CAPS
Convenient Access to PSD2 Services

Mobile strong customer authentication under PSD2: comparisons and considerations

About CAPS

The CAPS Open Framework is a large multi-stakeholder market initiative that aims to make Payment Services Directive 2 (PSD2) work safely, in practice and at scale for all. It is an open forum that proposes solutions to the technical, business and operational issues faced by potential PSD2 stakeholders across Europe. Banks, Third Party Payment Services (TPPs), FinTechs, service providers, corporates, mobile industry, etc. work together here to develop a framework that works for all – not just for one side of the industry.

The CAPS community has developed a good deal of the framework, much of which has resulted in significant contributions to the Euro Retail Payments Board (ERPB), and individual members are working towards piloting CAPS concepts to harden the framework. Since CAPS is an open organisation the framework, or elements thereof, can then be adopted by all those wishing to compete in the market to provide the services, thus making the market bigger and better for all.

PARTICIPANTS

equensWorldline   fidor SOLUTIONS   GSMA   isabel group   nets   TRUSTONIC

Contents

1. Introduction

The new PSD2 regulations will bring about major changes to the digital security landscape. Among the most significant of these will be the requirement to use strong customer authentication (SCA) in remote payment transactions. Additionally, SCA on mobile devices will be required to make use of a secure execution environment (SEE).

Mobile SCA has the potential to be a source of considerable innovation. For this to realised, however, there is a need to:

a) inform the payment ecosystem on how the mobile ecosystem can aid implementation of mobile SCA; and

b) explain the benefits of different approaches to that implementation.

To avoid fragmentation, this work should establish a common basis upon which collaboration on architecture may be undertaken, and the agreed results recommended.

Implementation of mobile SCA under PSD2 involves the following challenges:

- SCA as a regulatory concept must be translated into commercially effective authentication solutions.

- Third-party payment service providers (TPPs) are entitled to rely on the SCA process – as determined by the account servicing payment service providers (ASPSP) – leading to the involvement of more stakeholders in the payment transactions.

- As consumers strongly prefer to use mobile devices over alternatives, we can expect a rapidly increasing number of use cases in which mobile SCA is required.

This paper starts from the existing trust model, and considers how it will evolve in the new regulatory environment. The basic principles of existing technological options for implementation of mobile SCA are compared with those which may be used to do so as required by PSD2. This is not an exhaustive list, but a snapshot which can be amended with new technologies and players as they emerge.

2. Mobile SCA solutions available in the PSD2 environment

This paper looks at major mobile SCA solutions that are generically available in the EU at the time of writing. Whilst there are many proprietary and national solutions that comply effectively with the PSD2 requirements, we have focused on those that are generically available across the European Union. The profiles in this paper are indicative only of high-level considerations that payment service providers will have in mind when implementing mobile SCA. The aim of ASPSPs is to prevent a single point of failure and offer a variety of authentication solutions to their payment service users (PSUs); the solutions selected for consideration in this document, therefore, can be combined and implemented in a complementary way.

2.1 Standalone banking app

In most cases today, banks use all-in-one mobile applications for activities from authentication (e.g. by requesting a user ID and password) to authorisation (e.g. by requesting a PIN). If supported by hardware, the required authorisation code may be replaced by biometric elements like fingerprints. This shortcut is usually implemented locally on the mobile device without any server based components.

Customers must typically register their device with the ASPSP first. The ASPSP will securely link an authorised user to his authorised device(s), which can prevent cloning or repurposing of cryptographic keys (device binding). In some cases, this requires that the device be capable of receiving SMS on a pre-registered mobile phone number. This does not work on many tablet devices, so an additional mobile phone is required to register such a device.

Push messages can be used to alert the user and/or request authorisation. Device registration does not only improve security, it is also a way to fulfil the requirement to use more than one SCA factor – a message sent to a registered device can act as proof of possession. Requiring that authentication/authorisation be sent from a registered device can also fulfil this criterion.

Apps can be protected either by using software protection techniques or a trusted execution environment (TEE).

From a mobile security perspective, the following technologies are being used or explored by ASPSPs to strengthen the security of banking apps:

- OS sandboxing (together with rootkit/jailbreak detection mechanisms)
- Application code obfuscation
- Hardware secure elements
- Anti-virus software
- Run time application self-protection
- Mobile device analytics/behaviour
- Behavioural biometrics

2.1.1 Software development kits provided by vendors and banks

Many banking apps already make use of identity and security solutions from specialist vendors and service providers. They are integrated into the app via software development kits (SDKs). In SDK mode the bank app can gain access to all authentication methods supported by the SDK whilst maintaining full control over the user journey/experience and branding of the application.

SDKs simplify and standardise:

- the authentication and authorisation methods exposed to the mobile app;
- the security mechanisms to protect technical assets;
- secure communication methods with the central platforms for authentication and authorisation.

Using SDKs simplifies usage of a bank's SCA framework, but adds code and complexity to the TPPs app. In future a TPP may need to implement dozens of SDKs, some of which may not be interoperable. A better approach for a TPP might be to rely on SCA standards like FIDO.

SDKs can utilise various mechanisms to protect sensitive assets. The recommended minimum would be to use software protection techniques, such as white box cryptography and software based anti-tamper mechanisms to reduce the risk of attack. A much more secure solution, available in most Android devices, is a TEE. The TEE offers hardware-backed protection to sensitive parts of the application, and on many devices also offers the ability to secure peripherals such as user interface and biometric sensors. The TEE is highly resilient to large-scale software-based attacks.

2.1.2 Standalone banking app with standalone authentication app

Banks can also offer an application dedicated to the authentication functionality, often by customising a specific white label mobile application. An example is German Sparkasse's applications: while these apps belong to the same bank, each serve a distinct authentication functionality:

- **Main banking app** - used for viewing bank account info, managing transactions, and contacting the bank. Protected by password or fingerprint ID from the phone's data.
- **Authentication app** – (PushTan app) can be used to verify information for dynamic linking such as transaction amount and beneficiary; and generate a transaction authentication number (TAN), which would either be displayed to the PSU or silently sent to the ASPSP.

2.3 Banking apps deployed in TEE

A TEE is an environment within the main processor of a device which enables a secure operating system and trusted applications to run on it, and can therefore be used to protect sensitive aspects of an application. This secure operating system runs alongside the normal operating system. Most of a banking app's activities will be carried out via the main operating system, but the TEE can be used to guarantee that sensitive data is stored, processed and protected in a trusted and physically isolated environment.

