Was Sie schon immer über „SCA Strong Customer Authentication“ wissen wollten,

… aber sich nie trauten zu fragen

Markus Drespling

Consulting analyst

SHC Stolle & Heinz Consultants GmbH & Co. KG

4.08.2017

Im Folgenden soll ein bisschen Licht ins Dunkel gebracht werden, was es mit den Begriffen SCA, 2FA, RTS und weiteren auf sich hat. Zudem ist dieser Artikel der Frage gewidmet, in welchem Umfang und ab wann die starke Kundenauthentifizierung qua PSD II uns alle betrifft.

Was ist SCA und warum wird es eigentlich eingeführt?

Die Abkürzung SCA steht für „Strong Customer Authentication“ also die starke Kundenauthentifizierung. Ziel ist es, dass elektronische Zahlungen auf sichere Weise durchgeführt werden. Um dies gewährleisten zu können, ist die sichere Authentifizierung des Benutzers zu gewährleisten und somit das Betrugsrisiko soweit wie möglich zu reduzieren.

Das Authentifizierungsverfahren soll dabei Versuche ermitteln, die personenbezogenen Anmeldeinformationen eines Kunden zu verwenden, die verlorengegangen, gestohlen oder missbraucht wurden und somit sicherstellen, dass es sich bei dem Nutzer auch wirklich um den berechtigten Benutzer handelt, der gerade seine Zustimmung für die Übertragung von Geldern oder den Zugriff auf seine Kontoinformationen erteilt.

SCA ist erforderlich, wenn der Nutzer online auf sein Zahlungskonto zugreift bzw. eine elektronische Zahlung auslöst.

Kurz gesagt, die PSD II (zweite europäische Zahlungsdienstrichtlinie) hat unter anderem das wesentliche Ziel, die Sicherheit von elektronische Zahlungen zu erhöhen. Deshalb ist vorgesehen, dass die EBA (europäische Bankenaufsicht) in Kooperation mit der EZB technische Regulierungsstandards (RTS) zur starken Kundenauthentifizierung und sicheren Kommunikation ausarbeitet, die die Ziele und Anforderungen der PSD II unter technischen Gesichtspunkten ausgestaltet.

In diesen RTS wird ausgeführt, welche Voraussetzungen eine starke Kundenauthentifizierung zu erfüllen hat. Hier kommt nun die Zwei-Faktor-Authentifizierung (2FA) ins Spiel. Dabei müssen zwei von drei Faktoren richtig vorliegen um den Kunden zu authentifizieren.

Diese drei Faktoren können etwas sein,

- **das der Nutzer besitzt - bspw. die girocard oder das Smartphone,**
- **das der Nutzer weiß - z.B. ein Passwort bzw. eine PIN,**
- **das der Nutzer ist (sog. Inhärenz) - also ein biometrischer Nachweis wie bspw. der Scan des Fingerabdrucks oder der Iris.**

Ist das neu oder gibt’s schon so etwas?

Klar gibt es das schon. Jeder der mit Karte bezahlt macht das heute bereits – von der 3D Secure-Abfrage bei einer Onlinezahlung per Kreditkarte über die Zahlung per girocard an der Supermarktkasse. Auch die Anmeldung zum Online-Banking mit PIN und TAN ist eine Zwei-Faktor-Authentifizierung.

Nun wird sich der eine oder andere Fragen, sind das nicht zwei Passwörter und somit Wissenselemente? Die PIN ist ein klassisches Passwort und deckt den Faktor Wissen ab. Die SMS-/PushTAN ist zwar ein Einmalpasswort, jedoch ist der entscheidende Faktor das mobile Endgerät, über welches der Nutzer die TAN erhält, unabhängig davon ob der Code mithilfe eines kryptografischen Schlüssels auf dem Gerät selbst erzeugt oder per SMS an das Smartphone geschickt wird. Es handelt sich also um den Faktor Besitz.

Warum wird dann ein solches Aufhebens darum gemacht, wenn es das schon gibt?

Dies hat mehrere Gründe. Zunächst einmal wird die starke Authentifizierung grundsätzlich für alle elektronischen Zahlungen verpflichtend sein, abgesehen von einigen Ausnahmen (dazu später mehr). Insbesondere im eCommerce haben sich viele Händler zusammen mit ihren Zahlungsdienstleistern, immer mehr in Richtung eines risikobasierten Ansatzes begeben. Oberstes Ziel ist das reibungsfreie Einkaufserlebnis des Kunden um eine möglichst hohe Conversion-Rate zu erzielen. Plakativ könnte man sagen:

„Frei nach der Devise - ein bisschen Schwund ist immer.“ Ganz so einfach ist es natürlich nicht, aber aus Händlersicht ist es wenig attraktiv die Fraud-Rate im eigenen Shop auf Kosten der Conversion nahe der 0% zu treiben. Also wird der Sweetspot angepeilt, an dem die Betrugsfälle gering sind und gleichzeitig die Abbruchquote im Checkout-Prozess ebenfalls möglichst niedrig ist. Aufdringliche Sicherheitsabfragen, die das Shoppingerlebnis des Kunden trüben, kommen nur dann zum Tragen, wenn es die Risikobewertung vorsieht.

