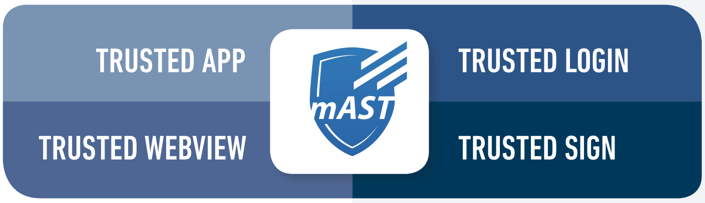
KOBIL has a holistic view on application security. We have two main perspectives – embedded app security and enabled app security.

EMBEDDED APP SECURITY

ENABLED APP SECURITY



Embedded app security ensures real-time security. The application is secured even when it is not in use. The application can be native, hybrid or even web-based. KOBIL Trusted App triggers the 7-layer security platform. KOBIL Trusted Webview delivers extra security for hybrid and web-based applications.

Enabled app security provides the security elements for user engagement. KOBIL Trusted Login orchestrates strong customer authentication for login process. On the other hand, KOBIL Trusted Sign is developed for strong customer authorization to sign transactions on a trusted level of security.

1 SECURE DEVICE

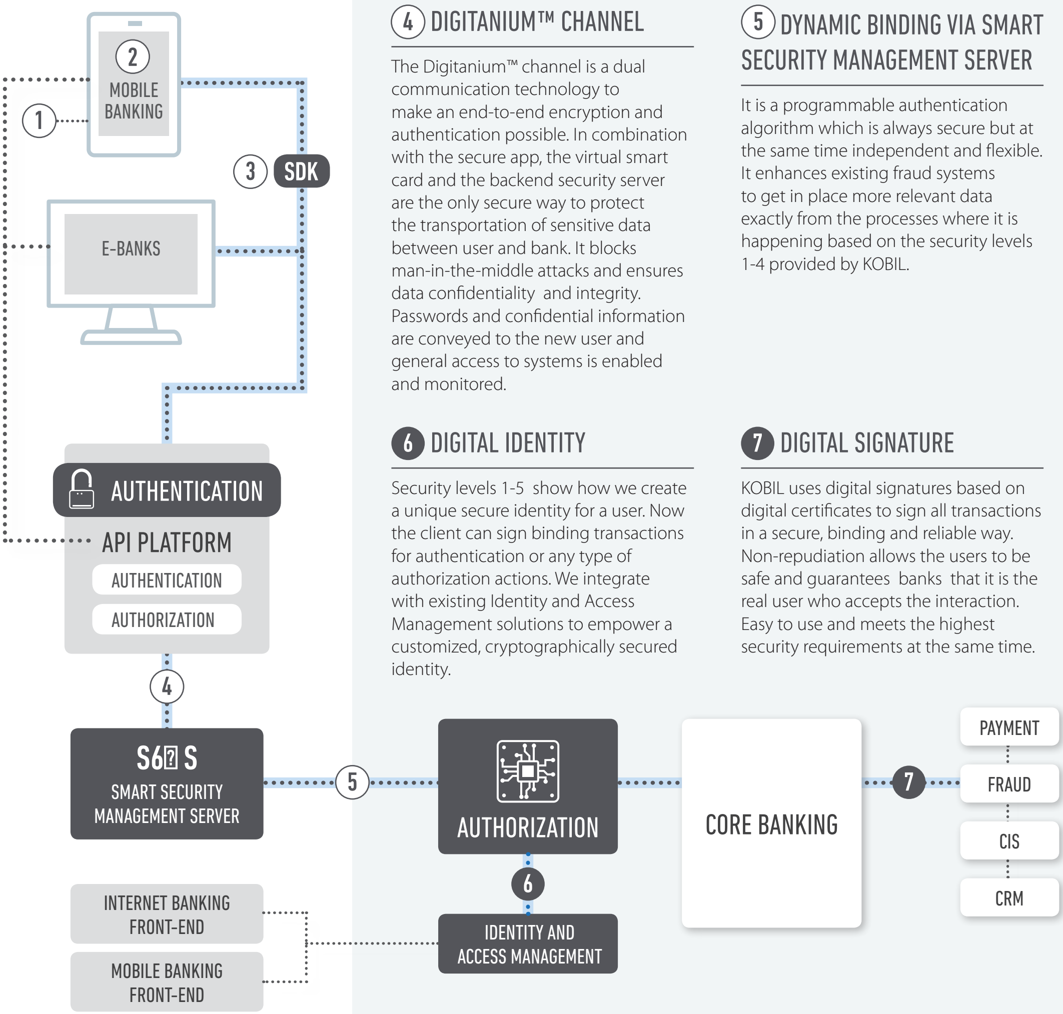
A trustful and secure environment is the base for a secure interaction within processes, because typical device management systems block the personal user behaviour and restrict usage of the device. KOBIL checks the device where the dedicated application is running secure before launching the app. After that the app is binded to this device to create a unique device of the user.

2 SECURE APPLICATION & WEB

Doesn't matter if you prefer a native app-, hybrid app- or a web app-development. KOBIL provide the protection levels for all of them. Every time the app launches, the app base will be checked by the Smart Security Management Server in the backend, which is installed on premise or in the cloud. The integrated Smart Security Management Server makes a lot of security checks for example it checks the integrity of the app, the secure environment, the version etc. before launching the application. If anything is not right the application will not start.