2.4 Mobile industry solution

The mobile industry, supported by GSMA,[1] has developed a global open standard called Mobile Connect which enables consumers to authenticate themselves, authorise transactions and share their data via mobile when accessing websites, payment accounts or initiating payments. The service is delivered for service providers as an industry standard API (based on Open ID Connect). The mobile phone is used as 'something I have' (possession); a PIN is then used as 'something I know'[2] (knowledge), or biometrics can be used as 'something I am' (inherence). Available security assurance levels match those defined in the eIDAS regulation.

The customer experience is simple and consistent. Where a PIN code is used, the consumer has only one - there is no need to remember further login details for each website, and therefore no password to steal from the service provider.

We have chosen here to describe Mobile Connect's application to the SCA requirements and refer to it as a standard. There are similar local solutions in some markets which may vary in how they leverage mobile network security. However, we believe that the concepts described with respect to Mobile Connect can be used to give a first understanding of this type of solution.

2.4.1 Mobile Connect as a second factor

Mobile Connect as a second factor authentication mechanism – via possession, knowledge, and/or biometric – complements any primary factor provided by the bank, for example a user ID and password or banking app. For this purpose, Mobile Connect can be delivered through different authenticators: an application in the SIM (SIM applet), a smartphone application (this can be a standalone application or an authenticator SDK integrated in a banking app), or seamless mobile network authentication.
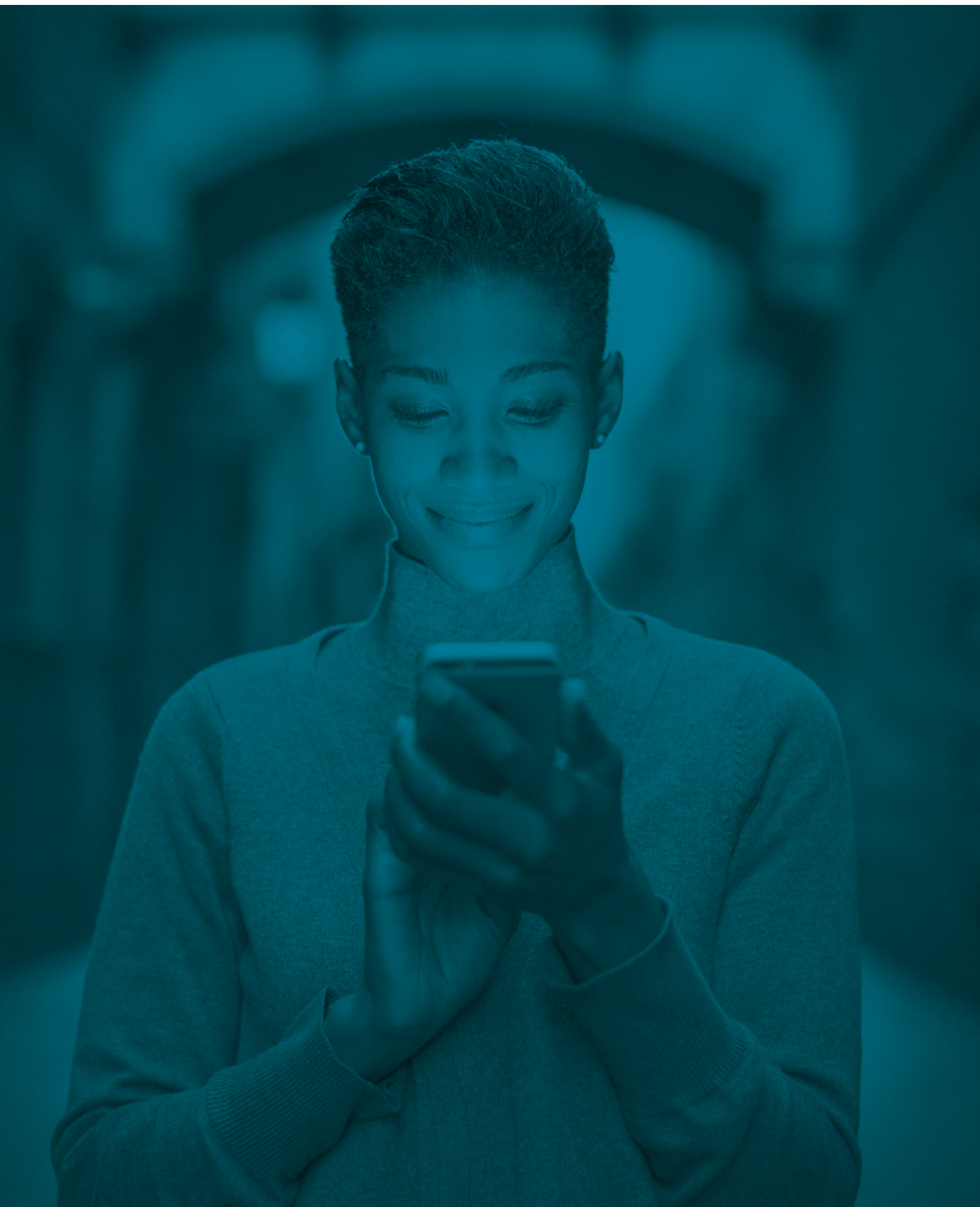
2.4.2 Mobile Connect as a two-factor solution

This solution provides a complete strong customer authentication solution for the ASPSP, offering two factors rather than merely a second factor as in the previous section. This allows service consumption and authentication to take place in separate channels if a SIM applet is used as the authenticator. Another option is for Mobile Connect to be based on a software smart authentication application: this can be a standalone authentication app, or Mobile Connect Smartphone App Authenticator included in an existing banking app via SDK (so no standalone authentication app required). The Mobile Connect SDK is invoked and operated by the mobile operator but it is embedded in the banking app.

---

1   The GSMA represents the interests of mobile operators worldwide, uniting nearly 800 operators with more than 250 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organisations in adjacent industry sectors. www.gsma.com.

