SecurePIM
by Virtual Solution

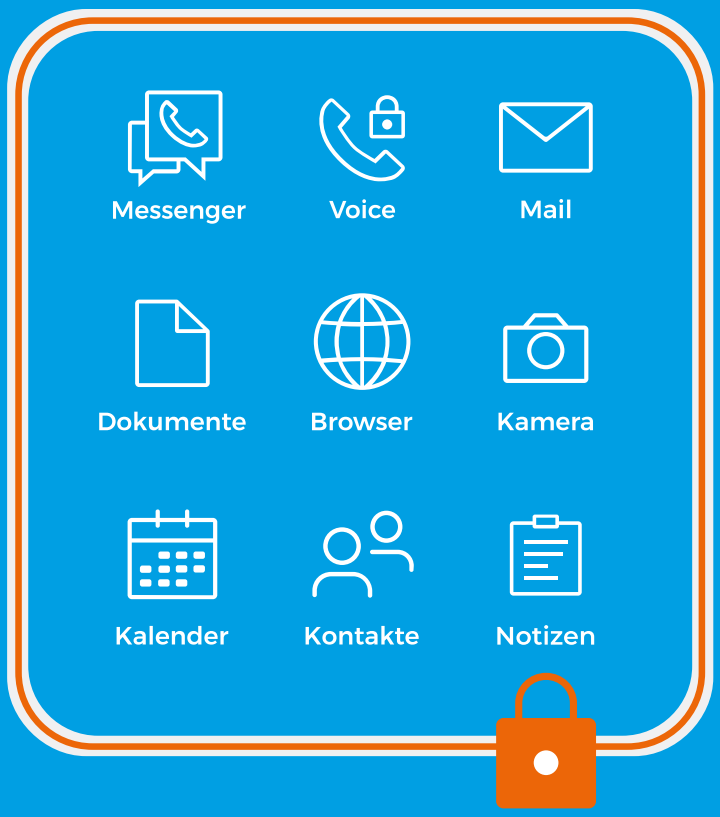
# SecurePIM

## Datenblatt

Virtual Solution AG

Februar 2022

Version 7.0

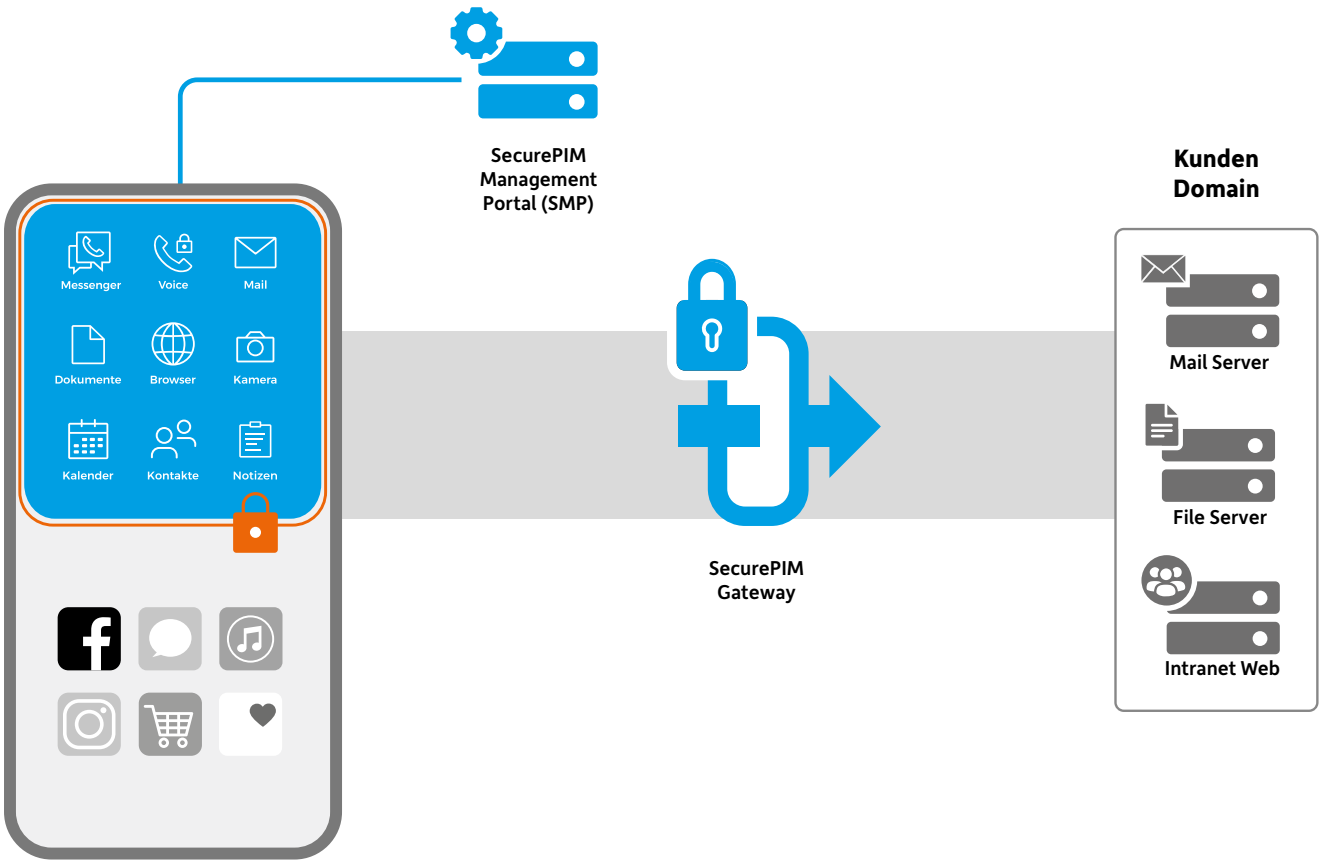


## Was ist SecurePIM?

SecurePIM ist eine mobile Kommunikationslösung, die Mitarbeitern und Mitarbeiterinnen von Behörden und Unternehmen ein sicheres mobiles Arbeiten ermöglicht. Der sichere Austausch der Daten ist dabei jederzeit durch die eingesetzte Container-Technologie und die Ende-zu-Ende Verschlüsselung gewährleistet. Unabhängig vom verwendeten Betriebssystem - iOS und Android - können Sie, je nach Ihren individuellen Bedürfnissen, verschiedene Varianten von SecurePIM einsetzen: Enterprise, Government und Government SDS (VS-NfD).

Die Sicherheit Ihrer Daten ist uns das wichtigste Anliegen, deshalb verwenden alle Komponenten von SecurePIM die höchsten Sicherheitsstandards und neuesten Verschlüsselungstechnologien.

## Komponenten



## SecurePIM App

Die SecurePIM App ist eine mobile Kommunikationslösung, die alle wichtigen Funktionen für das sichere und effiziente Zusammenarbeiten in einer App vereint, wie z. B. E-Mail, Kalender, Kontakte und Dokumente. Der Zugriff auf interne Dokumente, Intranetseiten und Webanwendungen ist über eine TLS-Verbindung ebenfalls von überall möglich.

