smsTAN vs pushTAN

in light of Strong Customer Authentication (SCA) under PSD2

August 2019

pwc

Table of contents

1

Starting Point

Starting Point

- Whereas the FMA has recently decided to grant vendors a temporary stay in applying a two-factor authentication (“**2FA**”), on 14 September 2019 new requirements will enter into force that will require a Strong Customer Authentication („**SCA**“) for online payments.
- As part of SCA, certain different technologies can be used by banks and payment service providers to comply with SCA-requirements. While biometric elements (fingerprint and facial-ID) get increasingly important, the TAN-technology in connection with one-time-passwords (“**OTP**”) is still at the cornerstone, also under SCA-requirements.
- The two most relevant TAN-technologies are smsTAN and pushTAN.
- In the following, PwC Legal Austria (registered as oehner & partner rechtsanwaelte gmbh) and PwC Advisory Services GmbH (together “**PwC Austria**”) will take a closer look at both technologies.
- We will be directly comparing certain features of both technologies. As currently the financial sector appears to move away from smsTAN to pushTAN, we want to assess whether smsTAN would still be a viable option to meet SCA-requirements.
- Finally, also outside of the financial sector, client or user authentication becomes increasingly important. Hence, the final chapter is dedicated to potential use cases for TAN-technologies outside the financial sector.

Strong Customer Authentication (SCA)

- Under SCA, a 2FA authentication shall be based on two or more elements from the following categories:

Knowledge

(= something the customer knows)

- PIN-code
- Password
- Passphrase
- Secret fact
- Sequences

Possession

(= something the customer owns)

- Mobile phone
- Laptop
- Wearable device
- Smart card
- Token

Inherence

(= something the customer is)

- Fingerprint
- Facial-ID
- Voice-ID
- Iris-scan

2

smsTAN vs pushTAN

Introduction

- In terms of SCA and 2FA (see above at 1.), both smsTAN and pushTAN appear as potential technologies to satisfy the requirement of “Possession” (i.e. something that the user owns). In case of smsTAN, the sim card is considered as element of “possession”, in case of pushTAN it would be the smartphone containing the pushTAN app.
- In the following, we have assessed smsTAN vs pushTAN under the criteria of „Security“, „Comfort“, „Costs“ and “Dependencies”.
- Currently, market trends in the financial sector are showing a clear preference of banks towards pushTAN. Also, current media coverage on SCA appears to misleadingly suggest that only pushTAN will continue to be a viable option in the future. This is often argued with more security and more convenience. However, do these arguments hold up to a direct comparison?
- Assessing smsTAN and pushTAN and directly comparing essential features of both technologies allows for an objective view.

Security

	smsTAN	pushTAN
Secure for purposes of SCA?	The European Banking Authority (EBA) has confirmed that smsTAN also in light of PSD2 and SCA remains a secure feature. smsTAN is considered a viable option for category 2 (= "Possession").	Yes, the banking sector considers pushTAN as a secure way to SCA.
Risk of phishing and hacking	Via phishing attempts, criminals have in the past gained access to online accounts.	With pushTAN apps operating on mobile operating systems, such apps are subject to the same general risks of phishing and hacking as are other apps operating on these systems. As is the case with SMS and underlying mobile phone numbers, passwords or PINs for pushTAN apps could potentially be subject to phishing attempts.
Risk of convenience – As studies have shown, many users are overwhelmed with different password- or PIN-requirements. While such features are intended to increase security, **users** – out of convenience – **often tend to use uniform passwords or PINs for different services**.	smsTAN is not subject to additional passphrase or PIN requirements. Rather the customers need to be in possession of the mobile phone housing the SIM card to which the SMS is relayed. In order to access the SMS, the customers must first access his/her mobile phone device. Hence, the risk of convenience is limited to the passphrase or PIN of the device itself. Many modern mobile phones can also be accessed via biometric features such as fingerprints or facial-ID, thereby reducing the risk of convenience by usage of the same PINs or passcodes for various devices.	Commonly, pushTAN apps require separate passwords or PIN codes as an additional layer of verification. Hence, to access the pushTAN, double-access is required – first, access to the mobile device (see left as to SMS) and second, access to the pushTAN app. While access to the device itself can be achieved through biometric features (see left for smsTAN), the pushTAN app requires the mentioned additional PIN. This additional layer of security may, however, in fact be reversed by clients' convenience use of uniform passcodes or PINs. As pushTAN apps progress, such PINs may also be replaced by biometric access though.

