DIE **SCHUTZMECHANISMEN** VON SECUREPIM

Alle von SecurePIM verwalteten Daten sind verschlüsselt und von anderen Daten auf dem Gerät getrennt. Zum Schutz der Informationen dient ein ganzes Bündel an Maßnahmen. Dies reicht von der Verschlüsselung der lokalen Daten auf dem Endgerät, über Jaillbreak-Protection, bis hin zur Absicherung der Kommunikation mit Backend-Systemen.

CONTAINER TECHNOLOGIE FÜR TRENNUNG VON PRIVATEN UND GESCHÄFTLICHEN DATEN

Der SecurePIM Container erstellt einen abgetrennten, sicheren Bereich auf dem Gerät. Alle Unternehmensdaten innerhalb dieses Containers sind verschlüsselt und strikt von anderen Apps auf dem Gerät getrennt. Keine andere Anwendung oder System auf dem Endgerät (z.B. Facebook, WhatsApp) oder eine nicht autorisierte Person kann Zugang zu den Daten im Container bekommen. Unternehmensdaten sind auf dem Gerät isoliert und passwortgeschützt. Dank der Container-Technologie haben Firmen eine einfach zu handhabende Lösung, die es Mitarbeitern ermöglicht flexibel auf mobilen Endgeräten zu arbeiten ohne sich Sorgen um die Sicherheit machen zu müssen.

LOKALE VERSCHLÜSSELUNG

Alle Daten innerhalb des SecurePIM Containers sind nach dem aktuellen Stand der Technik verschlüsselt (hybride Verschlüsselung mit RSA bis zu 4096 Bit und AES-256) und durch eine PIN, ein Passwort oder einen Fingerabdruck geschützt. Die Verschlüsselungsmethode wurde auch im Zuge der Zulassung der Systemlösung SecurePIM Government SDS vom BSI geprüft.

SMARTCARD-INTEGRATION

Die SecurePIM App ist durch Passwort, PIN oder Fingerabdruck des Nutzers gesichert. Für höchste Sicherheitsansprüche kann SecurePIM zusätzlich mit einer Smartcard geschützt werden. Alle asymmetrischen Verschlüsselungsoperationen basieren auf den privaten Schlüsseln der Smartcard. Der private Schlüssel und die Zertifikate sind physisch auf der Karte gespeichert und verlassen dabei niemals die Karte. Damit haben Sie einen weiteren Sicherungsanker, falls das Mobilgerät in fremde Hände gelangt.

VERSCHLÜSSELTE ÜBERTRAGUNG

Durch die verschlüsselte Datenübertragung wird sichergestellt, dass schützenswerte Informationen sicher über jedes Netzwerk übertragen werden. SecurePIM etabliert eine sichere Kommunikation mit folgenden Backend-Systemen:

- Die Kommunikation mit dem MS ActiveSync oder IBM Traveler Server erfolgt mittels ActiveSync Protokoll (TLS-Verschlüsselung).
- Die Kommunikation mit dem SecurePIM Management Portal erfolgt via Web Service Interface (TLS-Verschlüsselung).
- Die Kommunikation mit dem Intranet kann über das SecurePIM Gateway erfolgen. Die Sicherheit des Gateways ist schlüsselbasiert und benötigt weder eine VPN-Infrastruktur, noch VPN-Profile für die mobilen Geräte. Das Gateway unternimmt eine Identitätsprüfung des

Nutzers und erlaubt nur verifizierten Nutzern einen Zugriff auf Anwendungen und Daten des Unternehmens.

ENDE-ZU-ENDE E-MAIL VERSCHLÜSSELUNG MIT S/MIME UND IBM DOMINO

Um sensible Informationen vor potentiellen Abhörmaßnahmen zu schützen, können E-Mails verschlüsselt versendet werden. Dazu wird der Secure/Multipurpose Internet Mail Extensions (S/MIME) Standard genutzt. Damit bleibt eine E-Mail vom Absender bis hin zur Entschlüsselung beim Empfänger auf allen Datenstrecken und Servern vor dem Zugriff durch Dritte geschützt. So wird sichergestellt, dass nur autorisierte Personen die E-Mail und die Anhänge lesen können.

