April 2005

PGP® White Paper

PGP® Universal 2.0 – Technical Overview

Table of Contents

Executive Summary

PGP Universal is PGP Corporation's solution for securing confidential email communications and managing desktop storage security. PGP Universal automates email security to overcome the fundamental challenges that previously prevented organizations from successfully rolling out secure messaging to internal users and external partners. By transparently enforcing an organization's security policy, PGP Universal secures email without requiring user or administrator action.

At the core of PGP Universal is the Self-Managing Security Architecture (SMSA), a system that enables message security while minimizing the action required by either end users or administrators. Tasks handled by the SMSA include the following:

- **Creating and managing user keys** – The SMSA enrolls internal users automatically based on header information extracted from the mail stream. PGP Universal generates keys for users as needed and manages the lifecycle of individual keys, relieving administrators of the burden of creating and managing users' keys.
- **Discovering business partners' keys** – The SMSA can query a business partner's PGP Universal Server or LDAP directory or the PGP Global Directory to automatically discover the key required to secure a message. By automating the discovery of keys, PGP Universal relieves organizations of the overhead previously required to establish secure email communications with business partners.
- **Enrolling users** – For users outside an organization without encryption keys, PGP Universal provides secure delivery via PGP Universal Web Messenger. PGP Universal Web Messenger is a Web-based mail system that ensures secure delivery of mail and allows external users to enroll in the SMSA and choose how to secure future messages. By providing a secure delivery option for users without an existing key, PGP Universal eliminates the barriers to deploying secure email to users outside the organization.

PGP Universal can be deployed either in the mail stream to provide transparent gateway-based encryption or end-to-end encryption, or deployed out of the mail stream to provide management of PGP Desktop installations. When deployed in the mail stream, PGP Universal's proxy-based encryption engine applies security policy to detect messages that should be encrypted and uses the SMSA to either find a key for the recipient or provide secure delivery using PGP Universal Web Messenger. When deployed out of the mail stream, PGP Universal can dynamically control the security policy applied by PGP Desktop installations within the organization.

All aspects of PGP Universal Server's operation are configured using a Web-based administrative interface. This interface provides an organization with the ability to centrally manage, maintain, and monitor all aspects of its secure-messaging infrastructure. Using the administrative interface, an administrator configures the security policy that dictates the conditions under which an outbound email message must be encrypted. When deployed in conjunction with PGP Desktop, an administrator can also use the administrative interface to manage the security policy of PGP Desktop installations as well as the use of PGP Virtual Disk and PGP Whole Disk to encrypt local files for protection from unauthorized access.

PGP Universal's automated approach to email security allows organizations to overcome the fundamental challenges that previously prevented them from successfully rolling out email encryption to internal users and external partners.

Introduction

This PGP White Paper provides a technical overview of PGP Universal 2.0, PGP Corporation's solution for securing confidential email communications and managing desktop storage security. PGP Universal solves the fundamental problems that have plagued organizations seeking to secure their confidential information using public key cryptography:

- How can an organization easily secure email communications with its partners without requiring its partners to pre-enroll in the organization's email encryption solution?
- How can an organization enforce its security policy so that confidential information being sent to business partners is encrypted automatically without requiring end users to take any action?

This paper details the features of PGP Universal 2.0 and how they address these questions as part of providing an enterprise message and storage encryption solution that preserves the user experience, automates the application of security policy, and minimizes administrative overhead.

Intended Audience

This PGP White Paper is intended for technical personnel seeking to understand PGP Universal as part of their evaluation of the product's ability to meet their organization's requirements. These technical personnel may include the following:

- Executives, such as CSOs, CIOs, or CTOs, responsible for securing confidential organizational data and ensuring compliance with regulatory or corporate security mandates
- IT administration staff responsible for installing, configuring, maintaining, and managing the email and network infrastructure and for supporting desktop users

Prerequisite Knowledge

Before reading this PGP White Paper, technical personnel should have a general knowledge of email and networking technology, standards and industry best practices, and public-key encryption technology.[1]

Learning Objectives

After reading this PGP White Paper, readers should be able to:

- Identify the elements of the PGP Ecosystem and explain how these elements cooperate to enable secure communications between individuals and organizations.
- Explain how PGP Universal's Self-Managing Security Architecture automates the enrollment of new users both inside and outside an organization and enables business partners to leverage keys created by PGP Universal.
- Understand how PGP Universal automatically enforces an organization's security policy without requiring action by the user.
- Illustrate the different ways in which PGP Universal may be deployed to encrypt email messages, automatically apply security policy, and manage PGP Desktop installations.

[1] For an introduction to public-key cryptography, see the "Introduction to Cryptography" White Paper available at http://www.pgp.com/library/whitepapers/index.html#cryptography

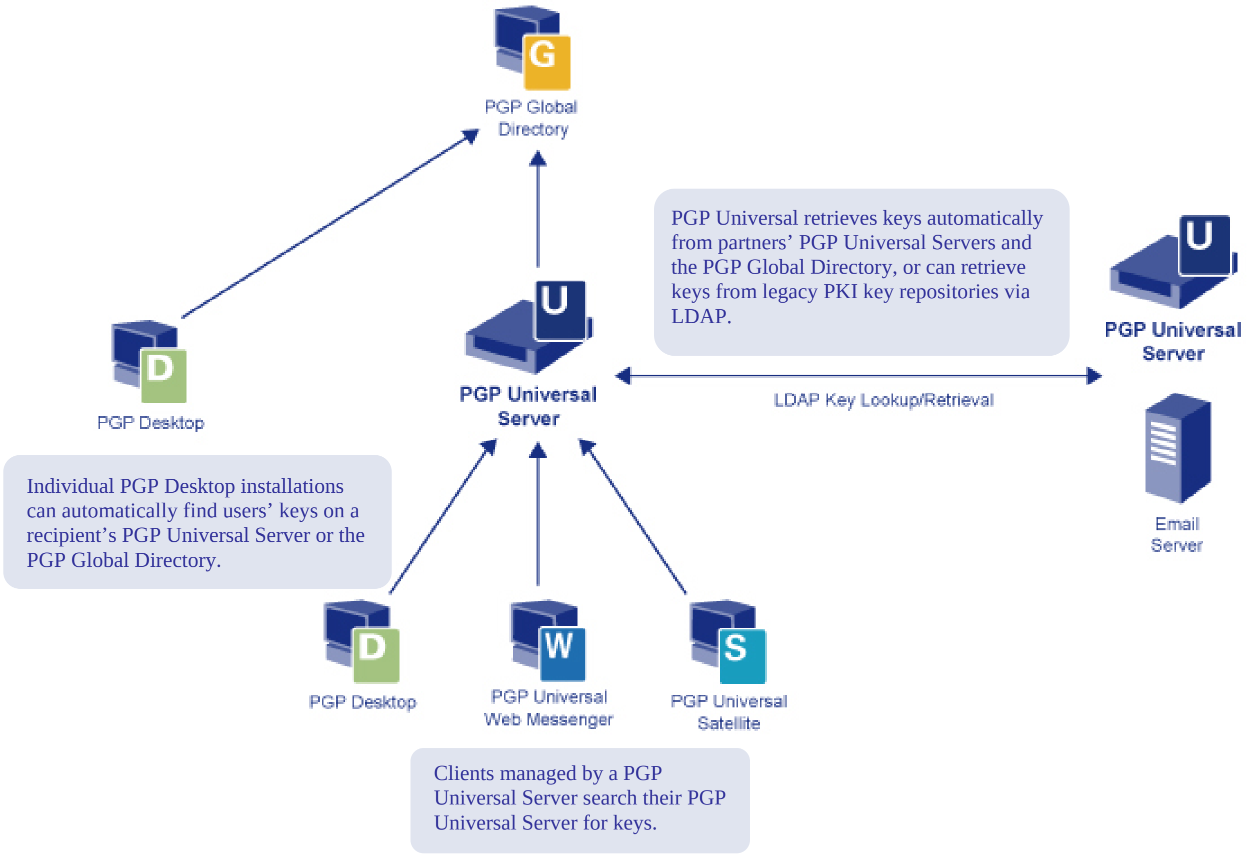
- Identify the functionality of the PGP Universal's administrative interface, including how it manages access to the server, enables server monitoring and maintenance, and manages deployments of PGP Desktop and PGP Universal Satellite[2].

The PGP Ecosystem

Before delving into an explanation of PGP Universal, it's important to explain how this product relates to the suite of encryption solutions provided by PGP Corporation. These solutions work together to enable an organization to easily and automatically find the encryption key required to secure an email message to a specific recipient's email address. These solutions are collectively called the PGP Ecosystem.

What is the PGP Ecosystem?

The PGP Ecosystem is the collection of PGP solutions responsible for automatically distributing the encryption keys PGP Universal and other PGP solutions require to encrypt email messages or verify digital signatures on email messages. PGP Desktop users, PGP Universal users, and users of another OpenPGP or X.509 encryption solution are all part of the PGP Ecosystem.



