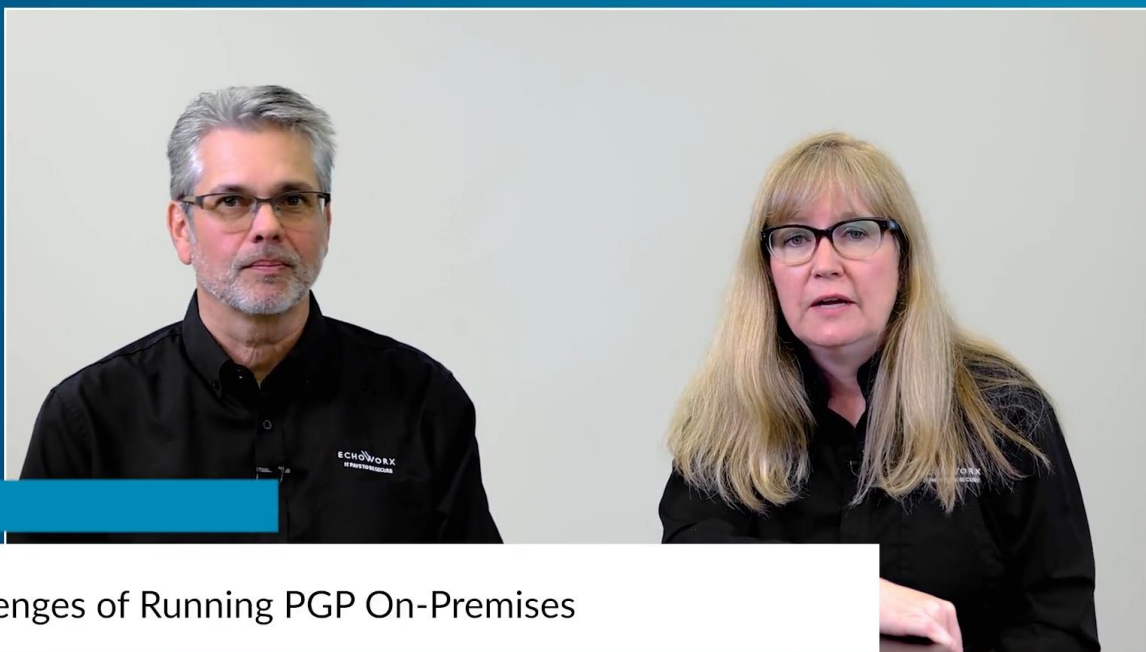
Introduction

Echoworx presents a dedicated exploration of the seamless migration of PGP encryption to the cloud, shedding light on the challenges and advantages that accompany this transformation. Leading this conversation are industry experts Sarah Happé, Director of Client Engagement, who specializes in addressing the unique demands of PGP encryption and ensuring customer success, and Chris Peel, VP of Customer Engineering, who offers valuable insights into customer needs and product development direction, and a comprehensive understanding of this vital process. The focus is on streamlining PGP encryption in the cloud, catering to both basic and intricate use cases, particularly in the realm of B2B communication and traditional certificate-based encryption requirements that are dictated by business needs.

Challenges of running PGP on-premises

Migrating PGP encryption from on-premises environments to the cloud addresses several pressing challenges and offers substantial benefits. The transition is prompted by the desire for modern, efficient email encryption solutions. Traditional on-premises PGP deployments are often plagued by outdated technology, difficulties in managing systems, and resource depletion due to staff turnover. Maintaining and ensuring the reliability, redundancy, and scalability of on-premises solutions can be burdensome. Furthermore, these legacy systems, such as PGP Universal, are no longer receiving updates or security patches, which leaves organizations vulnerable to potential risks and non-compliance. As security threats continue to evolve, keeping pace with security patches and updates becomes paramount. Migrating to the cloud not only addresses these challenges but also aligns with the broader trend of cloud adoption in the IT landscape.

ECHOWORX™



Challenges of Running PGP On-Premises

Echoworx emerges as a valuable solution, specializing in boundary-based encryption that enhances email security while accommodating the shifting landscape of security and data protection. Boundary-based encryption at the point of sending replaces the outdated practice of encrypting emails at rest, allowing for improved DLP inspections and compliance checks. Echoworx leverages cloud infrastructure, providing a secure, up-to-date, and scalable solution that supports modern encryption needs, making it a compelling choice for organizations seeking to enhance their email security posture.

Identifying critical business needs for PGP

In discussions regarding PGP encryption functionalities, whether implemented in the cloud or on-premises, the primary focus revolves around meeting customer requirements. Key aspects include seamless key rollover and the automation of encryption processes, ideally without involving staff members. The goal is to eliminate the need for individuals to decide when PGP encryption should be used, opting for policy-based encryption solutions.

