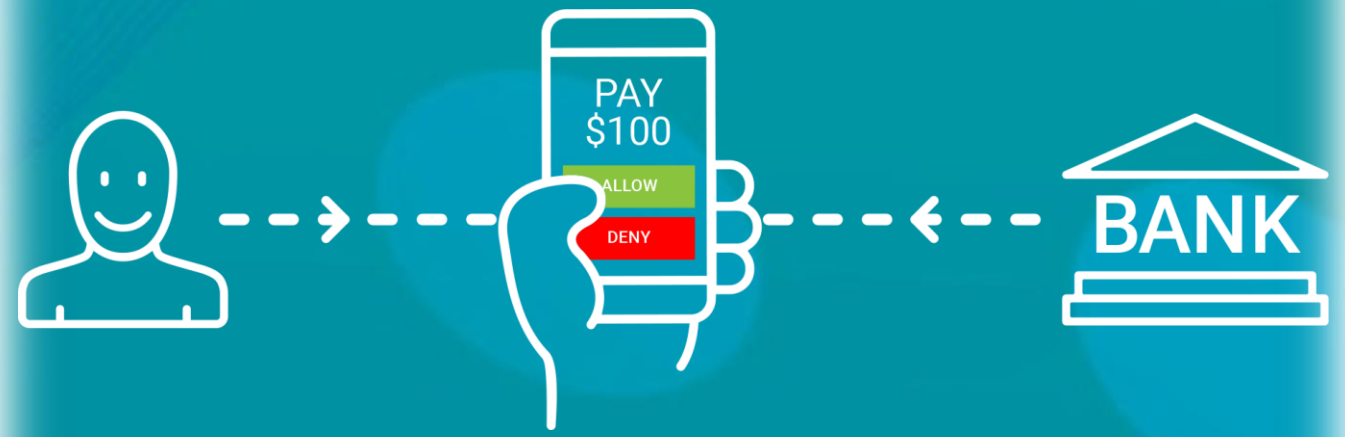
White Paper

Convenient Mobile Authentication for Customer-Focused Banking



GOODE INTELLIGENCE
YOUR PARTNER FOR BUSINESS RESEARCH & ANALYSIS

Entersekt

First Edition September 2017

Published by:
Goode Intelligence

Sponsored by:
Entersekt

www.goodeintelligence.com
info@goodeintelligence.com

CONTENTS

Banking is being reinvented and the biggest winner is the customer. Bank customers are demanding full-banking service delivery to any new piece of consumer technology they are purchasing, and as a result banks have to adapt or die.

A combination of competition from agile challenger banks and FinTech service providers plus regulatory pressure to open up the banking and payment markets is putting pressure on established banks to adopt strategies that place the customer firmly at the centre when designing and deploying new, predominantly digital, financial services.

This white paper from cyber security research and consulting company Goode Intelligence (GI) details the changing face of customer-focused banking exploring how customer authentication can make bank customer's lives easier and more secure. By matching agile digital banking services with convenient, standards-based mobile authentication solutions, banks can concentrate on delivering innovative and competitive solutions that ensure they retain existing customers and acquire new ones.

This means delivering mobile-based authentication solutions that are:

1. Easy to use
2. Proven in preventing fraud
3. Compliant with existing and forthcoming regulation
4. Proven to counteract the most damaging security threats
5. Omni-channel – one authenticator for many digital banking channels

CUSTOMER-FOCUSED BANKING IN THE DIGITAL WORLD

There are many disruptive forces affecting the financial services industry. The dynamics of the banking world have been fundamentally altered as a result of new consumer-facing digital services that deliver an immediate customer experience. A combination of powerful, always-on and always-connected personal computers – smart mobile devices – and API-driven services have placed the customer at the centre of a new range of financial services. Banks recognise that they must quickly adopt a customer-focused strategy that embraces new digital channels or they risk being disintermediated in a similar manner to telecommunications providers by over-the-top (OTT) services.

Customers are demanding full-banking service delivery to any new piece of consumer technology they are purchasing; from smart mobile devices, smart wearable devices to smart home devices such as Amazon Echo and Google Home.

Alternative payment systems are fundamentally changing how we transact. Bank branches are closing at an accelerated rate and paper cash usage is being eroded by a variety of digital payment systems including contactless cards, mobile payments and alternative digital systems including Alipay and PayPal.

