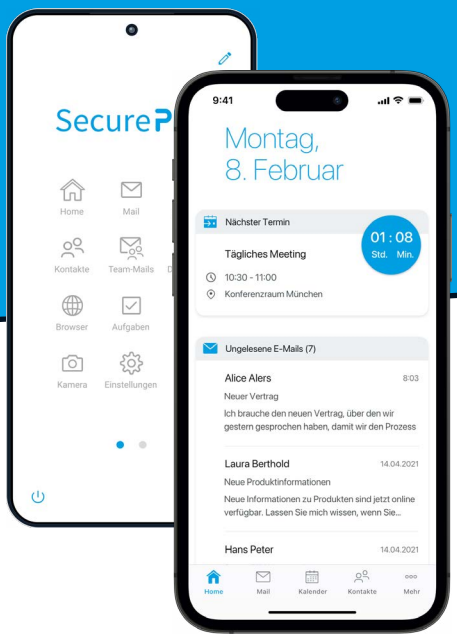
SecurePIM
by Materna Virtual Solution

SecurePIM Government SDS

Smartphone und Tablet dienstlich nutzen

Zuverlässiger Schutz für mobile Kommunikation



SecurePIM Government SDS bietet Bundes- und Landesbehörden die Möglichkeit, in einer sicheren Umgebung mobil zu arbeiten – jederzeit von überall.

SecurePIM Government SDS ist eine vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zugelassene Systemlösung für die Verarbeitung von Daten mit dem Geheimhaltungsgrad VS-NfD (Verschlusssachen – nur für den Dienstgebrauch) auf iOS- und Android-Geräten (Einsatzerlaubnis für Android). Damit ist SecurePIM Government SDS in Verbindung mit einer Smartcard die einzige plattformübergreifende und geräteunabhängige Lösung für VS-NfD. Zusätzlich ist die iOS-Version auch für NATO RESTRICTED zugelassen.

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 sicher in die tägliche Arbeit zu integrieren. Die Daten werden über einen zentralen Zugang des Informationsverbunds Berlin-Bonn (IVBB/NdB) oder ähnlichen Netzwerken mit den Servern der Hausnetze synchronisiert.

Produktivität überall

SecurePIM Government SDS erlaubt es Mitarbeitenden 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 Dokumentenablagesystemen 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 Mitarbeitende Smartphones und Tablets für ihre tägliche Arbeit von unterwegs nutzen und sogar offline auf diesen Geräten arbeiten.

