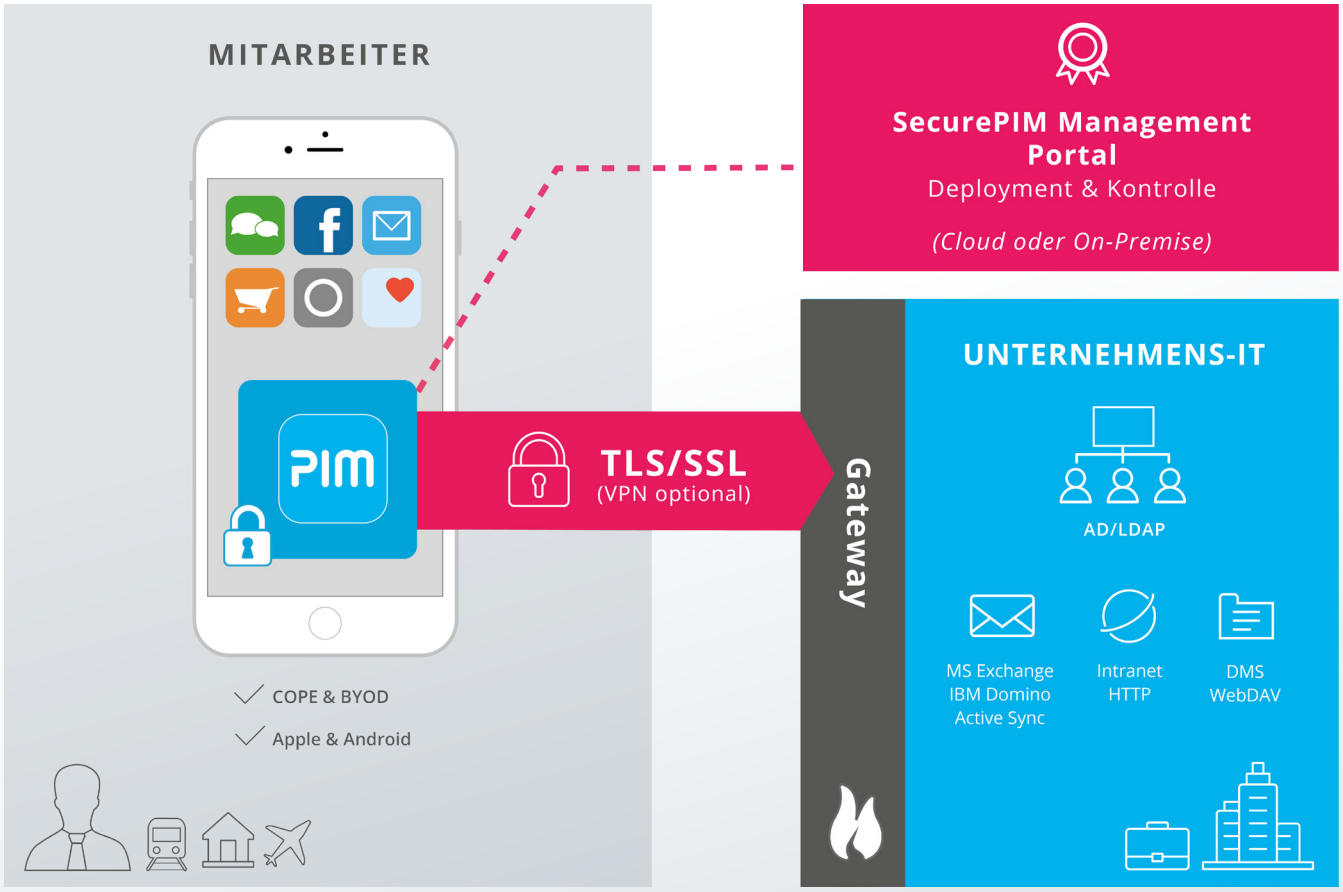
PRODUKTÜBERBLICK
SecurePIM

SecurePIM ermöglicht Mitarbeitern einen sicheren Zugriff auf berufliche Daten auf mobilen iOS oder Android Geräten. Mit SecurePIM haben Mitarbeiter alles um von unterwegs aus zu arbeiten, einen Zugang zu Firmendaten herzustellen und sich mit dem Firmennetzwerk zu verbinden, ohne sich um Sicherheit und Privatsphäre sorgen zu müssen.

