DEFINING NEW CUSTOMER JOURNEYS

The Second Payment Services Directive: Scoping out the impacts of the Regulatory Technical Standards
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTRODUCTION: A CRITICAL MOMENT FOR PSD2</td>
<td>3</td>
</tr>
<tr>
<td>KEY ASPECTS OF THE FINAL DRAFT RTS</td>
<td>4</td>
</tr>
<tr>
<td>IMPACTS OF PSD2 AND THE RTS ON USE CASES AND BUSINESS MODELS</td>
<td>6</td>
</tr>
<tr>
<td>STANDARDIZATION</td>
<td>8</td>
</tr>
<tr>
<td>CALL TO ACTION: TIME TO BLEND A FRICITIONLESS CUSTOMER EXPERIENCE WITH STRONG SECURITY</td>
<td>9</td>
</tr>
</tbody>
</table>
INTRODUCTION: A CRITICAL MOMENT FOR PSD2

The revised Payment Services Directive (PSD2) aims to drive increased competition, innovation and transparency in Europe’s payments market, while also enhancing security. It will also regulate new types of payment institutions, introduce new interaction models, and require banks to open up their systems to third parties through application programming interfaces (APIs).

A TIMELAG BETWEEN COMPLIANCE WITH PSD2 AND THE RTS

In June 2017, the EBA rejected the EC’s amendments, and it is now for the EC to make a final decision on the RTS text, 18 months after which the RTS will become law. The EC can either ignore the EBA and proceed with its amendments, or take into account the EBA’s suggestions which accompanied its rejection. The EU Council and EU Parliament have the right of scrutiny on the final draft, so with PSD2 set for introduction in January 2018, the already significant gap between the point where banks have to be PSD2 compliant, and the deadline for complying with the RTS is likely to extend well into 2019.

THE EUROPEAN COMMISSION’S CHANGES

In February 2017, the European Banking Authority (EBA) published its final draft Regulatory Technical Standards (RTS) on strong customer authentication (SCA) and common and secure communication under PSD2. On 1 June 2017, the European Commission (EC) asked for changes to the EBA’s RTS, including:

- The permitting of contingency measures, including screen-scraping in cases where the dedicated communication interface is unavailable for more than 30 seconds or has performance issues.
- An exemption for SCA for secure corporate payments systems.
- Independent auditing of the security measures where Transactions Risk Analysis exemption is applied.
- Fraud reporting by payment service providers directly to EBA.
### Timeline for PSD2 and the RTS for SCA and Secure Communication

<table>
<thead>
<tr>
<th>Year</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015</td>
<td>December 8, 2015: EBA releases discussion paper on authentication and secure communication.</td>
</tr>
<tr>
<td>2016</td>
<td>August - October 12, 2016: Consultation phase for draft RTS—considering industry input—Accenture is one of the contributors.</td>
</tr>
<tr>
<td>2016</td>
<td>January 13, 2017, belatedly on February 23, 2017: Deadline for EBA to submit the RTS on authentication and communication to the EC.</td>
</tr>
<tr>
<td>2017</td>
<td>June 1, 2017: The EC publishes the amended version of EBA’s RTS. The RTS to be adopted by EBA within 6 weeks.</td>
</tr>
<tr>
<td>2017</td>
<td>August, 2017?: EC, EBA and European Parliament agree upon the final RTS.</td>
</tr>
<tr>
<td>2018</td>
<td>January 13, 2018: Deadline for member states to transpose PSD2 into law within all 28 EU member states. At this point, both payment service providers (PSPs) and banks need to be compliant.</td>
</tr>
<tr>
<td>2018</td>
<td>Q1 2019 (estimated): Deadline for EBA RTS implementation: member states should ensure payments institutions comply with the RTS.</td>
</tr>
<tr>
<td>2018</td>
<td>August – October 12, 2016: Consultation phase for draft RTS—considering industry input—Accenture is one of the contributors.</td>
</tr>
<tr>
<td>2018</td>
<td>January 13, 2017, belatedly on February 23, 2017: Deadline for EBA to submit the RTS on authentication and communication to the EC.</td>
</tr>
<tr>
<td>2018</td>
<td>Q1 2019 (estimated): Deadline for EBA RTS implementation: member states should ensure payments institutions comply with the RTS.</td>
</tr>
</tbody>
</table>
KEY ASPECTS OF THE FINAL DRAFT RTS

BANKS’ OBLIGATIONS AND SERVICES TO AISPS AND PISPS

The EBA’s final draft RTS clarified banks’ obligations and service provision to AISPs (Account Information Service Providers) and PISPs (Payment Initiation Service Providers). These clarifications included:

OPEN APIs FOR AISPs AND PISPs

Banks offering online payment accounts must offer at least one interface enabling secure communication with AISPs for account information, and with PISPs and PSPICBPIs (payments service providers issuing card based payments instruments) for payment initiation. We recommend that banks use open (external) APIs to implement this interface.