PGP Universal retrieves keys automatically from partners' PGP Universal Servers and the PGP Global Directory, or can retrieve keys from legacy PKI key repositories via LDAP.

Individual PGP Desktop installations can automatically find users' keys on a recipient's PGP Universal Server or the PGP Global Directory.

Clients managed by a PGP Universal Server search their PGP Universal Server for keys.

Figure 1: The PGP Ecosystem

[2] PGP Universal Satellite is an optional client application that automatically and transparently encrypts and decrypts email communications and enforces security policy on all email messages sent from the user's email client to and from the PGP Universal Server. For more about PGP Universal Satellite, see page 8.

The PGP Ecosystem eliminates the laborious, time-consuming, and costly process of manually exchanging users' encryption keys that previously hampered organizations' ability to effectively adopt secure email. Instead of requiring business partners to manually exchange keys, the individual components of the PGP Ecosystem cooperate to enable automated key distribution and lookup. The PGP offerings that make this possible are the PGP Global Directory, PGP Universal, and PGP Desktop.

PGP Global Directory

The PGP Global Directory (https://keyserver.pgp.com) is a free service designed to make it easier to find and trust the universe of PGP keys. The PGP Global Directory is a repository of keys uploaded automatically by individual PGP Desktop users or manually by those using other OpenPGP solutions.

PGP keys uploaded to the PGP Global Directory have their email address verified before the key is made public, ensuring that the key corresponds to an active email address. Periodically, PGP Corporation will notify the email addresses associated with the keys in the PGP Global Directory to re-verify users' desires to have their keys available to the public. Users who fail to re-verify their keys will have their key removed, ensuring that the PGP Global Directory only contains current, valid keys that can be used to encrypt email communications.

Installations of PGP Universal and PGP Desktop automatically consult the PGP Global Directory to find a key to use when encrypting email to a specific recipient's email address. The participation of PGP Global Directory in the PGP Ecosystem increases the likelihood that an email for a given recipient can be encrypted without requiring any effort on the part of the sender.

PGP Universal

PGP Universal contributes to the PGP Ecosystem in a number of ways:

1. **Managing users' keys –** Keys created and managed by an organization's PGP Universal Server are made available to PGP Universal and PGP Desktop users within the organization.
2. **Querying a recipient's PGP Universal Server –** When attempting to encrypt a message to an external recipient, the sender's PGP Universal Server will attempt to locate a PGP Universal Server responsible for managing the keys for the recipient's domain. If such a PGP Universal Server can be located, the sender's PGP Universal Server will query the recipient's PGP Universal Server for the recipient's key.
3. **Querying the PGP Global Directory –** If the sender's PGP Universal Server is unable to locate a PGP Universal Server responsible for managing the recipient's domain, it will search the PGP Global Directory to find a verified key for the recipient's email address.
4. **Leveraging legacy X.509 certificates –** PGP Universal bridges legacy X.509 systems and the PGP Ecosystem. Using LDAP directory synchronization, a PGP Universal administrator can import existing certificates for an organization's users, allowing it to leverage existing PKI investment. PGP Universal can also query business partners' LDAP directories to find X.509 certificates to use when encrypting email communications.
5. **Serving keys to external users –** PGP Universal allows external partners to search and query the server via LDAP to find keys to enable secure email messaging. PGP Desktop can be configured to use SSL/TLS client certificates over LDAPS, which PGP Universal Server can be

configured to require for authentication if an organization chooses to prevent broader key lookup capabilities.

6. **Enabling self-service upload of PGP keys –** PGP Universal includes a self-service feature called the PGP Verified Directory that allows users to upload keys for use by the PGP Universal Server to encrypt messages.

PGP Desktop

PGP Desktop provides a desktop application suite that allows individual users to control the security of their hard drives as well as their email communications. PGP Desktop participates in the PGP Ecosystem by allowing users to publish their keys to the PGP Global Directory automatically, thereby enabling others to find keys for use when sending encrypted email and verifying signatures. PGP Desktop also automatically discovers and queries a message recipient's PGP Universal Server to find a recipient's key. In the event the recipient does not have a PGP Universal Server, the sender's PGP Desktop installation will automatically query the PGP Global Directory to try to find a recipient's key to use to encrypt the message.

Benefits of the PGP Ecosystem

The PGP Ecosystem provides a number of benefits for organizations that need to encrypt email communications with their business partners:

1. **Easier to send encrypted messages –** PGP products can automatically encrypt a message if a PGP key is found. Individual installations of PGP products automatically publish and discover keys associated with an email address, increasing the likelihood of finding a key for a recipient's email address and that an email can be encrypted without requiring additional effort by the user.
2. **Faster deployment of business partners –** By automating the discovery of keys, PGP products relieve organizations of the overhead previously required to establish secure email communications with business partners. Business partners can use the organization's PGP Universal Server to access keys without requiring the involvement of IT personnel.
3. **Preserves investments in legacy PKI solutions –** PGP Universal can leverage a business partner's preexisting X.509 certificates to send S/MIME-formatted email messages. Interoperating with a business partners' S/MIME secure email solutions allows an organization to forego managing the key exchange process while allowing partners to continue using existing email encryption solutions.

PGP Universal

PGP Universal is a self-managing, automatic, network-based encryption solution that protects an organization's internal email communications as well as email messages between the organization and its external business partners and customers. Consisting of software running on a dedicated server deployed in the mail stream, PGP Universal proxies standard mail protocols (SMTP, POP, IMAP) and applies message security policy to email messages coming into and flowing out of the organization.

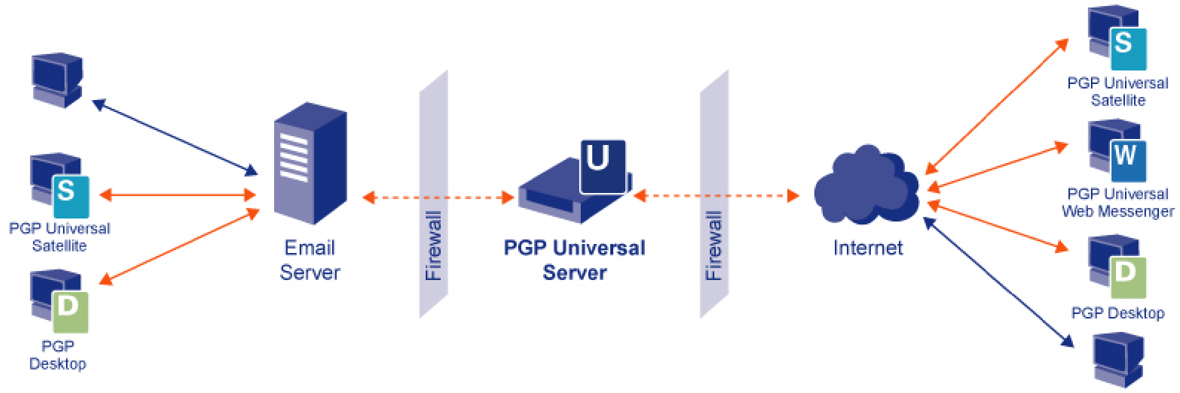


Figure 2: PGP Universal

For organizations that require a tactical email and storage encryption solution that does not reside in the organization's mail stream, PGP Universal can also be deployed out of the mail stream to manage the configuration and security policy of PGP Desktop installations.

PGP Universal Components

- **Web-based administrative interface –** PGP Universal provides a centralized management console for administrative configuration and monitoring of the PGP Universal Server. When deployed in conjunction with PGP Desktop, PGP Universal allows administrators to use the administrative interface to manage the security policy of PGP Desktop as well as the use of PGP Virtual Disk and PGP Whole Disk.
- **Proxy-based encryption and policy-enforcement engine –** PGP Universal monitors inbound and outbound mail traffic to automatically encrypt, decrypt, sign, and verify individual email messages as dictated by security policy. Using the administrative interface, an administrator configures the security policy that sets the conditions under which an outbound email message must be encrypted to a recipient. PGP Universal can also use the optional integrated Symantec AntiVirus™ Scan Engine to perform virus scanning as part of its operations.
- **Web-based secure message delivery system –** PGP Universal supports secure delivery of email messages to users outside the organization without a preexisting secure email solution via PGP Universal Web Messenger. PGP Universal Web Messenger provides an SSL-secured Web-based mail interface for recipients to read messages and reply in a secure manner.
- **Automated enrollment and key-management system –** PGP Universal's Self-Managing Security Architecture (SMSA) automates the process of enrolling users, creating encryption keys as needed and managing user keys. PGP Universal allows partners to query for user keys over LDAP and LDAPS and supports client certificates to restrict access to the key database to authorized business partners.
- **PGP Verified Directory –** The PGP Verified Directory allows users managed by PGP Universal to upload preexisting PGP keys via a Web-based interface or LDAP directory. Keys uploaded to the PGP Verified Directory trigger a verification email that allows the server to automatically vet that uploaded keys correspond to managed email addresses. The

owner of the email addresses on the uploaded key must act on this verification email before the key can be used by PGP Universal. An administrator can also choose to verify keys uploaded to the PGP Verified Directory manually or automatically trust all keys uploaded without any verification.