Comfort

	smsTAN	pushTAN
Set-up	smsTAN does not require a separate set-up.	Users often need to download an additional pushTAN app from either the Google Play Store or the Apple AppStore. Most Austrian banks have not directly incorporated pushTAN into their primary banking apps. Users must activate this app in a separate process that usually requires an authentication via traditional smsTAN. Until the pushTAN app is fully operational, some defined steps have to be taken by the user.
Dependence on internet	smsTAN does not depend on the availability of an internet connection.	pushTAN requires a reliable internet connection and a smartphone with access to the pushTAN app.
Convenience to use	smsTAN is a very convenient form to use TAN-technology. Modern mobile smartphone operating systems such as iOS and Android allow for e.g. automatic pasting of smsTAN directly into banking apps, thereby eliminating the extra-step of copying & pasting the TAN.	pushTAN is a convenient way to use banking apps. However, as compared to smsTAN the users may have to use additional steps, depending on the mobile operating system. As pushTAN is operated via an additional app, additional steps may be required to access the app, including the entering of an additional PIN or password.
Security updates	Security updates (if any) are implemented directly by the bank's service provider processing smsTAN. No user action is required to implement potential security or software updates.	Security or other software updates require interaction by the user. The user must actively download security updates.
Change of device	smsTAN is linked to the SIM card. Hence, a change of device does not involve extra steps for the user other than inserting the SIM card into the new device.	When a device is changed, pushTAN apps usually need to be set-up anew (see above on the set-up process).

Costs & Dependencies

	smsTAN	pushTAN
Costs-per-TAN	Between the two technologies, the mere costs per TAN will, according to our market knowledge, be higher than with pushTAN.	On a purely costs-per-unit perspective, pushTAN appears to be the cheaper technology.
Total Costs of Ownership (TCO)	Depending on the exact pricing models of smsTAN service providers / processors, TCO of smsTAN will usually not vary substantially from costs-per-TAN. The cost of the software (and maintenance) for the generation of the OTP should essentially be the same.	pushTAN apps are expected to require higher maintenance efforts that are expected to result in higher ancillary costs: • Security updates need to be implemented; and • Security updates may need to be advertised to users in order for users to take note of (i) the update and (ii) its crucial nature in terms of security.
Dependencies	smsTAN is based on the general SMS technology that is available worldwide via an established global standard. Dependencies exist, however, with respect to SMS technology as such.	Dependencies may exist via the pushTAN app provider and via the operators of the mobile platforms (i.e. Google and Apple). If a mobile platform may become subject to governmental sanctions or prohibitions, app support may cease to exist (e.g. no further security updates could be implemented). These dependencies might ultimately lead to adverse impacts on the customers. The release of a pushTAN app is regulated by platform provider policies, as well as US and local based regulations. This means that if the bank is releasing a pushTAN app (and related updates) in the app stores, the app will be available after a certain (not always reasonable) time following approval from the platform service provider that the app satisfies all the internal policies and the US/local regulations.

Costs & Dependencies

	smsTAN	pushTAN
Market penetration	smsTAN requires a mobile phone. smsTAN is hence preferable for people who do not have access to smart phones with full internet connectivity (e.g. elderly people).	pushTAN requires a mobile device with internet connectivity and app store access.
Other	n/a	It is expected that banks / payment service providers will either use in-house pushTAN solutions or solutions provided by third parties. We believe this may have the following implications: • If both the transaction and the authentication run via the same network (in-house solution), additional security layers need to be implemented; and • If many banks / payment service providers go in-house, this may limit business opportunities for independent third party providers. This could increase dependencies vis-à-vis these limited operators for market participants, impacting costs and resulting in cluster risk (limited providers servicing large numbers of market participants)

“

We believe that both smsTAN and pushTAN are equally viable means to meet SCA-requirements as laid out by PSD2 and European implementing legislation.

We further believe that an objective view of both technologies may result in a less obvious preference for pushTAN than common market opinion would suggest.

- While smsTAN has in the past been subject to criminal phishing attempts, risks of phishing and hacking remain also with pushTAN. pushTAN requires mobile devices that mainly operate on two competing OS-platforms: iOS and Android. pushTAN apps are hence subject to the same general risks as other apps operating on these systems and depend on the mobile platform providers.
- As pushTAN introduces additional passcode or PIN requirements for users, there is a risk of users using the same PIN code as for other services or even the debit card out of convenience.
- smsTAN is arguably a more convenient format. Users do not need to download additional apps and do not need to undergo additional set-up processes. Users are also not required to participate in software updates.
- Studies have shown that most users in Austria (69%) currently prefer smsTAN over pushTAN*. In terms of subjective perception, smsTAN is considered safer by users (60% to 18% for pushTAN)*.
- Most recently, MasterCard Germany has recommended to use OTP via smsTAN as back-up solution for users who do not possess smartphones**.