2   The full Mobile Connect implementation allows more factors to be used in authentication:
- Something user has (Device and SIM)
- Something user knows (PIN)
- Something user is (fingerprint)
- Something user does (normal behaviour)
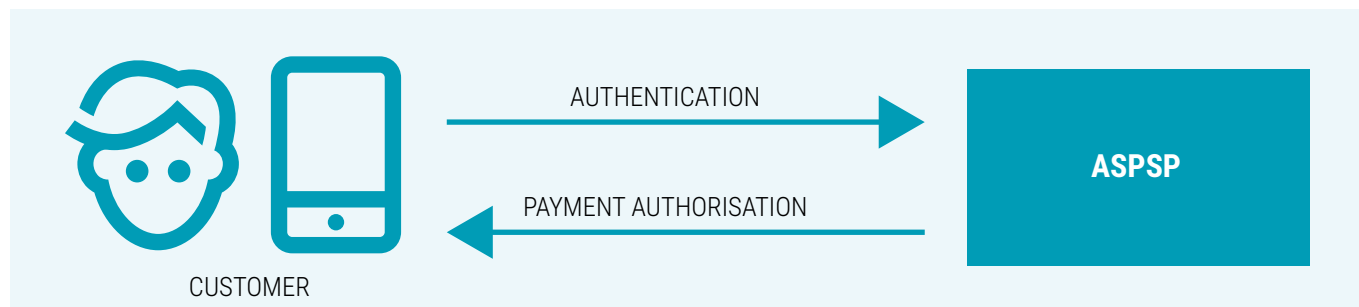- Something mobile network knows (network info – divert, status, roaming etc.)

3. Trust model

When looking at mobile SCA implementation, the question arises how the existing trust model in payments adapts to the implementation of mobile SCA. In the current environment, authentication and authorisation remains between PSU and ASPSP.

EXISTING TRUST MODEL PRE-PSD2

In the PSD2 environment, three methods are generally foreseen for personalised security credentials (PSCs) to be handled between ASPSPs, TPPs, users and third-party authentication providers.

1. **Embedded SCA model** – TPP designs the user interaction in which the PSU presents the PSCs to the TPP. TPP forwards these to the ASPSP via the dedicated ASPSP interface. There is a view in the market that this model is open to abuse and less robust than the redirect model described below, because the principle of 'sole control' over the PSC by the PSU is not maintained.

2. **Redirect SCA model** – the PSU does not present the PSCs to the TPP, but directly into the SCA service interface of the ASPSP. The TPP is therefore not involved in handling the PSCs.

3. **Decoupled SCA model** – the PSU presents the PSCs directly to a dedicated device and/or app. The decoupled approach is often viewed as a switch between two different physical devices, rather than a delegation to a third party identity provider. For instance, the PSU may be using a browser to access a merchant site and then an app to perform the SCA. A third-party identity provider would only be permitted if they were acting on behalf of a bank. The decoupled SCA may be deployed by the TPP as part of their service, by implementing an SDK which delivers the bank's SCA functionalities into the TPP service.

The following PSD2/RTS rules apply to all three models:

- No agreement is required between the TPP and the ASPSP.
- The TPP can rely on the SCA of the ASPSP.
- The principle of non-discrimination will require use of the same PSCs for the TPP as for the ASPSP.

When considering mobile SCA solutions, only the decoupled model seems to be a suitable method for credentials to be handled between users, ASPSPs, TPPs, and third-party authentication providers. The trust model changes from the simple existing trust model pre-PSD2 above if the ASPSP agrees with another entity that the latter should carry out the SCA. This may be a third-party authentication provider such as a mobile operator, or a TPP (typically integrating the ASPSP SCA service into its own service via an SDK).

4. Summary of relevant RTS requirements for mobile SCA[3]

RELEVANT RTS REQUIREMENTS FOR MOBILE SCA

General provisions

Transaction monitoring mechanisms	Transaction monitoring systems must be in place to detect unauthorised and fraudulent payment transactions. Those monitoring systems should be based on analysis of payment transactions taking into account elements which are typical of a PSU in the circumstances of normal use.

Security measures for the application of SCA

Independence of factors (knowledge, possession, inherence)	No information of any factor can be derived from the disclosure of the authentication code. It is not possible to generate a new authentication code based on knowledge of any other authentication code previously generated. Mitigating measures to ensure independence of factors: a) The use of separated secure execution environments through the software installed inside a multi-purpose device b) Mechanism to ensure that the software or device has not been altered by the payer or a third party c) Where alterations have taken place, mechanisms to mitigate the consequences thereof.
Dynamic linking	The authentication code generated shall be specific to the amount and the payee agreed to by the payer when initiating the transaction.

Confidentiality and integrity of the PSU's PSCs

The association of the PSU's identity with PSC, authentication devices and software	This association must be carried out in secure environments and is the responsibility of the PSP. This must comprise at a minimum the PSP's premises, the internet environment provided by the PSP, or other similar secure websites used by the PSP, and its ATM services (taking into account risks associated with devices and underlying components used during the association process that are not under the responsibility of the PSP).
Delivery of credentials, authentication devices and software	PSCs, authentication devices and software must be delivered to the PSU in a secure manner designed to address the risks of unauthorised use due to loss, theft or copying.
Renewal, destruction, deactivation and revocation of PSCs	PSPs have to ensure secure renewal, destruction, deactivation and revocation of PSCs.

---

3   At the time of writing the final draft RTS were published on the 27th November 2017. This version was used as a basis for the analysis. See also http://ec.europa.eu/finance/docs/level-2-measures/psd2-rts-2017-7782_en.pdf