Ergo: Eine verpflichtende starke Authentifizierung verträgt sich nicht besonders mit One-Click-Shopping.

Ein weiterer entscheidender Punkt, ist die Tatsache, dass die verpflichtenden Anforderung zur SCA die Zahlungsdienstleister und Banken betreffen. Die Händler haben keinerlei Entscheidungsspielraum und ein Verzicht auf SCA und 2FA unter der Prämisse einer Haftungsumkehr ist nicht vorgesehen.

Weshalb sieht die EU nun Handlungsbedarf?

In der Begründung zur PSD II wird ausgeführt, dass sich die Sicherheitsrisiken für elektronische Zahlungen in den letzten Jahren erhöht haben. Zuverlässige und sichere Zahlungsdienste sind eine entscheidende Voraussetzung für einen gut funktionierenden Zahlungsverkehrsmarkt und die Nutzer sollen vor den Risiken angemessen geschützt werden. Mit den „neugeschaffenen“ Rollen PISP und AISP, verwenden auch Dritte die Sicherheitsmerkmale des Kunden zur Authentifizierung.

(1) Account Information Service Provider (AISP): Kontoinformationsdienste aggregieren die Daten von verschiedenen Banken und stellen diese dem Nutzer bereit.

(2) Payment Initiation Service Provider (PISP): Zahlungsauslösedienste initiieren auf Antrag des Nutzers Zahlungen direkt von dessen Konto beim kontoführenden Institut.

Hier sah man wohl ein besonderes Schutzbedürfnis und im Zuge der Gleichberechtigung und Neutralität ist deshalb die starke Kundenauthentifizierung für alle Banken und Zahlungsdienstleister verpflichtend.

Gibt es Ausnahmen und wenn ja welche?

Wie bereits erwähnt, ja die gibt es. Die EBA hat im aktuellen Stand der RTS eine Reihe von Ausnahmen vorgesehen. Allerding enthalten die Ausnahmen mal mehr, mal weniger „Wenns“ und „Abers“.

- **Zugriff des Nutzers auf seine Kontoinformation**
    - Eine Anwendung der SCA ist nicht zwingend vorgeschrieben, wenn die Einsicht des Nutzes auf den Saldo und/oder die Zahlungstransaktionen der letzten 90 Tage eines oder mehrerer seiner Zahlungskonten beschränkt ist und keine sensiblen Zahlungsdaten offengelegt werden.
    - Dies gilt jedoch nur, sofern der Nutzer diese Informationen nicht erstmalig abruft bzw. die letzte SCA nicht mehr als 90 Tage zurückliegt.
- **Zahlung kontaktlos am POS**

  Eine kontaktlose Zahlung am POS muss nicht stark authentifiziert werden, wenn
    - der Betrag dieser Zahlung EUR 50 nicht überschreitet
    - und alle Transaktionen seit der letzten Anwendung der SCA kumuliert EUR 150 nicht überschreiten
    - bzw. nicht mehr als fünf Zahlungen ohne Anwendung der SCA getätigt wurden.
- **Zahlung von Parkgebühren oder für die Personenbeförderung**

  Hierbei handelt es sich um eine Befreiung von der starken Authentifizierung für Fälle, in denen der Nutzer eine elektronische Zahlung zum Zwecke der Personenbeförderung oder der Bezahlung von Parkgebühren **an einem unbeaufsichtigten Automaten** ausführt.

- **Vertrauenswürdig Zahlungsempfänger**

  Der Nutzer kann bspw. in seinem Online-Banking-Portal eine Art Whitelist mit vertrauenswürdigen Empfängern anlegen oder seine Bank bzw. sein Zahlungsdienstleister schlägt ihm eine Liste mit Empfängern vor.

  - In beiden Fällen müssen dann zukünftig die Zahlungen an diese Empfänger nicht stark authentifiziert werden.
  - Allerding muss die selbst angelegte Liste oder der Vorschlag des Dienstleisters einmalig unter Verwendung der SCA aktiv legitimiert werden.

- **Anlegen eines Dauerauftrags**

  Der klassische Dauerauftrag erfordert beim Anlegen eine starke Authentifizierung, die einzelnen, sich wiederholenden Zahlung selbstverständlich nicht.

- **Zahlung an eigenes Konto**

  Eine Überweisung bei der der Zahlender und Empfänger die gleiche natürliche bzw. juristische Person sind und beide Konten beim selben Institut geführt werden, sind ebenfalls von der Pflicht zur SCA befreit.

- **Kleinstbeträge**

  Elektronische Fernzahlungen sind vom Erfordernis der SCA ausgenommen, wenn

  - der Betrag EUR 30 nicht überschreitet
  - und sofern alle Transaktionen seit der letzten Anwendung der SCA kumuliert EUR 100 nicht überschreiten
  - bzw. nicht mehr als fünf Zahlungen ohne Anwendung der SCA getätigt werden.