- **Optional Client Software:**
  - **PGP Desktop –** A desktop client application responsible for encrypting local storage using PGP Virtual Disk and/or PGP Whole Disk as well as client-based encryption and decryption of email messages. PGP Universal can manage individual PGP Desktop installations, allowing an organization to centrally manage security policy without requiring PGP Universal to be located in the mail stream.
  - **PGP Universal Satellite –** A client application that transparently encrypts email communications sent from the user's email client. PGP Universal Satellite can be provided to users as part of PGP Universal's automated enrollment process to simplify the process of encrypting future email communications.

    PGP Universal Satellite secures email for users inside or outside the organization in accordance with the security policies controlled by an organization's PGP Universal Server. For external users of PGP Universal Satellite, downloading policy from the organization's PGP Universal Server provides two-way policy enforcement, ensuring the organization's security policy is applied to inbound as well as outbound email communications.

The Self-Managing Security Architecture

At the core of PGP Universal is the Self-Managing Security Architecture (SMSA), a system that enables message encryption while minimizing the action required by either end users or administrators. Tasks handled by the SMSA include the following:

- **Enrolling users for secure message delivery –** To enable secure message delivery, the SMSA handles enrolling internal and external users and automatically generates encryption keys for users, as needed.
- **Key management –** Central to the SMSA's role of enabling message security is its ability to automatically manage the lifecycle of a user's key from key creation to key expiration. Management of keys created by the SMSA also includes using existing keys and certificates contained in an organization's LDAP directory and ensuring corporate access to encrypted data using patented PGP Additional Decryption Key (ADK) technology, according to policy.

Enrolling Users for Secure Message Delivery

The process of enrolling users is a critical deployment hurdle for organizations to overcome when deploying an email encryption solution. An email encryption solution must enable enrollment of users within an organization as well as external partners outside the control of the organization's IT department. To be truly effective, the enrollment process must enable secure messaging without requiring prior enrollment by the external business partners' users.

PGP Universal addresses these challenges by automating the process of enrolling both internal and external users. Using user information extracted from the mail stream or configured via existing directory information, the SMSA automatically generates keys for users within the organization. For users outside the organization, the SMSA enables users to enroll automatically using a variety of methods:

- **Smart Trailer –** PGP Universal Server appends a short message to outbound emails that permits an external user to choose how to secure future email messages sent by the organization. This option is used when the organization has decided not to require encryption to a particular external user, but wishes to provide the user with the option of enrolling in the SMSA to enable future messages to be secured.
- **PGP Universal Web Messenger –** PGP Universal Web Messenger is a secure, Web-based message delivery system that delivers messages via a Web-based mail interface. PGP Universal Web Messenger is used to send encrypted messages to external users prior to their enrollment in the SMSA or when a previously enrolled external user has selected PGP Universal Web Messenger as the preferred method of receiving secure messages from the organization.

Enrolling Internal Users

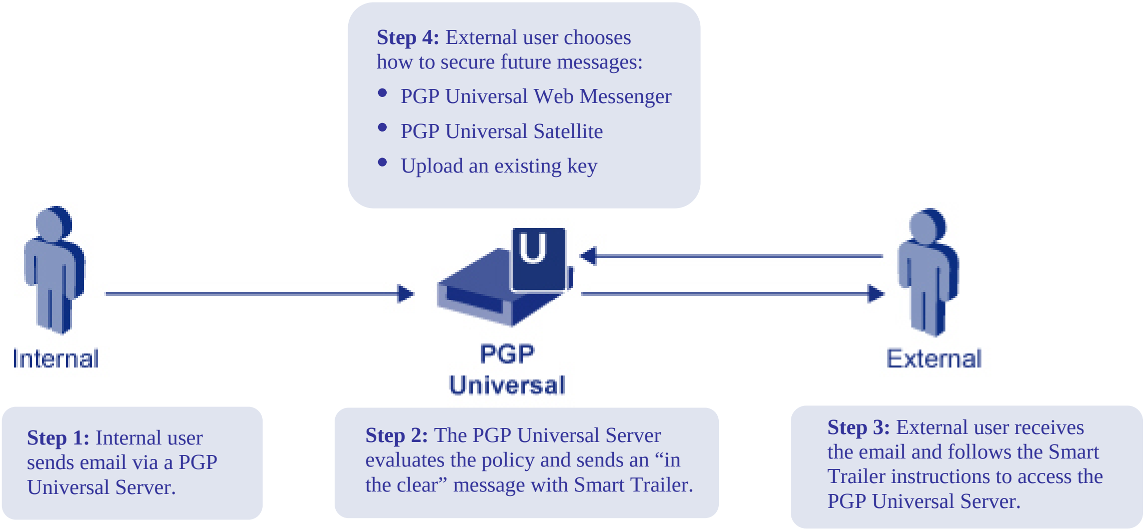
When a user inside an organization running PGP Universal sends an email, PGP Universal Server will observe the resulting mail traffic and use it to dynamically generate and store a key pair for the user if he/she does not already have one. PGP Universal Server will use the user's key pair to encrypt messages destined for that user and sign messages from that user, as dictated by policy. A key is automatically created each time PGP Universal observes an outbound email from an email address without an existing key.

If PGP Universal is deployed between the user's email client and the mail server, it will keep keys updated based on information obtained by observing each user's SMTP connection as he/she authenticates to the mail server via PGP Universal. This process allows PGP Universal Server to automatically detect the email aliases associated with a given user login and associate multiple email addresses with the same key, thereby avoiding creating multiple keys for the same user. If PGP Universal Server is deployed between the mail server and the Internet, it can use LDAP directory synchronization with any common enterprise directory such as Microsoft Active Directory to associate multiple email addresses with a single user.

Enrolling External Users

PGP Universal provides a solution to the fundamental question facing organizations that wish to encrypt their email communications: How can an organization extend security to external partners in a simple, flexible, incremental, and scalable fashion? An administrator can provide external users with the opportunity to enroll in the SMSA using either the Smart Trailer or PGP Universal Web Messenger features of PGP Universal. Once enrolled in the SMSA, an external user may continue to receive encrypted messages using PGP Universal Web Messenger, download and install PGP Universal Satellite, or upload an existing key or certificate. An administrator can configure a PGP Universal Server's policy to restrict which delivery options are made available to the recipient of a Smart Trailer or PGP Universal Web Messenger notification email.

Smart Trailer. A Smart Trailer consists of a short text message, configurable by the administrator, appended to an outbound email message by the PGP Universal Server. The message includes instructions enabling users to connect to the PGP Universal Server using their Web browser and choose how to secure future messages sent by that organization. An administrator can configure PGP Universal Server to send messages in the clear with a Smart Trailer appended to the message body in the event it cannot find a key for the message recipient.



Step 4: External user chooses how to secure future messages:

- PGP Universal Web Messenger
- PGP Universal Satellite
- Upload an existing key

Step 1: Internal user sends email via a PGP Universal Server.

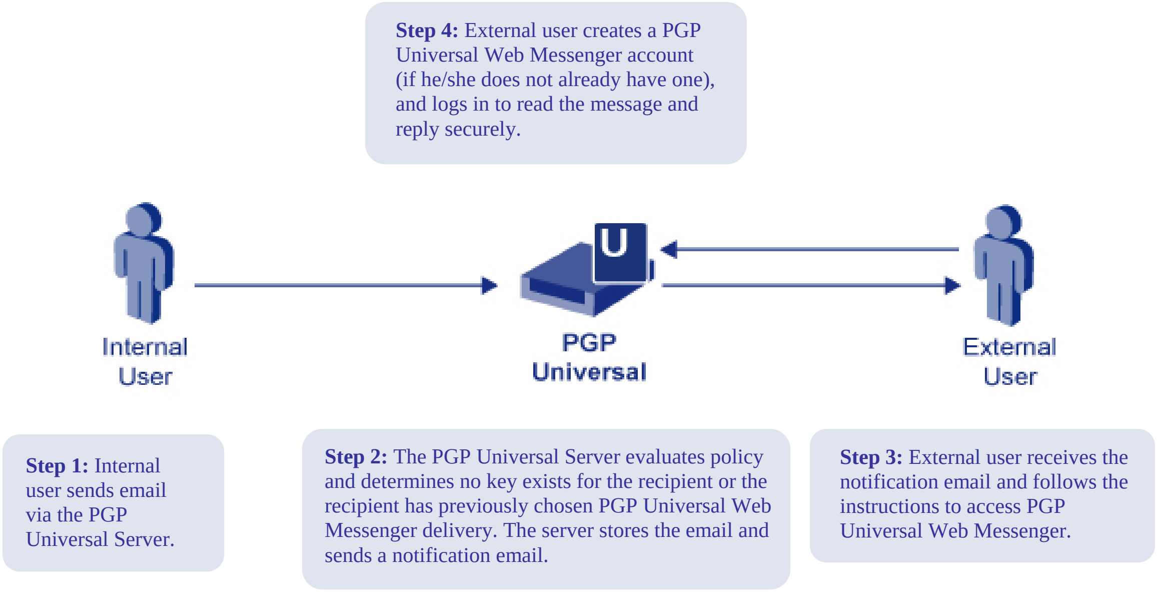
Step 2: The PGP Universal Server evaluates the policy and sends an "in the clear" message with Smart Trailer.