For instance, for organizations dealing with entities like the Bank of England or specific partners, automation can ensure PGP or S/MIME encryption is enforced. In cases where PGP is unavailable, fallback options such as secure portals or PDF delivery can be implemented based on customer preferences, with flexibility to apply these rules globally or for specific teams and recipient domains.

Furthermore, domain-based encryption is also a significant feature, allowing for communication encryption at the domain level, enhancing security across the organization.

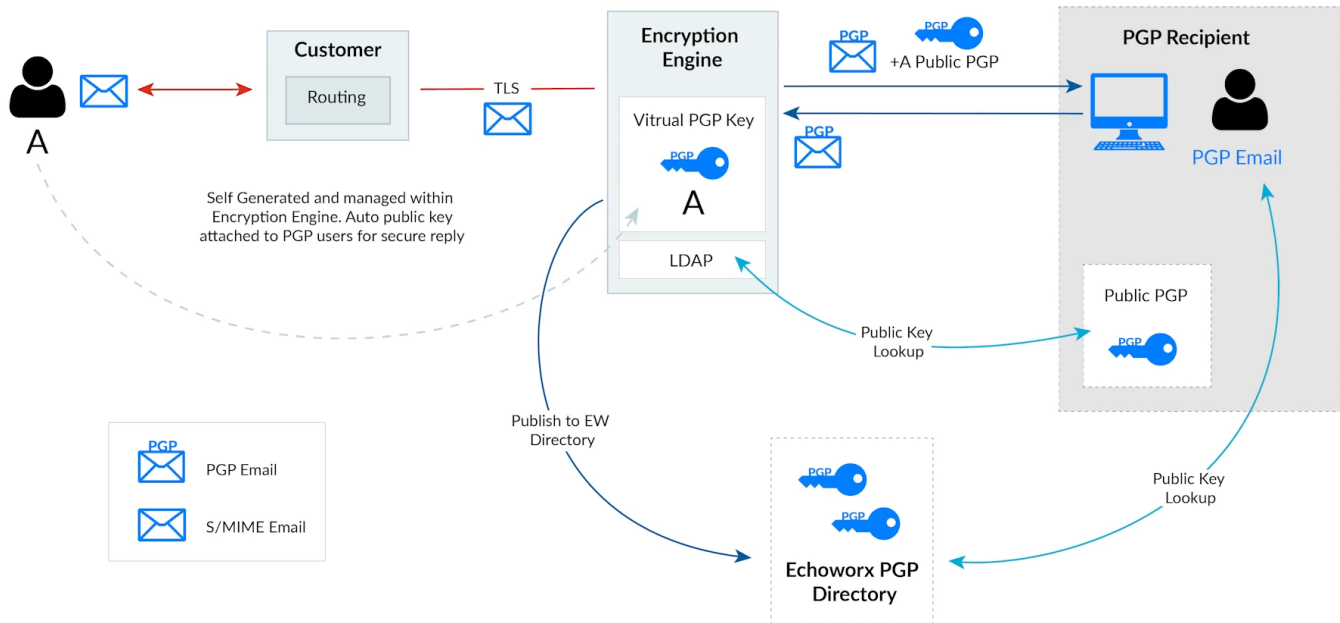
Migrating PGP to Echoworx: Key management essentials

When considering the migration of PGP or S/MIME encryption to a cloud-based platform like Echoworx, several crucial factors come into play. Customers may approach this transition from varying starting points, whether migrating existing PGP solutions or implementing PGP encryption for the first time. Key to a smooth migration is the seamless transfer of credentials from on-premises appliances to the cloud so as to ensure minimal disruption to communication with business partners. Echoworx facilitates this process, allowing customers to maintain their existing PGP keys, which reduces the need to inform third parties of key changes. The platform's integration capabilities streamline key management, automating key generation and renewal, and enabling LDAP publishing for bi-directional key lookup.

Moreover, Echoworx empowers end recipients to self-manage their encryption preferences, lowering support calls and administrative burdens and ultimately ensuring a hassle-free transition to cloud-based PGP encryption. An illustrative example of this successful migration can be seen in the case of Clydesdale Bank, part of Virgin Money, which seamlessly integrated its legacy PGP encryption into Echoworx, leveraging the platform's omni-channel encryption and key management features to maintain uninterrupted communication with its customers.