3 VIRTUAL SMART CARD

Liability and accountability, meaning binding and verifiable proof of relevant activity on the basis of secured identities, are protected by the principle of the virtual smart card technology. Reaching a level of smart card requires a PKI infrastructure, the usage of Private/Public Key Technology, digital certificates for each user and a smart card pin which has to be verified by an independent backend. It should also be blocked after 5 times wrong PIN entry like a real smart card and can be only unlocked by the server.



4 DIGITANIUM™ CHANNEL

The Digitanium™ channel is a dual communication technology to make an end-to-end encryption and authentication possible. In combination with the secure app, the virtual smart card and the backend security server are the only secure way to protect the transportation of sensitive data between user and bank. It blocks man-in-the-middle attacks and ensures data confidentiality and integrity. Passwords and confidential information are conveyed to the new user and general access to systems is enabled and monitored.

5 DYNAMIC BINDING VIA SMART SECURITY MANAGEMENT SERVER

It is a programmable authentication algorithm which is always secure but at the same time independent and flexible. It enhances existing fraud systems to get in place more relevant data exactly from the processes where it is happening based on the security levels 1-4 provided by KOBIL.

6 DIGITAL IDENTITY

Security levels 1-5 show how we create a unique secure identity for a user. Now the client can sign binding transactions for authentication or any type of authorization actions. We integrate with existing Identity and Access Management solutions to empower a customized, cryptographically secured identity.

7 DIGITAL SIGNATURE

KOBIL uses digital signatures based on digital certificates to sign all transactions in a secure, binding and reliable way. Non-repudiation allows the users to be safe and guarantees banks that it is the real user who accepts the interaction. Easy to use and meets the highest security requirements at the same time.

TRUSTED APP

PRODUCT FEATURES

1 APPLICATION SECURITY

mID Trusted App provides a fully secured environment to your application, helping you to enhance the experience of your users while protecting their data and also the entire communication. Trusted app not only secures the mobile application, but also the identities of persons, things and digital items. These security mechanisms ensure the confidentiality, authenticity and integrity of critical data at any time.

2 DEVICE BINDING

mID Trusted App allows you to bind your users to their devices so that you can ensure the user of the application and notice usages that are out of pattern. It also detects any attempt to copy or clone an app or key material to be used on a different device than it has been originally activated on.

3 APPLICATION HARDENING

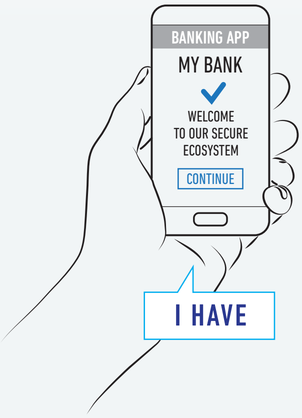
The application hardening feature of KOBIL's mID Trusted App establishes true end-to-end confidentiality, authenticity and integrity to detect code injections targeting the display of manipulated transaction data. KOBIL's security team continuously works on improving the anti-hacking mechanisms to react on new attacks, providing always up-to-date protection updates to your application.

4 SEAMLESS PKI CERTIFICATE-BASED APP VERIFICATION

Verification process with mID Trusted App is handled with KOBIL owned Public Key Infrastructure (PKI) certificate-based authentication. KOBIL's Digitanium Channel and virtual smart card technology enable that the customer's identity is protected during the entire digital process. Our easy-to-integrate software development kit enables you to use our product with your existing and intended applications on all platforms.

5 MULTISCREEN / MULTIPLATFORM

The number of screens we are exposed increases. As this exposure grows, the demand for applications for the increasing platforms rises. KOBIL is ready to help you to satisfy this demand since the mID Trusted App supports multiplatform applications, securing your users' data in any kinds of applications, in iOS, Android or Windows with 7-layer of security architecture.



RISKS MITIGATED BY KOBIL mID TRUSTED APP

1. App Cloning
2. Manipulated UI
3. Confidentiality Breach
4. Malicious Code Execution
5. Data Theft

KOBIL mID Trusted App triggers always on security. By this way, the application is secured even when not used actively. These are some of the risks that are managed.

KEY BENEFITS

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 can be used in many different scenarios. Four of these scenarios are summarized above. Please check our Solution Suites for more information.

ABOUT KOBIL

KOBIL solutions have set a benchmark in digital identity and high-secure data technology. Founded in 1986, the KOBIL Group is headquartered in Worms, Germany and is a pioneer in the fields of smart card, one-time password, authentication and cryptography. The core of KOBIL's philosophy is to empower complete identity and mobile security management on all platforms and communication channels Nearly half of KOBIL employees work in software development with specialists in cryptography. KOBIL plays a crucial role in the development of new encryption standards.

120 Employees	+1000 Corporate customers
31 Years of history	3 BILLION Transactions per year

OUR CUSTOMERS

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

Companies such as **Commerzbank**, **IBM**, **Migros Bank**, **Société Générale**, **UBS**, **ZDF** and many others put their trust in KOBIL.

KOBIL also works with **German Federal Network Agency** and offers them a German specialist solution meeting their requirements under the name of KOBIL Trust Center HS. KOBIL Trust Center HS has successfully been in use at the Federal Network Agency since 2003. It is designed to be redundant consisting of two systems working in parallel only. KOBIL Trust Center HS uses its own crypto library which among other things allows for the use of innovative security mechanisms such as the elliptic curve cryptography (ECC). KOBIL Trust Center HS is subject the "Common Criteria for Information Technology Security Evaluation" and meets all requirements of the German Digital Signature Act.

If you would like to request additional information, schedule a meeting with KOBIL representative, or just want to ask us a question, please contact us at sales@kobil.com

KOBIL Systems GmbH
Pfortenring 11, 67547 Worms, Germany

www.kobil.com