Bei SecurePIM steht die Sicherheit der Daten im Vordergrund. Die Lösung erzeugt einen „Sicherheitscontainer" auf dem mobilen Endgerät. Alle Daten innerhalb dieses Containers sind verschlüsselt. Zur **Verschlüsselung** wird der private Schlüssel des Nutzers bzw. ein in der App generierter Schlüssel verwendet. Dabei unterstützt SecurePIM optional eine Verschlüsselung mittels Smartcard über einen Smartcard-Leser.

Komponenten



SecurePIM App

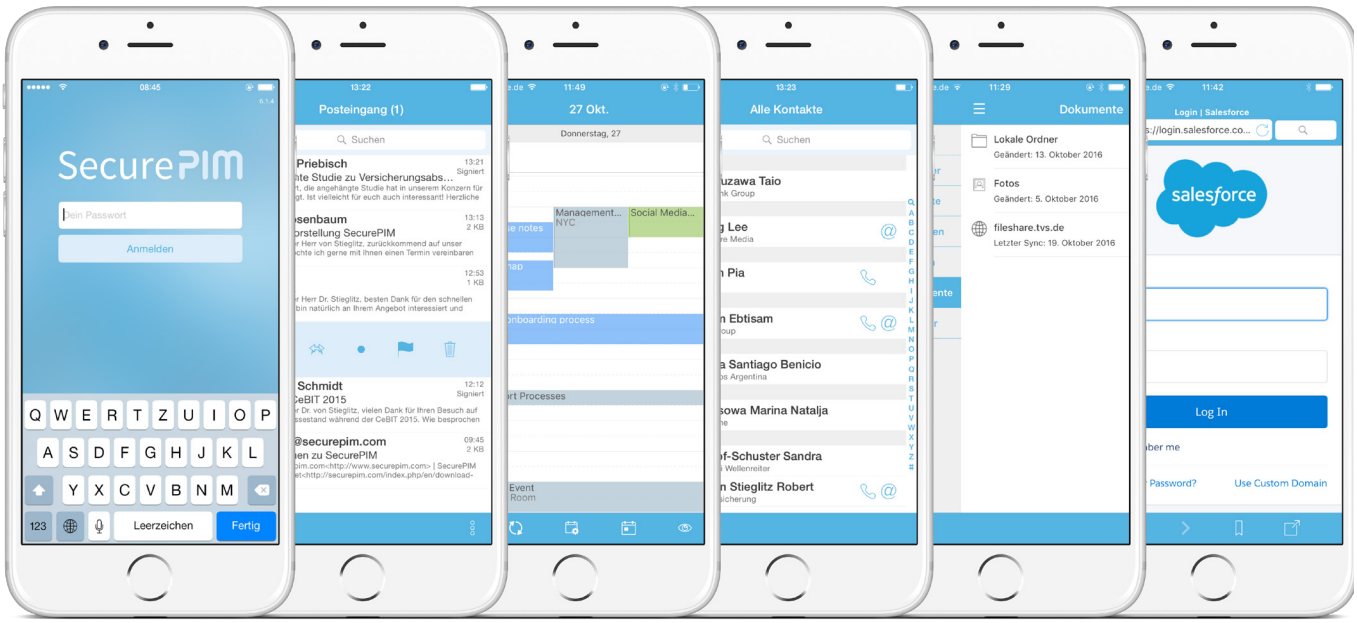
Die SecurePIM App, erhältlich für iOS und Android Geräte, ist ein sicherer Container auf dem mobilen Endgerät und ermöglicht einen Zugang zu Enterprise Tools, wie zum Beispiel E-Mails, Kontakte, Kalender, Notizen und Aufgaben über MS Exchange und/oder IBM Domino. Der Mitarbeiter kann auch von unterwegs mittels eines sicheren und kontrollierten Zugangs zu Firmendokumenten, Intranetseiten und Webapplikationen über die sichere TLS Kommunikation arbeiten.

