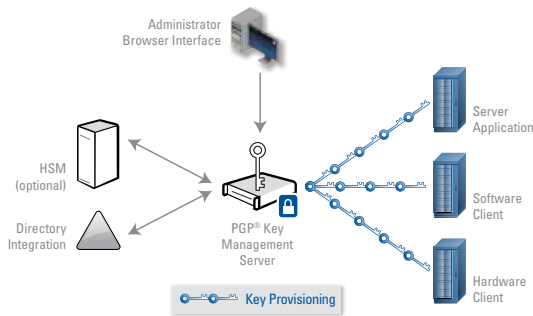
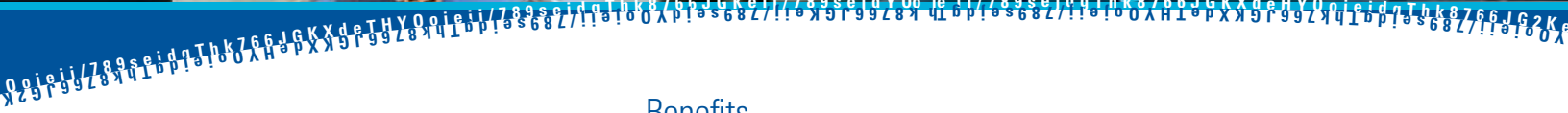




# PGP® Key Management Server

Manage cryptographic keys throughout the enterprise



**PGP® Key Management Server provides central administration for encryption keys and certificates.**

## Analyst Spotlight

If you currently have encryption in a variety of areas, then it is important to start evaluating enterprise key management solutions as part of your road map of data protection.

Gartner, Inc. – Hype Cycle for Data and Application Security, July 2009

## Benefits

- **Pare down operational cost and complexity** – Maintaining multiple key repositories requires extensive labor, resources, and expertise. PGP® Key Management Server simplifies the environment with a consistent administrative interface.
- **Reduce risk of unrecoverable data** – Ensure that dependable key recovery methods are in place before the need arises.
- **Prevent unexpected downtime** – Unanticipated certificate expirations can bring business to a standstill. Automate certification updates and eliminate certificate accidents that lead to system outages.
- **Stay in control** – IT leaders need to know if their security policy matches reality. Key management helps organizations account for encryption keys throughout their environment and demonstrate proof of compliance.

## Building a Better Encryption Strategy

Encryption is an essential element of any data protection plan. It applies from the employee desktop to the data center and the cloud, and all points in between. IT organizations are adding cryptographic measures to maintain consumer privacy, preserve data integrity, avoid data loss, prevent intrusions, and address compliance demands. Each new data protection technology contributes to a growing volume of keys that need to be managed, and fractures the hope of maintaining control.

Key management is the single most important element of an enterprise encryption strategy, and organizations often struggle to develop a comprehensive plan to address all of its intricacies. The challenge for the enterprise is to develop a plan that addresses how to deploy a growing volume of encryption technologies using a strong backbone for key management.

## Introducing PGP Key Management Server

PGP® Key Management Server provides organizations with the infrastructure and tools to manage large scale deployments of encryption keys and certificates for multiple applications. Instead of using proprietary standalone key repositories or custom single purpose tools, PGP Key Management Server delivers a better approach to managing encryption keys, built on design for supporting different types of keys, trust models and applications.

PGP Key Management Server provides a versatile foundation to centralize management of encryption throughout the enterprise to help organizations take control over their encryption keys, strengthen security, and reduce operational cost.

## Services

- **Author and enforce policy** – Control administrative processes and key attributes through policy. Use policy to ensure that the environment operates within expected parameters.
- **Automate administrative tasks** – Automate common tasks to reduce administrative effort and increase efficiency.
- **Generate key material** – Create keys and certificates for use with different applications. PGP Key Management Server includes support for asymmetric keys and certificates (including X.509 and OpenPGP), symmetric keys as well as proprietary keys.
- **Provision** – Provisioning works together with policy and automation to automatically deliver keys and certificates to applications.
- **Organize, protect and store keys** – Store keys within the protected, fault-tolerant, high-availability database. Restrict access with centralized control over authentication and access rights. Recover keys with the appropriate processes and workflow. PGP Key Management Server supports integration with a hardware security module (HSM).
- **Manage** – Oversee lifecycle management for distributed keys from the web-based administrative console.
- **Track** – Avoid compliance and audit issues by having full accountability for encryption keys used throughout the enterprise.

## Usage Scenarios

- **Certificate management** – Automate management for X.509 and SSL certificates. Centrally track certificate expirations and provision new certificates to clients automatically. Eliminate the risk of certificates accidentally expiring in production.
- **Distributed encryption** – Many organizations have individual business units that need to perform encryption operations. PGP Key Management Server provides the flexibility to distribute the encryption tasks to the business unit while maintaining a central repository to manage keys. For greater security, clients can perform cryptographic operations without local copies of the private key.
- **Managed secure file transfer** – Replace locally managed keys with PGP Key Management Server and PGP® Command Line. Support various configurations of key distribution.
- **Provide keys/certificates for in-house development** – Application developers can focus on business logic and implement security operations more easily without having to build their own key management.

## Components

- PGP Key Management Server
- PGP Key Management Client Access
  - PGP Key Management Client Access Agent – Client for rapid integration
  - PGP Key Management Client Access SDK – Software library for developers
- PGP Command Line – A multipurpose and multiplatform encryption client that uses PGP Key Management Server.

## A Part of the PGP Encryption Platform

In addition to support for 3rd party applications, the PGP Key Management Server also includes the same administrative capabilities for PGP® Encryption Applications as the PGP Universal™ Server. Organizations can use PGP® Encryption Applications to protect employee computing resources and leverage the same infrastructure to manage keys used in third party applications.



[www.pgp.com](http://www.pgp.com)

© 2010 PGP Corporation. PGP and the PGP logo are registered trademarks of PGP Corporation. Product and brand names used in the document may be trademarks or registered trademarks of their respective owners. Any such trademarks or registered trademarks are the sole property of their respective owners.

KMSDS100216