Building a better working world

Point of View

Implementing Strong Customer Authentication under PSD2

Background

The Revised Payment Services Directive (more commonly known as PSD2) comes into effect across Europe on January 13, 2018. PSD2 mandates a host of changes in the payments ecosystem (**summarised well here by Starling Bank**), but the game-changer is the concept of Access to Accounts (XS2A), which forces banks to allow regulated third party providers (TPPs) access to customer accounts, in order to initiate payments or to provide account information services.

The security measures governing such access are detailed in the Regulatory Technical Standards on Strong Customer Authentication and Common and Secure Communication (SCA RTS). This RTS has been hotly debated from the outset, with the EBA consultation paper published in August 2016 receiving a record 224 responses. The final draft of the RTS was published on the 23rd February 2017 and specifies:

- The requirements of Strong Customer Authentication (SCA)
- The exemptions from the application of SCA
- Requirements to protect the confidentiality and integrity of personalised security credentials
- The requirements for common and secure open standards of communication (CSC)

The key points of the final draft are **summarised well here by Finextra**.

The final draft RTS will be submitted to the Commission for adoption, following which they will be subject to scrutiny by the European Parliament and the Council before being published in the Official Journal of the European Union. The RTS will be applicable 18 months after its entry into force; while the final draft suggest an application date of 'November 2018 at the earliest', many in the industry believe a date in early 2019 is more likely.

Implementation roadmap

The implementation roadmap for the SCA RTS is not a straightforward one. Banks need to decide how they will manage (and audit) compliance across a variety of existing channels, including key customer touchpoints such as internet banking and mobile app propositions. If (as is likely) responsibility for compliance is devolved to the individual channel owners , banks will need a central design/ approval forum for security and authentication patterns, which may be governed under the CISO function. In an increasingly competitive environment, with customers less 'sticky' than ever (According to **EY's Global Consumer Banking Survey**, 42% of Irish consumers would not hesitate to change financial services provider if they found one with a better online/digital offer/experience), those who cannot find the right balance between security and simplicity will struggle.

We see implementation of the SCA RTS as a three step process:

1 Open API Channel Compliance

For many banks, PSD2 will be their first experience of exposing Open APIs. This exposure carries a fear factor, and ensuring that these APIs are fully secure will in general require new security capabilities. Given that the SCA RTS is the defined standard of security, we believe that banks will be aiming to have their API Channel compliant (for both SCA and CSC) in line with the XS2A deadline of January 2018.

The first instinct of many banks may be to make use of the various exemptions to SCA (low value payments, trusted beneficiaries etc.) to avoid applying strong authentication where possible. However, given the complexity associated with these exemptions (particularly transaction-risk analysis – discussed further below), banks may be better off investing up front in the development of a simple and delightful SCA experience rather than employing an avoidance strategy.

2 Full Channel Compliance

While the API Channel may be the first cab off the rank for SCA RTS compliance, other channels such as internet and mobile banking must follow quickly. Consistency of customer experience when performing strong authentication will be crucial, and will require central oversight. Again, up-front investment in a re-usable, customer-friendly SCA solution will be beneficial here.

3 Adoption of Transaction Risk Analysis (TRA)

In arguably the most significant change introduced in the final draft, Article 16 of the RTS allows an exemption from SCA where the transaction is identified as posing a 'low level of risk'. Reference fraud rates (which must be met in order to avail of the exemption) have been provided by the EBA, as well as a base set of conditions which must be met in order to deem a transaction low risk. While this exemption may allow banks to simplify the customer journey in some cases, there are a number of considerations to be addressed:

- Determination of, and the governance model for, risk analysis business rules
- The ability to accurately monitor fraud rates and adherence to reference rates
- Assessment and audit of the documented fraud rate, methodology, calculation and results
- Ability to 'turn off' transaction-risk analysis when required

Given the complexity involved in making use of this exemption, we feel that many banks will not be ready to make use of the TRA exemption at any stage in 2018; rather, the concept will be developed at a strategic level over the next 2-3 years.

Banks also need to carefully assess the benefits of this exemption. There are those who feel that TRA is of limited use and will confuse rather than clarify the customer journey; the fact that banks must be prepared to revert to full SCA if fraud rates are breached adds weight to the view that a frictionless SCA solution is required regardless of which exemptions are applied. A contrasting view here is that many customers are already familiar with TRA through using tools such Verified by Visa when making Card payments online. If TRA is going to be used, many banks will face a build/buy decision; outsourcing this capability to a trusted ecosystem partner may simplify the execution roadmap considerably.

What's next?

In the coming weeks and months, EY will publish a series of related articles covering:

- The technical standards for Common and Secure Communication under PSD2 – often overlooked, but a key part of the RTS.
- An assessment of some commonly used patterns for authentication today, considering their suitability for SCA as defined under PSD2.
- Our view on the emerging patterns that we see developing to meet the demand for strong authentication across the payments industry and beyond.
- An examination of the world of transaction-risk analysis, exploring some of the concept's major talking points.
- The overlap between cyber security and operational risk – how will the world of the CRO deal with the world of Open Banking?
- Leveraging investments in SCA, AML and KYC to create new 'digital identification' services.

Contact details

If you would like to discuss PSD2, the SCA RTS, or any of the topics discussed above, please contact:

Colin Ryan
Partner, Performance Improvement
EY Financial Services
T: +353 1 221 1505
E: colin.ryan@ie.ey.com

John Ward
Director, IT Architecture, Advisory
EY Financial Services
T: +353 1 2212 577
E: john.ward1@ie.ey.com

Conor McGoveran
Director, Cybersecurity
EY Financial Services
T: +353 1 221 1492
E: conor.mcgoveran@ie.ey.com

Eoin Dennehy
Manager, Performance Improvement
EY Financial Services
T: +353 1 221 1630
E: eoin.dennehy@ie.ey.com

EY | Assurance | Tax | Transactions | Advisory

About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organisation and may refer to one or more of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organisation, please visit ey.com.

31745.indd 06/17. Artwork by the BSC (Ireland)

ED None. Images sourced from Shutterstock.com

The Irish firm Ernst & Young is a member practice of Ernst & Young Global Limited. It is authorised by the Institute of Chartered Accountants in Ireland to carry on investment business in the Republic of Ireland.

Ernst & Young, Harcourt Centre, Harcourt Street, Dublin 2, Ireland.

ey.com