

SecurePIM Government SDS

Smartphone und Tablet dienstlich nutzen

Zuverlässiger Schutz für mobile Kommunikation



SecurePIM Government SDS bietet Behörden die Möglichkeit in einer sicheren Umgebung mobil zu arbeiten – jederzeit von überall. SecurePIM Government SDS ist die einzige vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zugelassene Sicherheitslösung für die Verarbeitung von Daten mit dem Geheimhaltungsgrad VS-NfD (Verschlusssache – nur für den Dienstgebrauch).

Sicherheit für Behörden - vom BSI geprüft

Im Auftrag des Bundesamtes für Sicherheit in der Informationstechnik (BSI) wurde SecurePIM Government SDS entwickelt, um es Behörden zu ermöglichen, Smartphone und Tablet in die tägliche Arbeit der öffentlichen Verwaltungen zu integrieren. Die Daten werden über einen zentralen Zugang des Informationsverbunds Berlin-Bonn (IVBB) oder ähnlichen Netzwerken mit den Servern der Hausnetze synchronisiert. Damit ist SecurePIM Government SDS in Verbindung mit einer Smartcard die einzige Lösung für VS-NfD.

Produktivität überall

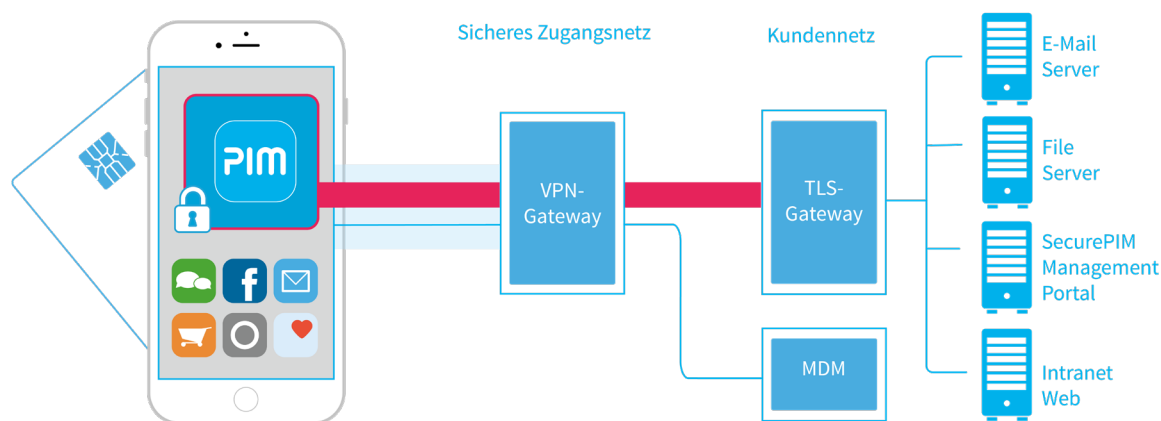
SecurePIM Government SDS erlaubt es Mitarbeitern von Behörden und anderen öffentlichen Einrichtungen von unterwegs auf E-Mails, Kalendereinträge und Kontakte zuzugreifen. Zudem steht ihnen eine sichere Kamera zur Verfügung, die Bilder in der gesicherten App speichert. Zusätzlich ist der Zugang zu Dokumentenablagensystemen und Intranet-Seiten von unterwegs über eine sichere Verbindung möglich. Die Bearbeitung von Dokumenten und die Einbindung von speziellen Fachverfahren ist ebenfalls möglich. Damit können Mitarbeiter Smartphones und Tablets für ihre tägliche Arbeit von unterwegs nutzen und sogar offline auf diesen Geräten arbeiten. Als zubuchbare Option bietet SecurePIM Government SDS auch die Möglichkeit direkt aus einem Kontakt heraus verschlüsselte Anrufe anzustoßen, ohne weitere Zwischenschritte tätigen zu müssen.