Der S/MIME-Standard wird sowohl zur Verschlüsselung und zur Entschlüsselung, als auch zur Signierung und zur Validierung von Signaturen von E-Mails eingesetzt. Diese hilft gegen E-Mail Phishing und Identitätsdiebstahl zu schützen.

Dank der engen Zusammenarbeit mit IBM ist SecurePIM auch für IBM Domino Benutzer erhältlich. Es bietet umfassende Unterstützung von S/MIME und IBM Domino Ver- und Entschlüsselung, ohne Middleware oder Companion Apps.

ZERTIFIKATSBASIERTE AUTHENTIFIZIERUNG

Durch die Aktivierung zertifikatsbasierter Authentifizierung kann der Zugriff auf sensible Systeme zusätzlich zur Verschlüsselung mit TLS erhöht werden. Beispielsweise kann der Zugriff auf den ActiveSync Server oder Intranet-Anwendungen optional zertifikatsbasiert konfiguriert werden. Bei Einsatz des SecurePIM TLS-Gateway ist dies standardmäßig der Fall. Dabei prüft nicht nur SecurePIM das Serverzertifikat, sondern der Server auch das Benutzerzertifikat. Client (SecurePIM App) und Server führen einen TLS-Handshake durch, bei dem sich die Kommunikationspartner gegenseitig authentisieren und die zu verwendenden kryptographischen Algorithmen vereinbaren. Dabei prüft der Server während des TLS-Verbindungsaufbaus die Signatur und Gültigkeit des Benutzerzertifikats und SecurePIM prüft das Serverzertifikat. Nachdem der TLS-Kanal etabliert ist, können Daten verschlüsselt übertragen werden.

ZENTRALE VERWALTUNG DER SICHERHEITSVORGABEN DURCH SECUREPIM MANAGEMENT PORTAL

Mit dem SecurePIM Management Portal lassen sich alle sicherheitsrelevanten Einstellungen von SecurePIM zentral steuern:

- Nutzerverwaltung
- Regeln und Voreinstellungen zur Verschlüsselung
- Passwortstärke
- Regelungen zu Timeouts und wann die App automatisch geschlossen wird
- Löschen aller dienstlichen Daten aus dem Sicherheitscontainer aus der Ferne bei Verlust des Gerätes („Remote Reset“)
- Gruppenmanagement und Einrichtung verschiedener Sicherheitsregeln für unterschiedliche Gruppen
- Verwaltung der freigegebenen Schnittstellen

- Sicherheitsvorgaben für das Arbeiten im Container (z.B. sind Copy/Paste, Auto-Vervollständigung, Open-In oder Screenshots erlaubt)

Dadurch ist sichergestellt, dass die Sicherheitsvorgaben auf allen mobilen Endgeräten der Mitarbeiter eingehalten werden. Sicherheitskritische Funktionen können je nach gewünschtem Konfigurationsspielraum durch skalierbare Sicherheitslevels eingeschränkt oder freigegeben werden. Falls gewünscht, kann SecurePIM auch durch ein MDM verwaltet werden.

SCHUTZ VOR MANIPULATION

Zum Schutz vor Manipulationen, die an Endgeräten vorgenommen werden können, bietet SecurePIM Möglichkeiten diese frühzeitig zu erkennen und die Verwendung von SecurePIM zu unterbinden.

- **Integritätscheck:**
  Der SecurePIM Integritätscheck bietet volle Kontrolle über die SecurePIM Versionen, die die SecurePIM Nutzer verwenden dürfen. Jede Version der App erhält einen „Fingerabdruck“. Dieser ist einzigartig und ermöglicht es, die Software exakt zu identifizieren. Dadurch wird sichergestellt, dass keine veralteten oder modifizierten Versionen von SecurePIM verwendet werden können.
- **Jailbreak Detektion:**
  Ein Jailbreak modifiziert das Betriebssystem und schaltet Sicherheitsmechanismen des Gerätes aus.
  Nutzer oder eine Anwendung erhalten Root-Rechte und können uneingeschränkt auf das Betriebssystem zugreifen. Manipulierte Geräte können im SecurePIM Management Portal erkannt und die Nutzung wird blockiert und der Container damit gesperrt.