5. The mobile ecosystem

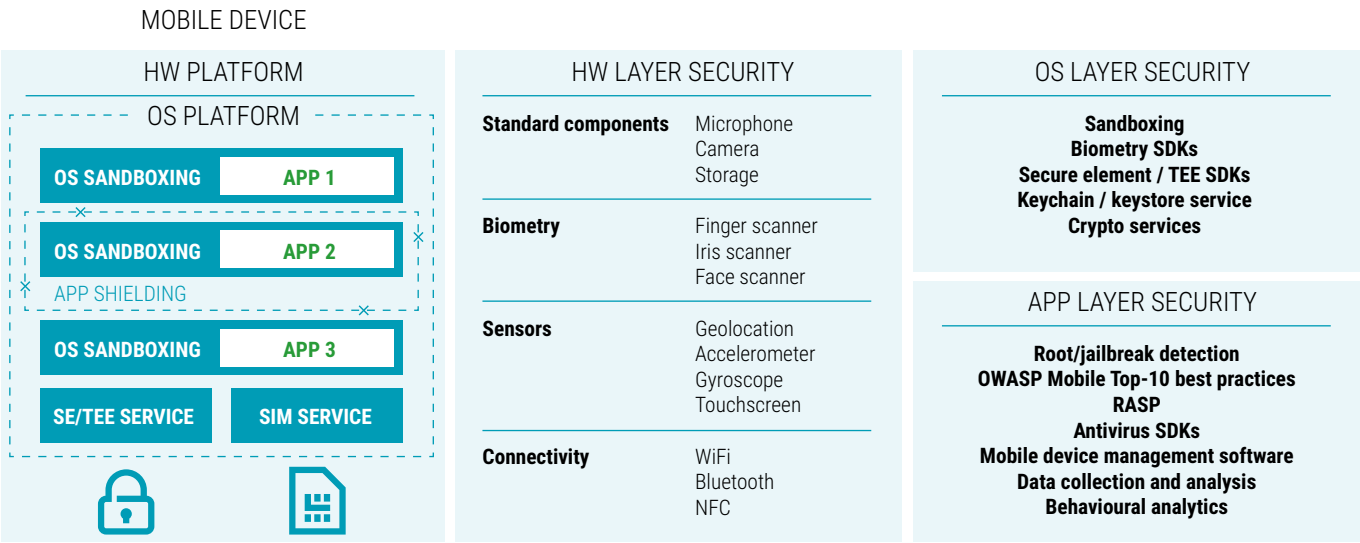This paper examines a broad range of technical options for implementation of mobile SCA, including solutions which rely on cooperation between PSPs and mobile operators. It has historically not been a mainstream approach for PSPs to procure authentication from mobile operators and the payment ecosystem; development of mobile solutions so far has drawn generally on the capabilities of mobile devices, rather of the entire mobile ecosystem. This section explores the different components of the mobile environment which could serve mobile SCA solutions.

MULTIPLE LAYERS CAN BE COMBINED INTO THE SECURITY DESIGN OF A MOBILE SOLUTION

	Communication protocol security including encryption (transport layer / messaging layer), use of secure protocols (e.g. Open ID Connect)
	Mobile network connectivity + security including dynamic attributes + mobile operator business processes to bar lost/stolen devices WiFi connectivity – weak security
	Application layer: bank app / authentication app including software protection e.g. whiteboxing, jailbreak and root detection, Runtime Application Self-Protection (RASP)
	Mobile operating system including access to biometric drivers
	Hardware security element: SIM, Trusted Execution Environment for isolated execution environment, Integrity of applications stored on it and confidentiality of associated credentials
	Phone hardware including fingerprint sensors, GPS etc. enabling security in combination with other layers

TYPICAL MOBILE OPERATOR PROCESSES TO BAR LOST/STOLEN DEVICES

MOBILE DEVICE

HW PLATFORM		HW LAYER SECURITY		OS LAYER SECURITY

HW PLATFORM

OS PLATFORM

OS SANDBOXING	APP 1
OS SANDBOXING	APP 2

APP SHIELDING

OS SANDBOXING	APP 3
SE/TEE SERVICE	SIM SERVICE

HW LAYER SECURITY

Standard components	Microphone
	Camera
	Storage
Biometry	Finger scanner
	Iris scanner
	Face scanner
Sensors	Geolocation
	Accelerometer
	Gyroscope
	Touchscreen
Connectivity	WiFi
	Bluetooth
	NFC

OS LAYER SECURITY

**Sandboxing
Biometry SDKs
Secure element / TEE SDKs
Keychain / keystore service
Crypto services**

APP LAYER SECURITY

**Root/jailbreak detection
OWASP Mobile Top-10 best practices
RASP
Antivirus SDKs
Mobile device management software
Data collection and analysis
Behavioural analytics**

5.2 Mobile device security in relation to the secure execution environment

The SEE may be implemented via a hardware or a software approach:

5.2.1 Hardware SEE

SIM cards store data including user identity, location, phone number, network authorisation data, personal security keys, contact lists and stored text messages. Security features include authentication and encryption to protect data and prevent eavesdropping.

The TEE is an isolated environment which runs in parallel with the operating system, providing security for the rich environm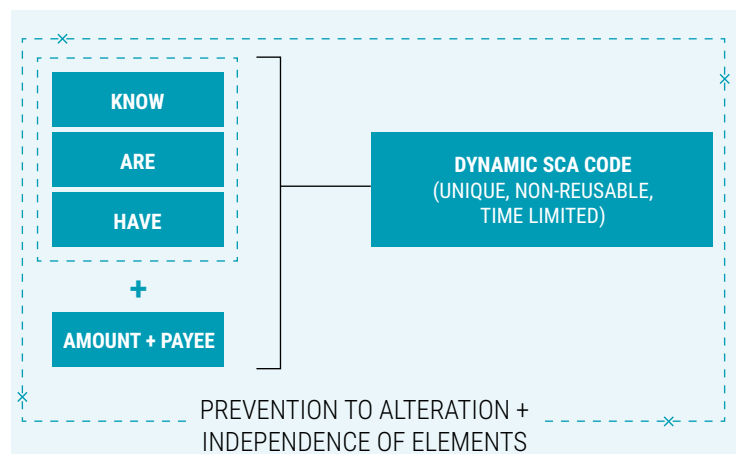ent. It is intended to be more secure than the user-facing OS, which GlobalPlatform calls the rich execution environment (REE).

Both the TEE and SIM are hardware protected systems of the device. Access is therefore highly restricted in terms of how the secure area may be accessed, and by whom. Both mechanisms ensure that interaction with the consumer's screen and keyboard is highly secure, by isolating the user interface functions from apps running in the normal operating system, for example when the customer enters their PIN. Whilst both options are very secure, they are often perceived as including a dependency on either the mobile operator, in the case of the SIM, or a TEE enabled handset. In terms of security these hardware mechanisms are regarded as very effectively meeting SEE requirements.

5.2 Software SEE

A secure implementation of the software SEE requires multiple software protection features, such as whiteboxing and one-time application self-protection.
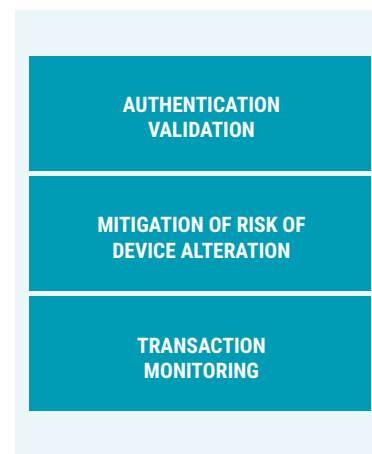
MOBILE DEVICE

BACKEND

Software solutions lack the physical protection of the hardware secure elements (SIM, TEE, Secure Enclave). However, with a broad range of the elements described above they can also be highly secure.

