SecurePIM Government SDS

Secure Mobile Productivity for iPhones and iPads

Government-grade protection for sensitive data

With more government workers using mobile devices, data security is becoming a greater IT challenge.

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 for Apple® devices (iPhone® or iPad®) by the German Federal Office for Information Security (BSI).

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 an Apple iPhone or iPad. 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" ("Verschlusssache - nur für den Dienstgebrauch" - VS-NfD) using an iPhone and iPad.

## 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. With this functionality, government employees can use an iPhone or iPad to access critical files from any location and even work while offline.

Benefits for Employees:

+ Secure access to sensitive data using iPhone and iPad
+ Intuitive and easy to use
+ 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 Vitual Solution AG
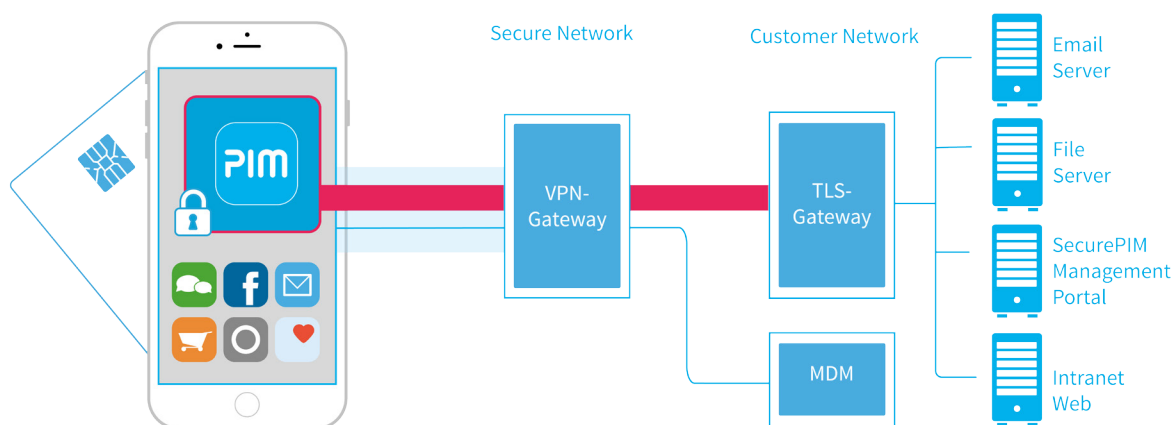
Smartcard Integration

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.

About Virtual Solution AG

Virtual Solution's primary goal is to unify security and usability for today's mobile working world. Since 1996, we have been developing security solutions that support the needs of an increasingly digital and mobile society.

Compatibility:

+ iOS (version 10 or higher)
+ Supports email servers using ActiveSync
+ Access to files using WebDAV
+ User sync with LDAP

Components of the System Solution:

+ iOS device (version 10 or higher)
+ 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