SCA

SCA processes will have to apply at least two of the three elements of knowledge, possession and inherence.

SCA CRITERIA

The final draft RTS say five criteria will be used to define SCA: dynamic linking; independence of channels; identity checking within the bank’s environment; undervivable authentication codes; and protection from unauthorized disclosure. However, the current RTS do not allow for today’s most user-convenient authentication methods, with only those using a separate device qualifying as SCA.

EXEMPTIONS ALLOWED FROM SCA

Transactions below €30 are exempt from SCA, and the RTS allow further SCA exemptions up to €500. These exemptions bring implications for some use cases and services. There are also specific exemptions in terms of payment initiation and account information services.
AN ASSESSMENT OF EXISTING AUTHENTICATION METHODS AGAINST THE RTS REQUIREMENTS

<table>
<thead>
<tr>
<th>AUTHENTICATION METHOD*</th>
<th>DYNAMIC LINKING</th>
<th>INDEPENDENCE OF CHANNELS</th>
<th>BANK ENVIRONMENT</th>
<th>UNDERIVABLE AUTHENTICATION CODES</th>
<th>NON-DISCLOSURE</th>
</tr>
</thead>
<tbody>
<tr>
<td>iTAN (list of printed indexed authentication codes)</td>
<td>X</td>
<td>✓</td>
<td>X</td>
<td>✓</td>
<td>X</td>
</tr>
<tr>
<td>smsTAN (authentication code is sent to a GSM mobile number)</td>
<td>✓</td>
<td>X</td>
<td>X</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>photoTAN (authentication code is sent as a graphic picture on a secure smartphone app)</td>
<td>✓</td>
<td>X</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>chipTAN (authentication code is generated on a separate security device with a smartcard and PIN)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>BestSign Touch ID® (authentication performed via Touch ID by Apple®)</td>
<td>✓</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>BestSign Dongle (authentication code is generated on a separate security device using Bluetooth® and PIN)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

*TAN stands for “transaction number” and is equivalent to “authentication code.”

EXEMPTION THRESHOLD VALUES (ETVs) FOR REMOTE CARD-BASED PAYMENTS AND CREDIT TRANSFERS

REFERENCE FRAUD RATE (%) FOR:

<table>
<thead>
<tr>
<th>ETV</th>
<th>REMOTE CARD-BASED PAYMENT</th>
<th>CREDIT TRANSFERS</th>
</tr>
</thead>
<tbody>
<tr>
<td>500€</td>
<td>0.01</td>
<td>0.005</td>
</tr>
<tr>
<td>250€</td>
<td>0.06</td>
<td>0.010</td>
</tr>
<tr>
<td>100€</td>
<td>0.13</td>
<td>0.015</td>
</tr>
</tbody>
</table>
IMPACTS OF PSD2 AND THE RTS ON USE CASES AND BUSINESS MODELS

IMPACTS ON CARD PAYMENTS
PSD2 and the RTS will have major impacts on the traditional card business—resulting in big changes in how customers use payment cards in almost all environments.

IMPACTS ON POS TRANSACTIONS
The requirement for SCA on card payments at a stationary point of sale (POS) means signatures will have to be phased out as an authentication method in Europe.

IMPACTS ON CARD-BASED MOBILE PAYMENTS
The SCA rules must also be implemented for mobile payments scenarios like host card emulation, Apple Pay® and Android Pay™.

UNATTENDED POS FOR PARKING FEES AND TRANSPORTATION TICKETS
Under PSD2 and the RTS, customers can use electronic payment instruments such as debit/credit cards to pay for transportation tickets and parking fees without SCA, boosting convenience for users.

IMPACTS ON E-COMMERCE TRANSACTIONS
Arguably the biggest impacts of the new PSD2 requirements will be on remote e-commerce transactions, with card issuers being obliged to perform an SCA check for every transaction above €30 that does not meet any exemption criteria.

IMPACTS ON RETAILERS INCLUDING ECOMMERCE GIANTS
Currently, e-commerce merchants can decide what balance to strike between strong security and a frictionless customer experience. With PSD2 and the RTS the PSPICIBPIs and account-holding payment service providers (APSPs) decide on the use and nature of SCA, not the retailer.

