mID
TRUSTED APP

Designed,
developed and
made in Germany

KOBIL
secure your identity

DIE mAST FAMILIE

KOBIL bietet mit der mIDentity Application Security Technology (mAST) eine ganzheitliche Lösung für die Sicherheit Ihrer Anwendungen. Hierbei gibt es zwei Ansätze - Embedded & Enabled Security.

EMBEDDED APP SECURITY

ENABLED APP SECURITY

Embedded App Security gewährleistet integrierte und durchgehende Sicherheit in Echtzeit. KOBIL mID Trusted App bietet mit der integrierten 7-Layer-of-Security eine einzigartige Sicherheitsplattform. Mit KOBIL mID Trusted Webview wird die Sicherheit für hybride und web-basierte Applikationen erweitert.

Enabled App Security bietet erweiterte Sicherheitselemente für ein einzigartiges Kundenerlebnis. Trusted Login orchestriert starke Kundenauthentifizierung auf allen Endgeräten. Trusted Sign ermöglicht digitale Signaturen für Transaktionen. Dadurch ist jede Transaktion sicher, verbindlich und nachweisbar.

1 SICHERES GERÄT

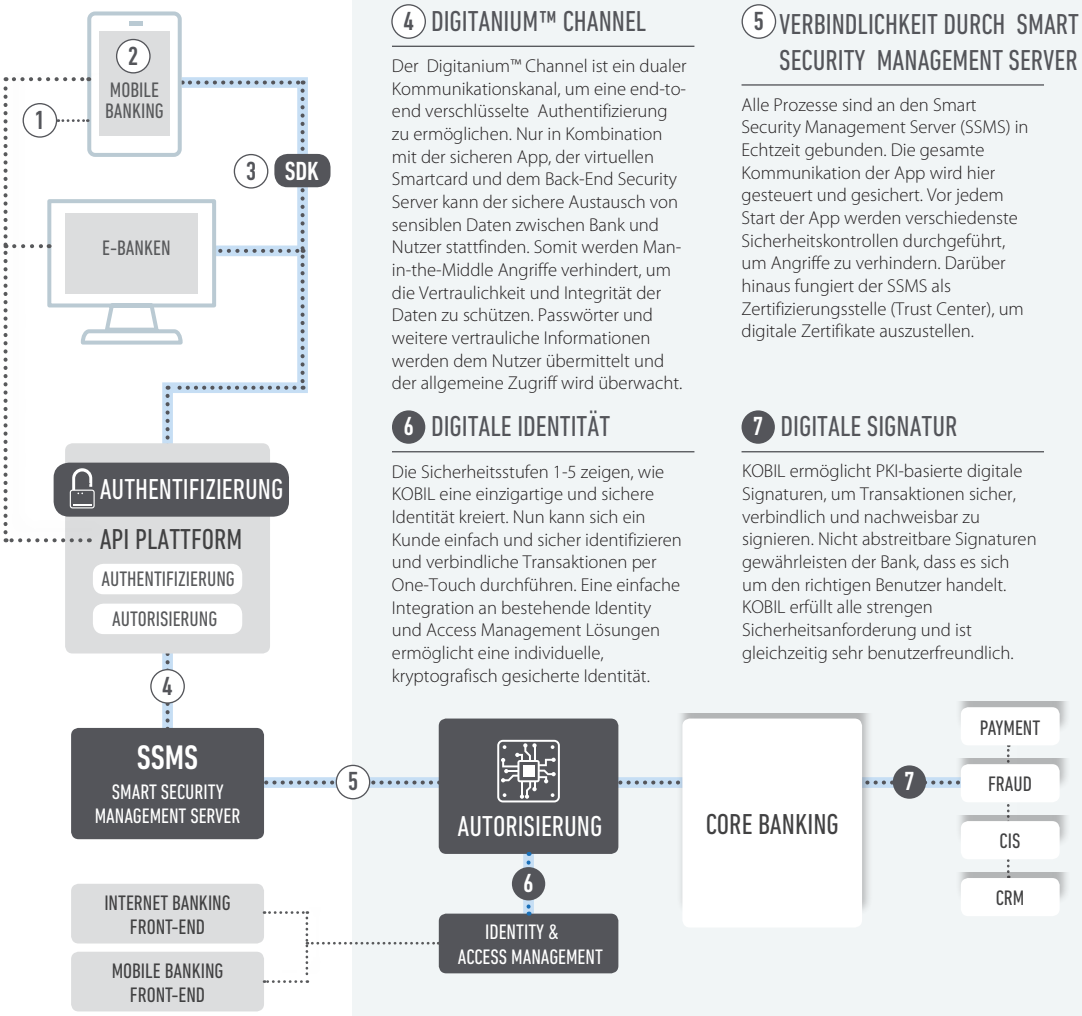
KOBIL prüft vor dem Start der App das Gerät, auf dem die dedizierte App sicher laufen soll und vergibt dem Gerät und der Applikation eine eindeutige Identität. Danach wird das eindeutige Gerät an die eindeutige Applikation gebunden.