Alle Daten innerhalb der SecurePIM App sind verschlüsselt (hybride Verschlüsselung mit RSA bis zu 4096 Bit und AES-256) und durch einen PIN, ein Passwort oder einen Fingerabdruck geschützt. Keine andere App oder eine nicht autorisierte Person hat Zugang zu den Daten im SecurePIM Container!

Durch die intuitive Bedienung der SecurePIM App, ist sie einfach einzurichten und zu benutzen. Das Rollout der App geht schnell und einfach, denn Mitarbeiter laden sich die App entweder über den Apple® App Store oder Google Play™ herunter und registrieren sich mit ihren Zugangsdaten.

Sprachen

Aktuell ist SecurePIM auf Deutsch, Englisch, Französisch, Italienisch, Spanisch, Russisch, Japanisch und vereinfachtem Chinesisch verfügbar.



SecurePIM App Für IBM Domino!

Dank der engen Zusammenarbeit mit IBM ist SecurePIM auch für IBM Domino Benutzer erhältlich. Es bietet umfassende Unterstützung von S/MIME und IBM Domino Ver- und Entschlüsselung, ohne Middleware oder Companion Apps.

Funktionalitäten der SecurePIM App

E-MAIL

- Navigation, Versand, Empfang, Markierung, Priorisierung und Swipe-Funktionalitäten
- E-Mail Anhänge werden ausschließlich innerhalb des Sicherheits-containers geöffnet
- Suche von E-Mails nach Betreff, Sender und Empfänger
- Abbildung der Ordnerstruktur wie auf dem Desktop
- Interaktion mit dem Kontaktemodul zur Auswahl der Adressaten
- Erstellung und Verwaltung von Abwesenheitsnotizen
- Push Mitteilungen individuell konfigurierbar
- Maximale E-Mail Größe bis zu 50 MB (iOS) bzw. 20 MB (Android)
- Weiterleiten und Beantworten von HTML E-Mails
- Anlegen einer lokalen E-Mail Signatur
- E-Mail Kommunikation durch S/MIME Verschlüsselung und S/MIME Signatur für MS Exchange und IBM Domino
- Unterstützung der IBM Notes Ver- und Entschlüsselung
- Verschlüsselte Speicherung aller E-Mails - auch von E-Mails, die unverschlüsselt empfangenen werden
- Verwaltung von bis zu drei E-Mail Konten (iOS)
- Unterstützung von E-Mail Adressen im IBM Domino/Notes Format
- Sprachnachrichten als E-Mail Anhängen können direkt in SecurePIM angehört werden
- Öffnen von PKPass Anhängen wie Bordkarten, Gutscheinen, Coupons

KONTAKTE

- Kontakte verwalten, erstellen, bearbeiten und löschen
- Suchen und Filtern von Kontakten
- Zugriff auf die globale Adressliste des Unternehmens bzw. auf die IBM Domino Liste
- Zur Anruferkennung können Kontakte (nur Name und Telefonnummer) in die Gerätekontakte exportiert werden
- Direkte Weiterleitung von Kontakten per E-Mail (Android)

KALENDER

- Termine verwalten, erstellen, bearbeiten und löschen
- Teilnehmerverfügbarkeit und zeitliche Konflikte sind sofort sichtbar
- Verschiedene Ansichtsoptionen, wie z.B. Listen-, Tages-, Wochen-, Monats-, und Jahresansicht
- Anzeige verschiedener Kalenderkonten, z.B. privater Gerätekalender und Kalender aus Exchange oder IBM Domino Konten
- Farbliche Differenzierbarkeit der einzelnen Kalender (iOS)
- Umfangreiche Möglichkeiten zur Navigation und Suche
- Unterstützung von Serienterminen
- Konfigurierbare Erinnerungen an Termine
- Zeitzonen-Unterstützung

AUFGABEN (NUR FÜR EXCHANGE)

- Aufgaben verwalten, erstellen, bearbeiten und löschen
- Übersichtliche Anzeige von fälligen und anstehenden Aufgaben
- Priorisierung von Aufgaben
- Konfigurierbare Aufgabenerinnerungen
- Erweiterte Sortier- und Filterfunktionen