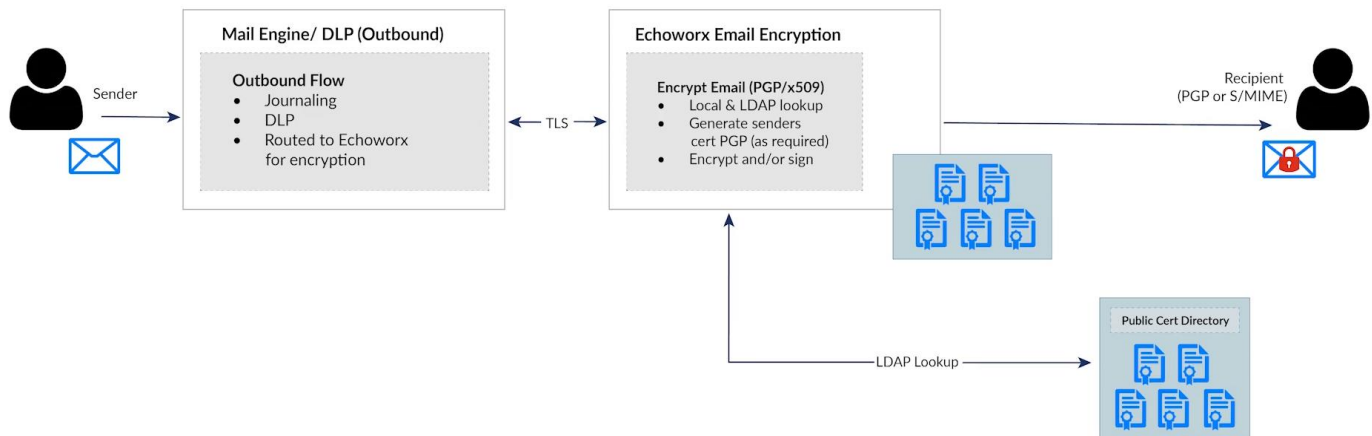
Comprehensive overview of boundary encryption process

Echoworx PGP



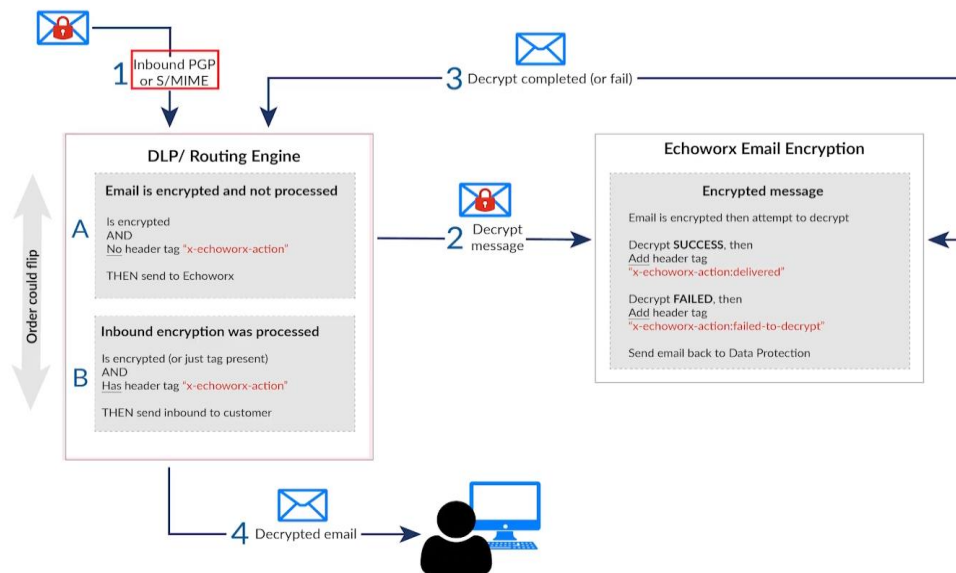
Boundary encryption, in a general sense, pertains to the process of securing outbound communications from an organization. Users within the organization can compose messages that may or may not trigger encryption, a choice that can be made by the sender or automated through Data Loss Prevention (DLP) systems or Secure Email Gateways (SEG). For instance, partnerships with solutions like Mimecast involve direct integrations with SEG gateways that determine when encryption is necessary and route the message accordingly. Outbound communications initially remain unencrypted, allowing for functions like journaling and archiving. However, once the need for encryption is established, the message is delivered to the cloud using Transport Layer Security (TLS), a standard integration technology, where encryption is applied to ensure secure transmission.

Outbound PGP/x509 Encrypt



At the outbound boundary, the system utilizes public certificates that may have been provided by recipients or retrieved from external directories in real-time. Additionally, it automatically generates certificates for senders and proceeds to deliver the outbound PGP messages. This approach ensures that external recipients receive fully signed and encrypted PGP messages, enhancing the security and integrity of the communication process.