Step 3: External user receives the email and follows the Smart Trailer instructions to access the PGP Universal Server.

Figure 3: Using Smart Trailer to Choose Future Secure-Delivery Options

Smart Trailer provides a simple, ad hoc, low-impact mechanism to enroll external users in the SMSA on-the-fly and enable secure communications. When recipients follow the instructions included with the Smart Trailer, they are given the option to tell the PGP Universal Server how to secure future messages. For example, a user may choose to have all messages delivered via PGP Universal Web Messenger; alternatively, the user may upload an existing PGP key or X.509 certificate, enabling future messages from the PGP Universal Server to be automatically encrypted to that key. If enabled by the administrator, the recipient may also choose to download PGP Universal Satellite to enable secure email encryption from the native email client.

PGP Universal Web Messenger. PGP Universal Web Messenger is a Web-based secure-message delivery system that enables a user within an organization to send a message to an external recipient securely without requiring prior enrollment by the recipient. Not only does PGP Universal Web Messenger allow recipients to receive a message in a secure manner immediately, it also provides them with the opportunity to choose the method PGP Universal Server will use to secure future emails.



Step 4: External user creates a PGP Universal Web Messenger account (if he/she does not already have one), and logs in to read the message and reply securely.

Step 1: Internal user sends email via the PGP Universal Server.

Step 2: The PGP Universal Server evaluates policy and determines no key exists for the recipient or the recipient has previously chosen PGP Universal Web Messenger delivery. The server stores the email and sends a notification email.

Step 3: External user receives the notification email and follows the instructions to access PGP Universal Web Messenger.

Figure 4: Using PGP Universal Web Messenger to Securely Deliver Email

When PGP Universal intercepts an outgoing message that policy requires to be secured, the PGP Universal Server will attempt to find an existing key for the recipient. If the PGP Universal Server is unable to find a key for the recipient and the administrator has chosen to allow PGP Universal Web Messenger as a delivery option, the server will store the message locally and send a notification email to the recipient. The text of this notification email can be modified by the administrator to provide customized instructions to the recipient on how to act on the email notification.

When the recipient receives the notification email, he/she follows the enclosed instructions to go to the PGP Universal Web Messenger SSL-secured website hosted by the PGP Universal Server, authenticate with the server, and create a PGP Universal Web Messenger account. The user will be able to access his/her inbox at any time to securely view messages, download attachments, and respond to messages. The user’s PGP Universal Web Messenger inbox is subject to disk space quotas allocated by the PGP Universal Server’s administrator.

The PGP Universal Server’s administrator can choose to use either “First Time Good” (also called Implicit Trust) or “Out of Band” (also called Require Sender Authorization) authentication as the authentication mechanism employed the first time a user accesses PGP Universal Web Messenger. First Time Good authentication assumes that the first person to access the unique, secure Web page via the URL contained in the PGP Universal Web Messenger message is the intended recipient. Out of Band authentication causes PGP Universal to generate a passphrase and email it to the message sender; the sender must communicate the passphrase securely to the intended recipient via a means other than email to allow the user to authenticate with PGP Universal Web Messenger.

PGP Universal Satellite. For external recipients who regularly exchange messages with an organization, it may be preferable for them to enable secure messaging from within their native email client. PGP Universal Satellite allows recipients to be part of the SMSA—transparently enforcing policy as well as encrypting, decrypting, and signing messages—as if they were inside the organization’s firewall. It allows users to avoid using the Web-based interface of PGP Universal Web Messenger and instead receive and send email using their preferred email client.

PGP Universal Satellite is a small piece of software that acts as a local mail proxy; a user-specific key pair is generated either on the PGP Universal Server or by PGP Universal Satellite, depending on whether the administrator chooses to enable Server Key Mode (SKM) or Client Key Mode (CKM). In SKM, keys are generated and stored on the PGP Universal Server. In CKM, a key is generated and stored on the individual desktop client.

PGP Universal Satellite is offered to users when they receive a Smart Trailer or a PGP Universal Web Messenger notification email, provided the administrator has enabled use of PGP Universal Satellite. Once installed, PGP Universal Satellite downloads its policy from the PGP Universal Server and runs transparently on the user's computer, automatically encrypting messages to and from the PGP Universal Server in accordance with the organization's security policy. By dynamically downloading its policy from the PGP Universal Server, PGP Universal Satellite achieves two-way security and policy enforcement. Two-way policy enforcement allows an organization to encrypt outgoing messages to external users and also require external users running PGP Universal Satellite to respond to the organization using encrypted messages.

In cases where the user is in communication with multiple organizations running PGP Universal, PGP Universal Satellite can download and enforce policy provided by each organization without requiring multiple installations of PGP Universal Satellite on the user's computer.

Importing an existing PGP Key or X.509 certificate. In some cases, an external user may prefer to secure email communications using a preexisting encryption key. This key may be a PGP key generated by a preexisting installation of PGP Desktop or an X.509 certificate created by a Public Key Infrastructure (PKI) solution.

Upon following the instructions in a Smart Trailer or PGP Universal Web Messenger notification email, a user with an existing key can choose to upload the key to the PGP Universal Server, thereby enrolling in the SMSA and ensuring all future communications are encrypted. If a user uploads an X.509 certificate, PGP Universal Server will automatically send encrypted messages to that user using the S/MIME message format, allowing the user to continue using his/her existing X.509 certificate and S/MIME-based application.

Other Enrollment Options

PGP Universal supports several additional mechanisms for obtaining keys for recipients without requiring any intervention or enrollment:

- **Querying business partners' PGP Universal Servers –** If a business partner has a PGP Universal Server, then the sender's PGP Universal Server will automatically contact the business partner's PGP Universal Server to attempt to find a key for a recipient.
- **Querying business partners' LDAP directories –** An administrator can configure PGP Universal to consult a business partner's LDAP directory to attempt to find a key for a recipient in the business partner's domain. PGP Universal supports using client-certificates to access partner LDAP directories that require authentication.

By leveraging external sources of recipient keys, PGP Universal increases the likelihood of finding an existing key for a recipient and being able to securely deliver a message using an organization's existing infrastructure.

Key Management

In any organization, users are continuously joining, changing departments, or leaving, and the organization is constantly adding or removing business partners. Beyond automating the process of enrolling users, the SMSA provides capabilities to manage how keys are created, to enable corporate access to encrypted data (according to policy), and to expire inactive keys. By automating the key creation and expiration process, PGP Universal eliminates the administrative burden normally associated with these activities.

Managing Key Creation

When PGP Universal creates keys automatically, it does so in accordance with the key generation settings configured by the administrator. The key generation settings control:

- **Key size –** Keys generated by the server can be up to 4,096 bits in length.
- **Key type –** The type of key that will be generated by PGP Universal can either be RSA[3] or DH/DSS[4] keys.
- **Allowed ciphers –** Administrators can choose to enable support for individual ciphers, including AES, IDEA, CAST, Twofish, and TripleDES.

By choosing the key size, key type, and allowed ciphers used when generating keys, an administrator can ensure the keys used by PGP Universal comply with regulatory requirements, organizational security policies, or the security mandates of business partners.

Using Existing User Keys

Some organizations may have users that have keys generated using PGP Desktop or that have legacy X.509 certificates deployed as part of a preexisting PKI. An administrator can import keys for internal users into PGP Universal in one of three ways:

- **LDAP Directory Synchronization –** If users' certificates are currently stored in an LDAP directory, PGP Universal Server can synchronize with the directory to create users and import the existing certificates.
- **Manual key importation –** PGP Universal also lets an administrator manually add keys for internal users through the administrative interface. This process is useful for creating internal users when no corporate LDAP directory is used to manage existing keys and users have been responsible for creating and managing their own keys using individual installations of PGP Desktop.
- **PGP Verified Directory –** End users in an organization can be allowed to send their keys to the PGP Universal Server via LDAP or a Web interface. This option is primarily applicable to organizations wanting to continue dual deployment of older solutions such as PGP Desktop 8.x while deploying PGP Desktop 9.0.