762 bank branches in the UK set to close in 2017, leaving approximately 8,000 branches open compared to 17,831 in 1989[1]

[1] Reuters https://uk.reuters.com/article/uk-britain-banks-branches/british-banks-set-to-close-record-762-branches-this-year-idUKKCN1B31AY

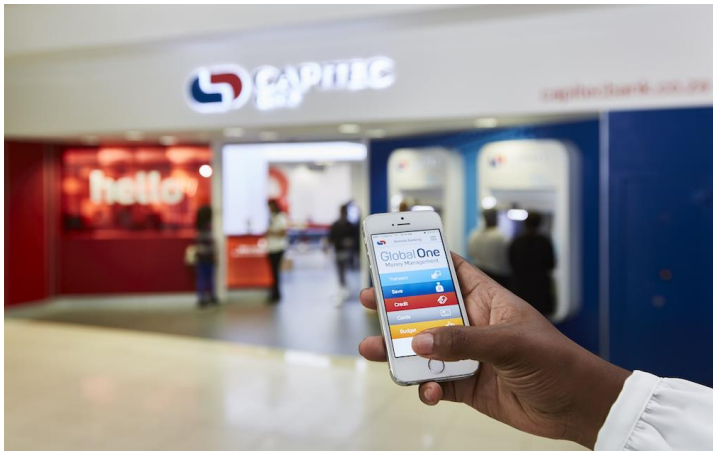
The very foundations of banking infrastructure are being shaken by disruptive technologies such as Blockchain (Distributed Ledger), a technology that is the basis for the explosive boom in Cryptocurrencies such as Bitcoin.

In this era of rapid technology-led change, agile FinTech companies are snapping at the heels of the established banks burdened by a lack of C-Suite technology knowledge and aging IT infrastructure.

Banks are fully aware that they must change. There are positive signs that they are evolving their culture and adapting to ensure that they meet the needs for customer-focused banking in the digital world.

The focus on the customer and technology innovation is resulting in transformation in how banks deliver services – much of it centred on the customer's smart mobile device (SMD). These include:

- Using a smartphone to withdraw cash at an ATM – no need for a bank card
- Speeding up loan processing and reducing the time it takes for customers to request a loan from days to minutes
- Supporting digital customer on-boarding using a smartphone for electronic identity and document verification (EiDV)
- Turning to biometric technology for convenient, low-friction customer authentication



46 percent of consumers now interact with their bank purely through the digital channel[2]

[2] PWC: https://www.pwc.com/us/en/financial-services/publications/assets/pwc-fsi-whitepaper-digital-banking-consumer-survey.pdf

ONE AUTHENTICATOR TO SUPPORT ALL CHANNELS

Bank customers are often frustrated by having to use a number of authentication methods when accessing bank services through different channels. A customer may use a hardware token for online banking, a knowledge-based authentication method for telephone banking and a PIN or biometric authenticator for mobile. This is an inconvenience for the customer and costly for the bank.

Would a FinTech or challenger bank adopt multiple authentication methods for every channel that they supported? Probably not.

Banks have built up different delivery channels over many years and organisationally silo each one into a separate business function, each having responsibility for security and customer authentication

A far more efficient approach would be to standardise on a single authentication method that can provide convenient and secure customer authentication across multiple bank channels. The smart mobile device is the natural authenticator to support omni-channel banking.

ENTERSEKT – THE NATURAL PARTNER FOR THE MODERN DIGITAL BANK

Putting the mobile at the heart of identity and authentication is a guaranteed method to make bank customer's lives easier and to simplify their interactions with their banks. Banks are able to meet their strong customer authentication requirements across all channels by adopting simple to use mobile-based authentication.

A vendor with a tried and tested mobile-based authentication solution that meets the needs of the modern digital bank is **Entersekt.**

Entersekt's security platform provides patented strong customer authentication that enables banks to allow their customers to approve any financial transaction in an easy, low-friction way.

Built for the Mobile

Entersekt's patented security platform has been designed for a mobile-first world – not an old authentication technology that has been retro-fitted to work with mobile.

The Entersket **Transakt** mobile security product offers multi-factor authentication for banks to integrate into their mobile banking apps using an easy-to-use SDK.

Banks such as Nedbank in South Africa are benefiting from Transakt's native SDK by allowing the bank's customers to authenticate online banking transactions using their mobile devices.

