

## Single Rulebook Q&A

<b>Question ID</b>	2018_4315
<b>Status</b>	Final Q&A
<b>Legal act</b>	Directive 2015/2366/EU (PSD2)
<b>Topic</b>	Strong customer authentication and common and secure communication (incl. access)
<b>Article</b>	97
<b>Paragraph Subparagraph</b>	-
<b>COM Delegated or Implementing Acts/RTS/ITS/GLs/Recom mendations</b>	Regulation (EU) 2018/389 - RTS on strong customer authentication and secure communication
<b>Article/Paragraph</b>	4 / 1
<b>Date of submission</b>	08/10/2018
<b>Published as Final Q&amp;A</b>	15/01/2021
<b>Disclose name of institution / entity</b>	No
<b>Type of submitter</b>	Credit institution
<b>Subject matter</b>	Strong Authentication
<b>Question</b>	Is one time passcode (OTP) Mail considered as a "Strong Customer Authentication" under Regulation (EU) 2018/389 – RTS on strong customer authentication and secure communication?
<b>Background on the question</b>	Authentication by OTP mail reunites 2 authentication factors :1. The one-time password received by mail, enrolled by the payer's bank2. The password to access mails, only known by the payer.OTP mail is convenient for expatriates that can not have access to the SMS. It aims at replacing authentication by birthday date which is not a valid authentication method regarding the RTS.
<b>EBA answer</b>	<p>Article 4 (30) of Directive 2015/2366/EU (PSD2) defines possession as 'something only the user possesses'.</p> <p>Paragraph 26 of the <a href="#">EBA Opinion on the elements of strong customer authentication under PSD2 (EBA-Op-2019-06)</a>, clarified that approaches relying on mobile apps, web browsers or the exchange of (public and private) keys may also be evidence of possession, provided that they include a device-binding process that ensures a unique connection between the payment service user's app, browser or key and the device.</p> <p>This means that apps or web browsers (i) where the email with the OTP is</p>

	<p>received by the payment service users and (ii) which have a unique connection with the device, could evidence possession and thus be considered as a valid factor in a two-factor strong customer authentication under PSD2 and the <a href="#">Commission Delegated Regulation (EU) 2018/389</a>. This would, however, require the email address where the OTP is sent to, to be accessible only via a registered device.</p> <p>Finally, it is for the payment service provider to ensure the unique connection between the device and the payment service user's app or browser.</p>
<b>Link</b>	<a href="https://www.eba.europa.eu/single-rule-book-qa/-/qna/view/publicid/2018_4315">https://www.eba.europa.eu/single-rule-book-qa/-/qna/view/publicid/2018_4315</a>

European Banking Authority, 25/02/2021  
[www.eba.europa.eu](http://www.eba.europa.eu)