ALLEN & OVERY

Strong customer authentication for payment services: further guidance and potential additional time for compliance

17 July 2019

In order to ensure the security of electronic payments and to reduce, to the maximum extent possible, the risk of fraud, payment service providers (**PSPs**) are due to apply strong customer authentication (**SCA**) to electronic transactions by 14 September 2019[1].

SCA is defined in Article 4(30) of PSD II which has been implemented by Sec. 1(24) of the German Payment Servces Supervisory Act (*Zahlungsdiensteaufsichtsgesetz* – **ZAG**) as an authentication based on the use of two or more elements categorised as knowledge, possession and inherence that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data.

In light of numerous queries from market participants, the European Banking Authority (**EBA**) has issued an opinion setting out which authentication approaches are considered to be compliant with these SCA requirements (EBA-Op-2019-06, the **Opinion**)[2]. The Opinion also addresses concerns about the preparedness and compliance of some actors in the payments chain − particularly those not directly subject to PSD II (ZAG), such as e-merchants − by the 14 September 2019 deadline.

Although the EBA's Opinion is primarily aimed at national competent authorities (**NCAs**), it provides guidance on regulators' expectations and, as such, is useful also for PSPs, payment service users (**PSUs**) and payment schemes.

I- SCA compliant approaches

The Opinion provides a non-exhaustive list of the authentication approaches currently observed in the market and states whether or not they are considered to be SCA compliant. The Opinion does so for each of the three SCA elements, namely: (i) inherence; (ii) possession; and (iii) knowledge, and also provides clarifications regarding combinations of these elements.

Inherence element

Inherence is defined in Article 4(30) of PSD II (Sec. 1(24) No. 1 ZAG) as "*something the user is*". The Opinion clarifies that it includes biological and behavioural biometrics identifying the PSU and relates to physical properties of the body parts, physiological characteristics and behavioural processes created by the body and any combination of these, for instance retina and iris scanning, vein, face and other body-part recognition and heart rate. Keystroke dynamics[3] also constitute an inherence element, as distinct from a PSU memorised swiping path performed on a device, which would not constitute an inherence element, but may constitute a knowledge element instead.

The Opinion stresses that beyond the mere identification of biometrics which may constitute inherence elements, PSPs must also guarantee the quality of the implementation of the inherence-based approach to ensure that a specific biometric is a compliant inherence element for SCA purposes. In this context, although the EBA states that

[1] Pursuant to Article 15(1) of the German Law on the Implementation of the Second Payment Services Directive (**PSD II**) and the Commission Delegated Regulation 2018/389/EU 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 (the **RTS**). The regulatory part of PSD II, in particular the requirements regarding SCA, are implemented into German law by the Payment Services Supervisory Act (*Zahlungsdiensteaufsichtsgesetz* – **ZAG**).

[2] The full text of the opinion is available via the following link: https://eba.europa.eu/documents/10180/2622242/EBA+Opinion+on+SCA+elements+under+PSD2+.pdf.

[3] That is, identifying a user by the way they type and swipe.

communication protocols such as EMV 3-D Secure version 2.0 and newer versions would not currently appear to constitute an inherence element (as none of the data points, or their combination, exchanged through this communication tool appear to include information that related to biological and behavioural biometrics), the EBA nonetheless encourages their use as a means for merchants to support the use of SCA.

Possession element

Possession is defined in Article 4(30) of PSD II (Sec. 1(24) No. 2 of ZAG) as "*something only the user possesses*". The Opinion clarifies that it does not only refer to physical possession but can also refer to something that is not physical (eg an app).

Hence a device can evidence possession as long as there is a reliable means to confirm possession through the generation or receipt of a dynamic validation element on the device such as a one-time password (**OTP**).

Mobile apps and web browsers may also evidence possession, provided that they ensure a unique connection between the device and the PSU's app or web browser (eg through hardware crypto-security, web-browser and mobile-device registration). Additionally, digital signatures generated by a private key may constitute a possession element.

While the EBA has already clarified, in its previous opinion on SCA,[4] that card details and a security code printed on the payment card itself cannot constitute a knowledge element, the EBA makes it clear that these details and code cannot constitute a possession element (the same applies for printed matrix cards or printed OTP). That being said, dynamic card security codes may provide the requisite evidence of possession (where the code is not printed on the card and changes regularly).

Knowledge element

Knowledge is defined in Article 4(30) of PSD II (Sec. 1(24) No. 3 of ZAG) as "*something only the user knows*". According to the Opinion, the following security elements constitute knowledge elements: a password, a passphrase, a PIN, knowledge-based responses or a memorised swiping path (as opposed to keystroke dynamics, which may be considered an inherence element).

