Giesecke+Devrient

# Convego® Mobile Authentication

## Highly secure, seamless, biometric based and PSD2 compliant

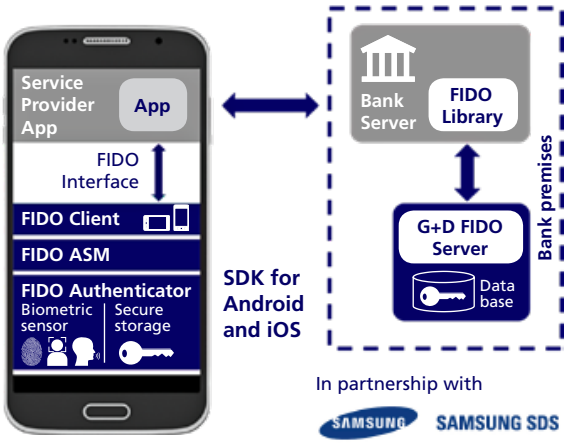
**As customers move to mobile to access digital services, so do the fraudsters. The mobile channel provides convenience, offering users any-time, any-place access, but it also opens up more points of attack and vulnerability that need safeguarding against. This means a strong mobile authentication solution becomes a vital building block for all critical services, particularly mobile banking.**

### Convego Mobile Authentication

- Secure PSD2-compliant solution certified by FIDO and Common Criteria
- Simple user experience with flexible integration of multiple biometrics
- No additional hardware tokens needed
- Tailored to customer environment using standard APIs
- Flexible private key storage options – WBC, TEE, Card (optional)

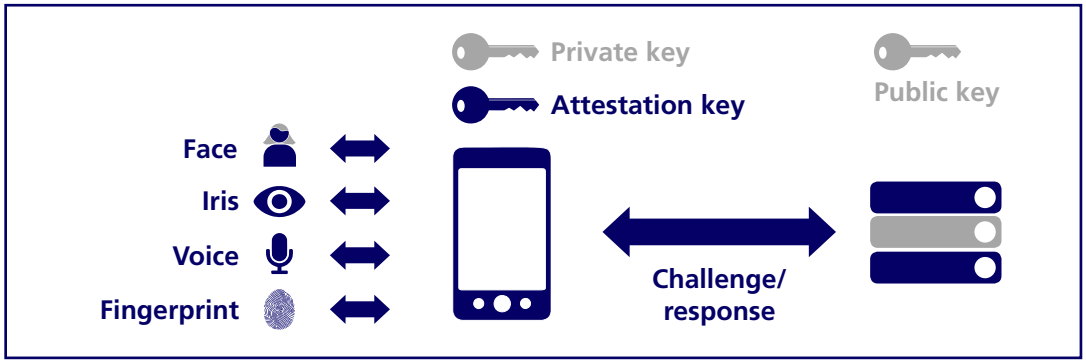
### Customer benefits

Simplified user experience, no passwords, no additional hardware. Scalable across both IOS and Android mobile device platforms. Choice of multiple biometric options, based on a future proofed industry standard with strong backing of major companies, reducing long-term investment risks.



