

SecurePIM Government SDS für iOS

Sichere Authentifizierung mit der internen Smartcard

Nutzungsfreundliches mobiles Arbeiten unter Einhaltung
höchster Sicherheitsstandards

Die interne Smartcard von SecurePIM ermöglicht eine sichere mobile Kommunikation auf VS-NfD-Niveau – und zwar ganz ohne den Einsatz einer externen Smartcard und den damit verbundenen Lesegeräten. Sie ermöglicht die vollständige Registrierung und Anmeldung bei SecurePIM durch die Nutzung der Security Hardware des Gerätes und eigenen Zertifizierungsdiensten und gewährleistet die Datenvertraulichkeit, sichere Datenspeicherung und Datenübertragung. Bei der Verwendung der internen Smartcard sind nur das mobile Gerät und die Geräte-PIN erforderlich.

Gewährleistung höchster Sicherheit

SecurePIM erstellt für jedes Gerät einen privaten Schlüssel, der in der Secure Enclave eines Gerätes gespeichert wird. Die Secure Enclave ist ein dediziertes, sicheres Subsystem, das vom Hauptprozessor auch auf Hardwareebene vom Rest des Systems isoliert ist, um eine zusätzliche Sicherheitsebene zu bieten. Sensible Daten werden auch dann geschützt, wenn der Kernel des Anwendungsprozessors kompromittiert wird. Wenn die interne Smartcard aktiviert ist und Nutzende sich bei SecurePIM anmelden, müssen sie ihre Geräte-PIN eingeben, um auf den privaten Schlüssel in der Secure Enclave zuzugreifen.

SDS ISCAS (Internal Smart Card Attestation Service)

Eine weitere zentrale Komponente für die Nutzung der internen Smartcard ist der SDS ISCAS Server. ISCAS steht für »Internal Smart Card Attestation Service«. Dieser Service stellt die notwendigen Zertifikate zur Authentifizierung an der gesicherten

Backend-Infrastruktur der Systemlösung SecurePIM Government SDS für autorisierte Nutzende aus. Die Zertifikate stehen so ohne den Einsatz externer Hardware auf den mobilen Endgeräten zur Verfügung.

Einfache Inbetriebnahme

Die erstmalige Registrierung ist in nur vier Schritten erledigt. Sie benötigen lediglich den QR-Code, den Sie von Ihrem Administrations-Team per E-Mail oder per Post vorab erhalten haben. Auch der Wechsel von der externen auf die interne Smartcard ist komfortabel. Die interne Smartcard lässt sich ohne Neuregistrierung mit SecurePIM verbinden – dabei bleiben lokale Daten und Einstellungen gespeichert und durchgehend geschützt.

Vorteile

- + Einfache und schnelle Registrierung
- + Keine externe Smartcard erforderlich
- + Kein zusätzliches Lesegerät erforderlich, das aufgeladen werden muss und Firmware-Updates benötigt
- + Keine zusätzliche Anmelde-PIN erforderlich (Anmeldung erfolgt mit Geräte-PIN)

Systemkomponenten

- + iPhone 11 oder neuer oder ein iPad ab der 9. Generation
- + SecurePIM App ab Version 8.73.x
- + SecurePIM Management Portal ab Version 2.44.x
- + SDS ISCAS

MATERNA
VirtualSolution

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