As stated above, the card details and security code printed on the card do not constitute knowledge elements (while, on the contrary, if the card security code is not printed on the card and sent separately to the PSU, it could constitute a knowledge element). Similarly, a user ID or an email address does not constitute a knowledge element.

Finally, the EBA is of the view that a knowledge element should exist prior to the initiation of the payment or the online access: OTP is therefore not a compliant knowledge element for SCA purposes under the approaches currently observed in the market (instead OTP provides evidence of possession).

Independence and dynamic linking

For SCA purposes, at least two elements, one from each of the different categories mentioned above, must be met.

For electronic payment transactions made remotely (for instance in the e-commerce environment), Article 97(2) of PSD II (Sec. 55(2) ZAG) and Article 5 of the RTS further require that these elements permit dynamic linking, meaning that in such cases PSPs must apply security elements which dynamically link the payment transaction to a specific amount and a specific payee. The EBA encourages NCAs to ensure that contemplated (new) SCA approaches allow for dynamic linking. In this context, the EBA clarifies that dynamic linking is not required for credit transfers performed at ATMs, given that those transactions are not remote.

Another requirement under Article 4(30) of PSD II (Sec. 1(24) ZAG) and the RTS is that the elements used for SCA be independent. According to the EBA, this condition will, for instance, be fulfilled in the case of use of a card reader, which requires first the insertion of a PIN to access the device and the subsequent generation of an OTP following the reading of the chip in the card. It will also be the case for a digital signature generated by a key, where access to that key requires the prior use of a knowledge element. In any case, a PSP must take measures to ensure that the two elements used for SCA be independent, such that, in terms of technology, algorithms and parameters, the breach of one element does not jeopardise the reliability of the other(s).

[4] EBA-Op-2018-04.

Existing SCA approaches within e-commerce

The EBA acknowledges that, within the e-commerce field, a number of existing approaches are already compliant (such as OTP-based approaches with a PIN or fingerprint scanning and a card reader with input of a knowledge element) while others are not (for instance, when two elements of the same SCA categories are used). In that respect, the Opinion urges NCAs to, in particular, require information from acquirers of payment transactions on the approaches that they are implementing with all their merchants to support the application of SCA.

II- Smooth transitioning process to SCA

The Opinion also addresses the concerns raised about market preparedness.

The EBA confirms that it is legally not able to postpone an application date that is set out in EU law. The Opinion further explains that sufficient time has been available for the industry to prepare for the application date of SCA, given that the definition of SCA had been set out in PSD II when it was published in 2015, which gave clear indications that existing authentication approaches would need to be phased out, and because PSD II had already granted an additional 18-month period for the industry to implement SCA.

However, the Opinion acknowledges the complexity of the payments markets across the EU and the challenges arising from the new SCA requirements, which may lead to some actors in the payments chain not being ready by 14 September 2019.

The EBA therefore accepts that, on an exceptional basis and in order to avoid unintended negative consequences for some PSUs after 14 September 2019, NCAs may decide to work with PSPs and relevant stakeholders, including consumers and merchants, to provide limited additional time for compliance. NCAs may therefore work with:

(a) issuers of payment instruments to ensure that they have in place or migrate to authentication approaches that are compliant with SCA; and/or

(b) acquirers of payment transactions to ensure that they offer solutions to their merchants that can support SCA.

However, additional time may only be granted if the relevant PSPs: (i) have set up an appropriate migration plan which has been approved by their NCA and which is to be implemented in an expedited manner; and (ii) have adequate customer communication plans in place. NCAs will then have to monitor the effective implementation of the migration plan in due course.

While other NCAs already have published statements confirming that they will grant firms additional time to comply with SCA requirements,[5] the German Federal Financial Supervisory Authority (*Bundesanstalt für Finanzdienstleistungsaufsicht* – **BaFin**) has not yet respondet to the Opinion. For market participants in Germany, it therefore remains to be seen how BaFin will position itself in this respect.

[5] For example, on 28 June 2019 the UK Financial Conduct Authority published a statement expressing its intention to agree and finalise a plan with stakeholders, including a timetable for achieving compliance, and stating that it "*will not take enforcement action against firms if they do not meet the relevant requirements for SCA from 14 September 2019 in areas covered by the agreed migration plan, where there is evidence that they have taken the necessary steps to comply with the plan*".

Your Allen & Overy contacts

Dr Alexander Behrens
Partner - Frankfurt

Contact
Tel +49 69 2648 5730
alexander.behrens@allenovery.com

Kai Schadtle
Associate - Frankfurt

Contact
Tel +49 69 2648 5768
kai.schadtle@allenovery.com

If you would like to discuss the issues raised in this paper in more detail, please contact any of the experts above or your usual Allen & Overy contact.