PROTECTION MECHANISMS OF SECUREPIM

All data within SecurePIM is encrypted and separated from other data on the device. A whole bundle of measures applies to protect the information within SecuerPIM. This ranges from the encryption of local data on the device, over jailbreak protection, to securing the communication with backend systems.

SEPARATION OF PRIVATE AND BUSINESS DATA VIA CONTAINER TECHNOLOGY

The SecurePIM container creates a segregated, secure area on the device. All corporate data within this container is encrypted and strictly separated from other apps on the device. No other application (e.g., Facebook, WhatsApp), system, or unauthorized person can gain access to the data within the container. Thus, company data is protected with a password. Thanks to this container technology, companies have an easy-to-use solution that enables employees to work mobile without worrying about security.

LOCAL ENCRYPTION

All data within the SecurePIM Container is secured with state-of-the-art encryption (hybrid encryption with RSA up to 4096 Bit and AES-256) and protected with a PIN, password, or fingerprint. As part of the approval of the SecurePIM Government SDS system-solution for processing information classified as “Restricted” (VS – NfD), the encryption method of SecurePIM has also been audited by the German Federal Office for Information Security (BSI).

SMARTCARD INTEGRATION

The SecurePIM app is secured by the user’s password, PIN, or fingerprint. For strongest security demands, SecurePIM can integrate a smartcard. All asymmetric encryption operations are based on the private key of this smartcard. The certificates and private keys are physically and permanently stored on the card. This protects the data with an additional security anchor, in case the device ends up in the wrong hands.

ENCRYPTION IN TRANSIT

Encryption of data in transit ensures that sensitive information is transmitted securely over any network. SecurePIM establishes a secure communication with the following backend systems:

- With MS ActiveSync or IBM Traveler servers via the ActiveSync protocol (TLS encryption)
- With the SecurePIM Management Portal via a web service interface (TLS encryption)
- Communication with the corporate network can be established via the SecurePIM Gateway. The gateway´s security relies on a key-based authentication and does not require a VPN infrastructure, nor VPN profiles for mobile devices. The SecurePIM Gateway checks the user‘s identity and allows access to verified users only.

END-TO-END ENCRYPTION WITH S/MIME AND IBM DOMINO

In order to protect sensitive information from potential spying, SecurePIM can encrypt emails. To do so, the Secure/Multipurpose Internet Mail Extensions (S/MIME) standard is applied. This way, the email remains protected from access by third parties during its entire trajectory, from the moment it is sent until the time of decryption by the receiver and throughout all data links and servers, to make sure that only an authorized person can read the email and its attachments.

The S/MIME standard is applied for both encryption and decryption, as well as for signing and validating the signature in emails. This helps to protect against email phishing and identity theft.

As a result of a tight cooperation with IBM, SecurePIM is also available for IBM Domino users. With this unique approach, IBM Domino users do not need middleware or additional companion apps for S/MIME and IBM Notes encryption and decryption.

CERTIFICATE-BASED AUTHENTIFICATION

By means of the activation of certificate-based authentication, access to sensitive systems can be made more secure in addition to TLS encryption. For example, access to the ActiveSync server or intranet applications can be configured so they require certificate-based authentication. This is a standard setting in case of the configuration of the SecurePIM TLS-Gateway. Here, not only SecurePIM checks the server certificate, but also the server checks the user certificate.

Client (SecurePIM App) and server thus perform a TLS handshake, in which the communication partners authenticate each other and agree on the cryptographic algorithms to be used. After the TLS channel is established, data can be transmitted in an encrypted format.

CENTRAL MANAGEMENT VIA SECUREPIM MANAGEMENT PORTAL

All security-related settings of SecurePIM can be centrally managed via its own Management Portal:

- User management
- Defining rules and settings for encryption
- Password policies
- Defining timeout periods, leading to an automatic log-out
- Remote reset of all company data within SecurePIM container in case of device loss
- Group management and configuration of different security policies for various user groups
- Granting access or blocking data interfaces between SecurePIM and the device
- Further security policies for working within the container (e.g. enabling or disabling functionalities like copy/paste, auto-complete, open-in or screenshots).

These policies help to ensure that the security requirements are met on all mobile devices of the employees. All security-related functionalities can be correspondingly changed, depending on the desired configuration latitude and security level. If desired, SecurePIM can also be managed via an MDM solution.

PROTECTION AGAINST MANIPULATION

In order to protect data on mobile devices from manipulation, SecurePIM offers the possibility to quickly identify attacks and prevent access to SecurePIM.

- **Integrity check:**

  The SecurePIM integrity check provides full control over all SecurePIM versions which users are allowed to use. Every version of the app has a fingerprint that is unique and enables the exact identification of the software. This ensures that only the versions of SecurePIM authorised by the company can be set up and used.

- **Jailbreak detection:**

  Jailbreaking modifies the device's operating system and can turn off the security mechanisms of the device. This way a user or an app can get root privileges and have full access to the operating system of the device. Manipulated devices can be detected in the SecurePIM Management Portal. The usage of the SecurePIM app and the container are then blocked.