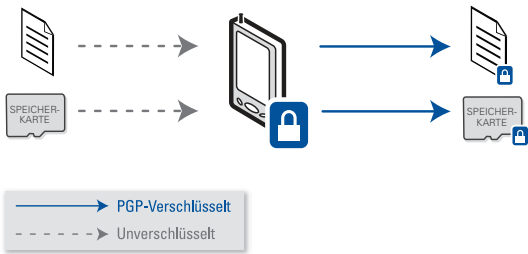


Vorteile

- **Einfache Nutzung** – Schützt E-Mail-Nachrichten, Anlagen, Daten und Speicherkarten mit minimalem Aufwand für den Anwender. Automatische Durchsetzung und konsistente Anwendung von E-Mail-Sicherheitsrichtlinien ohne Anwendereingriff.
- **Einfache Bereitstellung, Integration und Verwaltung** – Mit dem PGP Universal™ Server können über eine einzelne zentrale Verwaltungskonsole Richtlinien, Benutzer, Schlüssel und Konfigurationen über mehrere PGP®-Verschlüsselungsanwendungen hinweg verwaltet und bereitgestellt werden. Nutzt in Unternehmen die vorhandene Windows®-Infrastruktur zur Steuerung der Bereitstellung und Schlüsselverwaltung.
- **Erweiterbar** – Verschlüsselte Daten können gemeinsam sicher genutzt werden, sogar wenn sich die Empfänger außerhalb des Unternehmens befinden oder keine Verschlüsselungssoftware besitzen. Technologie auf Industriestandard bietet Interoperabilität mit bestehenden Infrastrukturen. Weitere PGP®-Verschlüsselungsanwendungen können als zusätzliche Sicherungsebenen integriert werden und dabei die zentrale Verwaltung nutzen.



Umfassender Schutz für Smartphone E-Mail-Nachrichten, Daten und Speicherkarten.

PGP®-Kunden im Fokus

„Nur die Produktlinie der PGP Corporation deckt unsere gesamten aktuellen Anforderungen an den unternehmensweiten Datenschutz ab.“

Tom Goschütz
 Chief Technology Officer
 Corporate Center
 Bertelsmann AG

Einfache, umfassende Verschlüsselung für Smartphones

Smartphones erhöhen die Produktivität und eröffnen neue Möglichkeiten für geschäftliche Aktivitäten jenseits der Bürowände. Allerdings stellen dieselben Geräte, mit denen sich Wettbewerbsvorteile erzielen lassen, die Unternehmen auch vor neue Sicherheitsrisiken. E-Mail-Nachrichten und Daten auf Smartphones können geistiges Eigentum oder Informationen enthalten, die gesetzlichen Regelungen unterliegen. Bei Verlust oder Diebstahl eines solchen Geräts oder Wechseldatenträgers werden vertrauliche Daten preisgegeben. Dies kann zu finanziellen Einbußen, juristischen Komplikationen und Rufschädigung führen.

PGP® Mobile löst dieses Problem durch umfassende E-Mail- und Datenverschlüsselung für Windows Mobile®-Smartphones und ermöglicht dadurch den sicheren Schutz gespeicherter, in Verwendung befindlicher und zur Benutzung durch mehrere Anwender freigegebener Daten.

Datensicherheit für mobiles Arbeiten

PGP Mobile bietet flexible Verschlüsselung auf Grundlage von bewährter Verschlüsselungsarchitektur und Schlüsselverwaltung, die den vielfältigen Ansprüchen mobiler Anwender an Datenschutz und Kommunikation gerecht wird. PGP Mobile kann Dateien, Archive oder Verzeichnisse verschlüsseln, die lokal oder auf Speicherkarten gespeichert sind. Mit den Diensten zur Schlüsselverwaltung und Bereitstellung von PGP Universal Server können Administratoren PGP Mobile schnell drahtlos bereitstellen. Die Anwender können ihre mit PGP Mobile verschlüsselten Daten auch für Anwender ohne eigene Verschlüsselungssoftware freigeben.

E-Mail-Verschlüsselung¹ für sichere mobile Kommunikation

Geschäftsentscheidende Informationen werden schnell und einfach per E-Mail ausgetauscht. Die neueste Version von PGP Mobile bietet Verschlüsselung für E-Mail-Nachrichten und E-Mail-Anlagen auf Smartphones unter Windows Mobile® 6.0 und 6.1 Professional Edition sowie digitale Signatur und eine automatisierte Schlüsselsuche. Unternehmen können sich auf den automatischen Schutz von E-Mail-Nachrichten während der Übertragung und am Speicherort bei nur geringen Änderungen für den Smartphone-Anwender verlassen.