Re-using existing keys allows an organization to provide an easy migration path from older solutions without requiring generation of new keys and certificates.

[3] Rivest-Shamir-Adleman
[4] Diffie-Hellman/Digital Signing Standard

Using an Additional Decryption Key (ADK)

For organizations with a regulatory or corporate security requirement to ensure access to encrypted data, PGP Universal supports adding an Additional Decryption Key (ADK) to user keys generated automatically by the PGP Universal Server. An ADK is a way to access an email message if the recipient is unable or unwilling to do so or if required by regulatory or corporate security policy.

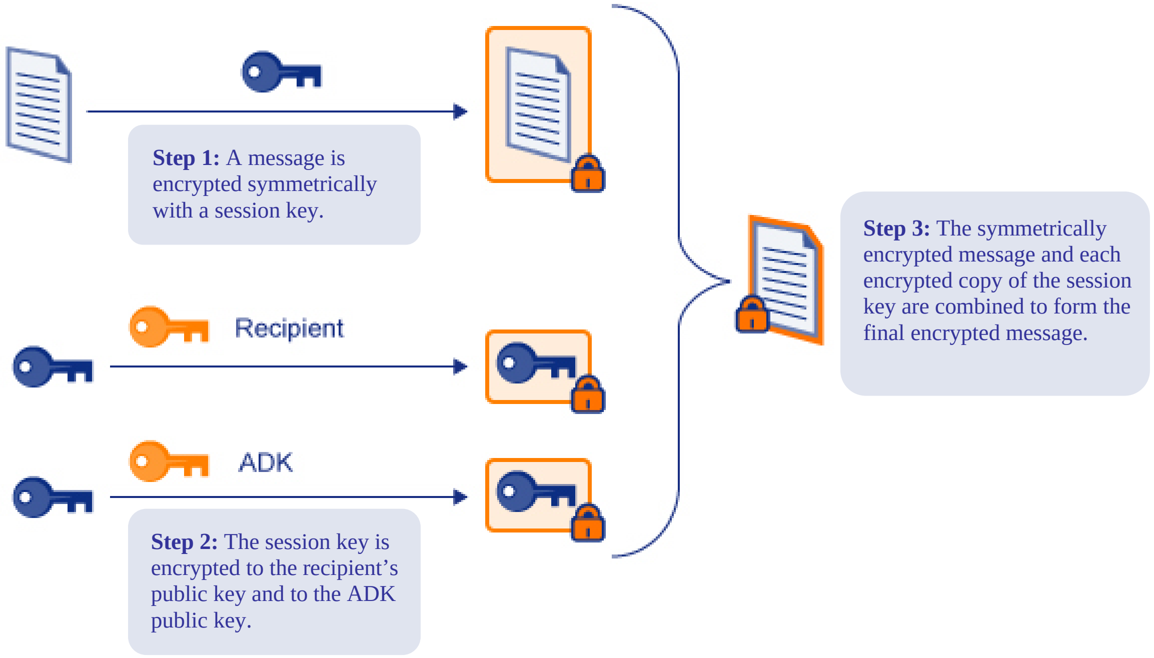

Step 1: A message is encrypted symmetrically with a session key.
Recipient
ADK
Step 2: The session key is encrypted to the recipient's public key and to the ADK public key.
Step 3: The symmetrically encrypted message and each encrypted copy of the session key are combined to form the final encrypted message.

Figure 5: Using the Additional Decryption Key (ADK)

When external users encrypt messages to a user's PGP key that contains an ADK, the message is also encrypted to the ADK, allowing the organization to access the encrypted data, if necessary. In essence, the ADK acts as an additional recipient for a PGP message, and hence a copy of the session key used to secure the message itself is encrypted to the ADK's public key. Both copies of the encrypted session key are stored along with the encrypted message; using the ADK does not require copies of the message. To access a message that has been encrypted to both a recipient public key and the ADK, an administrator uses PGP Desktop and the ADK's private key to decrypt the message.

In addition, every message sent by an internal user using PGP Universal is also encrypted to the ADK, ensuring that information flowing into and out of the organization can be access by authorized personnel if required by corporate or regulatory policy. The application of the ADK enables an organization to operate in compliance with corporate or regulatory data access requirements and ensure access to encrypted data in the event that a user's private key is lost or unavailable.

Key Auto-Renewal and Expiration

PGP Universal uses short-lived user keys to avoid the overhead associated with maintaining a directory of revoked keys. Keys created by PGP Universal are automatically renewed according to the schedule specified by the administrator; the default renewal period is 2 weeks. PGP Universal stops renewing the signature on keys automatically for users that have not sent email via PGP Universal within a period of time specified by the administrator; the default inactivity threshold is 3 months.

Keys that are no longer renewed by PGP Universal automatically expire, but remain in the PGP Universal Server unless they are deleted by the administrator. Expired keys are retained to allow PGP Universal, PGP Desktop, or PGP Universal Satellite to verify digital signatures created in the past by a user.

PGP Verified Directory

PGP Universal's Verified Directory feature gives an organization the option of hosting a Web-accessible keyserver for the public keys of its internal users. The PGP Verified Directory lets users manage their own keys, including submitting and removing them, as desired. Specifically, the PGP Verified Directory sends verification email messages to the email addresses on keys submitted to it. If the key owner responds to the verification message with permission to add the key, then the key is added to the directory. Once the PGP Verified Directory accepts an uploaded key, the verified key is used by PGP Universal to encrypt messages.

This automated vetting of user-submitted keys keeps the PGP Verified Directory free of useless keys and protects users' privacy by foiling third-party attempts to upload fraudulent keys that use a user's email address. Additionally, the PGP Verified Directory lets the owner of a key remove it from the directory even if the passphrase has been lost, thus preventing the buildup of unusable keys. Finally, the PGP Verified Directory lets users search the directory for the public keys of individuals to whom they want to send encrypted messages.

Security Policy Enforcement

PGP Universal allows an administrator to control when encryption should be used to protect an outgoing email message. This automated application of security policy relieves the user of the burden of deciding which messages need to be encrypted while providing an organization with the ability to enforce its security policy and comply with regulatory or corporate security mandates.

Centrally Enforced Message Security

PGP Universal allows an administrator to configure security policies on a per-domain basis. For a specified recipient domain, the administrator can configure the policy to require messages to be encrypted to the intended recipient's key, signed by the sender's key, or both encrypted and signed. In the event the policy requires the message to be encrypted but the intended recipient has no existing key, PGP Universal's behavior depends on whether the intended recipient is part of a domain managed by the PGP Universal Server or an external user in a domain not managed by the PGP Universal Server.

If the intended recipient is part of an external domain not managed by the PGP Universal Server, the administrator can configure PGP Universal to deliver the message using one of the following options:

- **PGP Universal Web Messenger –** The recipient will receive a notification email containing a link to a website that will allow him/her to read the email and respond securely.

- **Smart Trailer –** The email will be sent in the clear, but a Smart Trailer will be appended to the message, allowing the user to choose how to receive future messages requiring secure delivery.
- **Reject the message –** The message will be bounced back to the sender without sending anything to the intended recipient.
- **Send in the clear –** The message will be sent to the recipient unencrypted.

Because PGP Universal handles automatically enrolling internal users into the SMSA, it is unlikely an internal user will not have a key. However, in the event the intended recipient is an internal user for whom no key currently exists, PGP Universal can either block the message or send it unencrypted, as dictated by the policy set by the administrator.

User-Initiated Message Security

In some cases, an organization may wish to provide its end users with the ability to trigger encryption on an ad-hoc basis. In these cases, an administrator can enable users to trigger encryption based on one of these methods:

- **A specified keyword in the Subject –** A user can trigger encryption of a message by using an administrator-specified keyword in the Subject line of the email. For example, the administrator could configure PGP Universal to encrypt an email if the Subject line contains “[Sensitive]”.
- **The “Confidential” flag –** A user can trigger PGP Universal to secure a message by setting the “Confidential” flag supported by the email client. When PGP Universal handles a message containing the “Confidential” flag, it will attempt to deliver the message securely using the methods specified in the policy set by the administrator.

When encryption is triggered using either of these methods, PGP Universal will attempt to encrypt a message to the recipient’s email address. If no key exists for the recipient’s email address, PGP Universal will either deliver the message by sending a PGP Universal Web Messenger notification email, an email with a Smart Trailer, or an unencrypted message, or will bounce the message back to the sender in accordance with the policy configured by the administrator.

Deployment Options

PGP Universal provides flexible deployment options that allow an organization to tailor the PGP Universal Server to its needs while minimizing the impact on IT infrastructure. PGP Universal leverages existing resources and technology investments by adopting a protocol and message-format agnostic approach:

- PGP Universal supports standard Internet network protocols using SSL/TLS plus standard SMTP, POP3, and IMAP4 email protocols.
- PGP Universal Satellite supports MAPI for interoperability with Microsoft Exchange environments and Lotus Notes for interoperability with Lotus Notes environments.
- PGP Universal supports S/MIME v3 (128-bit or greater key length) and X.509 certificates.