NOTIZEN (NUR FÜR EXCHANGE AUF IOS)

- Notizen verwalten, erstellen, bearbeiten und löschen
- Suchen, Sortieren und Filtern von Notizen

BROWSER

- Zugriff auf Webseiten und webbasierte Anwendungen im Internet und Intranet
- Verwaltung von Lesezeichen und Desktopansichtsmodus
- Speichern von Benutzernamen und Passwörtern
- Verwaltung von erlaubten und verbotenen Webseiten (zentral zu definieren)
- Verwendung mehrerer Tabs
- Upload von HTML-Dateien aus SecurePIM Dokumenten
- Automatische Zerfifikatsauthentifizierung beim Zugriff auf Websites
- NTLM-Authentifizierung beim Zugriff auf SharePoint-Seiten ist im SecurePIM Management Portal oder Mobile Device Management von der IT definierbar

DOKUMENTE

- Sicheres Abspeichern von Dokumenten aus Anhängen und Zugang zu File-Servern der Organisation wie z.B. SharePoint (iOS)
- Unterstützung einer Vielzahl von Dokumenttypen (z.B. PDF, Microsoft Office Dokumente, Bilder, E-Mails, u.v.m.)
- Bearbeitung von Dokumenten mit Polaris Office Enterprise
- File picker (native iOS Anwendung) z. B. Dokumente aus verschiedenen Speicherorten innerhalb eines einzigen Dialogfensters auswählen
- Öffnen von Dokumenten im Offline-Modus
- Einfügen von Lesezeichen, Anmerkungen, Hervorhebungen
- Optimierung großer PDF-Dokumente mit Lesezeichen möglich (iOS)
- Versand von Dokumenten über das E-Mail Modul
- „Öffnen-In“ Funktion erlaubt Apps außerhalb des Containers Dokumente zu öffnen und zu bearbeiten (einstellbar im SecurePIM Management Portal durch den IT-Administrator)

KAMERA

- Verwendung der Gerätekamera im sicheren Container
- Aufgenommene Fotos werden immer auf dem Gerätespeicher verschlüsselt gespeichert (andere Apps auf dem Gerät haben keinen Zugriff auf die aufgenommenen Fotos, und die Fotos werden nicht auf Cloud-Server hochgeladen)
- Zugang zur Kamera direkt beim Verfassen einer E-Mail

SecurePIM Management Portal

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

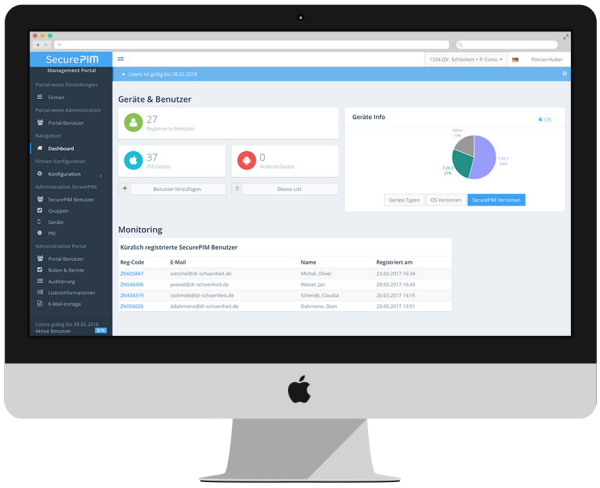
SecurePIM lässt sich einfach in die bestehende IT-Infrastruktur integrieren. Darüber hinaus kann es auch für verschiedene Mobile Device Management Systeme konfiguriert werden, die AppConfig Community Standards unterstützen.

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

Die Verwaltung und Pflege der Nutzer ist ebenfalls einfach. Administratoren können Nutzer entweder manuell oder durch LDAP Import hinzufügen, Nutzergruppen oder Abteilungen mit verschiedenen Sicherheitsstandards ausstatten und vieles mehr.