The actual security of software implementations depends on the quality of the implementation. The quality of the implementation for mobile SCA can range from unsatisfactory to extremely good (i.e. equivalent to hardware security level).

5.3 Two-way communication between device and ASPSP in case of device loss

Given the specific risk that mobile devices can be compromised, lost or stolen, it is important to ensure two-way communication between the device and ASPSP. This is especially true given that the regulatory technical standards (RTS) on SCA under PSD2 oblige the payment service provider (PSP) to secure renewal, destruction, deactivation and revocation of personalised security credentials (PSCs).

In the case of a lost or stolen phone, the options for two-way communication are as follows:

- The TEE does not allow for a way to disable the phone remotely, as there is no two-way communication channel; however, associated software apps may gain access through alternative channels such as WiFi to enable remote management.

- The SIM (and therefore the SCA capability if it is linked to the SIM) and the device can be disabled by the mobile operator remotely if the phone is switched on and connected to a mobile network. The association of mobile phone, SIM and the phone number (MSISDN) is stored very securely in the mobile network, and this information is not available to other agents in the ecosystem. Whenever a mobile device connects to a network, the network is aware of the interlinking of phone, SIM and mobile number. If the device is used with a different SIM, the network knows immediately that this is a new association and can take appropriate action if this is interpreted as fraud, such as marking the phone as stolen and blocking any associated authentication services. If a phone is marked as stolen by one mobile operator, this is known to mobile operators around the world. The mobile operator can also determine the location of the device.

- Software solutions also allow for two-way communication, by allowing push notification via the software app on WiFi, and collecting data via that app. It may however be difficult for the app to determine whether a device has been lost or stolen and for the ASPSP to then communicate with the app and act accordingly.

5.4 Independence of factors

PSD2 requires that authentication is based on use of two or more elements, categorised as knowledge, possession and inherence. The regulations also require that any breach of one factor does not compromise the reliability of the others[4]. For mobile SCA, the confidentiality of authentication data must remain protected even if the mobile device is compromised; in practice, this means that if the phone is lost or compromised, the SEE must remain intact and continue to protect the PSCs. Independence of factors is crucial here.

- The TEE is very conducive to independence, as it separates out a hardware environment which cannot be easily accessed from the rest of the device.
- The same is be true for the SIM.
- Software-based security environments must ensure that the software-based SEE is separate from the rest of the software to ensure that the software SEE cannot be accessed by other applications on the device.

5.5 Dynamic linking

Dynamic linking is important to ensure secure payment transactions. PSD2 requires a dynamic link between the payee and a specific transaction amount.[5] The SEE is critical for securely displaying the message to the user and capturing the user's response. It must ensure that any rogue application cannot read the display, or read/change the user's inputs.

Both the TEE and SIM ensure that there is 'protected input/output' to and from the device i.e. secure PIN input and pop up message, along with a protected execution boundary from the rest of the operating system.

5.6 Mobile ecosystem and TRA

PSPs have a very large number of data points which can be analysed to provide an excellent indication of fraud potential. Examples include:

- Location (GPS)
- Status (roaming, NFC-enabled)
- Event related to SCA (transaction signature, password change)
- Application information (version, installation date, language)
- OS information (type, version, language, encryption-enabled)
- Device (model, code)
- Behaviour (user, session)
- Environment information (hooking framework, debugger-enabled, keyboard overlay, library injection)
- Biometrics
- SIM (type, identifiers)

The mobile operators' data points can be useful complementary information for the ASPSPs fraud engine that helps PSPs to increase security by leveraging contextual information available to mobile operators. For example, a mobile operator can check whether the user's handset is in an unusual location, or whether their SIM card has been put into a different device. This contextual information is available at any time without the user being required to actively use the authentication service; it can be exposed to payment service providers through the standard Mobile Connect API and analysed by the PSPs as part of their existing fraud prevention engines. In relation to the RTS requirements, in particular the definition of transaction risk analysis, mobile operators are able to expose the following information:

- SIM swap, device change, call divert status, account status.
- Lost or stolen devices.
- Location (network location in case GPS has been spoofed).
- Other indicators relevant in specific scenarios which can be exposed through the same interface.

This supports PSPs in assessing the risk of:

- Abnormal behavioural pattern of the payer.
- Changes in pairing relationships between, device, SIM and MSISDN.
- Abnormal location of the payer.

---

4   PSD2, recital 30

5   PSD2, Article 7 (2)
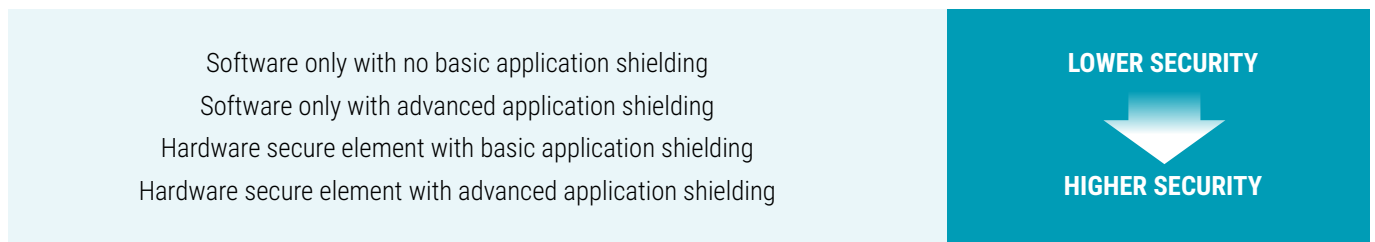
5.7 Frictionless (adaptive) authentication

Regardless of the nature of SCA solution, the goal is to create the best experience for end users. PSD2 considers this, and allows exemptions based on the nature of the operation – for example payments towards trusted beneficiaries, repeated payments, low-value payments, and low-risk balance enquires – or on real-time risk assessment. This, combined with ongoing advances in security technology, allows the design and deployment of solutions which only challenge the user with an SCA request when truly necessary.