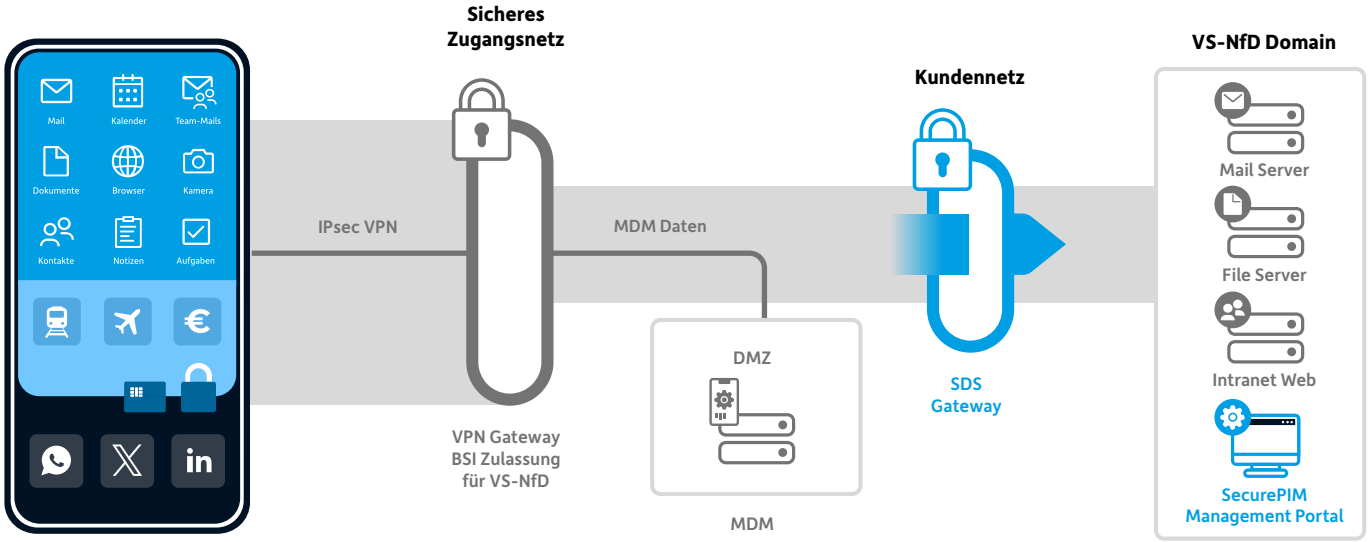
Vorteile für Ihre Teams

+ Sicheres mobiles Arbeiten mit Smartphone und Tablet
+ Einfache und intuitive Nutzung
+ Mobile dienstliche Kommunikation in nur einer App
+ Zugriff auf mehrere E-Mail Accounts
+ Dokumente online und offline editieren
+ Gerät kann durch biometrische Authentifizierung entsperrt werden
+ Die interne Smartcard (iOS) ermöglicht sicheres mobiles Arbeiten ohne den Einsatz einer physischen Smartcard mit Lesegerät

Sicherheit

+ Vom BSI zugelassene Lösung für VS-NfD (Zulassung für iOS; Einsatzerlaubnis für Android) und NATO RESTRICTED (iOS)
+ Nach deutschen Datenschutz-Richtlinien entwickelt
+ Zusätzliche Sicherung der Daten durch eine interne oder externe Smartcard
+ Trennung von öffentlichen und dienstlichen Daten durch den Container-Ansatz
+ Dienstliche Daten sind sowohl auf dem Gerät als auch bei der Übertragung verschlüsselt
+ Sichere Kommunikation mit dem Intranet via SDS Gateway
+ Vollständige S/MIME Unterstützung
+ Entwickelt vom deutschen Unternehmen Materna Virtual Solution GmbH

SecurePIM
by Materna Virtual Solution



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.

Alternativ kann für iOS das Feature »interne Smartcard« verwendet werden. Es ist in das mobile Gerät integriert und ermöglicht die Registrierung und Anmeldung bei SecurePIM. Dadurch wird wie bei der externen Smartcard die Datenvertraulichkeit, sichere Datenspeicherung und Datenübertragung gewährleistet – ohne dass eine externe Smartcard und Lesegerät erforderlich sind. Bei der Verwendung der internen Smartcard sind nur das mobile Gerät und die Geräte-PIN oder der Geräte-Code erforderlich.

Trennung von dienstlich und persönlich

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

Sichere E-Mail-Kommunikation

Neben dem Senden und Empfangen von S/MIME verschlüsselten E-Mails kann über eindeutige Signatur auch zuverlässig identifiziert werden, von wem die E-Mail gesendet wurde. Innerhalb der SecurePIM App werden alle Daten verschlüsselt abgelegt.

Kompatibilität

+ Plattformübergreifend und geräteunabhängig für iOS und Android
+ Unterstützung von Mail-Servern mittels ActiveSync
+ Zugang zu Dateien über WebDAV
+ Synchronisation mit Ihrem LDAP

Komponenten der Systemlösung

+ iOS- oder Android-Endgeräte (spezifische Vorgaben bei Android)
+ Interne oder externe Smartcard
+ NFC oder Lesegerät im Falle einer externen Smartcard
+ Frei wählbares Mobile-Device-Management-System (MDM)
+ SecurePIM App
+ Server-Komponenten: SDS Gateway, SecurePIM Management Portal
+ SERA Sicherheits-Framework

SecurePIM App Module

+ Mail
+ Team-Mails
+ Kontakte
+ Kalender
+ Notizen
+ Aufgaben
+ Dokumente (Erstellen, Bearbeiten und Speichern)
+ Browser (Zugang zu Intranet und Internet)
+ Sichere Kamera
+ Messenger (optional, in Zulassung)