Das SecurePIM Management Portal bietet auch ein Self-Service-Portal, das optional aktiviert werden kann. Im Self-Service-Portal können Benutzer 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 Administratoren eine Vielzahl an Möglichkeiten um die SecurePIM App zu konfigurieren.

Festlegen der Sicherheitseinstellungen für die Geräte, die SecurePIM nutzen:

+ 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 auf Geräten der Mitarbeiter erzwingen
+ Registrierung modifizierter Geräte (Jailbreak bzw. Root) zulassen oder verbieten

Einfache Benutzerverwaltung:

+ Sowohl manuelle Benutzererstellung als auch LDAP Import möglich
+ Bestehende Benutzergruppen oder Abteilungen (mit verschiedenen Sicherheitsstandards) können ebenfalls per LDAP importiert werden
+ Verwalten von E-Mail Vorlagen (z. B. zum Versand von Registrierungsinformationen) in beliebig vielen Sprachen

Schnelle Reaktion auf Bedrohungen & Gefahren:

+ Ferngesteuertes Blocken von SecurePIM für gezielte Geräte
+ Ferngesteuertes Zurücksetzen: Alle Daten im Sicherheitscontainer werden restlos entfernt (die privaten Daten außerhalb des Containers werden nicht beeinflusst)

Umfangreicher Support der SecurePIM Benutzer:

+ Log-Dateien einzelner Geräte abrufbar, um Fehlerursachen zu erkennen
+ Genaue Statusabfragen zum Registrierungsstatus
+ Möglichkeit ungenutzte SecurePIM Lizenzen automatisch zu entfernen und für andere Benutzer verfügbar zu machen
+ Verwaltung von mehreren MAM-Administratoren und deren Rechte

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
+ Zugang zu Zertifikatsperrlisten
+ Bereitstellung des öffentlichen Schlüssels des E-Mail Senders

SecurePIM Gateway

Das Gateway sichert die Verbindung der SecurePIM App mit der Infrastruktur der Firma. 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 DMZ der Firma installiert. Eine bestimmte Schnittstelle in der Firewall muss geöffnet werden damit die SecurePIM App von außen Zugang bekommt. Das Gateway unternimmt eine Identitätsprüfung des Nutzers und erlaubt nur verifizierten Nutzern einen Zugriff.

+ Zugang zu MS Exchange, File-Diensten (via WebDAV), Webseiten und Web-App-Diensten
+ Cloud oder On-Premise Einsatz möglich
+ Unterstützt bis zu 200 Nutzer gleichzeitig pro Gateway Vorgang (für mehr Nutzer kann ein Clustering eingestellt werden)
+ Konfiguration und Kontrolle über das SecurePIM Management Portal, welches Zertifikat generiert und an das Gateway zur Identitätsprüfung verteilt