Vorteile für Mitarbeiter:

- + Sicherer Zugang zu wichtigen Informationen mit Smartphone und Tablet
- + Einfache und intuitive Nutzung
- + Verschlüsselte Sprachanrufe aus der App heraus tätigen
- + Zugriff auf bis zu drei E-Mail Accounts
- + Dokumente online und offline editierbar
- + Gerät kann mit Touch ID entsperrt werden

Sicherheit:

- + Vom BSI zugelassene Lösung
- + Nach deutschen Datenschutz-Richtlinien entwickelt
- + Integration von verschiedenen Smartcard-Lesern
- + Trennung von öffentlichen und dienstlichen Daten durch den Container-Ansatz
- + Dienstliche Daten sind sowohl auf dem Gerät als auch bei der Übertragung auf das Gerät verschlüsselt
- + Sichere Kommunikation mit den lokalen Servern via SecurePIM TLS-Gateway
- + Vollständige S/MIME Unterstützung
- + Entwickelt vom deutschen Unternehmen Virtual Solution AG



Smartcard Integration

Für höchste Sicherheitsanforderungen nutzt **SecurePIM Government SDS** eine Smartcard als Sicherheitsanker. Alle asymmetrischen Verschlüsselungsoperationen basieren auf den privaten Schlüsseln der Smartcard. Der private Schlüssel verlässt dabei niemals die Karte.

Derzeit werden unterschiedliche Smartcard-Leser unterstützt, wie z.B. Unicept AirID® oder Precise™ Biometrics Tactivo™.

Trennung von privat und dienstlich

Dank seiner Container-Technologie bietet **SecurePIM Government SDS** den kontrollierten Zugang zu Verschlusssachen, ohne dass die flexible Nutzung des iPhones oder iPads wesentlich eingeschränkt wird. Die Daten innerhalb des Containers sind mit der Smartcard gesichert. Keine andere App auf dem Endgerät oder eine nicht autorisierte Person kann Zugang zu den Daten im Container bekommen.

Sichere E-Mail-Kommunikation

Mitarbeiter können S/MIME verschlüsselte E-Mails senden und empfangen. Der Absender einer E-Mail kann über eine eindeutige Signatur zuverlässig identifiziert werden. Innerhalb der **SecurePIM App** werden alle Daten verschlüsselt abgelegt.

Verschlüsselte Sprachanrufe

Als zubuchbares Modul bietet **SecurePIM** auch Ende-zu-Ende-Verschlüsselung für Sprache an. Dank der geringen benötigten Bandbreite und Funktion über GPRS, EDGE, 3G, WiFi und Satellit kommen Anrufe zuverlässig durch und werden in hoher Qualität übertragen. Die Technologie bietet höchste Sicherheit durch Verschlüsselung über zwei Algorithmen parallel und benutzt keine vorinstallierten Schlüssel. Dabei ist die Bedienung einfach und komfortabel. Die **SecureVoice** Funktion fügt sich nahtlos in die übrigen Module der **SecurePIM App** ein.

Kompatibilität:

- + Verfügbar für iOS (ab Version 11) und Android (ab Version 5.0)
- + Unterstützung von Mail-Servern mittels ActiveSync
- + Zugang zu Dateien über WebDAV
- + Benutzersynchronisation mit LDAP

Komponenten der Systemlösung sind:

- + iOS oder Android-Endgerät
- + Smartcard Reader
- + Smartcard (Support für TCOS 3.0 Signature Card Version 2.0)
- + Mobile Device Management (MDM)
- + SecurePIM App
- + Virtual Solution Server Komponenten: SecurePIM TLS-Gateway, SecurePIM Mobile Application Management Portal (MAM), SERA Sicherheits-Framework

SecurePIM App Module:

- + E-Mail
- + Kontakte
- + Kalender
- + Notizen
- + Aufgaben
- + Dokumente (Bearbeiten und Speichern)
- + Browser (Zugang zu Intranet und Internet)
- + Sichere Kamera
- + SecureVoice (zubuchbar)