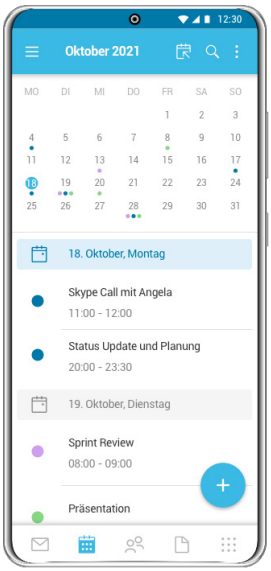
Der sichere Austausch der Daten ist dabei jederzeit durch die eingesetzte Container-Technologie und die Ende-zu-Ende Verschlüsselung gewährleistet (hybride Verschlüsselung mit RSA bis zu 4096 Bit oder ECC bis zu 256 Bit und AES-256). Zusätzlich sind alle Inhalte in SecurePIM durch ein persönliches SecurePIM Zugangspasswort, eine PIN oder Fingerabdruck vor unberechtigten Zugriffen geschützt. Keine andere App oder eine nicht autorisierte Person hat Zugang zu den Daten im SecurePIM Container.

SecurePIM lässt sich einfach und schnell einrichten und ist intuitiv zu bedienen. Das Rollout der Zugänge erfolgt zentral über das SecurePIM Management Portal und der Download der App im Apple® App Store oder Google Play™.
Nach nur wenigen Registrierungsschritten sind Ihre Teammitglieder perfekt aufgestellt für eine sichere mobile Kommunikation.

### Aktuell ist SecurePIM in folgenden Sprachen verfügbar

+ Deutsch
+ Englisch
+ Französisch
+ Italienisch
+ Spanisch
+ Russisch
+ Japanisch
+ vereinfachtes Chinesisch






# Funktionalitäten der SecurePIM App

Je nach Lizenzumfang oder Ihrer unternehmensspezifischen SecurePIM Konfiguration können einzelne Funktionalitäten nicht verwendet werden.

