

PGP Corporation

Leveraging your RSA SecurID Token Deployment for Enterprise Data Protection on the Endpoint



Partner Brief

About PGP Corporation

PGP Corporation is a global leader in email and data encryption software for enterprise data protection. Based on a unified key management and policy infrastructure, the PGP® Encryption Platform offers the broadest set of integrated applications for enterprise data security. PGP® platform-enabled applications allow organizations to meet current needs and expand as security requirements evolve for email, laptops, desktops, instant messaging, smartphones, network storage, file transfers, automated processes, and backups.

Business Challenge

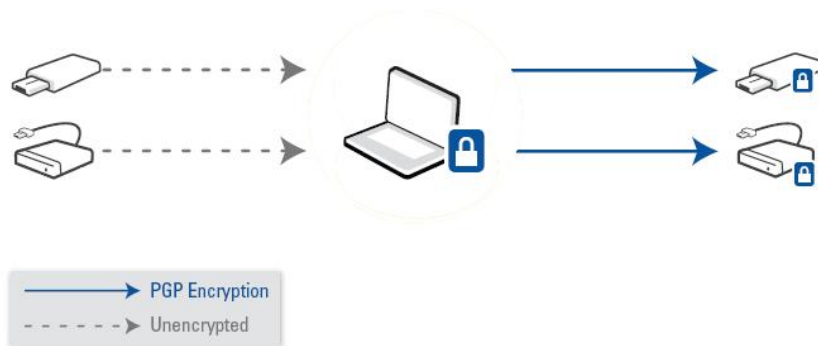
To prevent data breaches and address regulatory compliance, organizations are deploying strong authentication to uniquely validate the identity of users. This enables organizations that have deployed both RSA SecurID technology and award-winning PGP® Whole Disk Encryption to gain further leverage in their investment and enforce two-factor authentication policies alongside enhanced data protection for data on laptops, desktops, and removable media.

PGP Whole Disk Encryption provides comprehensive, non-stop disk encryption, enabling quick, cost-effective protection for data on PCs, laptops, and removable media. The encrypted data is continuously safeguarded from unauthorized access, providing strong security for intellectual property, customer and partner data, and corporate brand equity. PGP Whole Disk Encryption is technically interoperable with the RSA SecurID SID800 hardware authenticator to control access to systems at pre-boot authentication, preventing unauthorized use even before the operating system boots or resumes.



Solution Summary

RSA Authenticators and PGP Whole Disk Encryption combine seamlessly to provide end-users with a single form factor for laptop and desktop encryption. The PGP solution provides end-users with Preboot authentication, file and disk encryption, and Microsoft® Outlook mail encryption for PGP/MIME messages.



Comprehensive defense for local and remote media.



Solution Description

Mobile computers are quickly emerging as the industry standard for increasing user productivity. However, the portable nature of these devices increases the possibility of loss or theft. Consequent exposure of sensitive data can result in financial loss, legal ramifications, and brand damage.

PGP Whole Disk Encryption provides enterprises with comprehensive, nonstop disk encryption, enabling quick, cost-effective protection for data on PCs, laptops, and removable media. The encrypted data is continuously safeguarded from unauthorized access, providing strong security for intellectual property, customer and partner data, and corporate brand equity.

PGP Whole Disk Encryption can be deployed in conjunction with an optional PGP Universal™ Server. With PGP Universal Server, organizations can centrally define security policy to enforce protection of sensitive data for groups of users defined in an enterprise directory. Centralized reporting and logging provides details on the status of protection provided by PGP Whole Disk Encryption in an organization to simplify meeting compliance and auditor requirements.

PGP Whole Disk Encryption locks down the entire contents of a laptop, desktop, external drive, or USB flash drive, including boot sectors, system, and swap files. The encryption is transparent to the user, automatically protecting data.

PGP Whole Disk Encryption is a PGP Encryption Platform-enabled application. The PGP Encryption Platform provides a strategic enterprise encryption framework for shared user management, policy, and provisioning, automated across multiple, integrated encryption applications. As a PGP Encryption Platform-enabled application, PGP Whole Disk Encryption can be used with PGP Universal Server to manage existing policies, users, keys, and configurations, expediting deployment and policy enforcement. PGP Whole Disk Encryption can also be used in combination with other PGP encryption applications to provide

multiple layers of security.

The RSA SecurID SID800 hardware authenticator also integrates with other applications of the PGP Encryption Platform, such as email encryption (PGP® Desktop Email) and storage encryption (PGP® NetShare).

Key Features & Solution Benefits

- **Integrated with existing infrastructure** – Leverage your RSA token deployment for the protection of data on laptops, in emails and in files.
- **Higher security** – Increase the security level through two-factor authentication with existing tokens.
- **Easy, automatic operation** – Protects data without changing the user experience.
- **Enforced security policies** – Automatically enforce data protection with centrally managed policies.
- **Accelerated deployment** – Achieves full disk encryption using the existing infrastructure.
- **Reduced operation costs** – Results from centrally automating encryption policies.

About RSA

RSA, the Security Division of EMC, is the premier provider of security solutions for business acceleration, helping the world's leading organizations succeed by solving their most complex and sensitive security challenges. RSA's information-centric approach to security guards the integrity and confidentiality of information throughout its lifecycle - no matter where it moves, who accesses it or how it is used.

RSA offers industry-leading solutions in identity assurance & access control, data loss prevention & encryption, compliance & security information management and fraud protection. These solutions bring trust to millions of user identities, the transactions that they perform, and the data that is generated. For more information, please visit www.RSA.com and www.EMC.com.



RSA Security Inc.
RSA Security Ireland Limited
www.rsa.com

The Security Division of EMC