SecurePIM
by Materna 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* (Verschlusssachen – nur für den Dienstgebrauch – VS-NfD) on iOS and Android devices (Pre-Approval for Android). In combination with a smart card, SecurePIM Government SDS is the only certified cross-platform and device-independent solution for VS-NfD. In addition, the iOS version is also approved for NATO RESTRICTED.

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.

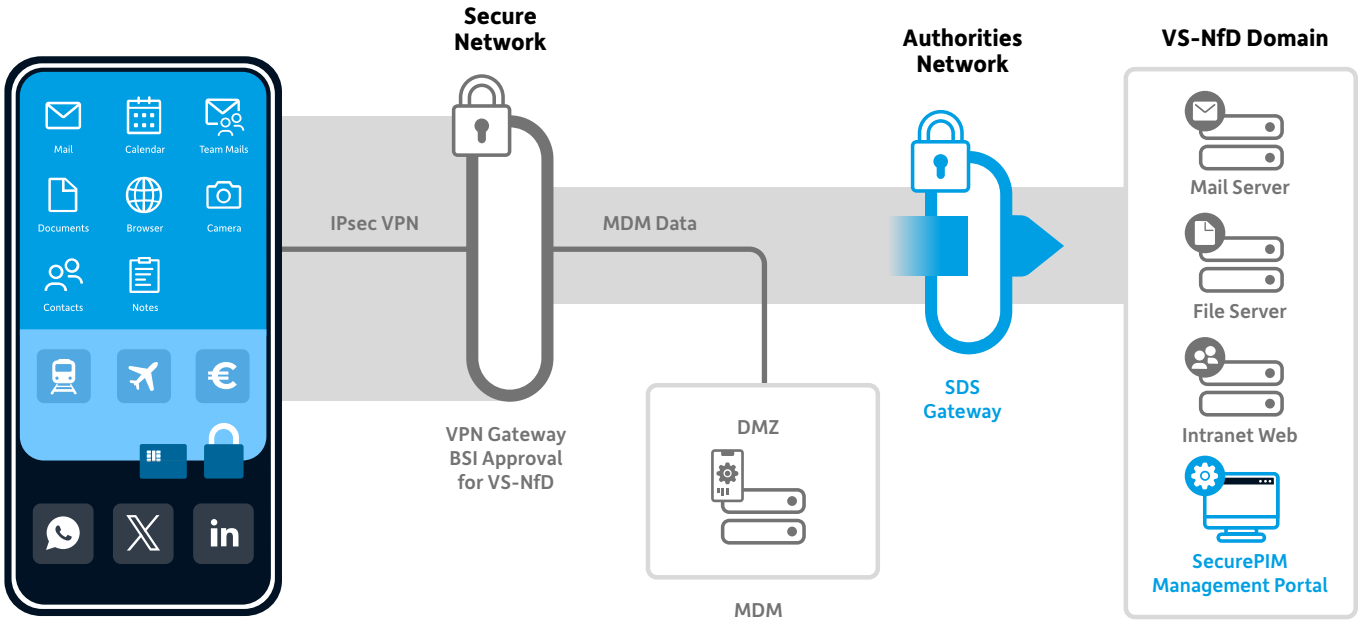
Benefits for employees

+ Work securely on smartphones and tablets
+ Intuitive and easy to use
+ Mobile business communication in just one app
+ Access multiple email accounts
+ Edit documents online and offline
+ Device can be unlocked by biometric authentication
+ The internal smartcard (iOS) enables secure mobile work without the use of a physical smart card and reader

Security

+ BSI certified solution for VS-NfD (Approval for iOS; Pre-Approval for Android) and NATO RESTRICTED (iOS)
+ Developed based on German data protection guidelines (GDPR compliant)
+ Additional data security by an internal or external smart card
+ 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 Materna Virtual Solution GmbH

SecurePIM
by Materna Virtual Solution



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.

Alternatively, the feature »internal smart card« can be used for iOS. It is integrated into the user's device and allows them to register and log in to SecurePIM. This eliminates the need for an external smart card and the necessary readers to ensure confidentiality, secure data storage, and transmission. When using the internal smart card, only the mobile device and the device PIN or device code are necessary.

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

In addition to sending and receiving S/MIME-encrypted emails, unique signatures can also be used to reliably identify who sent the email. Within the SecurePIM app, all data is encrypted.

Compatibility

+ Cross-platform and device-independent for iOS and Android
+ 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)
+ Internal or external smart card
+ NFC or reader in case of external smart card
+ Any Mobile Device Management (MDM) system
+ SecurePIM App
+ Server components: SDS Gateway, SecurePIM Management Portal
+ SERA Security Framework

SecurePIM App Modules

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

MATERNA
Virtual Solution

Materna Virtual Solution GmbH
Blutenburgstraße 18 · 80636 München · T +49 89 30 90 57-0
kontakt@virtual-solution.com · www.materna-virtual-solution.com

VS-NfD
FOR iOS UND ANDROID
SECURITY MADE IN GERMANY

NATO RESTRICTED
FOR iOS
SECURITY MADE IN GERMANY

P-23.0149_SPIM_Infosheet GOV SDS_en/uk_v11_11/23