2 SICHERE APP & WEB

Vor jedem Start der App prüft der Smart Security Management Server (SSMS) die Applikation auf Veränderungen und Sicherheitsrisiken. Der SSMS befindet sich im Back-End und ist on-premise oder in der Cloud installiert. Dieser kontrolliert u.a. die Integrität, Authentizität, Vertraulichkeit und die Version der Applikation. KOBIL unterstützt die verschiedenen App Alternativen, wie nativ, hybrid oder Web-App, stets auf dem gleichen Sicherheitslevel.

3 VIRTUELLE SMARTCARD

Sichere, verbindliche und nachweisbare Identitäten werden durch die virtuelle Smartcard-Technologie geschützt. Das Erreichen eines solchen Sicherheitslevels erfordert eine Public-Key-Infrastructure (PKI) mit digitalen Zertifikaten die für jeden Nutzer eine Smartcard-PIN verlangt. Dies wird durch den SSMS im Back-End verifiziert. Nach fünfmaliger falscher PIN Eingabe wird der Zugang wie bei einer realen Smartcard gesperrt und kann nur vom Server wieder freigeschaltet werden.



4 DIGITANIUM™ CHANNEL

Der Digitanium™ Channel ist ein dualer Kommunikationskanal, um eine end-to-end verschlüsselte Authentifizierung zu ermöglichen. Nur in Kombination mit der sicheren App, der virtuellen Smartcard und dem Back-End Security Server kann der sichere Austausch von sensiblen Daten zwischen Bank und Nutzer stattfinden. Somit werden Man-in-the-Middle Angriffe verhindert, um die Vertraulichkeit und Integrität der Daten zu schützen. Passwörter und weitere vertrauliche Informationen werden dem Nutzer übermittelt und der allgemeine Zugriff wird überwacht.

5 VERBINDLICHKEIT DURCH SMART SECURITY MANAGEMENT SERVER

Alle Prozesse sind an den Smart Security Management Server (SSMS) in Echtzeit gebunden. Die gesamte Kommunikation der App wird hier gesteuert und gesichert. Vor jedem Start der App werden verschiedenste Sicherheitskontrollen durchgeführt, um Angriffe zu verhindern. Darüber hinaus fungiert der SSMS als Zertifizierungsstelle (Trust Center), um digitale Zertifikate auszustellen.

6 DIGITALE IDENTITÄT

Die Sicherheitsstufen 1-5 zeigen, wie KOBIL eine einzigartige und sichere Identität kreiert. Nun kann sich ein Kunde einfach und sicher identifizieren und verbindliche Transaktionen per One-Touch durchführen. Eine einfache Integration an bestehende Identity und Access Management Lösungen ermöglicht eine individuelle, kryptografisch gesicherte Identität.

7 DIGITALE SIGNATUR

KOBIL ermöglicht PKI-basierte digitale Signaturen, um Transaktionen sicher, verbindlich und nachweisbar zu signieren. Nicht abstreitbare Signaturen gewährleisten der Bank, dass es sich um den richtigen Benutzer handelt. KOBIL erfüllt alle strengen Sicherheitsanforderung und ist gleichzeitig sehr benutzerfreundlich.

TRUSTED APP

PRODUKTMERKMALE

1 APP SICHERHEIT

mID Trusted App bietet eine vollständig gesicherte Umgebung für Applikationen. Die gesamte Kommunikation sowie sensible Daten sind vor unbefugten Angriffen durch Dritte geschützt. Vertraulichkeit und Integrität der Daten sind durch die Schaffung von Vertrauensankern an beiden Enden der Kommunikation gesichert.

2 GERÄTEBINDUNG

mID Trusted App ermöglicht die Bindung von Geräten an bestimmte Nutzer. So ist sichergestellt, dass es sich um den richtigen Benutzer und das richtige Gerät handelt. Verdächtige Aktivitäten wie das Kopieren oder Klonen der App werden erkannt und verhindert.