### Mail

+ Senden, Empfangen und Verwalten von E-Mails
+ Öffnen von E-Mail-Anhängen im sicheren Container
+ Bearbeiten von Anhängen direkt aus einer E-Mail heraus
+ Suche nach Begriffen im E-Mail-Betreff, E-Mail-Text oder nach Personen
+ Filter und Sortierung für E-Mail-Ordner
+ Abbilden Ihrer Ordnerstruktur
+ Festlegen von Favoriten-Ordnern und deren automatische Synchronisation
+ Schnittstelle zum Kontakte-Modul und zur globalen Adressliste für die Auswahl der adressierten Personen
+ Hervorheben favorisierter Kontakte
+ Erstellen von Terminen direkt aus einer E-Mail
+ Erstellen und Verwalten von Abwesenheitsnotizen
+ Indivduelle Konfiguration von Push-Benachrichtigungen
+ Maximale E-Mail Größe bis zu 50 MB
+ Anzeigen von ungelesen, markierten und neuen E-Mails und E-Mails mit hoher Priorität und mit offenen Einladungen im Home Modul
+ Verschlüsseln und Signieren nach S/MIME und HCL Domino Standard für MS Exchange und HCL Domino
+ Verschlüsselte Speicherung aller E-Mails – auch von E-Mails, die unverschlüsselt empfangenen werden
+ Verwaltung von bis zu sechs Exchange und HCL E-Mail-Konten
+ Anlegen lokaler E-Mail-Signaturen, individuell für jeden Account
+ Anlegen einer globalen E-Mail-Signatur
+ Unterstützung von E-Mail-Adressen im HCL Domino/ Notes Format
+ Zugang zur Kamera direkt beim Verfassen einer E-Mail
+ Scannen von Dokumenten beim Erstellen von E-Mails (iOS)
+ Sprachnachrichten aus E-Mail-Anhängen direkt anhören
+ Öffnen von PKPass-Anhängen (iOS)
+ Unterstützung von Meeting-Links verschiedener Apps
+ Schnellzugriff auf Dateiserver mit UNC-Links
+ URLs außerhalb von SecurePIM öffnen (iOS)
+ Festlegen als Standard-Mail-App (iOS, ab iOS 14 bzw. iPadOS 14 oder höher)

### Kontakte

+ Kontakte verwalten, erstellen, bearbeiten, löschen und durchsuchen
+ Kontakte gruppieren (nur iOS)
+ Standard-Telefonnummern und -E-Mail-Adressen festlegen
+ Zugriff auf die Globale Adressliste bzw. auf die HCL Domino Liste des Unternehmens
+ Zur Anruferkennung können Kontakte (Name, Telefonnummer und Firmenname) in den Gerätespeicher exportiert werden
+ Anruferkennung für alle iOS-Versionen (CallKit-Integration) und für Android ab Android 10
+ Direkte Weiterleitung von Kontakten per E-Mail
+ Kontakte favorisieren

### Kalender

+ Wählbarer Beginn der Arbeitswoche (Android)
+ Termine verwalten, erstellen, bearbeiten, löschen und durchsuchen
+ Verfügbarkeit von Kontakten anzeigen
+ Verschiedene Ansichtsoptionen, wie z. B. Listen-, Tages-, Wochen-, Monats- und Jahresansicht
+ Anhänge in Kalendereinträgen ansehen und direkt hinzufügen (nur verfügbar mit ActiveSync 16)
+ Anzeige verschiedener Kalenderkonten, z. B. privater Gerätekalender, Kalender aus Exchange und HCL Domino Konten sowie freigegebene Kalender anderer Personen (lesen und bearbeiten)
+ Farbliche Differenzierbarkeit der einzelnen Kalender
+ Unterstützung von Serienterminen und privaten Terminen
+ Erinnerungen an Termine individuell anpassbar
+ Zeitzonen-Unterstützung
+ Anzeige von bevorstehenden Terminen im Home Modul
+ Termin erstellen über Kurzwahlmenü mit 3D Touch Unterstützung (iOS)
+ Unterstützung von Meeting-Links verschiedener Apps
+ URLs außerhalb von SecurePIM öffnen (iOS)

SecurePIM
by Virtual Solution

### Messenger (Zusatzmodul optional)

+ Ende-zu-Ende-Verschlüsselung
+ 1:1 Chat und Gruppenchats mit bis zu 10 Personen
+ Channels mit bis zu 255 Personen
+ Audio- und Video-Anrufe in Chats, Gruppen oder Channels
+ Automatische Registrierung
+ Interaktion mit Kontakte-Modul
+ Anhänge (z. B. Fotos und Dokumente) aus dem sicheren Container, von der Kamera oder ggf. vom Gerät senden
+ Standortmarkierungen und Live-Standort versenden
+ Sprachnachrichten
+ Antworten auf einzelne Nachrichten
+ Editieren und Löschen von Nachrichten
+ Selbstlöschende Nachrichten
+ Vollbildmodus für Präsentationen
+ Teilen von Front- und Rückkamera-Ansichten in Video-Anrufen
+ Bildschirm teilen (Android)
+ Statusanzeige
+ Nachrichtenstatus und Lesebestätigung