Deployments of PGP Universal fall into one of three categories:

- **End-to-End deployment –** The PGP Universal Server is deployed between end users and their mail server to provide transparent message security while maintaining messages on the mail server in an encrypted form.
- **Managed PGP Desktop deployment –** The PGP Universal Server is used to deploy and manage the features used by PGP Desktop clients inside the organization and enforce use of PGP Virtual Disk and PGP Whole Disk.
- **Gateway-based deployment –** The PGP Universal Server is deployed in the mail stream between the organization's mail server and the Internet to provide transparent encryption of outgoing messages according to policy and decryption of incoming messages.

Organizations deploying PGP Universal may also use a combination of the deployment scenarios outlined above to address the specific security requirements of individual departments.

End-to-End Deployment – PGP Universal Series 500

The PGP Universal Server is deployed in End-to-End Mode in organizations that require email messages to be encrypted from the moment they leave the sender's machine to the moment they are received by the recipient. In this mode, PGP Universal ensures messages are stored in an encrypted form on an organization's mail servers and secured from unauthorized access. End-to-End Mode provides end-to-end email security while preserving the email user experience and providing centralized management of internal and external policy.

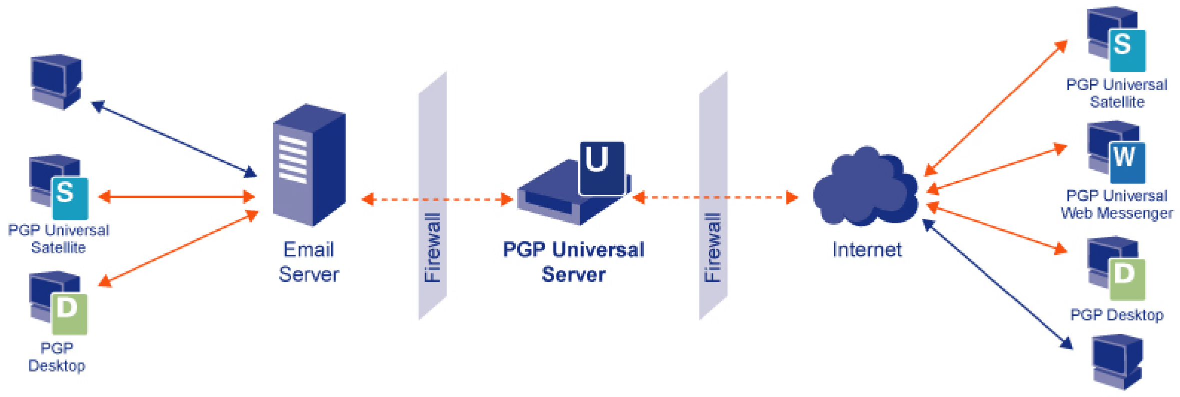


Figure 6: Deploying PGP Universal in End-to-End Mode

When deployed in End-to-End Mode, the PGP Universal Server resides in the mail stream between the organization's mail transport agent (MTA) and the public Internet. For external recipients without a key, PGP Universal provides PGP Universal Web Messenger delivery, PGP Universal Satellite deployment and policy management, and support for existing PGP Desktop and legacy X.509 certificate users. Internal deployments of PGP Desktop are managed centrally by PGP Universal, enabling individual control of message encryption and deployment of PGP Virtual Disk and PGP Whole Disk to enforce local document storage security policy.

Managed PGP Desktop Deployment – PGP Universal Series 200

A PGP Desktop deployment managed by PGP Universal provides an end-to-end email and local storage encryption solution for organizations looking to secure strategic internal workgroups.

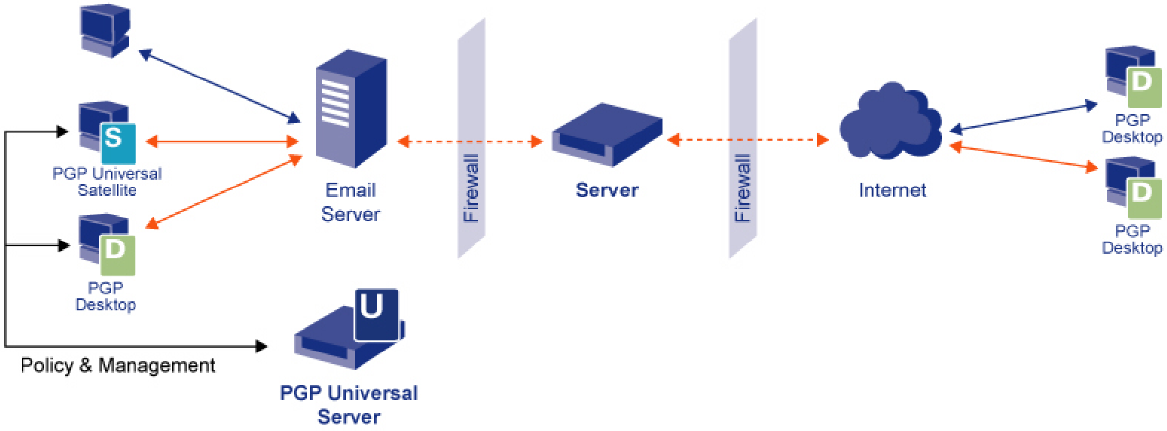


Figure 7: Managing PGP Desktop Deployments with PGP Universal

PGP Desktop allows desktop users to choose when it is most appropriate to encrypt outgoing emails sent from their email client. Users can configure local content filters and policies to automate the application of encryption to outgoing email messages or trigger encryption of selected individual messages using a specific subject keyword or the Outlook “Confidential” flag.

The PGP Universal Server administrator can require individual PGP Desktop installations to create a key, upload the key to the server, and create a PGP Virtual Disk to encrypt documents. For desktop users handling confidential documents on laptop systems, administrators can enable PGP Whole Disk functionality to protect the entire hard drive using non-stop encryption to secure user documents as well as operating system files. PGP Universal also allows central administration of PGP Whole Disk Recovery Tokens to enable remote access to a PGP Whole Disk-secured machine in the event an end user forgets the key’s passphrase.

Gateway-Based Deployment – PGP Universal Series 100

For organizations that require a simple, transparent solution to encrypt email sent to external business partners, PGP Universal can be deployed as a gateway encryption solution. In Gateway Mode, the PGP Universal Server resides between the organization’s MTA and the public Internet, and proxies SMTP connections to allow PGP Universal to intercept messages, encrypt and sign outgoing messages, and decrypt and verify incoming messages as dictated by policy.

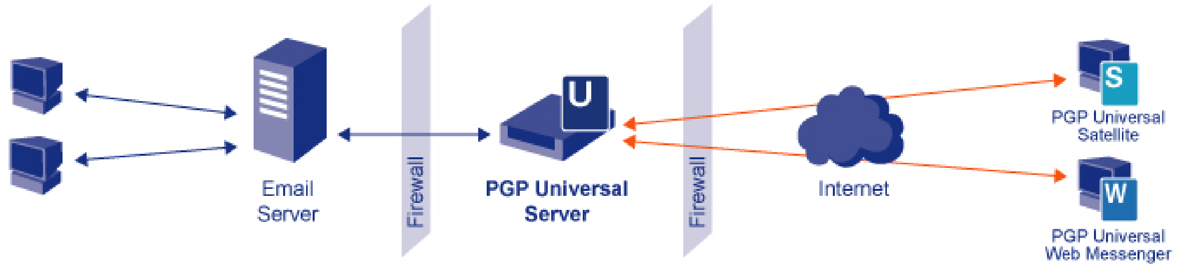


Figure 8: Deploying PGP Universal in Gateway Mode

For outgoing email requiring encryption to a recipient with no key, the PGP Universal Server stores the message and sends an email notification to allow the recipient to retrieve the message via PGP Universal Web Messenger over SSL. PGP Universal enables automated enrollment of new users in the SMSA using either Smart Trailer or PGP Universal Web Messenger, enabling future secure communications via PGP Universal Web Messenger, PGP Universal Satellite, or an existing X.509 certificate.

Other Deployment Considerations

Learn Mode

Many organizations want to test and fine-tune products before deployment. PGP Universal features a Learn Mode—a rehearsal setting where the server observes network traffic and logs the various security-related operations it would have performed, without actually encrypting, signing, decrypting, or verifying messages.

Learn Mode lets system administrators test security policy, review logs, and adjust settings before making the PGP Universal Server operational. When an administrator finishes configuring the PGP Universal Server using the Setup Assistant, it automatically begins operation in Learn Mode. This preview of what PGP Universal would be doing to email traffic if it were live allows administrators to continue to make changes to the server's policies until things are working as desired.

