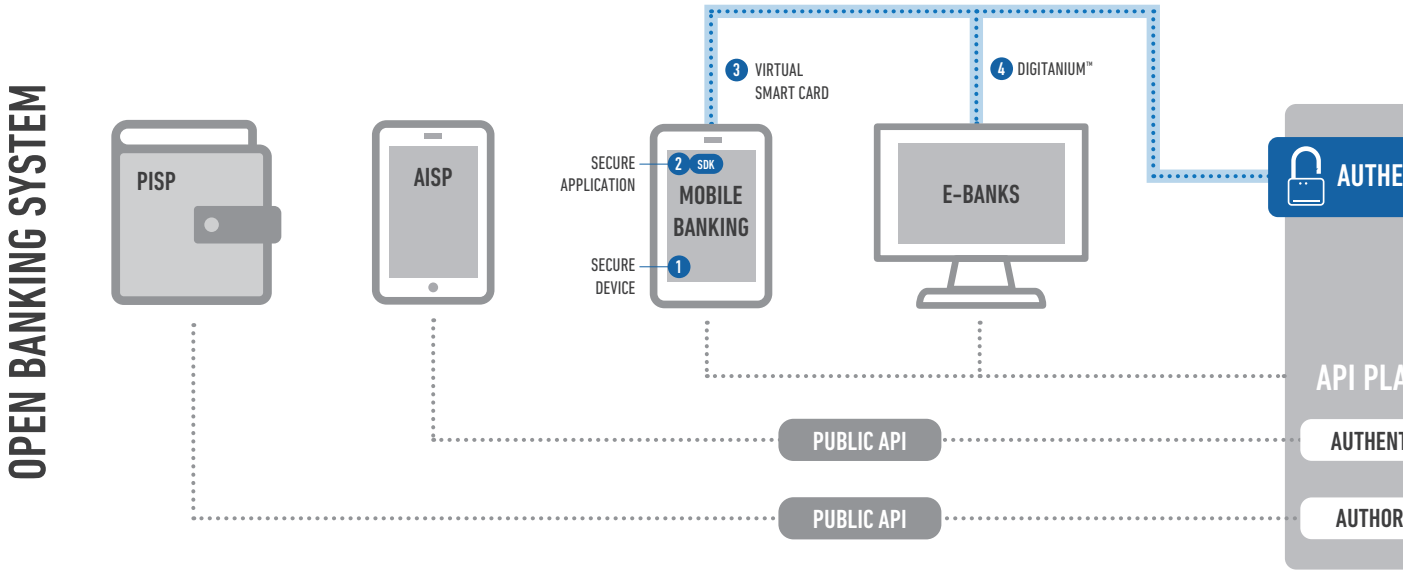
DUAL 7 LAYERS OF SECURITY

Are You Ready for PSD2?

KOBIL
secure your identity

DUAL 7 LAYERS OF SECURITY

PSD2 changes the security requirements fundamentally. Banks' current systems rely on direct interaction with the customer, meaning banks themselves possess all the information needed to establish whether a transaction is fake. Providing a secure environment and expanding the financial services while ensuring consumer protection against fraud and accountability will be a major challenge for banks. Strong customer authentication (SCA) – along with secure communication – is an enabler to overcoming this challenge. As the RTS identifies, PSD2's "strong customer authentication" is based on two or more of three elements that are independent of one another. KOBIL's core SCA technology is built on industry proven Public Key Infrastructure (PKI). KOBIL's mobile/web apps and devices (phone, tablet, desktop, IoT device) has its own protected private key and security certificate which are used to identify and authenticate the user, as well as signing transactions digitally. Research shows that 50 % of consumers have frequently abandoned online payments due to authentication problems. Security without usability obstructs business. KOBIL's "one device-one application-zero TAN" scenario is not just securing your identity but also delivering a superior customer experience.



1. SECURE DEVICE

A trustful 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. In our case we check the device where the dedicated application is running secure before launching the app and after that we bind the app to this device and makes it to 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. We have the protection levels for all of them. We ensure that the app base will be checked every time if they are launched by a security server in the backend each time. This server is checking the integrity of the app and even the version. If the version is not the latest one it enforces the user to update before continuing.