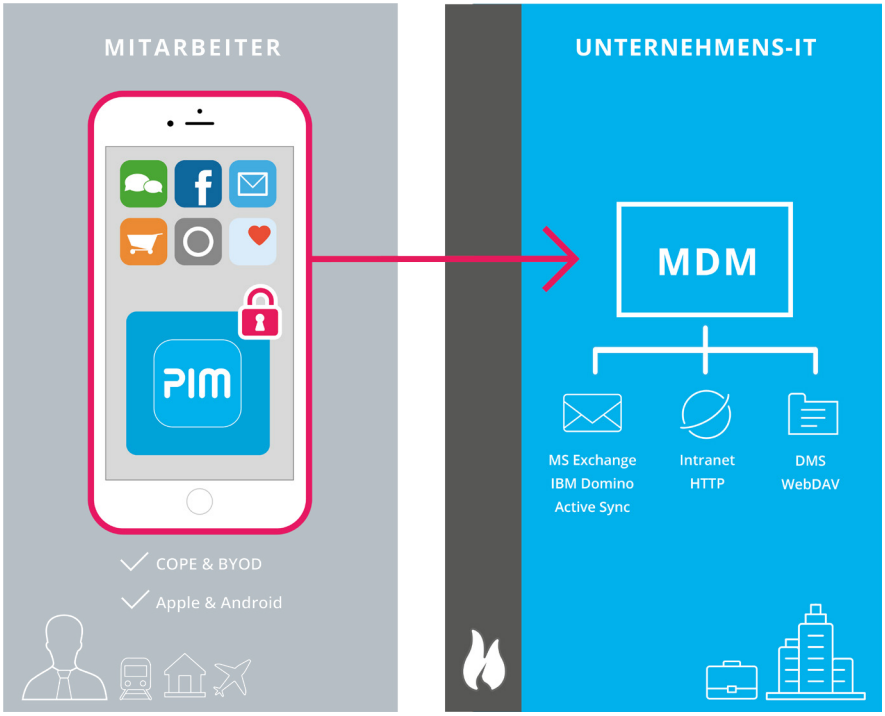
Mobile Device Management

Als alleinstehende Lösung kann SecurePIM über das SecurePIM Management Portal verwaltet werden. Darüber hinaus kann SecurePIM auch für gängige Mobile Device Management Systeme konfiguriert werden, wenn sie AppConfig Community Standards unterstützen.

Das MDM ermöglicht:

+ Die SecurePIM App auf dem Gerät des Nutzers erzwingen
+ Überwachung der App und des gesamten Gerätes

Des Weiteren, können auch Apple's Configurator oder Profile Manager verwendet werden.



Smartcard Integration (NUR FÜR IOS)

Die SecurePIM App ist durch Passwort, PIN oder Fingerabdruck des Nutzers gesichert. Für höchste Sicherheitsansprüche kann SecurePIM zusätzlich mit einer Smartcard gesichert werden. 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

+ Unterstützung von Bluetooth AirID von Unicept und Tactivo Smartcard-Lesern von Precise Biometrics
+ Unterstützung unterschiedlicher Smartcards (z. B. Atos® CardOS (4.2C, 4.3B, 4.4, 5.0, 5.3), TeleSec 3 TCOS® IDKey, TCOS 3 SignatureCard 2.0, StarCOS 3.2, Sm@rtCafe Expert 3.2/6.0, SmartCardHSM)
+ 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

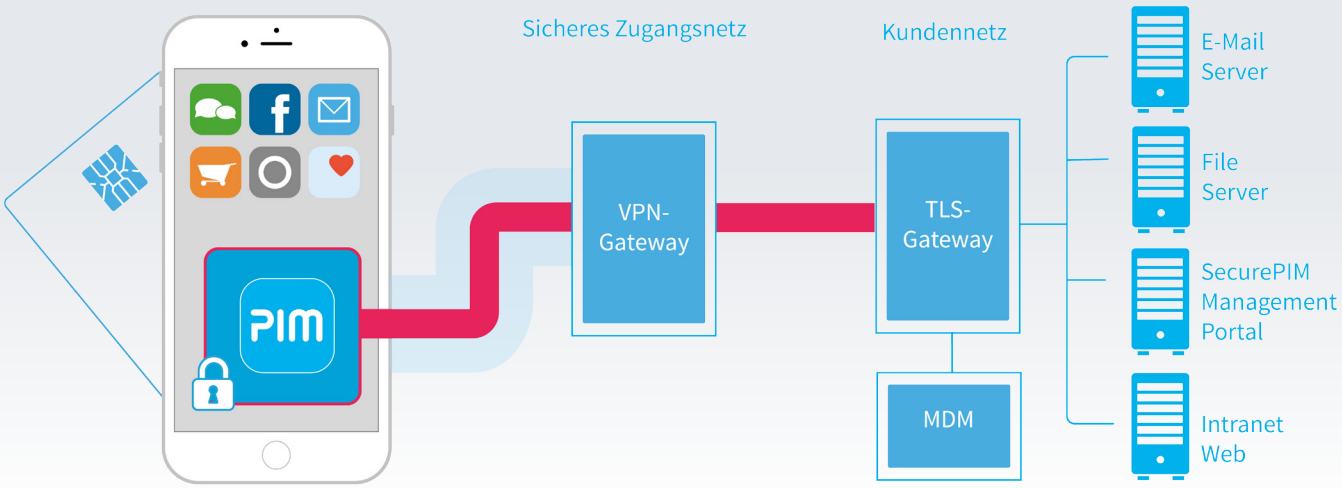
SecurePIM Government SDS

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, Apple® iPhone® oder iPad® 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 Informationen mit dem Geheimhaltungsgrad VS-NfD (Verschlusssache – nur für den Dienstgebrauch) auf iPhone und iPad.