Learn Mode also gives the PGP Universal Server a chance to apply the Self-Managing Security Architecture—creating keys for authenticated users, for example—so that when Learn Mode is turned off, the server knows the environment and can immediately begin encrypting messages.

Clustering

An organization can have many PGP Universal Servers, such as one for each department or workgroup, with each group having different security policies if such a configuration best meets security needs. Another alternative is to cluster PGP Universal Servers together.

PGP Universal Servers can be configured in clusters, all sharing the same policy and repository of keys. Different clusters may have different recipient domain policies, even for the same domains. If an ADK is defined for the primary PGP Universal Server in the cluster, its use is automatically enforced by all servers in that cluster. PGP Universal Servers operating in a cluster synchronize keys, policies, and domain-specific preferences and provide failover capability for other servers in the cluster when used with appropriate load balancing hardware. To ensure administrative control, one of the PGP Universal Servers in the organization is designated as the primary server and the others are designated as secondary servers.

A cluster's primary server is the authoritative keeper of certificates, policy, and domain-specific information on all matters relating to PGP Universal. It is the administrative server the IT staff uses to initiate policy changes throughout all the PGP Universal Servers in an organization. To prevent the insertion of a rogue PGP Universal Server into a network, the primary PGP Universal Server maintains an authenticated list of secondary servers from which it will accept updates and to which it will send them.

The primary PGP Universal Server keeps database information synchronized and current with its secondary servers, so that if a secondary server goes down, the primary server knows which of its files must be updated once the secondary server returns to fully functional network operation.

This clustering architecture also allows new secondary servers to be deployed quickly. Once a new server is visible on the network and has been introduced to the primary server, the latter automatically synchronizes all organization-specific policies and settings.

MTA Deployment

PGP Universal also supports deployment in conjunction with an MTA to support anti-virus, anti-spam, and content filtering for organizations requiring integration of email encryption with the existing email hygiene infrastructure.

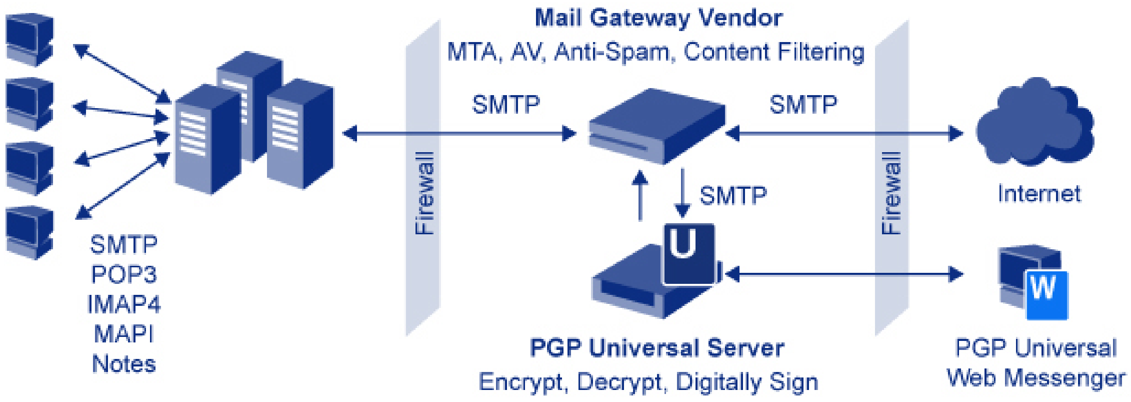


Figure 9: Deploying PGP Universal with an MTA

In this deployment scenario, the MTA has the responsibility for inspecting messages and determining, based on content-filtering rules, whether or not to forward the message to the PGP Universal Server for encryption or decryption. Outgoing messages containing confidential information are forwarded to the server to be encrypted and delivered; incoming encrypted messages are forwarded to the server for decryption before being passed back to the MTA for final delivery.

Deploying PGP Universal in conjunction with an MTA has the advantage that the server only needs to process email that must be encrypted, allowing an organization to secure, rather than quarantine, outgoing messages containing confidential information. Deploying PGP Universal with an MTA allows an organization to comply with regulatory mandates requiring rules-based security and also achieve granular application of policy that allows non-disruptive deployment of email encryption to select user groups.

The Administrative Interface

The PGP Universal Server's Web-based administrative interface controls all aspects of the operation of the server.

Through the administrative interface, an administrator can manage the following functionality:

- **Policy –** Allows the administrator to configure the encryption policies enforced on email domains managed by the PGP Universal Server and designate trusted keys to be used to establish trust relationships with keys retrieved from business partners' key directories. The administrator can also define policy through the creation of custom PGP Universal Satellite and PGP Desktop installers.
- **Users –** Permits the administrator to add, edit, and delete the user information in keys and email addresses stored by the PGP Universal Server and manually import and export user keys, including X.509 certificates. An administrator with the appropriate permissions can also add, edit, and delete administrators for the PGP Universal Server.
- **Mail –** Enables the administrator to alter the PGP Universal Server's proxy configuration and mail routing as well as configure use of the optional Symantec AntiVirus Scan Engine. The administrator can also customize the content of email messages sent by the PGP Universal Server to enroll users via Smart Trailer and PGP Universal Web Messenger as well as other notification emails.
- **Organization –** Allows the administrator to configure the Organization Key, which the PGP Universal Server will use to sign keys it hosts, and the Additional Decryption Key (ADK) to be used to enable access to encrypted messages.
- **Services –** Permits the administrator to configure the operation of the PGP Universal Web Messenger, the internal PGP Keyserver, the PGP Verified Directory, and the Simple Network Management Protocol (SNMP) capabilities of the PGP Universal Server.
- **System –** Allows the administrator to backup and restore the server, update the PGP Universal Server software, and configure cluster, network, and ignition key settings.
- **Reporting –** Allows the administrator to view system graphs and log files reporting on the status of the PGP Universal Server.

Managing Server Access

PGP Universal provides two mechanisms to limit and manage access to the server's administrative functionality: role-based administration and ignition keys. Limiting access to the server's configuration ensures that only authorized personnel have access to user information and keys and authorization to start, stop, or alter the server's operation.

Role-Based Administration

PGP Universal features role-based administration, allowing an organization to partition administrative responsibilities among several administrators. PGP Universal supports the following administrator roles:

- **Read-Only Admin –** Provides access to a PGP Universal Server to IT support administrators for diagnostic or auditing purposes. These administrators are given the ability to examine the configuration of the server, but cannot make changes to it.
- **Service Admin –** Provides all the capabilities of a Read-Only Admin plus the ability to restart the PGP Universal Server services.
- **Basic Admin –** Provides all the capabilities of a Service Admin plus the ability to perform the day-to-day operations required to start, stop, and backup the PGP Universal Server as well as add or remove users.
- **Full Admin –** Provides all the capabilities of a Basic Admin plus the ability to manage users' private keys, configure clustering, and manage organization, trusted, ignition, and Additional Decryption Keys (ADKs).
- **Super User –** Provides all the capabilities of a Full Admin plus the ability to add or remove administrators and access the PGP Universal Server via SSH.

Role-based administration increases server security by limiting each administrator to only those privileges needed to perform the appropriate tasks. This approach allows an IT organization to spread administrative tasks across multiple administrators without providing unrestricted access to the PGP Universal Server.

Ignition Key Support

Ignition Keys protect the data on a PGP Universal Server in case an unauthorized person gains physical control of it. PGP Universal Server supports two kinds of Ignition Keys:

- **Soft-Ignition Passphrases –** A Soft-Ignition Key protects the PGP Universal Server with a passphrase.
- **Hardware Ignition Keys –** A Hardware Ignition Key protects the PGP Universal Server with a PKCS-11 token.

The Ignition Key is used to encrypt user keys and the Organization Key, thereby preventing unauthorized access to private keys stored on the PGP Universal Server. When configured to use an Ignition Key, the PGP Universal Server will require the Ignition Key to start the server's services; once the server has started, the administrator can safely remove the Ignition Key.

Server Monitoring & Maintenance

SNMP Monitoring

PGP Universal Server supports monitoring of the server health using SNMP, allowing an administrator to use standard monitoring applications. SNMP monitoring enables an administrator to read a variety of server attributes, including CPU load, available hard drive space, and network traffic, enabling real-time inspection of server performance as well as proactive system capacity planning.

Logging & Reporting

One goal of PGP Universal's design is to provide network administrators with as much information as possible about server operations. Any time a PGP Universal Server is asked to process a message or respond to a query, it time-stamps the request, uses the policy engine to determine how to proceed, and then logs any actions taken, based on the policy.

PGP Universal Servers provide statistics and metrics to system administrators and generate email synopses of their operation. These synopses contain information about the total number of messages sent, the number of users who sent messages, and other pertinent figures. PGP Universal's Administrative Interface allows IT staff to choose what kind of filters are to be applied to log data when viewing it without affecting the amount of logging that occurs. PGP Universal allows network administrators to make choices about which kinds of data have priority for retention and examination as well as what level of detail will be associated with this data.