- **Befreiung auf Basis der Transaktionsrisikoanalyse (TRA)**

  Hier wird es nun etwas komplexer. Nach der Konsultationsphase mit ca. 220 Stellungnahmen hat die EBA in ihren finalen Entwurf auch noch diese vielfach geforderte Ausnahme aufgenommen. Hierbei hat sie Schwellen bis zu EUR 500 auf Basis festgelegter Betrugsraten aufgestellt. Wenn ein Zahlungsdienstleister eine dieser Referneznraten unterschreitet kann er von der Ausnahme bis zur Höhe des jeweiligen Schwellenbetrags Gebrauch machen. Dabei wird zwischen Card-Not-Present-Transaktionen und SEPA Credit Transfer unterschieden.

	Referenzbetrugsrate in %:	
Befreiungs-schwelle	Card-Not-Present-Transaktionen[1]	SEPA Credit Transfer[2]
EUR 500	0,01	0,005
EUR 250	0,06	0,01
EUR 100	0,13	0,015

Die Berechnung und das Monitoring der Betrugsraten ist jedoch an einige Voraussetzungen geknüpft und muss fortlaufend erfolgen sowie gemeldet werden.

Neue Ausnahme für Corporate Payments

Die EU-Kommission hat darüber hinaus noch eine Ausnahme für Corporate Payments gefordert, wenn diese dedizierte Zahlungsprozesse bzw. -protokolle nutzen. Eine Legaldefinition des Begriffs „Corporate“ fehlt jedoch. Dies hat die EBA in ihrer Stellungnahme moniert und deshalb einen Gegenvorschlag unterbreitet.

Hierbei handelt es sich um einen neue B2B-Ausnahme im Rahmen der Transaktionsrisikoanalyse. Für Fernzahlungsvorgänge, bei denen dedizierte Zahlungsprozesse und -protokolle verwendet werden, die nur im B2B-Bereich Einsatz finden und für welche die Referenzbetrugsrate von 0,005% unterschritten wird, kann die Befreiung auf Basis der Transaktionsrisikoanalyse in Anspruch genommen werden und zwar ohne begrenzenden Schwellenbetrag.

Lastschrift nicht betroffen

Richtig gelesen, die Lastschrift ist vom SCA-Erfordernis nicht betroffen. Aus Sicht der EBA ist die Lastschrift Out-Of-Scope, da sie durch den Zahlungsempfänger initiiert wird. Nur die Erteilung eines E-Mandats, welches jedoch in Deutschland nicht verbreitet ist, fiele unter das SCA-Erfordernis.

Ein abschließender wichtiger Punkt bzgl. der Ausnahmen: Der Zahlungsdienstleister des Zahlenden hat immer das letzte Wort, ob SCA zur Anwendung kommt, wenn grundsätzlich eine Ausnahme anwendbar ist. Sollte nun bspw. der Acquirer eines Händlers Gebrauch von der Befreiung auf Basis der Transaktionsrisikoanalyse machen wollen, könnte der Issuer sich darüber hinwegsetzten und für die Zahlung seines Kunden, also des Karteninhabers, die starke Authentifizierung erzwingen. Dies stellt einen

[1] Kartenzahlung im Fernabsatzgeschäft
[2] SEPA Überweisung

Widerspruch zum aktuellen, oben bereits skizzierten Ansatz dar, bei dem die Händler entscheiden, ob sie die Haftungsumkehr in Kauf nehmen wollen, um für ihre Kunden ein reibungsloses Einkaufserlebnis zu schaffen.

Und wie sieht der Zeitplan und die Übergangsfrist dazu aus?

Der 13. Januar 2018 nähert sich zügig, dann müssen die nationalen Umsetzungsgesetze zur PSD II spätestens in Kraft treten. Wann allerdings die technischen Regulierungsstandards zur starken Kundenauthentifizierung von der EU-Kommission verabschiedet und folglich 18 Monate später in Kraft treten, ist noch ungewiss. Aktuell wäre dies frühestens im Februar 2019 der Fall. Die Übergangsfrist läuft also vom 13. Januar 2018 bis zum Inkrafttreten der RTS.

Ob SCA vor oder während der Übergangszeit verwendet wird, ist den Banken und Zahlungsdienstleistern freigestellt. Nach Ablauf der Übergansfrist ist SCA verpflichtend, es sei denn eine Ausnahme ist anwendbar.

Sicher ist, die verpflichtende starke Kundenauthentifizierung für elektronische Zahlungen kommt. Sicher ist auch, dass sich vielerorts der Kopf zerbrochen wird, wie man den viel beschworenen Conversion-Killer möglichst weitreichend umschifft. Ganz werden wir jedoch nicht darum herumkommen. Entscheidend wird daher die Transparenz und Nutzerfreundlichkeit der Sicherheitsmechanismen sein. Darüber hinaus muss den Kunden klar vermittelt werden, warum in einem Fall die Zwei-Faktor-Authentifizierung erforderlich ist und ein andermal eine Ausnahme greift.