Transakt forms the security platform on which the award-winning Nedbank App Suite is built. The mobile banking app enables customers to access full digital bank services, including retail, business, personal financial management and online stock trading all accessible with single sign-on (SSO).

The Transakt SDK allows banks to establish a separate, fully encrypted out-of-band channel to their customer's mobile devices that is 100 percent in the control of the banks, preventing fraudsters from eavesdropping on this channel.

The solution works by sending push notifications to the end-customer, which they approve with a simple yes or no response. Allowing the bank customer to actively authorise a transaction with a simple yes is an important component of the user experience.

Transakt allows bank customers to:

1. View account balances and transactions
2. Create, change or pay beneficiaries
3. Transfer funds
4. Use their credit card to pay safely and easily online
5. Digitally sign sensitive transactions
6. Send messages securely
7. Add recurring and future-dated payments

Transakt is also FIDO and Google U2F Certified.

Supports All Channels

There are benefits of using a single strong customer authentication solution for multiple bank channels. These include cost reduction and providing customers with a single easy-to-use method of proving their identity.

A mobile-based authentication solution can be positioned firmly at the centre of many banking channels. Authentication requests are automatically pushed to a customer's mobile device who responds by simply selecting **Accept** or **Reject**.

No clumsy re-entry of one-time passwords or answers to challenge questions is required when accessing mobile, web or telephone banking channels.

Secure – Mitigates Major Threats

There are many threats that a bank must counteract to managed and prevent fraud.

Common attacks on banking technology and authentication systems include Man-in-the-Middle (MiTM), malware, key-logging and SIM swapping attacks.

Man in The Middle (MiTM) attacks

Malware

Key-logging

SIM swap attacks

Transakt ensures that banks are protected against the major threats by providing:

- **An encrypted channel for out of band authentication** (OOBA) using Transakt's self-contained, NIST-compliant cryptographic stack and communications layer, which provides an isolated end-to-end encrypted communications channel between a customer's mobile and a bank's mobile app server
- **Protection from malware, SIM swap and brute force attacks** using a layered security approach that involves server-side detection and prevention
- **Dynamic public key pinning** that protects against Man-in-the-Middle attacks that exploit rogue certificates
- **The Transakt Secure Gateway hardware appliance,** a NIST FIPS 140-2 Level 3 on-premise endpoint to work in partnership with the mobile SDK

Compliant with Regulation – PSD2 and GDPR

Banks are increasingly under pressure from regulation, especially now with the European Union's (EU) Second Payment Services Directive (PSD2) and General Data Protection Regulation (GDPR) specifying how organisations must support Strong Customer Authentication (SCA) and protect EU citizens' data.

Time is running out for companies needing to comply, with PSD2 coming into effect January 2018 and GDPR in May 2018.

PSD2 Compliance

A major component of PSD2 is the European Banking Authority's (EBA) Regulatory Technical Standards on Strong Customer Authentication (SCA) and Common and Secure Communication (CSC).[3] This defines the enhanced security and authentication requirements that must be met by payment providers to ensure that they are compliant with PSD2.

SCA is mandatory, except in defined circumstances, when a payer or a proxy:

- Accesses payment accounts online
- Initiates an electronic payment transaction
- Carries out any action through a remote channel that may imply a risk of fraud or other abuses

SCA is defined as a multi-factor authentication solution that is derived from at least two of the following three categories:

1. **Knowledge:** Something only the customer knows, e.g. a password, PIN or identification number
2. **Possession:** Something that a customer has, e.g. token, smart card or mobile phone
3. **Inherence:** Something they are, e.g. a biometric

The selected factors must be mutually independent, so that a breach of one does not compromise any other. At least one of them should be non-reusable and non-replicable. The entire procedure must also be designed to protect the confidentiality and integrity of the authentication data.

Entersekt's Transakt multi-factor and out-of-band authentication product meets and even exceeds the EBA's SCA technical standards. Transakt's patented push-based

33

https://www.eba.europa.eu/documents/10180/1761863/Final+draft+RTS+on+SCA+and+CSC+under+PSD2+%28EBA-RTS-2017-02%29.pdf

authentication and mobile app security product leverages industry-standard X.509 digital certificates that uniquely identifies each registered mobile device, transforming them into trusted factors of possession.

GDPR Compliance

GDPR is the EU's revision to its data protection legislation becoming law from May 2018. Although the breach notification regulation is getting the bulk of the attention, with its 48-hour notification requirements and heavy fines for non-compliance (up to 2 percent of a company's global annual turnover), there are significant implications for authentication driven by important changes related to ***informed consent***: how a company must manage the way their customer's data is used.

