Single Rulebook Q&A

Question ID	2019_4984
Status	Final Q&A
Legal act	Directive 2015/2366/EU (PSD2)
Topic	Strong customer authentication and common and secure communication (incl. access)
Article	Article 98
Paragraph	1
Subparagraph	(c)
COM Delegated or Implementing Acts/RTS/ITS/GLs/Recommendations	Regulation (EU) 2018/389 - RTS on strong customer authentication and secure communication
Article/Paragraph	7/1
Date of submission	05/11/2019
Published as Final Q&A	25/09/2020
Disclose name of institution / entity	Yes
Name of institution / submitter	Sebastian Nielsen
Country of incorporation / residence	Sweden
Type of submitter	Individual
Subject matter	"Push based" authentication and SCA requirements
Question	Does "push based" authentication fall in the Strong customer authentication (SCA) requirements, based on the security risks "push authentication" poses?
Background on the question	Currently, when using a mobile app or other internet-connected device as means of "possession" when it comes to strong authentication, many entities use an approach, where the customer enters an username or identifier on the device where the customer is authenticating on (for example computer), and as a next step, receives a "notification" or "push request" on the possessed authenticating device (mobile phone or internet-connected security token), whose the customer then accepts or approves the transaction using a PIN or a fingerprint. The main problem with such "push authentication", is that there is no binding between the session by the user and the authenticating device, making it possible to

authenticate as another user using push authentication. Its fully possible for someone in for example Japan, to enter the customer's identity details in a banking webpage, and then the user in Member State A could mistakenly or wrongfully accept this, causing the person in Japan to be logged in, even if the authentication device does not have any physical vicinity to the user in Japan performing the login. There have come a rise of fraud in Member State A using a electronic mobile app called "BankID", which is based on "push authentication". The fraud works like this: The fraudster calls the customer, impersionates the bank, and tells the customer "There are suspicious charges on the account". The customer panics, and goes to his computer and tries to login. He enters his identity details in the banking webpage. BUT - the fraudster has already entered the customer's identity details into his computer. When the fraudster times the click on the "Next" or "Login" button correctly, the customer receives a push request in the phone. The customer believes this push request is for logging himself into the banking webpage, but since the fraudster timed the click correctly, the push request is actually for logging the fraudster into the banking page. Customer approves login/transaction believing it is his transaction, but instead approves the fraudster into his bank account. There are already solutions that prevent this type of fraud. One of the best solution requires the customer to use his mobile phone or authentication device, to scan a QR code, that binds the computer session to the actual login request. In other cases, the data that causes the binding is automatically sent in the background to the authenticating app, for example if the login is made on the same device as the authenticating app is installed on. Another solution requires the customer to enter a "challenge" - a random PIN code displayed on the computer screen, into his posessed device. This ensures that there exist a binding between the computer and the posessed device. By requiring the customer to either: 1: Enter a "challenge code" from the computer or service he is performing the login/transaction on, into the authentication app, OR 2: Scan a QR code displayed on the computer or service he is performing the login/transaction on, into the authentication app, OR 3: Performing the login from the same device as he has the authentication app on, so the challenge data is sent in the "background" (via inter-app communication, NOT over any internet connection). The security is guranteed, because it links the session to the posessed device, in a way making it very difficult to subdue a customer in this way. Its very important that its the customer authenticating, that initiates the authentication, not that the device asks the user for authentication via a push request or notification, as many users also press "YES" or "ACCEPT" without reading whats it about. Solutions that show a random PIN code on the screen on both computer and device, and ask the users to compare the codes before approving authentication, isn't secure either, because most users don't compare and verify the codes. Its very important that if a challenge or verification code is used, the user must manually ENTER the challenge/verification code in

	the posessed device, to make sure the user performs the verifying step. The QR code function is already implemented by "BankID", and the technology exist, but not all services and banks have implemented it. I think it is important to make it clear that any external triggering of posessed authenticating devices should be considered insecure, so all entities are forced to switch to QR scanning or similiar.
EBA answer	Article 7(1) of the Commission Delegated Regulation (EU) 2018/389 provides that "payment service providers shall adopt measures to mitigate the risk that the elements of strong customer authentication (SCA) categorised as possession are used by unauthorised parties". Table 2 of the EBA Opinion on the elements of SCA under PSD2 (EBA-Op-2019-06) provided a non-exhaustive list of possible possession elements, which includes "possession of a device evidenced by an OTP generated by, or received on, a device". Paragraph 25 of this Opinion further clarified that a "device could be used as evidence of possession, provided that there is a 'reliable means to confirm possession through the generation or receipt of a dynamic validation element on the device'. Evidence could, in this context, be provided through the generation of a one-time password (OTP), whether generated by a piece of software or by hardware, such as a token, text message (SMS) or push notification." It follows from the above that a "push-based" notification can be used as a means of evidencing possession, provided that the requirements of Article 7 of the Delegated Regulation are met. It is for each payment service provider to prove these requirements are met.
Link	https://eba.europa.eu/single-rule-book-qa/qna/view/publicId/2019_4984