* MindTake Research, n=1052 – Online Banking User, June 2019

** https://www.spiegel.de/netzwelt/web/auslaufmodell-mtan-das-aendert-sich-beim-onlineshopping-a-1279982.html

3

Use Cases for TAN-Technologies Outside the Financial Sector

Use Cases for TAN-Technologies Outside the Financial Sector

- With the General Data Protection Regulation (GDPR's), increased requirements apply to all companies processing personal data, not only regulated entities:
  - Data subjects have the right to receive information on the their processed data;
  - Data controllers and data processors are required to implement appropriate technical measures to ensure compliance with the GDPR; and
  - High penalties incentivise compliant behaviour.
- Often, processed data may also contain sensitive information such as details on a person's health records or previous criminal records (that are subject to higher protection under GDPR).
- Currently, most companies processing client information do not use any additional layers of security and usually do not require authentication for users uploading or accessing their stored information.

Use Cases for TAN-Technologies Outside the Financial Sector

- Based on these considerations, implementing TAN-technology as a means of authentication may be an attractive form of risk mitigation for all companies processing personal data of clients.

- TAN-solutions may e.g. be used for the following:

  - **allowing <u>authenticated</u> data subjects (i.e. clients / users) access to their online client accounts**: Many companies operate online user accounts for their clients. Certainly not all user accounts will warrant the extra-effort of a secure user authentication. However, user accounts on which sensitive personal data is stored or made available for download, may benefit from a secure authentication, e.g. via smsTAN or pushTAN. For instance, in case of a data breach resulting from access to an online account by an unauthorized person, having employed customer authentication via TAN could serve as an argument as to compliance with GDPR by the data controller / processor.

  - **<u>authentication of data subjects</u>** (clients / users) for purposes of rights of a data subject: As mentioned, data subjects have substantial rights vis-à-vis the data controller. These rights include the right of information, erasure, etc. In particular the right of information will result in the controller having to disclose personal data to the relevant data subject. It is largely unclear which level of identification the controller may request from the data subject requesting information. A smsTAN or pushTAN solution for authentication of a data subject appears to be a viable option.

Use Cases for TAN-Technologies Outside the Financial Sector

- In our opinion, the following sectors in particular may benefit from more secure authentication measures:
  - **Employment recruitment agencies and head-hunters** often operate via web-platforms. Via such platforms, potential job applicants can upload all sorts of data that is processed by the agency. Such data is often of sensitive nature (e.g. previous criminal records, ethnic origins etc).
  - **Insurance companies** often operate platforms and apps that allow clients / users to up- and download sensitive data, often relating to medical records and health information.
  - **Health care providers** such as healthcare centres, doctors or laboratories, which offer clients e.g. online platforms for diagnostic findings and the like.

Contacts

Stefan Paulmayer
Attorney-at-law
Senior Manager
PwC Legal
M: +43 664 883 69 611
stefan.paulmayer@pwc.com

Stefan Paulmayer is Senior Manager and Attorney-at-Law at PwC Legal (oehner & partner rechtsanwaelte gmbh).

He holds a degree from the University of Vienna (Mag. iur.) and has been registered as a lawyer with the Vienna Bar Association since 2013.

IFLR 1000
LEADING LAWYER
RISING STAR
2019

Fields of Work

- Banking Supervision
- Capital Markets
- Financing
- Banking M&A
- Derivatives
- Restructuring
- Securitisations

Industry Experience

- Banks
- Insurances
- Industry
- Technology
- FinTechs

Enzo Orsi
Senior Manager
PwC Financial Services
Technology Consulting
M: +43 699 16305209
enzo.a.orsi@pwc.com

Enzo Orsi is Senior Manager in the Technology Consulting Practice of PwC Austria.

He holds a degree in Computer Science and Engineering from *Politecnico di Milano*.

Fields of Work

- IT Strategy & Transformation
- DWH/Business Intelligence
- CFO/CRO Reporting
- Data Modelling
- DQ Assurance & Reconc.
- IT Architecture design
- Mainframe technologies
- IT cost optimization
- IT Security

Glossary

2FA	Two-factor authentication: A method to authenticate a user by an additional layer of security other than a password or username
FMA	Austrian Financial Market Authority (*Finanzmarktaufsicht*)
OTP	One-time-password
PIN	An identifying number allocated to an individual by a bank or other organisation and used for validating electronic transaction
PSD2	Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC
SCA	Strong Customer Authentication pursuant to Art 97 of PSD2 and Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication
SMS	Short message service

pwclegal.at
pwc.at

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and to the extent permitted by law, PwC Legal and PwC do not accept or assume any liability, responsibility, or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.