This requires implementing powerful authentication and risk-management backends, which can be easily configured and reprogrammed to respond quickly to newly available authentication methods, applications, devices and user journeys while having full up-to-date coverage of security threats.

6. Comparison of SCA approaches

Below is a summary and high-level comparison of the different SCA solutions available across the EU. All the solutions considered below are fully compliant with the RTS on SCA. Our understanding of security levels from low to high is based on the following view:

Software only with no basic application shielding Software only with advanced application shielding Hardware secure element with basic application shielding Hardware secure element with advanced application shielding	**LOWER SECURITY** ⬇ **HIGHER SECURITY**

Hardware solutions are secure by design. Software solutions are implemented widely, and if well implemented can be equally secure as hardware solutions.

The table below compares the different solutions in relation to these criteria:

- **Secure execution environment** - how is the SEE provided? While all solutions compared in this paper comply with PSD2, we have tried to show relative strengths and weaknesses.
- **Independence of factors** - how is independence realised, i.e. how does the solution ensure that if one factor is compromised, the other factor is not?
- **Ease of use for consumers** - ability to optimise the user experience.
- **Dependencies** - from a technical and commercial perspective.
- **Confidentiality of security credentials.**

Criteria for comparison	Standalone banking app	Standalone banking app with standalone authorisation app	Banking app deployed in TEE	Cross-mobile operator standard providing second factor	Cross-mobile operator standard providing two factor solution
General description	Banking app combined banking and SCA functionality in one app, with SCA often integrated through an SDK	Banking app and separate authentication app offering SCA functionalities only (can be provided by vendor as a white label app to be customised by bank)	Banking app (or SCA app) uses security from the hardware provided by TEE	Mobile Connect as a secondary factor (typically possession) complementing any primary bank factor provided by the bank	This solution provides a complete SCA solution for the ASPSP with the cross-operator solution providing both factors. It can rely on a SIM applet as the authenticator or a software smart authentication application, possibly embedded in existing banking app via SDK
Secure execution environment	The flexibility of SDK allows the reliance on multiple security technologies including: whitebox cryptography, app shielding, TEE, contextual risk analysis	The flexibility of SDK allows the reliance on multiple security technologies including: whitebox cryptography, app shielding, TEE, contextual risk analysis	TEE	SEE could be the SIM or device security	SEE can be the SIM; if a network-bound smartphone app authenticator is used instead, then it can be disabled in a lost/stolen scenario
Independence of factors	Requires additional software protection features to ensure independence typically provided by SDK vendors	Requires additional software protection features to ensure independence typically provided by SDK vendors	TEE can support security and independence of factors, because the TEE separates out a hardware environment that cannot be easily accessed from the rest of the device	Mobile Connect works in a separate authentication channel (for example SIM applet) from the primary bank solution; if a network-bound smartphone app authenticator is used instead, it can be disabled in a lost/stolen scenario	Independence is achieved through hardware or network binding. In the case of SIM applet, compromising the device does not compromise the knowledge factor (Mobile Connect pin stored on the SIM as a hardware protected secure execution environment); in the case of a smartphone authentication app, as it is bound to the network, it can be disabled in a lost/stolen scenario
Ease of use for consumer	Very good consumer experience (frictionless, fast). No limitation of the application functionality.	Very good consumer experience (frictionless, fast). No limitation of the application functionality. Consumer is dealing with 2 apps. Invocation of a standalone authentication app can be transparent to the end user providing excellent user experience	Very good consumer experience (i.e. touch ID/ Android fingerprint API or PIN, and potentially other biometrics authentication factors) Look and feel fully customisable	User uses a first factor provided by the bank and a 2nd factor provided by Mobile Connect. Similar to SMS OTP implementations, this means the user experience consists of two elements of user experience being combined. However Mobile Connect experience offers much superior user experience vs SMS OTP	Mobile Connect provides the entire SCA user experience. As a minimum it will offer an upgrade vs the SMS OTP user experience; with a rich user experience possible through Mobile Connect implemented as a smart authentication app
Dependencies	Widely adopted. Available on smartphone only	Available on smartphone only	Dependency on availability of accessible TEE on the device, today majority of phones	Available on all phones. Dependency on cooperation with mobile operators through standard contract	Available on all phones. Dependency on cooperation with mobile operators through standard contract
Confidentiality of security credentials	Managed by security on the device (security depends on quality and efficiency of software protection capabilities). SDK vendors make sure to utilise the best platform features for extra security such as secure enclave	Managed by security on the device (security depends on quality and efficiency of software protection capabilities). SDK vendors make sure to utilise the best platform features for extra security such as secure enclave	Managed by TEE (secured through hardware)	Managed by Mobile Connect. Security credential can be stored in the SIM secure element	Managed by Mobile Connect. Security credential can be stored in the SIM secure element

6.1 SMS OTP in the context of PSD2

SMS One-Time-Password (OTP) is a ubiquitous and reliable technology. However, according to the National Institute of Standards and Technology's Digital Identity Guidelines (SP 800-63),[6] a PSP relying on SMS OTP cannot easily mitigate the risks of social engineering. This means an-out-of-band secret sent via SMS can be received by a hacker, who has convinced the mobile operator to redirect the victim's messages.

Another risk is endpoint compromise, where a malicious app on the endpoint reads an out-of-band secret sent via SMS, and the hacker uses this secret to authenticate. Recognising the security risks to which SMS is exposed, the GSMA's Fraud and Security Group (FASG) recommends using alternative solutions, such as Mobile Connect, but is also undertaking work to establish what mitigation options may exist that could have a positive impact.

It is therefore worth noting that Mobile Connect is not susceptible to such man-in-the-middle attacks, because Mobile Connect's authenticators like the SIM Applet Authenticator uses Class 2 SMS, which is encrypted. The messages sent are also encrypted, making it a dual-encrypted system. There is also no PIN, code or OTP exchanged over the air – only a strongly encrypted signature is exchanged to communicate the strong authentication.

Mobile Connect can also be used to provide PSPs with fraud signals that strengthen SMS OTP. These fraud signals include SIM swap and call divert information, which can be obtained from the mobile network and exposed through Mobile Connect.

---

6   https://www.nist.gov/itl/tig/projects/special-publication-800-63

7. Conclusion

This overview is intended to aid those planning to implement mobile SCA in compliance with PSD2. The aim is to provide a framework of high-level considerations, that will help the coming PSD2 ecosystem unlock potential innovation, avoid fragmentation, and work together on standardised implementations. With effective communication and a collaborative approach, the new regulatory landscape across the EU could give rise to considerable improvements in digital security, to the benefit of those devising them and end users alike.

