nexmo® | The Vonage® API Platform

Strong Customer Authentication (SCA):

A Set Scene with a Twist

The Author

Alison Donnelly

Alison is a payments policy expert with in-depth knowledge and understanding of the payments and regulatory landscape. A former FSA/FCA e-money policy specialist, Alison is now Leader of the Emerging Payment Association's Project Regulator and the Association of Professional Compliance Consultants' PSD2 Working Group as well as the EWPN's Ambassador for Ireland. With a career background in policy development and influencing, Alison applies her experience and skills to work with clients to strategic stakeholders, Alison holds the ICA Diploma in Anti-Money Laundering.

14 September 2019 has come and gone. For payment service providers (PSPs), the run up to the date became like the countdown to Y2K; there was confusion over what changes were necessary and concern about what would happen. Questions arose from all corners as rules written to enforce strict authentication standards on online payments for business models that had never been available in a live market before were about to be enforced. But unlike Y2K, the ticking clock wasn't inevitable and at the last minute, regulators gave some leeway, or at least, some of them did. Maybe I am getting ahead of myself; let's set the scene first.

The Scene

- **25 November 2015** – The European Commission (EC) publishes the final version of the second payment services directive (PSD2), one of the goals of which was to create a more secure market of electronic payments. Within PSD2, one of the many obligations put on the European Banking Authority (EBA) was to develop regulatory technical standards for customer authentication and common and secure communication.
- **23 February 2017** – The EBA publishes its final version of their 'regulatory technical standard for strong customer authentication (SCA) and common and secure open standards of communication'… we will refer to it as the "RTS" for everyone's sanity.
- **27 November 2017** – The EC agreed to an adaption of the EBA's RTS but only published it in March 2018. Following an 18 month implementation period (bringing us to 14 September 2019), PSPs will have to perform strong customer authentication (SCA) on all instances that a payer accesses their payment account online, initiates an electronic payment transaction, or carries out any action through a remote channel that may imply a risk of payment fraud or other abuse; the RTS defines how SCA works and how any of this should actually happen.
- **21 June 2019** – The EBA acknowledges the difficulty of implementing SCA within the e-commerce environment, for card-not-present transactions, and allows competent authorities to 'provide limited additional time' for the enforcement of SCA for card-not-present transaction.

Each competent authority in the EEA must decide the extent of the limited period of additional time that it will give the PSPs in e-commerce. The UK's FCA, for example, has given 18 months. Those are the key dates. Now it is time to get into the details of SCA. Simply speaking it is two-factor authentication ("2FA"), with a twist.

SCA

PSPs are required by PSD2 to perform SCA on all instances that a customer accesses their online portal or instructs a payment, unless an exemption applies.

In the interest of clarity, there are nine exemptions PSPs can utilise:

1. Payment account information
2. Contactless payments
3. Unattended terminals for transport fares and parking fees
4. Trusted beneficiaries
5. Recurring transactions
6. Credit transfers between accounts held by the same natural or legal person
7. Low-value transactions
8. Secure corporate payment processes and protocols
9. Transaction risk analysis

Each exemption has its subtleties, however the prevailing point becomes that the majority of PSPs will have to apply SCA at some point in the customer journey, so 'how do you perform SCA?'

2FA

Unlikely to be a novel concept for most, two-factor authentication (2FA) has been the standard for customer authentication for quite a while. The majority of us use it every day, whether you realise it or not. Customers must prove two out of three possible elements to perform an action, the three elements being:

- **Knowledge:** Something you know
- **Possession:** Something you have
- **Inherence:** Something you are

When withdrawing cash from an ATM a customer is performing a form of 2FA, they are presenting their card (possession) and entering in their unique PIN (knowledge). Another example is logging into an online portal, often you will be asked for a password (knowledge) and then a one-time-password ("OTP") will be sent via SMS to your phone (possession). Interestingly, an OTP sent to your phone is proving possession of your SIM-card, not your phone. For completeness the most common form of inherence is biometrics, so using your fingerprint to open your phone for example.

The Twist

This is where life becomes more difficult for PSPs that are seeking compliance. The legislation states that 2FA must create an authentication code, and this authentication code must be dynamically linked to the payment instructions details. This sets out two obligations that the PSP is keeping an audit log and that they have set up suitable protection against man-in-the-middle attacks.

Thankfully, the technological neutrality of the legislation means that there is some wiggle room around these requirements. A PSP can use the OTP both for authentication, as the possession element, and use it as the dynamically linked authentication code. However, in order for a PSP to take this position they must be able to ensure all the security that the dynamically linked authentication code brings is present in their solution.

What protections must PSPs ensure is present in their SCA solution?

- The authentication code must be unique and unforgeable.
- If authentication fails, then after no more than five attempts the access should be blocked.
- The confidentiality and integrity of the communication session is protected.
- If a session has no activity for a time not exceeding five minutes, then the session should be closed.
- The payer is aware of the payment transaction amount and the payee.
- The authentication code is generated specific to those payment details.
- The authentication code that is accepted corresponds to the original details; if the payment details change then the code is refused.
- The information is protected during all stages of the payment and communication.

How We Can Help

My experience within the payments sector has shown that PSPs are having trouble with their SCA obligations, especially developing a compliant dynamically linked authentication code. PSPs have struggled with the technical complexities of dynamically linking an authentication code to the payment instruction; it simply isn't as common in the market as standard 2FA, therefore PSPs can struggle with developing a system capable of dynamic linking.

Nexmo, the Vonage API Platform, is offering a solution that provides a possession element (OTP via SMS) that can additionally act as a dynamically linked authentication code. Nexmo use SMS delivery due to a variety of factors.

1. **Availability** – SMS is perhaps the most widely available communication method when compared to other delivery methods for 2FA. Not every phone has the capability to read a fingerprint or facially ID someone, or even the ability to download an authenticator app. Every phone does, however, have the capability to receive a text message.
2. **Compliance** – Although SMS has taken some recent criticism due to security concerns, due to the vulnerabilities identified in the SS7 protocol, it has been accepted by the EBA as a compliant delivery system for a possession factor. Therefore, the EBA has determined that SMS is secure enough for SCA compliance.

Online payments are a consistent balancing act between security and accessibility. If you apply a security process that few of your legitimate users can actually operate then payments don't work. If you apply a payment process that has no security, then you have not protected your customer and fraud will be rife. Nexmo aims to strike the balance of security and accessibility.

Set out below is what Nexmo can deliver and what they can help you deliver to your customers.

Requirements	Nexmo Can Deliver	Nexmo Can Help You Deliver
The authentication code must be unique and unforgettable.	✓	
If authentication fails, then after no more than five attempts the access should be blocked.		✓
The confidentiality and integrity of the communication session is protected.		✓
If a session has no activity for a time not exceeding five minutes, then the session should be closed		✓
The payer is aware of the payment transaction amount and the payee.	✓	
The authentication code is generated specific to those payment details.	✓	
The authentication code that is accepted, corresponds to the original details, if the payment details change then the code is refused	✓	
The information is protected during all stages of the payment and communication		✓

"Nexmo's history is deeply rooted in European tradition. We are constantly evaluating the regulatory trends and work to anticipate customer problems and to build compelling APIs and software to help solve those new customer challenges," said Roland Selmer, VP of Product at Nexmo, The Vonage API Platform. "We want to demonstrate to our customers that we're a trusted partner and they're not alone in navigating the world of compliance in Europe whether it's related to data privacy, payments, and more."

For more information contact us, here at Nexmo.