SecurePIM Government SDS Architektur



Die folgenden Komponenten sind für SecurePIM Government SDS immer obligatorisch:

+ Geräte mit Betriebssystem iOS Version 10 und höher
+ Smartcard (TCOS 3.0 Signature Card Version 2.0)
+ SecurePIM Management Portal
+ MDM zur zentralen Geräteverwaltung
+ TLS Gateway
+ IPSEC-VPN

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. IPsec ermöglicht dabei:

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

TLS-Gateway

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

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

TECHNISCHE VORAUSSETZUNGEN

Mobilgeräte:

- **iOS:** Aktuell werden alle Betriebssystemversionen ab iOS 10 unterstützt
- **Android:** Android Gerät mit von Google zertifiziertem Android Betriebssystem - *Ab Android Version 4.4 und API Level 19*

E-Mail Server:

- Microsoft Exchange Server mit dem ActiveSync Protokoll 14.0 oder 14.1
- IBM Domino Server mit ActiveSync / Notes Traveler ab 9.0.1.15.

Datei-Server:

- SharePoint Versionen 2007, 2010 or 2013
- WebDAV-Standard-Systeme

Technische Voraussetzungen für SecurePIM Management Portal

Hardware:

- Prozessor: 2-Kern-Prozessor mit mindestens 2 GHz
- RAM: Mindestens 8 GB
- Plattenplatz: Mindestens 20 GB

Betriebssystem:

Alle Betriebssysteme, die von der eingesetzten Version der Servlet Engine (Apache Tomcat) unterstützt werden

Servlet Engine:

Apache Tomcat 7 oder höher

Web-Server:

Apache Web-Server (HTTP-Server) Version 2.4 mit mod_ssl und mod_proxy_ajp

Java-Laufzeitumgebung:

Eine der Folgenden:

- Oracle JDK 8 und Java Cryptography Extension (JCE) Unlimited Strength Policy Files
- OpenJDK 8

Datenbank:

Eine der Folgenden:

- H2 Database (im Installationspaket des SecurePIM Management Portals enthalten)
- MySQL 5.5; weitere Versionen auf Anfrage

Server-Zertifikat:

- Server-Zertifikat, um die Verbindung zum SecurePIM Management Portal zu verschlüsseln

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/clm/
  Port 443 (HTTPS) muss für ausgehende Verbindungen offen sein

Service & Support

Sicherheitsexperten von Virtual Solution stehen zur Verfügung, um Service und Support in höchster Qualität zu leisten. Als zusätzlichen Qualitätsservice implementiert Virtual Solution außerdem Code Hardening und stellt eine detaillierte technische Dokumentation bereit.

Integrationsservice

Die erfahrenen Sicherheitsspezialisten von Virtual Solution stehen auch für zusätzliche Trainings und Integrationsdienstleistungen innerhalb eines Beratungsprojekts zur Verfügung:

+ Bereitstellung von TLS Konfigurationen
+ Technische Integrationstests

Produktbezogener Update und Upgrade Support

Sowohl die SecurePIM App als auch das Management Portal werden durch einen fortlaufenden Produktsupport unterstützt. Updates und Upgrades sind im Jahresabonnement enthalten.

Über Virtual Solution AG

Virtual Solution hat es sich zur Aufgabe gemacht Sicherheit und Benutzerfreundlichkeit in der mobilen Arbeitswelt der Zukunft zu verbinden. Bereits seit 1996 entwickelt und vertreibt das deutsche Unternehmen Sicherheitslösungen, die zugeschnitten sind auf die Sicherheitsbedürfnisse einer zunehmend digitalisierten und mobilen Gesellschaft.

KONTAKT

Virtual Solution AG
Blutenburgstr. 18
80636 München

kontakt@virtual-solution.com
+49 (0)89 30 90 57-100
www.virtual-solution.com