Annex 1

Introduction to Mobile Connect

Mobile Connect is a global open standard supported by GSMA that enables consumers to authenticate themselves, authorise transactions and share their data via a mobile device when accessing websites, payment accounts or when initiating payments.

More general information can be found on **https://mobileconnect.io/business/**. Technical details can be found on **https://developer.mobileconnect.io/** for more technical details.

What are the benefits of Mobile Connect for payment service users and payment service providers?

- Convenience – the customer experience is simple and consistent. The consumer has only one PIN – there is no need to remember further passwords or usernames for each website, reducing friction for the consumer, and there is no password to steal from the service provider. No other hardware device is necessary, so the consumer has the comfort of using their own device which they always have available. During the authentication process Mobile Connect will contact the device and generate a pop up on which the user provides the PIN if required. The solution is extensible in that other data factors, such as inherence (something the consumer is), can be added as necessary to enhance transaction authorisation.

- Security – once the user has authenticated via Mobile Connect, only an anonymised token is shared with the service provider. The token confirms that the authentication was successful and that all mobile operator checks showed no problems. No token is shared if there is a problem. Each token is specific to a service provider, i.e. different service providers get a different token for the same user. Mobile Connect works with the Open ID Connect standard; i.e. all interactions are encrypted and the token is signed (inherent security). Dynamic linking is available through an additional authentication code, which is based on the user identity (phone number) and the payment amount along with a one-time code or globally unique ID (GUID) and the payee identifier (payee ID). For traceability, PSPs can trace the transaction end-to-end through the authentication code which is digitally signed by the operator.

- Privacy and user control – service providers can only receive user data with the permission of users. The user is in control over their data as they give consent (or not) to the mobile operator to share more attributes about them. This consent may be gathered by the mobile operator directly, or by a trusted service provider where it is more practical and aligned with local legislation. Both operators and service providers agree on the Mobile Connect Privacy Principles[7].

- Global availability and interoperability – Mobile Connect is globally available to all consumers and service providers and therefore ensuring consistency, reach and interoperability. The same user experience will apply whatever the service provider. Mobile Connect works with all mobile network providers globally, and on all devices worldwide independently of the operating system. In the European Union alone, Mobile Connect is already supported by major mobile network groups such as Orange, Telefonica, Vodafone, TIM (Telecom Italia Mobile), Telenor and Telia Company to name a few[8].

Introduction to the trusted execution environment

What is it?

A trusted execution environment (TEE) is an environment within the main processor on a device which enables a secure operating system and trusted applications to run on it.

How does it work?

This secure operating system runs alongside the normal operating system. When an application is created, sensitive parts of the application are isolated from the main code, and are loaded into the TEE. The TEE can be used to guarantee that sensitive data is stored, processed and protected in a trusted and physically isolated environment.

The TEE can also be used to protect certain peripherals. On many devices, the TEE can be used to protect the user interface. Both the screen and touchpad can be isolated, so that any applications running on the normal operation system cannot gain access to the data. By delivering a Trusted User Interface, ability to perform functions such as secure passcode entry and secure messaging can be performed. Biometric sensors in phones use the TEE to protect the biometric data and pattern matching.

---

7   https://www.gsma.com/identity/mobile-connect-privacy-principles
8   https://developer.mobileconnect.io/operators

Annex 2

Overview of approaches to achieve mobile SCA in a secure execution environment

1. BANKING APP WITH ITS OWN SECURITY ELEMENTS

Secure execution environment (SEE)	No hardware SEE by design on the mobile device (dependent on strong software protection features e.g. whiteboxing technology). Banking apps can also employ other mechanisms to mitigate fraud: • user behaviour (on the device); • device/connection type; • device state (jailbroken etc.)
Independence of factors	No independence by design: requires additional software protection features to ensure independence
Ease of use for consumer	The user experience is as seamless as possible: SCA app is fully integrated inside the bank mobile app, the authentication can rely on the knowledge and inherence authentication factors ('something I know' and 'something I am'). If the SCA app is bound to a specific SIM/device then the factor ('something I have') is also available. Biometrics authentication can be a powerful way to simplify the user experience. Whatever the use case, the end user will always get the same workflow during an authentication. In terms of graphical interface, the implementation with an SDK allows the banks to display exactly the same look and feel during authentication phases independently of other parts of the banking app. When applied to an external use case (e.g. card payment on a merchant web site), it allows the banks to explicitly show that it is its own mobile app which takes control of the authentication.
Dependencies	Dependency on security provided by the device or by software protection technologies. Available on smartphone only.
Confidentiality of security credentials	Managed by security on the device (security depends on quality and efficiency of software protection capabilities).

2. STANDALONE BANKING APP WITH STANDALONE AUTHENTICATION APP

Secure execution environment	The flexibility of SDK allows the reliance on multiple security technologies including: • Whitebox cryptography • App Shielding • TEE • Contextual Risk Analysis
Independence of factors	Requires additional software protection features to ensure independence, typically provided by SDK vendors
Ease of use for consumer	Very good consumer experience: • Frictionless • Fast No limitation of the application functionality. Consumer is dealing with 2 apps Invocation of a standalone authentication app can be transparent to the end user providing excellent user experience.
Dependencies	Available on smartphone Dependency on security provided by the device or by software protection technologies.
Confidentiality of security credential	Managed by security on the device (security depends on quality and efficiency of software protection capabilities) SDK vendors typically utilise the best platform features for extra security such as secure enclave

3. BANKING APP DEPLOYED IN TEE

Secure execution environment	TEE is an environment within the main processor on a device which enables a secure operating system and Trusted Applications to run on it. This secure operating system runs alongside the normal operating system, i.e. Android. The TEE can be used to guarantee that sensitive data is stored, processed and protected in a trusted and physically isolated environment.
Independence of factors	TEE can support security and independence of factors, because knowledge and inherence factors are more secure compared to software solution, as the TEE separates out a hardware environment that cannot be easily accessed from the rest of the device.
Ease of use for consumer	As for standalone banking app, very good consumer experience (i.e. touch ID/ Android fingerprint API or PIN, and potentially other biometrics authentication factors). Look and feel fully customizable.
Dependencies	Dependency on availability of accessible TEE on the device (smartphone only).
Confidentiality of security credentials	Managed by TEE (secured through hardware).