Mit der PGP® Encryption Platform kompatibel

PGP Mobile ist mit der PGP Encryption Platform kompatibel, die den strategischen Rahmen für das Management der gemeinsamen Datennutzung, zur Verwaltung von Richtlinien und für die Bereitstellung automatisierter plattform-, system- und anwendungsübergreifender, integrierter Verschlüsselungsanwendungen bildet. So können die vorhandenen Richtlinien, Anwender, Schlüssel, und Konfigurationen mit PGP Universal™ Server verwaltet werden, um die Bereitstellung und Richtlinienumsetzung zu beschleunigen. PGP Mobile kann auch in Kombination mit anderen PGP-Verschlüsselungsanwendungen verwendet werden.

Einfacher, automatischer Betrieb

PGP Mobile verschlüsselt E-Mail-Nachrichten und Daten ohne Beeinträchtigung der Leistung von Smartphones. Benutzer von mobilen Geräten und von Desktop-PCs können mit den folgenden Anwendungen Daten untereinander austauschen:

- **E-Mail¹** – Ermöglicht automatische E-Mail-Verschlüsselung (einschließlich Anlagen) auf Smartphones unter Windows Mobile® 6.0 und 6.1 Professional Edition.
- **PGP® Virtual Disk** – Speichert Dateien oder Ordner in einer einzelnen verschlüsselten Datei, die wie ein Wechseldatenträger genutzt wird.
- **PGP® Zip** – Erstellt verschlüsselte, komprimierte Dateien zur Archivierung und zum Datenaustausch. Verwendet Passphrasen oder Zertifikate, um Daten während der Übertragung zu unterschiedlichen Benutzern zu schützen.
- **Selbstentschlüsselnde Archive** – Schnelle Übermittlung in Windows-kompatiblen EXE-Dateien, die sich ohne zusätzliche Software selbst entschlüsseln.

Umsetzung von Sicherheitsrichtlinien

PGP Mobile setzt E-Mail-Sicherheitsrichtlinien durch und integriert sich in die vorhandene Unternehmensinfrastruktur:

- **E-Mail-Richtlinie** – Richtlinien werden entsprechend der Definition durch PGP Universal Server konsequent und automatisch angewendet.
- **Windows-Domänenauthentifizierung** – Verwendet Windows®-Domänenauthentifizierung und Active Directory®-Richtlinien zur Steuerung der Bereitstellung und Schlüsselverwaltung.

Schnellere Bereitstellung

Die folgenden Merkmale ermöglichen Administratoren das schnelle und einfache Bereitstellen von PGP Mobile für neue und vorhandene Smartphone-Benutzer:

- **OTA (drahtlose)-Bereitstellung** – Zur Installation, Einrichtung oder Verwendung von PGP Mobile ist keine Synchronisation mit Desktop-Geräten erforderlich.
- **Verwaltungssysteme für mobile Endgeräte** – PGP Mobile kann über die im Unternehmen üblichen Geräteverwaltungssysteme wie Standard-CAB-Dateien bereitgestellt werden.
- **Integrierte Bereitstellung** – Schnellere Bereitstellung mit PGP Mobile durch automatische Einrichtung von Benutzerkonten und Schlüsselverwaltung über PGP Universal Server; keine Eingriffe durch Anwender oder Administrator erforderlich.

Reduzierte Betriebskosten

Da PGP Mobile mit PGP Encryption Platform kompatibel ist, können Unternehmen dieselbe gemeinsame Infrastruktur mit mehreren PGP®-Anwendungen verwenden. PGP Universal Server optimiert Verschlüsselungsvorgänge durch die Nutzung einer einzelnen Verwaltungskonsole für Schlüsselverwaltung, Bereitstellung und Richtlinien für PGP Mobile und weitere PGP-Anwendungen.

PGP Universal Server-Verwaltung

PGP Mobile wird über PGP Universal Server bereitgestellt und verwaltet. Nachfolgend einige Vorteile:

- **Einheitliche Verwaltung** – Zentrale Definition, Verwaltung und Durchsetzung von Verschlüsselungsrichtlinien für E-Mail-Nachrichten.
- **Schlüsselverwaltung** – Das Schlüsselmaterial wird während der Bereitstellung automatisch übermittelt.
- **Additional Decryption Key** – Mit dem sicheren geteilten Wiederherstellungsschlüssel wird gewährleistet, dass Unternehmen auf die Daten zugreifen können.

Technische Daten

Eine vollständige Übersicht über die technischen Daten erhalten Sie unter www.pgp.com/de/products/mobile.

¹ PGP Mobile 9.9 unterstützt Datenverschlüsselung auf Smartphones unter Windows Mobile® 5, 6 oder 6.1 Standard und Professional Edition. PGP Mobile 9.10 unterstützt E-Mail- und Datenverschlüsselung auf Smartphones unter Windows Mobile 6.0 und 6.1 Professional Edition.



www.pgp.com

© 2010 PGP Corporation. PGP und das PGP-Logo sind eingetragene Marken der PGP Corporation. Die in diesem Dokument genannten Produkt- und Markennamen sind Marken oder eingetragene Marken ihrer jeweiligen Inhaber. Diese Marken oder eingetragenen Marken sind alleiniges Eigentum ihrer jeweiligen Inhaber.

MDS100119