Inbound PGP/x509 Decrypt

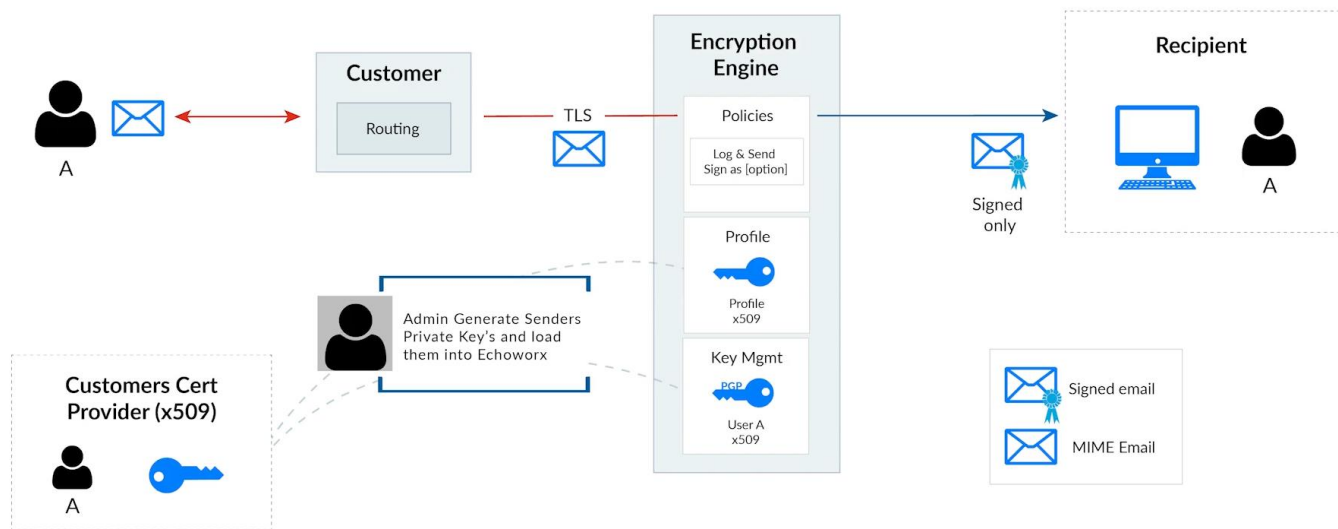


On the inbound side of communication, there is a reversal of the process. When the SEG gateway detects an inbound PGP message and determines it to be encrypted, it directs the message to Echoworx. Echoworx then handles the decryption and forwards the message accordingly. Importantly, this approach ensures compliance with AVAS, journaling, and archiving, while also facilitating easy delivery to internal recipients. Users can seamlessly send and receive messages as usual, whether on mobile devices like iPhones or iPads, while maintaining security compliance.

This approach eliminates the need for specialized desktop software or key distribution, resulting in significant cost savings. It also avoids the necessity to modify SPF and DKIM settings, as the gateway serves as the authoritative delivery point, with a dedicated route or connector to and from the Echoworx cloud. This is transparent to end users, even as all reporting and message flow tracking remains within the gateway.