4. MOBILE CONNECT AS SECOND FACTOR

As explained in section 2.4. we use Mobile Connect in the following description as a global approach, acknowledging that there are other local solutions in some markets.

Secure execution environment	SEE could be the SIM and/or device security. Mobile operator authentication works in a separate channel from the primary bank authentication solution e.g. user ID and password or banking app. It relies on a second set of credentials (decoupled from banking app credentials). For this purpose Mobile Connect may be delivered through different "authenticators": an application in the SIM (SIM applet), a smartphone application (this can be a standalone application or an authenticator SDK that integrates in a banking app) or seamless mobile network authentication.
	'This solution is more secure than One Time Passwords' which can be forwarded or intercepted by malware. This solution is not susceptible to man-in-the-middle attacks because the SIM Applet Authenticator uses Class 2 SMS, which is encrypted.
	Seamless mobile network authentication also relies on network data and cannot be spoofed by device malware. The message level is also encrypted. Moreover no PIN, code or OTP is exchanged over the air; only the strongly encrypted signature is exchanged.
Independence of factors	This option can work in a separate authentication channel (e.g. SIM applet) from the service consumption channel. With one factor being provided and controlled by the bank and the other being controlled by the mobile operator, a compromise of one factor does not affect the other factor.
Ease of use for consumer	A relevant comparison is the user experience associated to the use of One Time Passwords / TANs including SMS OTP. This solution offers a simpler experience whereby a user does not need to receive and copy a short code. Instead the user simply interacts with a pop-up window – pressing OK to confirm or entering their PIN code for added security.
	The user uses a first factor provided by the bank and a 2nd factor provided by Mobile Connect. Similar to SMS OTP implementations, this means the user experience consists of two elements of user experience being combined. However Mobile Connect experience offers much superior user experience than SMS OTP.
Dependencies	Dependency on cooperation with GSMA/mobile operators through standard interface and contract.
Confidentiality of security credentials	The security credentials can be stored in the SIM secure element.
	The bank delegates the performance of the second factor while retaining overall control of the authentication process.
	The second factor can be blocked if device is stolen with the first factor continuing to work.

5. MOBILE SCA WITH THE HELP OF A CROSS-MOBILE OPERATOR TWO-FACTOR SOLUTION

As explained in section 2.4. we use Mobile Connect in the following description as a global approach, acknowledging that there are other local solutions in some markets.

Secure execution environment	A SIM applet may be used as the authenticator, offering the possibility of a decoupled approach where service consumption and authentication take place in separate channels. Another option is for Mobile Connect to be based on a software smart authentication application; this can be a standalone authentication app, or Mobile Connect Smartphone App Authenticator embedded for SCA can be included in an existing banking app via SDK (i.e. no standalone authentication app required). In this case, the Mobile Connect SDK is invoked and operated by the mobile operator.
	SEE could be the SIM and/or device security.
	• In case of SIM security, the SIM applet uses the SIM as a container for the authenticator.
	In practice this service initiates an authentication request by sending an encrypted Class 2 SMS from the operator's network to the application on the SIM (SIM applet), which is invisible to the user; it invokes the SIM applet to present the user with an authentication challenge, prompting the user to enter the Mobile Connect PIN. The hashed PIN is stored within the SIM applet and the PIN comparison occurs locally. The hash cannot be reversed to get the PIN. The messages sent back from the SIM applet are encrypted and signed within the SIM using encryption keys stored on the SIM. Mobile Connect validates this signature.
	Fraud attacks are not scalable because each device would have to be hacked individually. Intercepting the SMS communication between the mobile operator network and the SIM applet is of no use to a potential fraudster, as no credential is exchanged over the air.
	• In case of smartphone app authenticator there is no hardware SEE by design; the SEE is dependent on network binding and strong protection software, e.g. whiteboxing technology. In terms of confidentiality and integrity of the security credentials, the smartphone app authenticator is bound to the mobile network; the Mobile Network Operator can validate the integrity of the association between SIM (identified by IMSI), phone user (identified by MSISDN) and device (identified by IMEI) and the Mobile Connect SDK will only function if the integrity of the association is confirmed. If the phone is stolen, the SIM can be blocked and the IMEI of the device barred; the Mobile Connect SDK will then become invalidated, i.e. cannot be misused. The smartphone app authenticator will not be able to perform any authentication.
Independence of factors	This option can work in a separate authentication channel (e.g. SIM applet) from the service consumption channel. In the case of SIM applet, compromising the device does not compromise the knowledge factor (Mobile Connect PIN stored on the SIM as a hardware protected secure execution environment); in the case of a smartphone authentication app, as it is bound to the network, it can be disabled in a lost/stolen scenario.
Ease of use for consumer	This service provides the entire SCA user experience. As a minimum it will offer an upgrade vs the SMS OTP user experience; with a rich user experience possible through this service implemented as an authentication app or authenticator SDK. With an SDK integrated in the banking app, this offers a seamless user experience since the authentication user experience fully sits in the banking app (i.e. touch ID/ Android fingerprint API, and potentially other biometrics authentication factors can be leveraged). The look and feel are fully customizable. From user perspective there is no need to download a second app for authentication purposes.
	The solution offers a good user experience which importantly will be consistent for users across verticals, services and devices (feature phones, smartphones), as this operator service can be used by any service provider. This includes private sector services as well as public services (as demonstrated through the use of this service for eIDAS[9] cross-border services).
Dependencies	Dependency on cooperation with GSMA/mobile operators through standard contract. Available on all devices if based on SIM applet, on smartphones only if based on smartphone app solution.
Confidentiality of security credentials	Security credentials can be stored in the SIM SE.
	Otherwise, the smartphone app authenticator is bound to the mobile network; the Mobile Network Operator can validate the integrity of the association between SIM (identified by IMSI), phone user (identified by MSISDN) and device (identified by IMEI) and the Mobile Connect SDK will only function if the integrity of the association is confirmed. If the phone is stolen, the SIM can be blocked and the IMEI of the device barred; the Mobile Connect SDK will then become invalidated, i.e. cannot be misused. The smartphone app authenticator will not be able to perform any authentication (dependency on operator).

---

9   EU regulation on electronic Identification, Authentication and trust Services

CAPS
Convenient Access to PSD2 Services