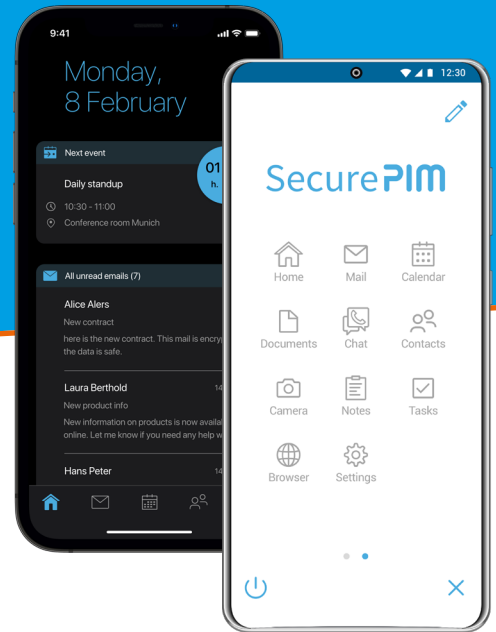# SecurePIM
by Virtual Solution

SecurePIM Government SDS

Using smartphones and tablets for classified data

Reliable protection for mobile communication

SecurePIM Government SDS enables government employees to work remotely, any time from any location.

SecurePIM Government SDS is a security solution approved by the German Federal Office for Information Security (BSI) for processing data classified as "restricted" ("Verschlusssache - Nur für den Dienstgebrauch" - VS-NfD) on iOS and Android devices ("Freigabeempfehlung" for Android). In combination with a smart card, SecurePIM Government SDS is the only certified cross-platform and device-independent solution for VS-NfD.

Security for government authorities - certified by the BSI

Commissioned by the German Federal Office for Information Security (BSI), SecurePIM Government SDS was developed to enable government authorities to securely integrate smartphones and tablets into their daily work. All data is securely synchronized with local network servers via central access to the Berlin-Bonn (IVBB/NdB) or comparable specific networks.

Productivity from anywhere

SecurePIM Government SDS allows employees of government authorities and other public institutions to access email, calendar and contacts while on the go. They also have access to a secure camera that stores images in the secured app. Additionally, access to document filing systems and intranet sites is possible via a secure connection. Includes document editing and the integration of specific processes. This allows employees to use smartphones and tablets for their daily work on the go and even work offline on these devices.

SecurePIM Government SDS can also enable encrypted calls directly from the contact directory (optional, requires additional app).
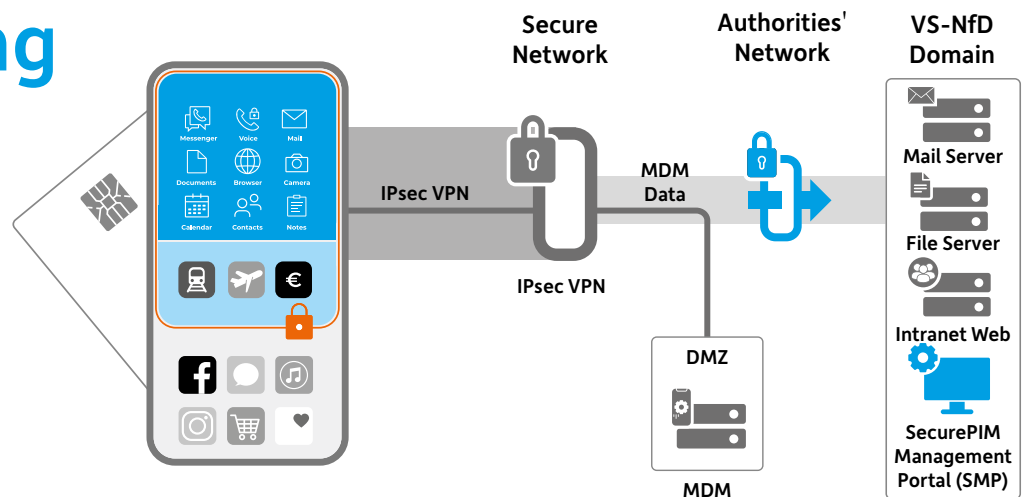
Benefits for employees
+ Work securely on smartphones and tablets
+ Intuitive and easy to use
+ Mobile business communication in just one app
+ Start encrypted voice calls within the app
+ Access multiple email accounts
+ Edit documents online and offline
+ Device can be unlocked by biometric authentication

Security
+ BSI certified solution for VS-NfD ("Zulassung" for iOS; "Freigabeempfehlung" for Android)
+ Developed based on German data protection guidelines (GDPR compliant)
+ Integration of various smart card readers
+ Strict separation of personal and classified data through the container approach
+ Internal data is encrypted at rest on the device as well as in transit
+ Secure communication into the intranet via SDS Gateway
+ Full S/MIME support
+ Developed by German company Virtual Solution AG

SecurePIM by Virtual Solution

Everything secure in one app.

Secure Network
Authorities' Network
VS-NfD Domain

IPsec VPN
MDM Data
IPsec VPN
DMZ
MDM

Mail Server
File Server
Intranet Web
SecurePIM Management Portal (SMP)

Smart card integration

For the highest security requirements, SecurePIM Government SDS is using a smart card for secure authentication. All asymmetric encryption operations are based on the private key of the smart card. The private key never leaves the card in the process.

Separation of "internal" and "personal"

Thanks to secure container technology, SecurePIM Government SDS provides controlled access to classified information without significantly limiting the flexible use of the smartphone or tablet. Data within the container is secured with the smart card. No other app on the device or unauthorized persons can get access to the data in SecurePIM Government SDS.

Secure email communication

Employees can send and receive S/MIME encrypted emails. The sender of an email can be reliably identified via a unique signature. Within the SecurePIM app, all data is encrypted.

Encrypted voice calls

As an optional module, SecurePIM also offers end-to-end encryption for voice. Even with only low bandwidth and using GPRS, EDGE, 3G, WiFi and satellite, calls are reliably connected and transmitted in high quality. At the same time, operation is easy and convenient. The SecureVoice function fits seamlessly into the other modules of the SecurePIM app. SecureVoice is only available for German government authorities.

Compatibility

+ Available for iOS (version 13 and above) and Android (version 7.0 and above)
+ Support for email servers via ActiveSync
+ Access to files via WebDAV
+ User synchronization with LDAP

Components of the system solution

+ iOS or Android end devices (specific requirements for Android)
+ Smart card readers AirID 1®, AirID 2®, AirID 2 mini®
+ Smart card (support for TCOS 3.0 Signature Card version 2.0)
+ Any Mobile Device Management (MDM) system
+ SecurePIM App
+ Virtual Solution server components: SDS Gateway, SecurePIM Management Portal (SMP)
+ SERA Security Framework

SecurePIM App Modules

+ Email
+ Contacts
+ Calendar
+ Notes (Exchange only)
+ Tasks (Exchange only)
+ Documents (create, edit and save)
+ Browser (access to intranet and web)
+ Secure Camera
+ SecureVoice (optional)
+ Messenger (optional, in approval)

>450 Authority & Enterprise customers

>100 Authorities & Defense

>45 Federal Authorities

>330.000 Users on iOS and Android

>90% Of our customers extend & renew their licenses

BSI RESTRICTED
Approval for iOS
Release for Android
SECURITY MADE IN GERMANY