### Browser

+ Workspace für Schnellzugriff auf Lesezeichen und Web-Apps
+ Zugriff auf Webseiten und webbasierte Anwendungen im Internet und Intranet
+ Desktop-Modus
+ Anmeldedaten speichern
+ Verwaltung von erlaubten und verbotenen Webseiten (von IT definiert)
+ Verwendung mehrerer Tabs
+ Upload von HTML-Dateien aus dem Dokumente-Modul
+ Automatische Zertifikats-Authentifizierung beim Zugriff auf Websites
+ NTLM-Authentifizierung beim Zugriff auf SharePoint®-Seiten
+ vBrowser-Ansicht von PDF-Dokumenten
+ Unterstützung von Meeting-Links verschiedener Apps
+ Festlegen der Suchmaschine
+ Zugriff auf Dateiserver oder SharePoint-Systeme mit Kerberos-Authentifizierung

### Dokumente

+ Sicheres Abspeichern von Dokumenten aus Anhängen und Zugang zu mehreren File-Servern des Unternehmens
+ Unterstützung einer Vielzahl von Dokumententypen (z. B. PDF, Microsoft Office Dokumente, Bilder, E-Mails, ZIP u.v.m.)
+ Erstellen und Bearbeiten von Dokumenten mit Polaris Office Enterprise ohne die App zu verlassen
+ File Picker Unterstützung, um Dokumente aus anderen Speicherorten auszuwählen (iOS, wenn von der IT zugelassen)
+ Öffnen und Bearbeiten von Dokumenten im Offline-Modus
+ Erstellen von Office Dokumenten (docx, xlsx, pptx, txt)
+ Einfügen von Lesezeichen, Anmerkungen, Hervorhebungen
+ Ordner und Dateien mit Lesezeichen markieren
+ Versand von Dokumenten über das E-Mail-Modul
+ *Öffnen-In* Funktion erlaubt Apps außerhalb des Containers Dokumente zu öffnen und zu bearbeiten (wenn von der IT zugelassen) (iOS)
+ OneWay-Synchronisation von ausgewählten Ordern
+ Dokumentenscanner: Speichern und Bearbeiten von gescannten Dokumenten (iOS)
+ URLs außerhalb von SecurePIM öffnen (iOS)
+ Zugriff auf Dateiserver oder SharePoint-Systeme mit Kerberos-Authentifizierung

### Kamera

+ Verwenden der Gerätekamera im sicheren Container
+ Andere Apps haben keinen Zugriff auf aufgenommene Fotos
+ Fotos werden nicht auf Cloud-Server hochgeladen
+ Fotos können nur nach dem Anmelden angesehen werden

### Aufgaben (nur für Exchange)

+ Aufgaben verwalten, erstellen, bearbeiten, löschen und priorisieren
+ Übersichtliche Anzeige von fälligen und anstehenden Aufgaben
+ Erinnerungen an Aufgaben verwalten
+ Erweiterte Sortier- und Filterfunktionen

### Notizen (nur für Exchange)

+ Notizen verwalten, erstellen, bearbeiten und löschen
+ Notizen suchen, sortieren und filtern

## SecurePIM Management Portal

Die Verwaltung und Konfiguration der Anwendung erfolgt zentral über das SecurePIM Management Portal, ein integrierter Teil der SecurePIM Lösung. Es kann als Serverkomponente (On-Premises) zur Installation bereitgestellt oder auf einem von der Virtual Solution AG gehosteten Server mit entsprechenden Rechten (Cloud) verwaltet werden.

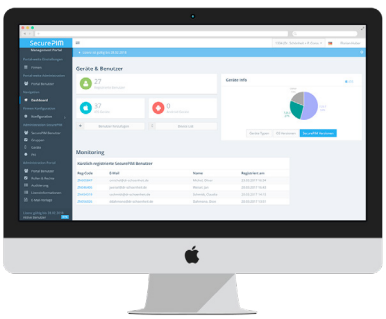
SecurePIM lässt sich einfach in die bestehende IT-Infrastruktur integrieren. Darüber hinaus kann es auch für verschiedene Mobile Device Management Systeme konfiguriert werden, die AppConfig Community Standards unterstützen.

Mithilfe des SecurePIM Management Portals können Administrations-Teams Sicherheitsvorgaben für die SecurePIM App definieren und auf Mobilgeräten durchsetzen.

Die Verwaltung und Pflege der Accounts ist ebenfalls einfach. Diese können entweder manuell oder durch einen LDAP-Import hinzugefügt und z. B. in Gruppen oder Abteilungen mit verschiedenen Sicherheitsstandards verwaltet werden.

