

SecurePIM Government SDS

Secure Mobile Productivity for Smartphones and Tablets

Government-grade protection for sensitive data



SecurePIM Government SDS enables government employees to work remotely, any time from any location, while complying with high security and data protection standards. SecurePIM Government SDS is the only security solution approved by the German Federal Office for Information Security (BSI) to allow the processing and transfer of information marked as “restricted” (“Verschlussache - nur für den Dienstgebrauch” – VS-NfD) on iOS devices.

Top-Notch Security

SecurePIM Government SDS is a special-system solution developed with BSI’s high security requirements and it enables government employees to work remotely using a smartphone or tablet. All data is securely synchronized with local network servers via a central access to Information Network Berlin-Bonn (IVBB) or other similar networks. In combination with its smartcard solution, SecurePIM Government SDS is the only certified solution to allow the processing and transfer of information marked as “restricted” (VS-NfD) on iPhones and iPads.

Powerful Productivity and Access from Anywhere

SecurePIM Government SDS provides public sector employees with access to critical data, such as email, contacts, calendars, notes, tasks, documents, and a protected camera and photo album. Additionally, users can access intranet sites and web applications while on the go. Further functionalities include document editing and integration of specialized processes. With these functionalities, government employees can use smartphones and tablets to access critical data from any location and even work while offline. As an optional feature SecurePIM Government SDS also offers the possibility to initiate encrypted calls directly from within the app, without any intermediate steps.

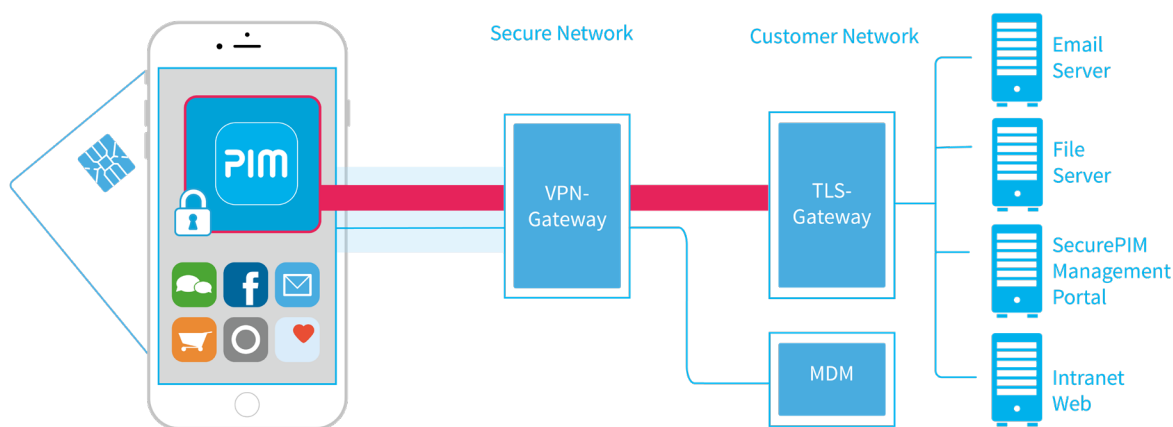


Benefits for Employees:

- + Secure access to sensitive data using smartphones and tablets
- + Intuitive and easy to use
- + Initiate encrypted calls directly from within the app
- + Management of up to three email accounts
- + Document editing while online and offline
- + Touch ID support

Security:

- + BSI certified solution
- + Developed based on German data protection guidelines
- + Smartcard integration with support for various smartcard readers
- + Strict separation of public and classified data via SecurePIM Container technology
- + State-of-the-art encryption for data at rest and in transit
- + Secure communication to local network via SecurePIM TLS Gateway
- + Full S/MIME support
- + Developed by German provider Virtual Solution AG



Smartcard Integration

For the highest security requirements, **SecurePIM Government SDS** integrates a smartcard as its security anchor. All asymmetric encryption operations are based on private keys stored on and never leaving the smartcard. Currently **SecurePIM Government SDS** supports various smartcard readers, like AirID® by Unicept and Tactivo™ by Precise™ Biometrics.

Separation of Personal and Government Data

Implemented as a Container solution, **SecurePIM Government SDS** provides controlled access to classified data by strictly separating it from all other content on the mobile device. All data within the Container is highly encrypted with a smartcard, so no other app or unauthorized person can access information in the Container.

Built-in Secure Email

SecurePIM Government SDS encrypts all data and communication. Employees can send and receive S/MIME encrypted emails and sender verification is provided with a unique S/MIME signature.

Encrypted Voice Calls

As an optional feature **SecurePIM Government SDS** also offers end-to-end encryption for voice calls. The functionality requires low band width and works over GPRS, EDGE, 3G, WiFi and satellite, so that calls are transmitted reliably and in a high voice quality. No pre-installed keys are used and encryption using two parallel algorithms provides the highest level of security. All this while being easy and comfortable to use. The **SecureVoice** functionality integrates seamlessly with the other modules of the **SecurePIM App**. Please note that SecureVoice is only available for German authorities.

NEW!

Compatibility:

- + iOS (version 11 or higher) or Android (approval expected in Q4/19; version 5.0 or higher)
- + Supports email servers using ActiveSync
- + Access to files using WebDAV
- + User sync with LDAP

Components of the System Solution:

- + iOS (approved version) or Android device (approval expected in Q4/19)
- + Smartcard (support for TCOS 3.0 Signature Card Version 2.0)
- + Smartcard reader
- + Mobile Device Management (MDM)
- + SecurePIM App
- + Virtual Solution Server Components: SecurePIM TLS Gateway, SecurePIM Mobile Application Management Portal (MAM), SERA security framework

SecurePIM App Modules:

- + Email
- + Contacts
- + Calendar
- + Notes
- + Tasks
- + Documents (edit and store files securely)
- + Browser (secure access to intranet and web)
- + Secure Camera
- + SecureVoice (optional)