Setting up your digital signatures

Echoworx Signature Flow



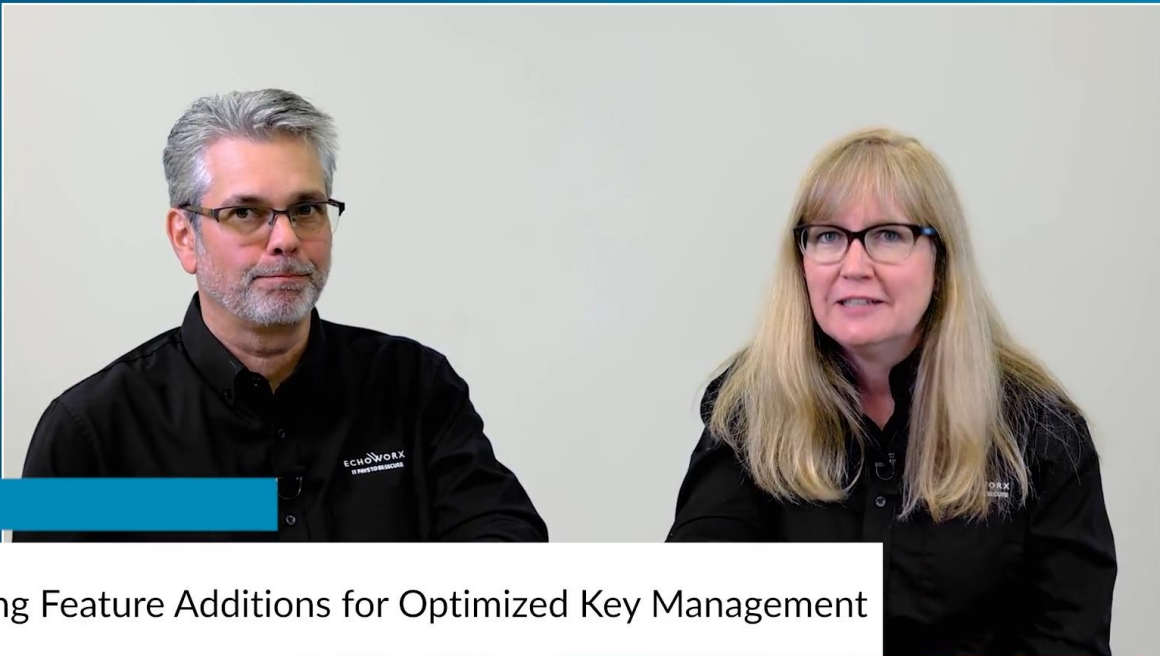
In the context of certificate-based encryption and signing within Echoworx, various signing options are worth discussing. Ideally, the sender's email address is associated with a key, allowing for the message to be signed by the sender, thereby ensuring authenticity. However, in cases where this isn't feasible, fallback options come into play. Echoworx can sign messages with an enterprise key, a practice more common in S/MIME scenarios. This approach still adds a layer of trust, indicating that the message has been signed by the company, albeit not by the specific sender. Signatures play a crucial role in message encryption, providing non-repudiation and verifying the sender's identity. Both PGP and S/MIME offer signature capabilities.

Echoworx also plans to introduce auto-key generation for S/MIME in the future, ensuring parity in digital signatures and non-repudiation for outbound communications. In terms of inbound scenarios, verifying signatures when messages are de-crypted at the gateway can be challenging. To address this, Echoworx allows customizable footers to be added to emails after decryption, providing users with information about the trustworthiness of the message, thus simplifying the verification process and enhancing security and compliance.

These measures help users make informed decisions and avoid potential phishing threats by ensuring that they can trust the messages they receive.

Ongoing feature additions for optimized key management

Echoworx continues its commitment to platform evolution, introducing new features and capabilities. This ongoing development encompasses aspects like key generation, S/MIME functionality, and email signature management. One noteworthy addition to the platform is certificate harvesting, a feature that ensures feature parity with legacy on-premise servers, responding to customer expectations. Certificate harvesting focuses on capturing and storing public certificates from third parties when inbound messages are signed, facilitating their reuse in outbound communications. Another recent enhancement involves the adoption of Key Management Service (KMS), an enterprise-specific key management approach. KMS safeguards essential enterprise keys in Hardware Security Modules (HSMs), providing an additional layer of security for user keys imported into the system. This integration allows for improved key export capabilities, which were previously limited. KMS, essentially an HSM-backed credential storage, bolsters data protection, aids in compliance with privacy regulations like GDPR, and enhances auditability and control, which reinforces Echoworx' commitment to robust security and compliance measures.



Ongoing Feature Additions for Optimized Key Management

Transitioning to the Echoworx cloud: A straightforward approach

In the process of bringing customers onto the Echoworx platform, the engagement team follows a well-established procedure. This encompasses various steps, not limited to PGP encryption alone. The initial discussions revolve around understanding the project's timeline, requirements, and resource allocation. The team assists the customer in configuring key importation, auto key generation, and setting up key lookup and configuration. This process, while accommodating PGP encryption, is seamlessly integrated into the overall onboarding strategy. The engagement team's expertise in handling such transitions ensures a smooth and efficient migration process for customers moving to the Echoworx Cloud.

Navigating test and configuration phases



ROUTE TEST MESSAGES

oooooooooooooooooooooooooooo

Route keyword-triggered
test messages to Echoworx
(test domain or user group).

The initial step in transitioning to the Echoworx platform involves defining the test and configuration phase in contrast to the go-live phase. Often likened to step-in testing, this process enables customers to safely evaluate the platform's functionality without disrupting their production mail flow. Companies approach this transition with varying environments; some maintain separate test environments, while others perform testing within their production setup, necessitating careful handling. Regardless of the approach, the engagement team assists in configuring and connecting the chosen email routing to the Echoworx Cloud through the existing gateway. This standard cloud integration point ensures that all routes are enforced with TLS for secure communication into the cloud platform.