Das SecurePIM Management Portal bietet auch ein Self Service Portal, das optional aktiviert werden kann. Im Self Service Portal können Nutzer:innen die eigenen Mobilgeräte verwalten und auf einfache Weise S/MIME Zertifikate auf die Mobilgeräte übertragen. Das SecurePIM Management Portal ist eine Java Webanwendung. Diese läuft in einem Apache Tomcat mit einem Apache Webserver als Frontend.

Aktuell ist das SecurePIM Management Portal auf Deutsch und Englisch verfügbar.



## Funktionalitäten des SecurePIM Management Portals

Das SecurePIM Management Portal bietet eine Vielzahl an Möglichkeiten, um die SecurePIM App zu konfigurieren.

### Festlegen der Sicherheitseinstellungen für Geräte, mit denen SecurePIM genutzt wird

+ Verschiedene Timeouts, die zum Logout von SecurePIM führen
+ *Öffnen-In* zur Ansicht oder Bearbeitung von Dateien außerhalb des Sicherheitscontainers zulassen oder verbieten
+ Definition von vertrauenswürdigen Zertifizierungsstellen
+ Definition gruppenabhängiger Einstellungen, um unterschiedliche Sicherheitsstandards zu verwalten
+ Updates von SecurePIM erzwingen
+ Registrierung modifizierter Geräte (Jailbreak bzw. Root) zulassen oder verbieten
+ CallKit-Integration bzw. Kontakte-Export zur Anruferkennung erlauben oder verbieten
+ Einbindung von mehreren E-Mail-Konten in SecurePIM erlauben
+ Mindestversion des Betriebssystems von Geräten festlegen
+ Passwort-/PIN-Richtlinien festlegen, biometrische Authentisierung zulassen
+ Kopieren und Einfügen innerhalb der App erlauben oder verbieten
+ Herunterladen von externem Inhalt in E-Mails zulassen oder verbieten
+ Screenshots erlauben oder verbieten (nur Android)

### Schnelle Reaktion auf Bedrohungen & Gefahren

+ Sperren von SecurePIM für einzelne Geräte
+ Fern-Reset: Alle Daten im sicheren Container werden restlos entfernt (die privaten Daten außerhalb des Containers werden nicht beeinflusst)

### Einfache Accountverwaltung

+ Sowohl manuelle Erstellung als auch LDAP bzw. Excel-Import möglich
+ Bestehende Gruppen oder Abteilungen (mit verschiedenen Sicherheitsstandards) können ebenfalls per LDAP importiert werden
+ Verwalten von E-Mail-Vorlagen (z. B. zum Versand von Registrierungsinformationen) in mehreren Sprachen
+ Self-Sign-Up: Nutzer:innen können sich über Einladungslink selbstständig registrieren
+ Account-Übersicht als XLSX, XLS oder CSV exportieren
+ Geräte-Monitoring

### Umfangreicher Support

+ Log-Dateien einzelner Geräte abrufbar, um Fehlerursachen zu erkennen
+ Genaue Statusabfragen zum Registrierungsstatus
+ Ungenutzte SecurePIM Lizenzen automatisch für andere freigeben
+ Smartcard-User-Management
+ Browser-Einstellungen konfigurieren: Standard-Lesezeichen; Liste mit erlaubten oder geblockten Domains, Proxy
+ Standard-E-Mail-Signatur festlegen
+ Support-E-Mail-Adresse angeben

# Zusätzliche Funktionalitäten von SecurePIM

## Integration von Public Key Infrastructure (PKI)

Falls im Unternehmen bereits eine eigene PKI-Umgebung in Form eines Active Directory Certificate Service in Betrieb ist, kann diese einfach in das SecurePIM Management Portal eingebunden werden. Dabei wird die Bereitstellung der Zertifikate (öffentliche Schlüssel) aus dem LDAP/AD unterstützt.

Für Firmen, die keine eigene PKI-Intrastruktur haben, kann das SecurePIM Management Portal dank seiner Auto-PKI-Funktion die wichtigsten Funktionalitäten einer PKI bereitstellen:

+ Hochladen und Löschen von Zertifikaten
+ Beschaffung von Lizenzen direkt vom Portal
+ Bereitstellung der persönlichen Zertifikate der Nutzer:innen
+ Zugang zu Zertifikatsperrlisten
+ Bereitstellen von öffentlichen Schlüsseln, z. B. zum Öffnen einer verschlüsselten E-Mail