IMPACTS OF THE PARTIAL PERMISSION OF SCREEN-SCRAPING
PSD2 is technology-neutral, and banks can rely on screen-scraping to be compliant from January 2018. However, we believe this is not a long-term solution. While it may appeal to smaller banks with limited resources, for those banks that want to participate in the API economy, remain competitive and reap the benefits of Open Banking, open APIs are the way to go.

IMPACTS OF SCA ON E-BANKING
The low-value exemption from SCA will apply for e-banking transactions as well as SEPA credit transfers, meaning customers can initiate credit transfers on the e-banking platforms for transactions below €30 without SCA being required.

IMPLICATIONS OF THE TRANSACTION MONITORING REQUIREMENTS
PSD2 and the RTS require all APSPs—including banks—to monitor levels of fraud in online and mobile payments down to the individual transaction. This will require a far greater degree of monitoring than in the past.
One of PSD2’s greatest benefits is the opportunity for greater standardization and interoperability of payments processes and technologies. At a European level, progress is being made through bodies such as the Berlin Group. However, many initiatives are being driven at the national level—such as STET for France, the Open API Initiative in the UK and CAPS for the Netherlands—risking fragmentation of API standards in Europe.
CALL TO ACTION: TIME TO BLEND A FRICTIONLESS CUSTOMER EXPERIENCE WITH STRONG SECURITY

MAPPING OUT FIVE STRATEGIC STEPS

As your bank faces up to the timelag between the enactment of PSD2 on 13 January 2018 and the implementation of the EBA's RTS, you should not take the gap as a reason to hold back on your development of PSD2-compliant solutions. By moving now to create offerings that combine a frictionless customer experience with strong security, you'll position yourself to gain competitive edge while also meeting the goals of PSD2 and the RTS. Your strategy should involve taking five steps:

- Develop a good customer experience for SCA: what would that look like?
- Identify what solutions are available—such as behavioral biometrics—that can both help to improve the customer experience and also meet your service offering requirements.
- Define how you will use exemptions from SCA in your service offerings and customer experience.

Above all, banks require a strategic vision for Open Banking. With one, a strategy for PSD2 and the RTS will fall into place. Without one, banks will struggle.

- Identify the customer experience you want to offer, including for online/mobile banking.
- Clarify the services you want to offer online and at POS: for example, what choice will you offer merchants on SCA, and how will you price it if it is better than their own online banking solutions?
CONTACT US

JEREMY LIGHT
Managing Director, Accenture Payments Europe, Africa and Latin America
jeremy.light@accenture.com

ANDREW MCFARLANE
Financial Services, Accenture Ireland
andrew.g.mcfarlane@accenture.com

HAKAN EROGLU
Financial Services, Accenture Switzerland
hakan.eroglu@accenture.com

OLIVER HOMMEL
Financial Services, Accenture Germany
oliver.hommel@accenture.com

To request a copy of our detailed report on the impact of PSD2 RTS, please contact lakshmi.kv@accenture.com or jeremy.light@accenture.com.

STAY CONNECTED

Visit us at www.accenture.com/banking

Accenture Banking

@bankinginsights

bankingblog.accenture.com

ABOUT ACCENTURE

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world’s largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With more than 411,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at www.accenture.com.

ABOUT ACCENTURE PAYMENT SERVICES

Accenture Payment Services, a business service within Accenture’s Financial Services operating group, helps banks improve business strategy, technology and operational efficiency in three key areas: core payments, card payments and digital payments. Accenture Payment Services and its more than 4,800 professionals are dedicated to helping banks simplify and integrate their payments systems and operations to reduce costs and improve productivity, meet new regulatory requirements, enable new mobile and digital offerings, and maintain payments as a revenue generator. More than 50 clients worldwide have engaged Accenture Payment Services to help them turn their payment operations into high-performing businesses. To learn more, visit www.accenture.com/payments.

Views and opinions expressed in this document are based on Accenture’s knowledge and understanding of its area of business, markets and technology and are provided for information purposes only. This document does not contain legal advice or interpretation of any legal or regulatory requirements applicable to such areas (e.g. PSD2, the RTS or any other documents) and its full impact on such documents or their implementation has not been considered.

This document makes descriptive reference to trademarks that may be owned by others.

The use of such trademarks herein is not an assertion of ownership of such trademarks by Accenture and is not intended to represent or imply the existence of an association between Accenture and the lawful owners of such trademarks.