Baseline testing and fallback delivery



DEFINE ENCRYPTION POLICIES

oooooooooooooooooooooooooooo

Define encryption policies
in Echoworx for customized
message actions.*

In the process of baseline testing, Echoworx engagement teams emphasize the importance of having a fallback delivery mechanism alongside the primary PGP encryption. This ensures flexibility and efficiency in message delivery. The ability to tailor message encryption based on recipients' capabilities is a unique feature offered by Echoworx.

Echoworx Delivery Options

Encryption Options

Pull					Push		Direct		
Portal User (default)		Portal Message Level			Full Message	Attachment (PDF, Office, ZIP)	TLS	PGP	S/MIME (with certificate harvesting)

Authentication Options

OAuth	OpenID	SSO	2FA (TOTP & SMS)	PassKey	Sender Set	Out Of Band	No Auth	SMS	Sender Set	User Managed	Sender Set	User Managed
-------	--------	-----	---------------------	---------	---------------	----------------	---------	-----	---------------	-----------------	---------------	-----------------

DigiCert

During baseline testing, a simple route is established, allowing messages to flow from the customer's gateway to Echoworx, where they can be encrypted into the portal, ensuring notifications are delivered. This step-by-step approach enables customers to define and refine their encryption policies while accommodating various business requirements and legacy rules seamlessly.

Key steps of platform branding and testing



CUSTOMIZE

oooooooooooooooooooooooo

Customize brandable
headers/footers for encrypted
and decrypted messages.*

When configuring branding for the platform, it becomes evident that branding plays a crucial role in the overall user experience. The process primarily involves defining key elements such as logos, service names, and business colors. These foundational branding components can be seamlessly integrated into various templates and notifications within the platform, typically with a quick turnaround time of just a couple of days. Moreover, the platform offers extensive branding possibilities, allowing for singular or even channel-specific branding, catering to diverse business units if necessary. With routing, rules, and branding now in place, the next steps involve baseline testing, ensuring the connected mail flow and examining specific branding points, particularly within PGP notifications. This comprehensive approach ensures that customers can establish a robust test plan, enabling them to visualize all aspects of their branding before going live.

Key migration for enhanced encryption security

The process of migrating keys, particularly in the context of PGP encryption or S/MIME, involves several crucial aspects. The first step focuses on the Enterprise Signing Key, a unique component that plays a significant role in ensuring trust and chain of trust within the system. This key is typically present in the legacy PGP server and serves as an Enterprise Key capable of signing auto-generated keys within Echoworx, creating a sense of trust within the system. It is important to note that this Enterprise Key can mimic the role of a Certificate Authority (CA) by signing all end-user certificates, thereby establishing a chain of trust.



TRANSFER SIGNING KEY

oooooooooooooooooooooooo

Transfer enterprise signing
private key from legacy PGP
gateway to Echoworx.

To migrate the Enterprise Signing Key, administrators log into their old console, export the key into a file, and then access the Echoworx admin console to upload it. This approach ensures that private keys are not exposed or transmitted insecurely, providing a secure migration process. The Echoworx platform offers the necessary tools and guidance for administrators to perform this migration efficiently.



EXPORT USER KEYS

oooooooooooooooooooooooo

Export user keys from legacy
PGP gateway.
Import keys to Echoworx.

The next phase of key migration involves transferring all user keys from the legacy appliance. This includes both private and public keys. For external and public recipient keys, administrators should export them as a set of public keys, typically as a blob of data, from the legacy appliance. This data can be readily imported into Echoworx.

The most critical aspect of the migration pertains to the public-private key pairs stored in the legacy appliance. Administrators should export these pairs separately into a file that includes the private keys. It is essential to handle these files securely and not distribute them extensively. The private key files are then promptly imported into the Echoworx platform, ensuring a smooth and secure transition. To streamline the process, it's advisable to keep the number of keys in each file to approximately 500 or less to prevent issues associated with handling large data sets during migration. By following these steps, organizations can seamlessly migrate their keys to the Echoworx platform, maintaining the integrity and security of their encryption infrastructure.

Final steps for enabling PGP encryption in Echoworx



ENABLE KEY GENERATION

oooooooooooooooooooooooooooo

Enable automatic PGP key
generation and signing with
Enterprise key.

Once the foundational setup is complete, the migration process to enable PGP encryption within the Echoworx platform involves several key steps. First, administrators can enable PGP private key generation within the Echoworx console to ensure that new senders or expiring keys trigger the auto-generation of new keys, simplifying key management. The platform retains old keys for decrypting existing inbound messages while making the new key active.



ENABLE DIRECTORIES

oooooooooooooooooooooooooooo

Enable automatic addition
of public third-party PGP
directories to Echoworx.