## SecurePIM Gateway

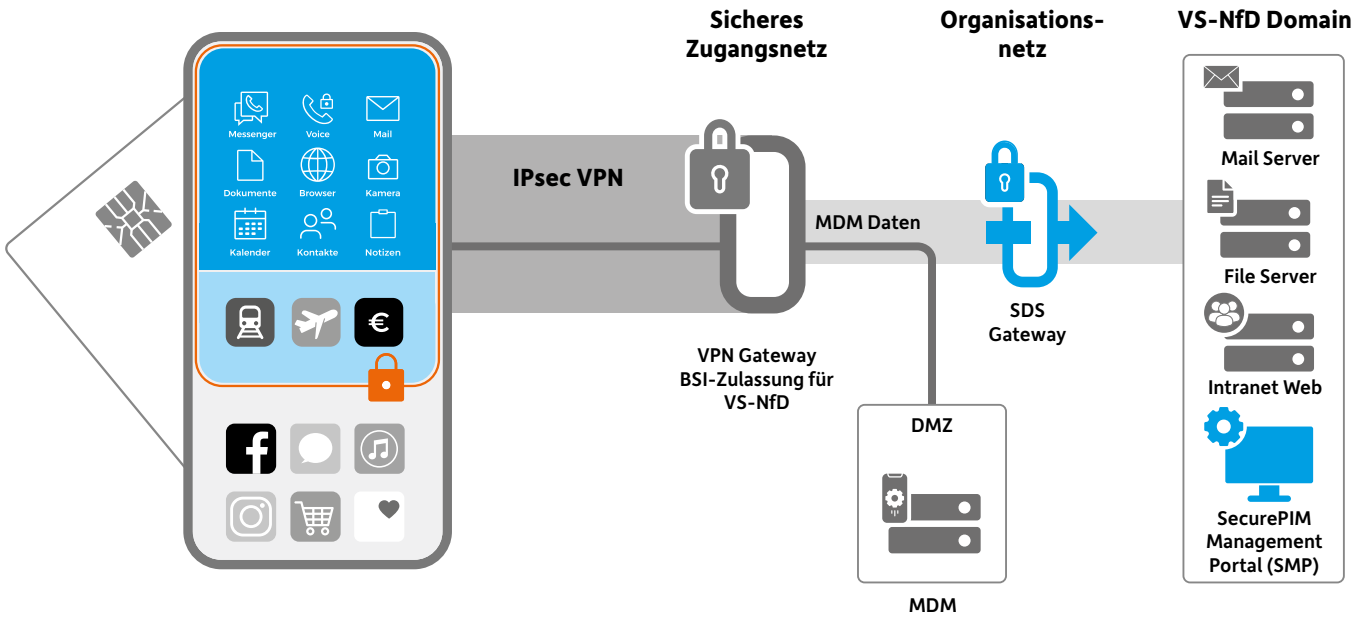
Das SecurePIM Gateway sichert die Verbindung der SecurePIM App mit der Infrastruktur der Firma ab. Die Sicherheit basiert auf der Authentifizierung durch Zertifikate und benötigt weder eine VPN-Infrastruktur, noch VPN-Profile für die mobilen Geräte. Die Gateway Software Appliance wird in der Demilitarisierten Zone (DMZ) der Firma installiert. Eine bestimmte Schnittstelle in der Firewall muss geöffnet werden, damit die SecurePIM App von außen Zugang bekommt. Das SecurePIM Gateway unternimmt beim Verbindungsaufbau eine Identitätsprüfung und erlaubt nur nach erfolgreicher Authentifizierung den Zugriff auf den Exchange Server. Gleichzeitig können auch viele andere Anwendungen im Unternehmensnetz damit abgesichert werden. Ein direkter Zugriff aus dem Internet auf Exchange Server ist dafür nicht nötig.

### Die wichtigsten Funktionen

+ Zugang zu MS Exchange, File-Diensten (via WebDAV), Webseiten und Web-App-Diensten
+ Cloud oder On-Premises Einsatz möglich
+ Konfiguration und Kontrolle des SecurePIM Gateway über das SecurePIM Management Portal

## Mobile Device Management

SecurePIM kann auch für gängige Mobile-Device-Management-Systeme konfiguriert werden, wenn diese AppConfig Community Standards unterstützen.
Das MDM kann die Installation von SecurePIM auf Endgeräten erzwingen sowie App und Gerät zentral konfigurieren und überwachen.
Für die Erstellung eines Konfigurationsprofils können unterstützend Apple's Configurator oder Profile Manager verwendet werden.




## SecurePIM Government SDS Höchste Sicherheit für Behörden

SecurePIM Government SDS (*Sicherer Datensynchronisationsdienst*) ist eine spezielle Systemlösung. Im Auftrag des Bundesamtes für Sicherheit in der Informationstechnik (BSI) wurde SecurePIM Government SDS entwickelt, um es Behörden zu ermöglichen, Smartphones und Tablets auch für die Arbeit mit Informationen VERSCHLUSSSACHE – NUR FÜR DEN DIENSTGEBRAUCH (VS-NFD) und NATO RESTRICTED einzusetzen.

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 zu den Netzen des Bundes, wenn die Verarbeitung und Übertragung von Informationen mit dem Geheimhaltungsgrad VS-NfD auf iOS- und Android-Geräten erforderlich ist (Zulassung für iOS, Freigabeempfehlung für Android).