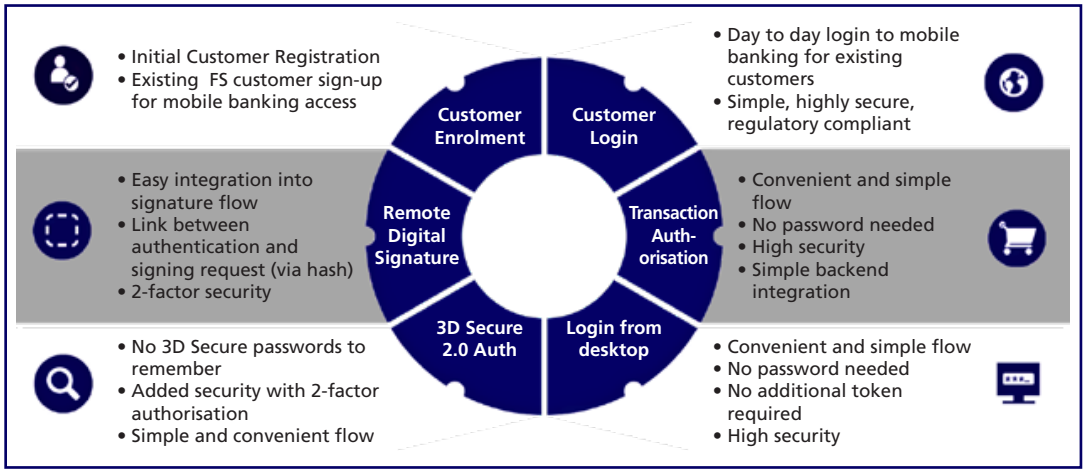

## OVERVIEW

Convego Mobile Authentication solution builds on the FIDO UAF industry specifications, providing strong customer authentication via mobile devices (Android, iOS) and using biometric options for user verification. It is powered by Samsung SDS Nexsign technology and offers a balanced combination of usability, security and reduced operating costs. Users authenticate by presenting biometrics such as face, voice or fingerprint. An end-to-end secured challenge response protocol based on the FIDO lightweight-PKI approach is then executed in the client-server solution, invisible to the user. It assures a strong cryptographic proof of the successful authentication and provides additional attestation on the integrity of the client authenticator. The combination of private key on the user device (possession) and biometrics (inherence) provides a very robust two-factor authentication with scalable security. Depending on the transaction risk, the types of authenticators (e.g. software or hardware) as well as the level of biometrics (e.g. single mode, like fingerprint only or multimodal like face+voice combined) can be freely chosen by server policy. No passwords or PINs are required anymore for the end user. Accordingly, no cumbersome password-renewal procedures are necessary by the service provider if the user forgets a password. Besides security, user privacy is another key challenge. The G+D Mobile Authentication solution addresses this need by storing all biometric data securely encrypted on the user device. No biometric user data ever leaves the device. As a consequence, no biometric server database exists removing any risk of scalable attack.



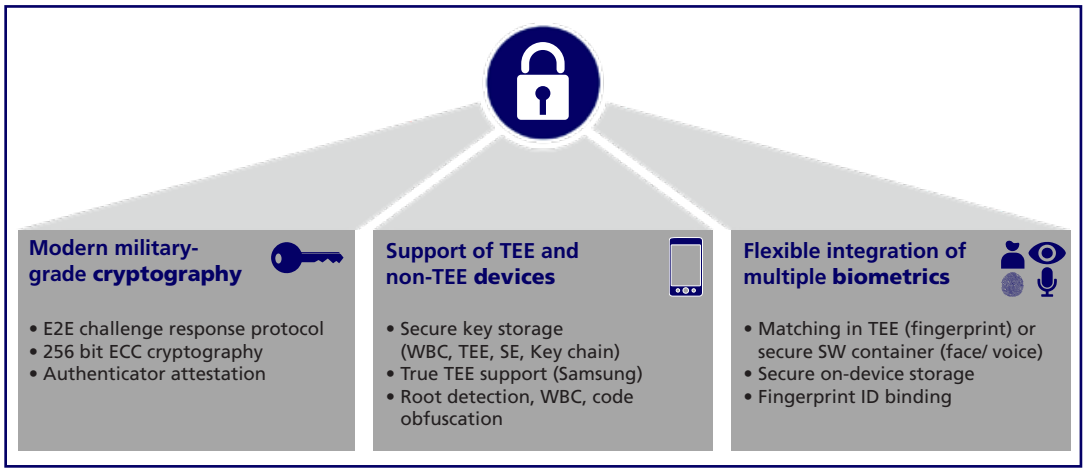
## USE CASES

Based on well-established FIDO specifications, Convego mobile authentication solution can be easily integrated into a large variety of use cases, ranging from secure account access to authorization of transactions, e-commerce transactions (3D Secure 2.0), identity-based applications as well as digital signature schemes.




## SCALABLE END-TO-END SECURITY

One unique feature of Convego Mobile Authentication is the use of both hardware and software protection. Where Trusted Execution Environments (TEE) are available, as found on many Android devices, this can be utilized to store private keys and fulfil biometric matching. Where TEE isn't available, market-leading white box cryptographic techniques are deployed to provide the necessary secure environment.




## TECHNICAL SPECIFICATIONS

**General Features**
- Type of solution
- Strong mobile authentication
- Supported protocols
- FIDO UAF V1.0, mOTP
- Supported Operating Systems
- Android, iOS
- Supported security tokens
- Software-only (Whitebox Crypto or TEE protected), Mastercard/ Visa DI cards (optional)

**Components**
- Server
- FIDO Server (Unix/Linux), Admin Portal, FIDO Server SDK
- Client
- FIDO Client SDK, incl. biometrics (face, voice, fingerprint)
- Middleware
- FIDO Client/ASM library, face/ voice/fingerprint/PIN authenticators

**Server Deployment**
- On-premise deployment
- Supported (installation package or VM image)
- Managed service
- Supported, operated by G+D Mobile Security in high security certified data centre

**Certifications**
- Functional: FIDO UAF certified
- Security: Common Criteria

## EXPERTS IN PAYMENTS

G+D Mobile Security supplies banks, wireless operators, local public transit authorities, other companies, and original equipment manufacturers (OEMs) with scalable security solutions comprising hardware, software, and services for mobile security applications, especially in telecommunications and electronic payments. G+D Mobile Security has decades of experience in secure digital architectures, as proven by our industry-leading mobile payment and mobile identity solutions. Our versatile portfolio of trusted products and services will support you on your journey towards intelligent digitalization. And our expert advisors are with you every step of the way to help you master the challenges that lie ahead.

**Giesecke+Devrient Mobile Security GmbH**

Prinzregentenstrasse 159
81677 Munich
Germany

P +49 89 41 19-0
mobilesecurity@gi-de.com
www.gi-de.com/mobile-security



June 2018