Another essential step is configuring third-party key lookup. While Echoworx already recognizes universal key repositories, administrators can specify additional LDAP directories to search for keys, enhancing key discovery efficiency. Regarding user initiation of encryption, administrators can choose to deploy the Echoworx add-in for staff to trigger encryption.



INSTALL ADD-IN

oooooooooooooooooooooooooooo

Install Email Encryption
Add-In for Outlook and Gmail
across the Enterprise.*

This add-in is configurable, allowing users to initiate encryption either through a simple button or by specifying encryption types within the message. Configuration flexibility is a core feature of the Echoworx platform. Administrators should establish production triggers and keywords for encryption, ensuring that the correct rules and settings are applied for live use. Test data and rules can be separated from production settings to maintain clarity during testing. Testing both outbound and inbound communication is crucial to the migration process. Administrators must verify that messages encrypted with PGP or S/MIME are successfully decrypted upon receipt and that verification footers and headers function as intended. This two-way communication validation ensures the seamless integration of PGP encryption within the Echoworx platform.



ROUTE OUTBOUND EMAILS

oooooooooooooooooooooooo

Go-live:

Route outbound emails to
Echoworx for encryption.

Replicate existing PGP gateway
encryption rules.

The migration process involves setting up key generation, configuring third-party key lookup, defining user initiation methods, establishing production triggers, and thoroughly testing both outbound and inbound PGP or S/MIME encryption to ensure a smooth transition to the Echoworx platform.