PGP Universal keeps logs for each server that are compressed and backed up to the designated backup system. Log information can also be sent to an existing remote syslog server for central log gathering.

Server Backups

All PGP Universal Server backups are encrypted with the Organization Key, guaranteeing that backup data is never in a decrypted state when it is not on a PGP Universal Server. PGP Universal Server backups can be sent via File Transfer Protocol (FTP) to any location a network administrator specifies. Therefore, in the unlikely event of a catastrophic hardware failure of a PGP Universal Server, all keys and operational data have been securely stored elsewhere. All the domain, network-specific, and operational information needed to set up a replacement PGP Universal Server is safely stored and retrievable outside the server. Restoration via a fresh installation using the PGP Universal Server backup takes just a few minutes.

Managing PGP Universal Satellite & PGP Desktop

PGP Universal offers customers a choice of modes that determine where to store users' keys, providing flexibility while balancing digital signature requirements with electronic signature automation and the needs of mobile PGP Universal Satellite users.

PGP Universal Satellite Key Generation & Storage Administration

Even with the automatic, network-based encryption provided by PGP Universal, some individuals within an organization may require the ability to manage their own keys, as they do with today's PGP Desktop software. PGP Universal accommodates this requirement by allowing administrators to specify which users can manage their own keys. However, these individuals still must conform to the defined security policy. Messages that are already encrypted before the PGP Universal Server receives them are still checked against policy. For example, if an organization's policy requires the use of an ADK, the PGP Universal Server will ensure the ADK is used in all encrypted messages, even those from individuals who manage their own keys. Messages that do not conform to policy will be rejected.

The PGP Universal Server client can be configured for management of the user's private and public key pair in one of two ways: Client Key Mode (CKM) or Server Key Mode (SKM). An organization's decision to choose CKM or SKM depends on its security policy as well as the need for strong authentication versus ease-of-use and administration. It is possible for an organization to have both CKM and SKM deployed. It is also possible that a specific user may be an external user of multiple PGP Universal Server domains where the key management mode is different for those organizations.

- **Server Key Mode (SKM)** – In SKM*,* the PGP Universal Server is responsible for generating and storing both the user's private key and public key, but all cryptographic operations are performed by the computer on which PGP Universal Satellite is installed. The PGP Universal Server temporarily sends the private key to PGP Universal Satellite via SOAP/TLS once the user has been authenticated. PGP Universal authenticates the user either by observing the authentication to the mail server over SMTP, POP, and IMAP or by authenticating the roundtrip email path in the case of MAPI and Lotus Notes. The private key is stored only on the PGP Universal Server, and the server handles all private key management.
- **Client Key Mode (CKM)** – In CKM, all cryptographic operations are performed by the computer on which PGP Universal Satellite is installed. The private key stays on that computer (that is, the private key is not transmitted to the PGP Universal Server unless the user chooses to store it there encrypted); the computer also handles all private key management. CKM is intended for those end users who need control over their private keys. Users often invoke this mode when a higher level of user authentication is required or when the user's data must also be secured from IT staff. This higher-level authentication comes from prompting the user for a passphrase during a session or interfacing to a PKCS#11-compatible hardware token.

  Users who choose CKM can also choose to have an encrypted copy of their private key stored on the local PGP Universal Server (the original private key is stored on their computer). Synchronizing their private key with the PGP Universal Server is useful for CKM users if a key is accidentally deleted or they want to access their key and the policy to which it applies from a different computer: the private key will be provided when needed, but because it is stored encrypted, the PGP Universal Server cannot do anything with it. The user will need to use the same passphrase for the key from any system where this mobile key is used.

Management of PGP Desktop Deployments

PGP Desktop is typically deployed when individual users require an additional level of control over the encryption of email communications in combination with desktop storage security. PGP Universal provides administrators with a centralized management console to deploy and administer large installations of PGP Desktop. Centralized management allows an administrator to enable or disable the following functions of PGP Desktop to enforce corporate security mandates.

- **Multiple policy configurations –** Administrators can define groups of users based on LDAP attributes, thereby allowing an administrator to assign a group of users with the same configuration options for PGP Desktop.

- **Dynamic configuration of PGP Desktop –** PGP Desktop can be deployed to retrieve configuration information from a PGP Universal Server and adjust its behavior according to the centrally administered configuration for the user. When combined with LDAP-driven group definitions, this feature simplifies the process of modifying a user's PGP Desktop configuration when he/she changes organizational units and also eliminates any need to reinstall PGP Desktop.
- **Customized PGP Desktop installers –** PGP Universal can generate a preconfigured PGP Desktop installer that binds the installation of PGP Desktop to a specific policy on the PGP Universal Server. The policy can then be changed on the server and the client automatically receives the updates. This functionality allows an organization to define different policies for different groups of users; for example, members of the Human Resources department can be assigned a different policy from the Engineering department.
- **Centralized policy administration –** PGP Desktop will download domain-based encryption policies from a PGP Universal Server to augment encryption policies created by the user in PGP Desktop. The PGP Universal administrator determines whether or not an end user has the privilege to create his/her own policies. The user's PGP Desktop policies cannot be used to circumvent the encryption policies specified by the PGP Universal Server.
- **Centralized update control –** When PGP Desktop is used in conjunction with PGP Universal, the PGP Universal Server is responsible for retrieving and distributing software updates obtained from PGP Corporation's update service. This functionality allows a PGP Universal administrator to choose the appropriate time to distribute software updates to users.
- **Centralized license management –** The PGP Universal Server tracks the number of deployed PGP Desktop installations associated with each license to allow the administrator to observe the ratio of PGP Universal Satellite and PGP Desktop clients synchronizing policy. Policy groups can also be migrated instantly from an expiring license to a new license or from a license that does not activate PGP Whole Disk to a license that does. End users never need to enter a license into deployed clients.
- **Management of PGP Virtual Disk and PGP Whole Disk –** For users that need desktop storage security, PGP Universal can require a PGP Desktop user to deploy PGP Virtual Disk automatically to provide encryption for isolated documents requiring additional protection. In cases where users require more comprehensive document security to protect all data on a system, such as a mobile laptop computer, PGP Universal can require deployment of PGP Whole Disk to provide comprehensive encryption of the user's entire hard drive, including free space and virtual memory swap files.

Summary

PGP Universal offers organizations the ability to encrypt email communications with both internal and external users, eliminating the need for either administrators or users to take action. PGP Universal achieves this security by providing the following:

- **Automated key distribution within the PGP Ecosystem –** The PGP Universal Server cooperates with other components of the PGP Ecosystem—other PGP Universal Servers, PGP Desktop, and PGP Universal Satellite—to automate the exchange of encryption keys required to enable secure messaging.
- **A Self-Managing Security Architecture –** PGP Universal's Self-Managing Security Architecture relieves administrators of the burden of creating and managing user's keys. The PGP Universal Server enrolls internal users automatically and facilitates enrollment of external users via PGP Universal Web Messenger and Smart Trailer. For both internal and external users, the PGP Universal Server manages the process of generating keys as needed, leveraging preexisting encryption keys, serving keys to external business partners, and managing the key lifecycle.
- **Automated enforcement of security policy –** PGP Universal transparently enforces security policy, thereby eliminating the need for a user to take action when attempting to send an email securely. Whether deployed in the mail stream or deployed out of the mail stream as a policy management console for PGP Desktop, the PGP Universal Server provides a centralized mechanism to ensure an organization's confidential information is protected with strong encryption in accordance with corporate or regulatory security mandates.
- **Deployment flexibility –** The PGP Universal Server can be deployed in the mail stream to provide either organization-wide, transparent, gateway-based security or end-to-end security, or deployed out of the mail stream as a management console for tactical PGP Desktop installations.
- **Centralized administration –** The PGP Universal Server's administrative interface enables an organization to centrally manage, maintain, and monitor all aspects of its secure messaging infrastructure while limiting access to that infrastructure to authorized personnel.

It is this unique approach to automating and simplifying email encryption that allows PGP Universal to overcome the fundamental challenges that previously prevented organizations from successfully rolling out secure messaging to internal users and external partners.

PGP Corporation
3460 West Bayshore Road
Palo Alto, CA 94303 USA
Tel: +1 650 319 9000
Fax: +1 650 319 9001
Sales: +1 877 228 9747
Support: www.pgpsupport.com
www.pgp.com

The information in this document is provided "as is" without warranty of any kind, either express or implied, including, but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement.

This document could include technical inaccuracies or typographical errors.

All strategic and product statements in this document are subject to change at PGP Corporation's sole discretion, including the right to alter or cancel features, functionality, or release dates.

Changes to this document may be made at any time without notice.