## SecurePIM Government SDS Architektur

**Die folgenden Komponenten sind für SecurePIM Government SDS immer zwingend notwendig**

+ Geräte mit iOS ab Version 14 oder Android ab Version 8.1
+ Smartcard (Unterstützung der Smartcards TCOS 3 Signature Card 2.0 und PKIBw Card 1.7 (nur iOS))
+ Berührungslose Near Frequency Communication (NFC) Nutzung oder AirID 1, AirID 2, AirID 2 mini Smartcard-Leser
+ SecurePIM Management Portal
+ MDM zur zentralen Geräteverwaltung
+ SDS Gateway
+ IPsec-VPN

## Smartcard-Integration

Für höchste Sicherheitsansprüche ist SecurePIM zusätzlich mit einer Smartcard gesichert. Alle asymmetrischen Verschlüsselungsoperationen basieren auf den privaten Schlüsseln der Smartcard. Der private Schlüssel und die Zertifikate sind physisch auf der Karte gespeichert und verlassen dabei niemals die Karte.

### Die Smartcard übernimmt folgende Operationen

+ Erzeugung von Zufallszahlen
+ Zertifikatsbasierte Authentifizierung
+ Containerverschlüsselung – lokale Datenverschlüsselung
+ S/MIME Ver- und Entschlüsselung

### Funktionalitäten mit Smartcard

+ Anzeige der verfügbaren Smartcard-Leser sofort bei der Registrierung von SecurePIM
+ Einmal mit SecurePIM gekoppelte Smartcard-Leser werden bei jedem nachfolgenden Login automatisch wieder verbunden
+ Wechsel des Smartcard-Lesers direkt im SecurePIM Login-Fenster oder über die Einstellungen
+ Alternativ kann NFC berührungslos ohne Smartcard-Leser eingesetzt werden (iOS)

### Smartcard-on-Demand für zusätzliche Authentifizierung beim

+ Senden signierter E-Mails
+ Öffnen verschlüsselter E-Mails
+ Öffnen mit Zertifikaten geschützter Webseiten

## SDS Gateway

Die gesamte Kommunikation zwischen der SecurePIM App und den Datenquellen im Firmennetzwerk kann für einen sicheren Datenverkehr durch das TLS-Protokoll (hybrides Verschlüsselungsprotokoll) verschlüsselt werden.
Das SDS Gateway kommuniziert mit dem E-Mail-Server, dem File Server, den internen Websites und Web-Applikationen und dem SecurePIM Management Portal.

### Die wichtigsten Funktionen

+ Sicherer Kanal für die Kommunikation zwischen der SecurePIM App und dem Firmennetzwerk
+ TLS-Verschlüsselung des ActiveSync-Protokolls für die Kommunikation mit dem ActiveSync-Server
+ Web-Service-Schnittstelle mit TLS-Verschlüsselung für die Kommunikation mit dem SecurePIM Management Portal
+ Die Anmeldung in das SDS Gateway ist zertifikatsbasiert
+ Zertifikatsbasierte Authentifizierung für das SDS Gateway um Zugang zu Dokumentenmanagementsystemen und Intranet-Applikationen zu bekommen

## IPsec-VPN

Für die zugelassene Systemlösung verbindet sich SecurePIM mit der internen IT-Infrastruktur über einen VPN-Tunnel, der die Protokoll-Suite IPsec (Internet Protocol Security) verwendet. Bei einem Massenrollout von Android-Geräten erleichtert die Begleitapp SecureVPN die Einrichtung des IPsec IKEv2 VPNs. Die Installation wird dadurch weitestgehend automatisiert.

### IPsec ermöglicht dabei

+ Sichere Kommunikation im Internet
+ Gesicherte VPN-Verbindung
+ Der IPsec-VPN-Tunnel endet am IPsec-VPN-Gateway, wo die Daten kanalisiert werden

## SecureDOK (iOS)

Mit der Dokumenteneditor-App SecureDOK wird die allgemeine Datensicherheit erhöht und die Gefahr von potentiellen Angriffen reduziert. Durch die Prozesstrennung »Arbeiten in SecurePIM« vs. »Öffnen und Bearbeiten von Dokumenten« wird sichergestellt, dass der Ausführungs- und Speicherbereich des Dokumenteneditors von SecurePIM getrennt ist. Die Nutzer:innen können dabei nahtlos und bequem mit SecurePIM und SecureDOK arbeiten.

## SecureVoice

Als optionales Modul bietet SecurePIM Government SDS deutschen Behörden auch Ende-zu-Ende-Verschlüsselung für Telefonie an. Dank der geringen benötigten Bandbreite kommen Anrufe zuverlässig durch und werden in hoher Qualität übertragen. Die Technologie bietet höchste Sicherheit durch die parallele Verschlüsselung mit zwei Algorithmen 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.