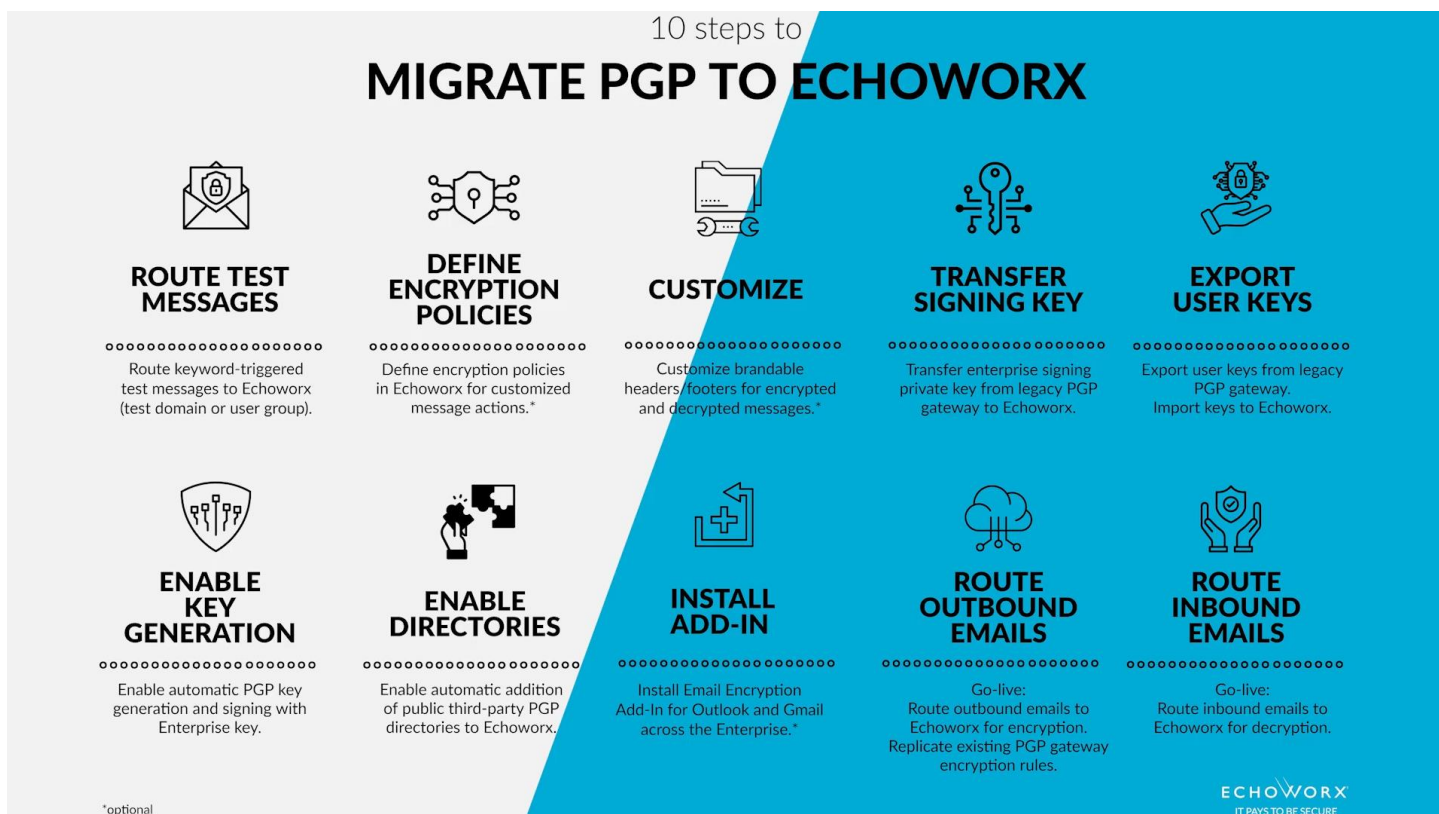
ROUTE INBOUND EMAILS

oooooooooooooooooooooooooooo

Go-live:
Route inbound emails to
Echoworx for decryption.

In terms of the inbound process for PGP messages, a separate set of rules is involved. Detecting incoming PGP messages typically entails using straightforward settings in the customer's email gateway, often as simple as checking a box to identify PGP messages. However, for more precision, Echoworx can provide guidance on defining specific headers for detection if needed. It's important to ensure that these rules are well-defined to avoid any potential message loops, which is a topic discussed and addressed early in the Mailflow configuration process. Echoworx has extensive experience in this area, spanning nearly two decades, and can assist customers in setting up and optimizing their inbound PGP message handling.

Echoworx migration process overview



In terms of the migration process to Echoworx, it's important to consider a few key factors. The overall timeline can vary depending on the complexity of the customer's needs and the extent of their specific requirements. Typically, the engagement process begins with a project planning phase that involves organizing stakeholders and establishing the groundwork for the migration.

Next, the service configuration and discovery phase comes into play. This involves familiarizing the customer with Echoworx' options and settings, including branding and delivery methods. While this phase can ideally be completed in two to three days, the actual duration may vary based on the customer's internal processes and decision-making.

Once the service configuration is in place, integration and baseline testing take center stage. During this phase, a test plan is developed, recommended tests are performed, and the customer executes the testing process. This phase typically spans a week or two as the customer fits testing into their schedule.

The migration of keys, a crucial step in the process, can take anywhere from five to eight business days or longer, depending on factors like the volume of keys and the customer's specific requirements. This step involves the secure transfer of sensitive information, and the timeline is often customer driven.

Following the key migration, training and acceptance testing become the focus. This phase typically lasts three to seven days, with the duration influenced by the thoroughness of the service setup and the transition from a proof of concept (POC) to a production environment. Echoworx offers a flexible approach that allows customers to leverage their POC work for a smooth transition to a live production environment.

Overall, the migration to Echoworx is a collaborative process that accommodates the customer's pace and requirements, with the engagement team providing dedicated support throughout.

PGP migration made easy with Echoworx

How to complete the migration process

Task	Duration (business days)
Kick-off meeting and Project Planning	2-3
Service configuration discovery	2-3
Echoworx service provisioning	2-3
Integration and baseline testing	2
Service set up, customization and testing	3-7
Migration of Keys	5-8
Administrator training	1
Acceptance testing	3-7
Project wrap-up, Go-live and roll out to your end-users and recipients	1

Echoworx offers seamless migration solutions for clients looking to transition their current PGP encryption systems from on-premises to the cloud. With an extensive track record of successfully migrating key customers like Clydesdale, Bird & Bird, Clifford Chance, Citigroup, and NTT Securities, Echoworx provides a comprehensive approach to managing encryption services in the cloud. By handling hardware management, software updates, and patches, Echoworx simplifies the process and offers additional message encryption options tailored to each client's unique business needs. Interested parties are encouraged to reach out to Echoworx for expert guidance on migrating to the cloud and exploring the full range of message encryption capabilities the platform offers. Clients often discover that transitioning to Echoworx not only enhances their PGP capabilities but also opens up new possibilities for securely communicating with a broader audience. With Echoworx as a unified message encryption platform, clients can consolidate their encryption solutions and streamline their operations for both B2C and B2B communications.

©TechTarget, Inc. or its subsidiaries. All rights reserved. TechTarget, and the TechTarget logo, are trademarks or registered trademarks of TechTarget, Inc. and are registered in jurisdictions worldwide. Other product and service names and logos, including for BrightTALK, Xtelligent, and the Enterprise Strategy Group might be trademarks of TechTarget or its subsidiaries. All other trademarks, logos and brand names are the property of their respective owners.

This publication may contain opinions of TechTarget, which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent TechTarget's assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, TechTarget makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.

Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of TechTarget, is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact your TechTarget client representative.