MATERNA
Virtual Solution

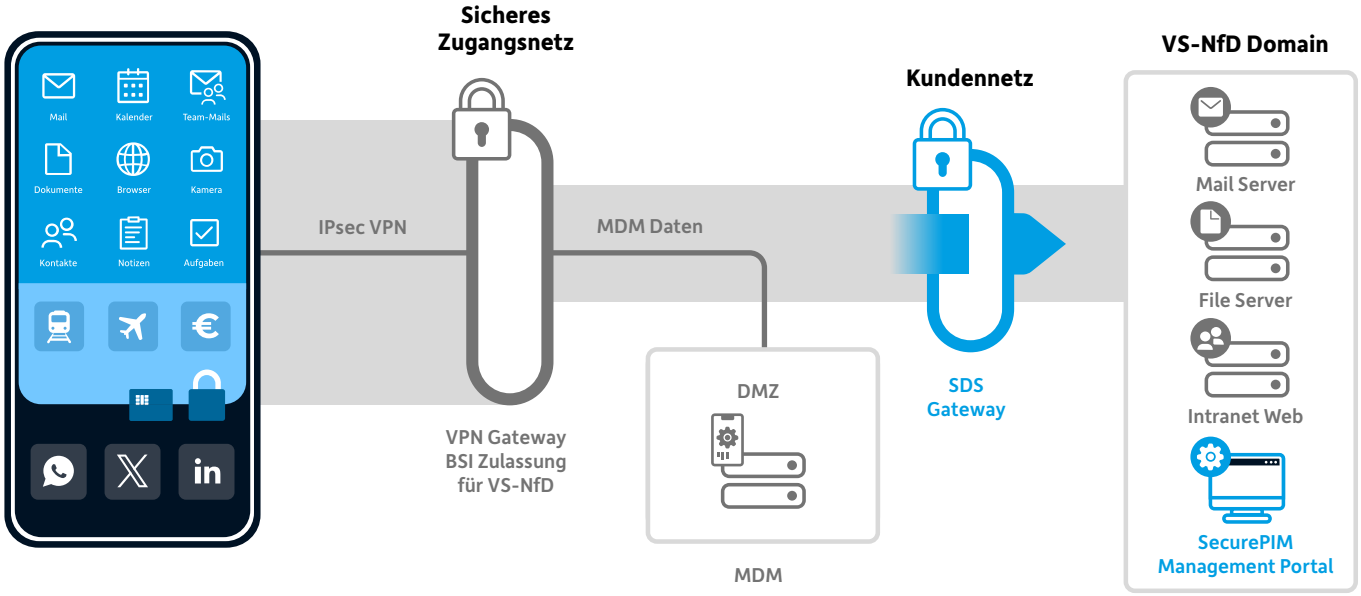
Materna Virtual Solution GmbH
Mühldorfstraße 8 · 81671 München · T +49 89 30 90 57-0
kontakt@virtual-solution.com · www.materna-virtual-solution.com

VS-NfD
FÜR iOS UND ANDROID
SICHERHEIT MADE IN GERMANY

NATO RESTRICTED
FÜR iOS
SICHERHEIT MADE IN GERMANY

P-24.0072_SPIM_Faktenübersicht GOV SDS_de/de_v16_11/24

SecurePIM
by Materna Virtual Solution



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.

Alternativ kann für iOS das Feature »interne Smartcard« verwendet werden. Es ist in das mobile Gerät integriert und ermöglicht die Registrierung und Anmeldung bei SecurePIM. Dadurch wird wie bei der externen Smartcard die Datenvertraulichkeit, sichere Datenspeicherung und Datenübertragung gewährleistet – ohne dass eine externe Smartcard und Lesegerät erforderlich sind. Bei der Verwendung der internen Smartcard sind nur das mobile Gerät und die Geräte-PIN oder der Geräte-Code erforderlich.

Trennung von dienstlich und persönlich

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

Sichere E-Mail-Kommunikation

Neben dem Senden und Empfangen von S/MIME verschlüsselten E-Mails kann über eindeutige Signatur auch zuverlässig identifiziert werden, von wem die E-Mail gesendet wurde. Innerhalb der SecurePIM App werden alle Daten verschlüsselt abgelegt.

Kompatibilität

+ Plattformübergreifend und geräteunabhängig für iOS und Android
+ Unterstützung von Mail-Servern mittels ActiveSync
+ Zugang zu Dateien über WebDAV
+ Synchronisation mit Ihrem LDAP

Komponenten der Systemlösung

+ iOS- oder Android-Endgeräte (spezifische Vorgaben bei Android)
+ Interne oder externe Smartcard
+ NFC oder Lesegerät im Falle einer externen Smartcard
+ Frei wählbares Mobile-Device-Management-System (MDM)
+ SecurePIM App
+ Server-Komponenten: SDS Gateway, SecurePIM Management Portal
+ SERA Sicherheits-Framework

SecurePIM App Module

+ Mail
+ Team-Mails
+ Kontakte
+ Kalender
+ Notizen
+ Aufgaben
+ Dokumente (Erstellen, Bearbeiten und Speichern)
+ Browser (Zugang zu Intranet und Internet)
+ Sichere Kamera
+ Messenger (optional, in Zulassung)

MATERNA
Virtual Solution

Materna Virtual Solution GmbH
Mühldorfstraße 8 · 81671 München · T +49 89 30 90 57-0
kontakt@virtual-solution.com · www.materna-virtual-solution.com

VS-NfD
FÜR iOS UND ANDROID
SICHERHEIT MADE IN GERMANY

NATO RESTRICTED
FÜR iOS
SICHERHEIT MADE IN GERMANY

P-24.0072_SPIM_Faktenübersicht GOV SDS_de/de_v16_11/24