3 APP-HÄRTUNG

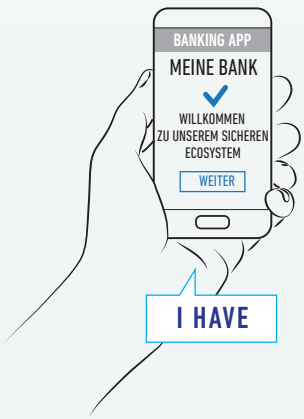
mID Trusted App lässt sich einfach in andere Anwendungen einbinden. So wird aus einer einfachen App schnell eine gehärtete App. Durch eine vollständige End-to-End-Verschlüsselung werden Code Injections erkannt und Manipulationen von Transaktionsdaten verhindert. Transaktionsdaten. Das Sicherheitsteam von KOBIL arbeitet kontinuierlich daran, Anti-Hacking Mechanismen zu verbessern, um auf neue Angriffe zu reagieren.

4 PKI TECHNOLOGIE

Die Verifizierung der Applikation basiert auf Public-Key-Infrastructure (PKI) mit KOBIL eigener Certificate Authority. Der KOBIL Digitanium Channel und die virtuelle Smartcard ermöglichen den Schutz der Identität des Kunden während des gesamten digitalen Prozesses. Die Integration in bestehende oder zukünftige Applikationen erfolgt einfach über KOBIL's Software Development Kit.

5 MULTIPLATTFORM

Durch die Erhöhung der zur Verfügung stehenden Bildschirme steigt die Anfrage nach plattformübergreifenden Apps deutlich an. mID Trusted App unterstützt Applikationen auf allen Plattformen und Endgeräten, um dem Nutzer eine einfache und bequeme Nutzung zu ermöglichen.



RISIKOMINDERUNG DURCH KOBIL mID TRUSTED APP

1. Klonen von Apps
2. Manipulierte UI
3. Vertraulichkeitsverletzung
4. Schadecodes
5. Datendiebstahl

KOBIL mID Trusted App triggers always on security. Somit ist die App auch bei nicht aktivem Einsatz immer geschützt. Dies sind einige Risiken, mit denen mID Trusted App entgegen wirkt.

NUTZEN

DIGITAL BANKING

- Mobile Banking
- Online Banking
- Transaction Security

BRING YOUR OWN DEVICE

- Device Management
- Corporate Applications
- Access Management

PAYMENT APPLICATIONS

- Wallet Solutions
- Debit / Credit / Prepaid Card Solutions
- ATM / POS / IoT Scenarios

PSD2 SCENARIOS

- Open Banking
- PISP Led Approvals
- AISP Led Approvals

KOBIL mID Trusted App kann für viele verschiedene Szenarien eingesetzt werden. Vier dieser Szenarien sind oben aufgezeigt. Mehr Informationen finden Sie in unseren Solution Suites.

ÜBER KOBIL

KOBIL Lösungen sind heute ein Standard für digitale Identität und hochsichere Datentechnologie. 1986 gegründet, ist die 120 Personen starke KOBIL Gruppe, mit Hauptsitz in Worms, Pionier in den Bereichen Smartcard, Einmalspasswort, Authentifikation und Kryptographie. Kern der KOBIL Philosophie ist durchgängiges Identitäts- und Mobile-Security-Management auf allen Plattformen und allen Kommunikationskanälen zu ermöglichen. Knapp die Hälfte der KOBIL Mitarbeiter sind in der Entwicklung tätig, darunter führende Spezialisten Kryptographie. KOBIL wirkt bei der Entwicklung neuer Verschlüsselungsstandards entscheidend mit.

120 Mitarbeiter	+1000 Firmenkunden
31 Erfahrung	3 BILLION Transaktionen pro Jahr

UNSERE KUNDEN

MIGROSBANK	ING DiBa Die Bank und Du
UBS	VONTOBEL
SOCIETE GENERALE	COMMERZBANK

Unternehmen wie **Commerzbank**, **IBM**, **Migros Bank**, **Société Générale**, **UBS**, **ZDF** und viele weitere vertrauen auf KOBIL.

Die **Deutsche Bundesnetzagentur** setzt ebenfalls auf die Sicherheitslösung von KOBIL. KOBIL Trust Center HS ist bei der Bundesnetzagentur seit 2003 äußerst erfolgreich im Einsatz. Sie ist zudem redundant ausgelegt, besteht also aus zwei parallel arbeitenden Systemen. KOBIL Trust Center HS verwendet eine eigene Kryptobibliothek, die unter anderem den Einsatz von innovativen Sicherheitsmechanismen wie der elliptischen Kurven-Kryptographie (ECC) ermöglicht. Diese Lösung wird nach den "Common Criteria for Information Technology Security Evaluation" geprüft und entspricht allen Anforderungen des Deutschen Signaturgesetzes.

Wenn Sie weitere Informationen erhalten möchten, senden Sie uns gerne eine Email oder vereinbaren Sie einen Termin mit einem unserer Spezialisten unter sales@kobil.com.

KOBIL Systems GmbH
Pfortenring 11
67547 Worms
Deutschland

www.kobil.com