+ Wenig Bandbreite benötigt (4.8 kbps)
+ Funktion über 2G (GPRS, EDGE), 3G (UMTS), 4G (LTE), WiFi, Satellit
+ 4.096 Bit Diffie-Hellman-Schlüsselaustausch
+ Man-in-the-middle-Schutz
+ AES256 und Twofish
+ Keine vorinstallierten Schlüssel
+ Source Code verifizierbar

# Technische Voraussetzungen

### Mobilgeräte
+ iOS: Aktuell werden alle Betriebssystemversionen ab iOS 14 und iPadOS 14 unterstützt
+ Android: Von Google zertifiziertes Android Beriebssystem ab Android Version 8.1

### E-Mail Server
+ Microsoft® Exchange 2013 bis Exchange 2019 und Office 365 mit dem ActiveSync Protokoll 14.0 oder 14.1 bzw. 16.0 oder 16.1
+ HCL Domino Server 9.0.1 FP10 mit ActiveSync 14.0 oder 14.1 / HCL Traveler 11.x oder höher

### Datei-Server
+ WebDAV-Standard-Systeme

# Technische Voraussetzungen für SecurePIM Management Portal

### Betriebssystem
+ Ubuntu 20.04 LTS (empfohlen) oder Ubuntu 18.04 LTS
+ Red Hat Enterprise Linux 8

### Servlet Engine
+ Apache Tomcat 9 (empfohlen) oder 8.5

### Java-Laufzeitumgebung
+ Java 11

### Datenbank
+ MariaDB 10.2
+ MariaDB 10.3 (empfohlen)
+ MariaDB 10.4
+ MySQL 8
+ MySQL 5.7
+ PostgreSQL 12
+ PostgreSQL 13

# Firewall-Konfiguration
+ Wenn die SecurePIM App über eine Firewall mit dem SecurePIM Management Portal kommuniziert, muss in der Firewall Port 443 (HTTPS) für eingehende Verbindungen zum Portal offen sein
+ Das SecurePIM Management Portal muss den SecurePIM License Manager unter folgender URL erreichen können: https://clm.securepim.com
  Port 443 (HTTPS) muss für ausgehende Verbindungen offen sein

# Service und Support

Die Support-Teams von Virtual Solution und unseren Partnerunternehmen stehen Ihnen bei allen Fragen rund um Sicherheit, Service und Support jederzeit gerne zur Seite.

## Integrationsservice

Auch für zusätzliche Trainings oder Integrationsdienstleistungen im Rahmen der Einführung von SecurePIM stehen unsere Support-Teams Ihnen gerne zur Verfügung.

## Produktbezogener Update und Upgrade Support

Sowohl die SecurePIM App als auch das SecurePIM Management Portal werden fortlaufend verbessert. Updates und Upgrades sind im Lizenzumfang enthalten.

SecurePIM
by Virtual Solution

## Über Virtual Solution

Virtual Solution, ein Unternehmen der Materna-Gruppe, ist ein auf sichere mobile Anwendungen spezialisierter Softwarehersteller mit Sitz in München und Entwicklungsstandort in Berlin.

Das Unternehmen entwickelt und vertreibt die Applikationen SecurePIM, SecureCOM und die Sicherheitsarchitektur SERA für iOS und Android. SecurePIM ermöglicht verschlüsseltes und benutzerfreundliches mobiles Arbeiten. Behörden können mit Smartphones und Tablets auf Geheimhaltungsstufe VERSCHLUSSSACHE – NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD) und auf der Sicherheitsstufe NATO RESTRICTED kommunizieren.

Für Unternehmen stellt SecurePIM die Anforderungen der Datenschutzgrundverordnung (DSGVO) auf mobilen Geräten sicher und senkt damit die Risiken strafbewährter DSGVO-Verstöße und des Verlustes von Unternehmensdaten.

Virtual Solution wurde 1996 gegründet und beschäftigt rund 90 Mitarbeiter:innen. Alle Produkte der Virtual Solution tragen das Vertrauenszeichen »IT-Security made in Germany« des TeleTrust-IT-Bundesverbandes IT-Sicherheit e.V.

**>500**
Behörden & Unternehmen

**>120**
Behörden & sicherheitsbetreute Industrie

**>45**
Bundesbehörden

**>330.000**
Nutzer:innen auf iOS & Android

**>92%**
erweitern & erneuern ihre Lizenzen

Virtual Solution

Virtual Solution AG
Blutenburgstraße 18 · 80636 München · T +49 89 30 90 57-0
kontakt@virtual-solution.com · www.virtual-solution.com

P-22.0023_SPIM Datenblatt_de/de_v8_02/22