GDPR dictates that the power to decide on sharing personal data with a company must be with the customer – the owner of their personal data. Informed consent on using and sharing customer data can be managed by Transakt.

Transakt's PKI-based solution enables companies to capture cryptographically signed consent from a customer when that is required, e.g, when sharing it with a third party.

Consent is a similar process to customer authentication and is presented to a customer in a simple accept or reject statement using a push-based request to a mobile device

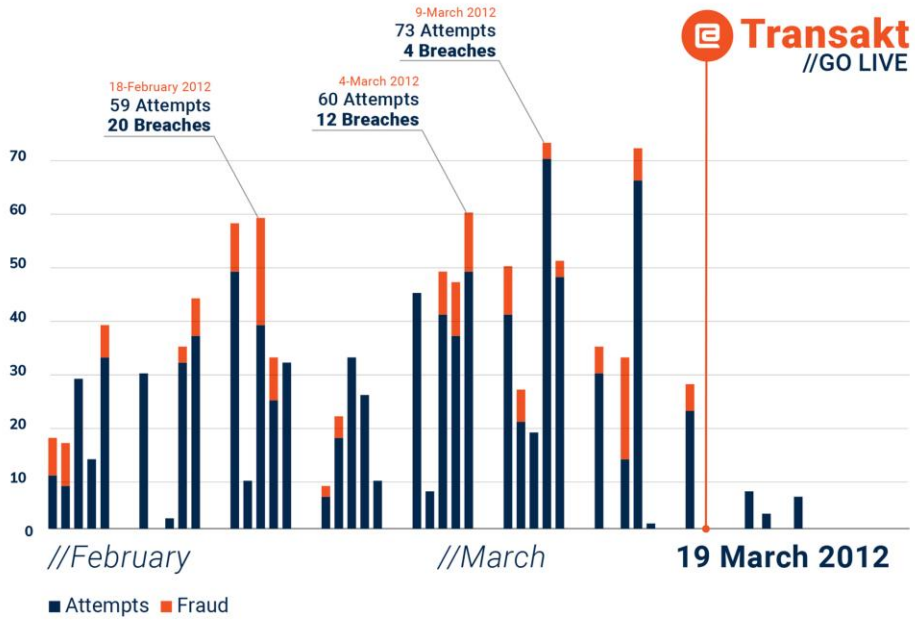
HOW ENTERSEKT REDUCES FRAUD LEVELS

Entersekt's patented security platform is used by millions of users in 45 countries and secures around 30 million transactions every month.

The company has a strong European presence, working with Coutts and Investec in the UK, Swisscard in Switzerland, Sparkasse and PLUSCARD, as well as other card issuers and processors in Germany.

Entersekt's Transakt mobile authentication solution has a demonstrable impact on reducing levels of fraud. When Nedbank deployed Entersekt's app-based push authentication in 2012 it witnessed an immediate 99 percent drop in phishing losses as demonstrated in Chart 1 below.

Chart 1: Transakt reduces fraud for Nedbank



The ability to have an immediate impact on fraud has been repeated by other Entersekt clients including Capitec Bank, which followed Nedbank in deploying the in-app push authentication solution in 2013. In addition to winning digital bank of the year for 2017, the bank has seen no fraud on app-protected digital channels and its mobile-first strategy has saved it millions in personnel and branch costs.

SUMMARY

This white paper from Goode Intelligence investigates the changing face of customer-focused banking and explores how easy-to-use customer authentication makes bank customer's lives easier and secure. Convenient, standards-based mobile authentication enables banks to deliver innovative and competitive solutions that both retain existing customer and acquire new ones.

Entersekt protects tens of millions of bank customer across the globe (including millions in Europe) with its patented mobile-based authentication technology that is:

1. Easy to use
2. Proven in preventing fraud
3. Compliant with existing and forthcoming regulation
4. Proven to counteract the most damaging security threats
5. Omni-channel – one authenticator for many digital banking channels

For more information on Entersekt's authentication solutions, please visit www.entersekt.com

ABOUT GOODE INTELLIGENCE

Since being founded by Alan Goode in 2007, Goode Intelligence has built up a strong reputation for providing quality research and consulting services for the cyber security industry.

For more information on this or any other research please visit www.goodeintelligence.com.