3. VIRTUAL SMART CARD

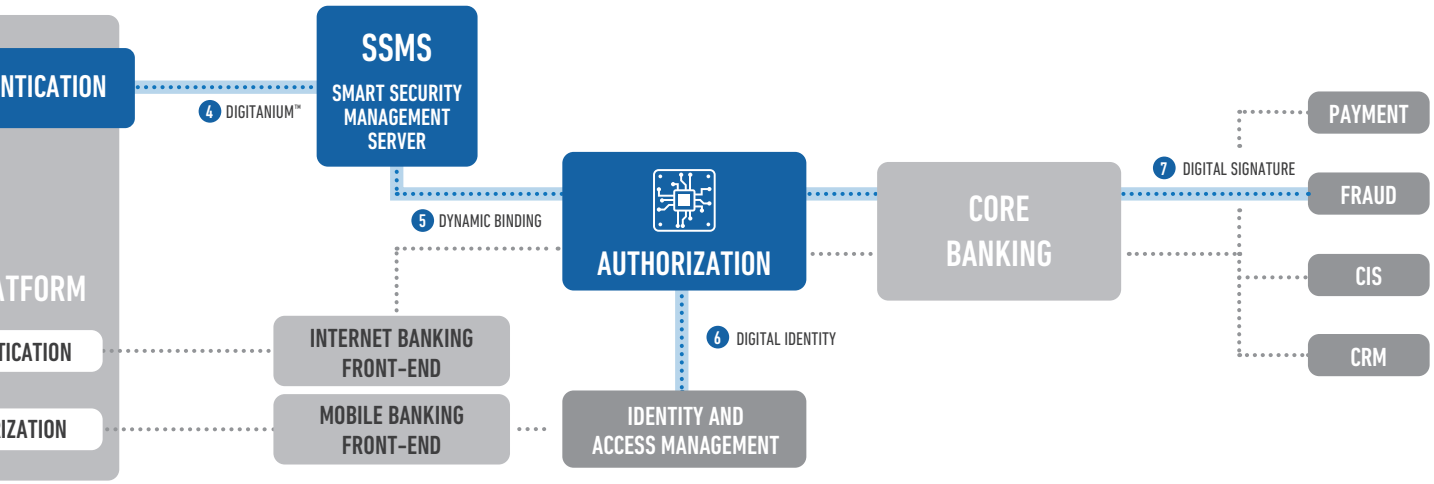
Liability and accountability, meaning binding and verifiable proof of relevant activity on the basis of secured identities, are protected by the principle of the virtual smart card technology. Reaching a level of smart card requires a PKI infrastructure, the usage of Private/Public Key Technology, digital 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.

KOBIL'S MOBILE APPLICATION SECURITY TECHNOLOGY CUSTOMER AUTHENTICATION SOLUTION

The user has a device with an app that is linked to them ("I have" = "ownership and device binding"), knows the PIN ("I know" = "knowledge") in order to use the app and will be identified in future by means of biometric characteristics such as a finger print, facial recognition and/or behaviour ("I am" = "recognition of the person"). Only if those factors come together, the end user's private key can be used to create the "authentication code", which is a digital signature ("I sign") in case of KOBIL mAST.

CYBER SECURITY & DUAL 7 LAYERS OF SECURITY

By providing APIs to TPPs, banks open up a significantly greater attack surface to potential cyber adversaries, and can no longer hide critical applications behind perimeter firewalls. KOBIL's SDK and core library takes care of all the security related functions and works everywhere from mobile and tablets, to PC and TV, and even at the point of sale. That's why KOBIL developed these dual 7 layers of security to protect the system and customer data and why it's needed to take action now to make sure the information is there when it's needed.



4. DIGITANIUM™ CHANNEL

The Digitanium™ channel is a dual communication technology to make a point-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

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.

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.

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.

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

MILESTONES

1986 **KOBIL Systems GmbH**
Ismet Koyun founds KOBIL Systems GmbH with the focus on PC and data security

1989 Redundant Server Power-Supply

1998 **SecOVID**
Smart Card Based OTP Generation

1998 **First Patent**
KOBIL receives first patent ever related to digital signatures

1999 **Gastromax**
Mobile POS Terminal with DECT

1999 **KAAN**
Smart Card Reader with PinPad and Display

2003 **mIDentity**
No-installation Smart Card Reader with hardened browser onboard

2006 **Success in Turkish Market**
KOBIL achieves 80% market share in the Turkish e-banking sector

2011 **KOBIL in the USA**
Founding of KOBIL Inc., USA

2011 **mAST**
Virtual smart card with server protection

2012 **IDtoken**
A safer and cost-effective Smart Card Reader for NFC cards

2012 **AST**
Introduction of Application Security Technology