PSD2 Draft RTS: Ten Key Points

WHITEPAPER

COMPLEXITY SIMPLIFIED

The European Banking Authority (EBA) have published the long-awaited draft of the Regulatory Technical Standards (RTS) covering Secure Customer Authentication (SCA) and secure communication.

Apologies in advance for the Three Letter Acronyms (TLAs) which litter the PSD2 landscape! There's a lot to digest, but ten key points are highlighted here, along with some thoughts around the impact on the market.

1. Banks to define their own interfaces

It's up to banks – referred to in the legislation as Account Servicing Payment Service Providers (ASPSPs) – to define their own interfaces. Article 19.4 says "Account servicing payment service providers shall make sure that the technical specification of their communication interface is documented, the documentation made available for free and publicly on their website."

This drives a stake through the heart of the idea of a defined, interoperable standard for these interfaces. The EBA mention that they considered the arguments for a "governing entity" to define and police a standard, but decided that "the future RTS must not prescribe the use of a specific industry standard of internet communication".

To provide true interoperability, a detailed, centrally imposed standard would be needed. This would be inflexible and difficult to police. Although Account Information Service Providers (AISPs) and Payment Initiation Service Providers (PISPs) have managed to survive and thrive in the current "Wild West" of ad-hoc interfaces and screen-scraping, a set of principles will at least be a step forward, and much less onerous than a rigorous standard.

2. APIs, not screen scraping

The paper effectively mandates the use of "proper" APIs. It says that "each ASPSP shall offer at least one communication interface… which shall be documented and freely available on the ASPSP's website". This interface "shall use ISO 20022 elements, components or approved message definitions." This definition excludes the use of existing Internet Banking interfaces, which generally don't use ISO 20022 data elements and would be extremely difficult to document.

While it is possible to implement interfaces using "screen scraping" of Internet Banking websites, it is certainly not good practice. There are plenty of technologies specifically designed to support dedicated machine-to-machine APIs which can offer a more secure and robust interface, including the required controls on which entities can perform which operations and on which accounts.

3. Payment security up to the banks

The paper clarifies that it's up to the banks to define the security procedures to be applied when a third party initiates a payment. The EBA say that normally "the authentication procedure will remain fully in the sphere of competence of the ASPSP" and that the Payment Initiation Service (PIS) would only authenticate the customer (Payment Service User or PSU) in case of a prior contractual agreement between the PIS and the ASPSP, and that agreement would be outside the scope of PSD2.

This means that the model that PISPs like Paypal and Amazon currently use for card payments, where the user authenticates himself using credentials issued by the PISP, cannot be used for PSD2 payments unless separate contractual agreements are established with each ASPSP used by European customers. If such agreements would be "outside the scope of PSD2", does that mean they would be outlawed because the regulation does not allow discrimination between PIS? If so, the plans of some organizations to transparently replace current card payment methods with PSD2 push payments may be confounded.

4. Generating authentication codes

The process of Secure Customer Authentication is at the heart of the draft RTS. Article 1.1 says that "the authentication procedure shall result in the generation of an authentication code that is accepted only once by the payment services provider..." The output code could be an access token which is returned to the AISP or PISP to authorise subsequent access to the customer's account.

The Article seems to confuse authentication (the customer proving their identity) with authorisation (the customer approving the execution of a particular operation, such as a payment). In fact,1.3e explicitly refers to authorisation rather than authentication.

As a further point of confusion, bearer access tokens are generally meant for repeated use, such as granting an AISP permission to access a customer's account details repeatedly, without requiring explicit customer authorisation every time. This would align with Articles 8.1a and 22.5b which allow an AISP to request a customer's account information twice a day, while only requiring Strong Customer Authentication once per month.

In this case, the discussion confuses rather than clarifies the draft legislation. It talks about the authentication code as a "One Time Password", but the Article clearly states that the code is an output from the authentication process, rather than a One Time Token delivered to the customer as an input to the authentication process.

5. Dynamic Linking of authentication codes

Article 2 goes on to discuss dynamic linking of the authentication code to the amount of the transaction and the payee, and says that "any change to the amount or payee shall result in a change of the authentication code." As mentioned above, the correct term for a customer giving consent to a specific transaction is authorisation rather than authentication, which makes this whole article difficult to interpret if taken at face value.

Ignoring the misleading terminology, this article again seems to be proposing the use of an access token specific to a single payment transaction, and explicitly authorised by the customer using secure authentication. To implement this in a secure way probably represents the "nightmare scenario" for consumers and PISPs, whereby the customer has to go through their bank's authentication process virtually every time they make a payment. Far from providing a more seamless payment experience than cards, this may actually be more painful than keying in card details.

6. Exemptions from Secure Customer Authentication

While acknowledging the trade-off between SCA and usability, the EBA has decided to constrain the exemptions from SCA – roughly speaking, contactless card payments under €50, card not present transaction under €10, and payments to a payee that the payer has explicitly whitelisted.

This leaves no discretion for PISPs to differentiate themselves by providing a smoother customer experience by reducing the level of authorisation needed on transactions that they identify as low risk. Perhaps a better solution would be a voluntary "liability shift", whereby the PISP can choose to bypass Secure Customer Authentication for a transaction that they consider to be low risk; but should that transaction turn out to be fraudulent, the responsibility for compensating the customer automatically lies with the PISP rather than the ASPSP. This kind of liability shift is used in the cards world to allow some discretion on the trade-off between convenience and risk.

> **"To implement this in a secure way probably represents the "nightmare scenario" for consumers and PISPs"**

7. Real Time Fraud Detection and Prevention

The document says that “the strong customer authentication procedure shall include mechanisms to prevent, detect and block fraudulent payment transactions before the PSP’s final authorisation.”

The world is moving towards real time payments, and real time fraud detection and prevention is a vital part of this move. This has long been the norm in card processing, and it’s high time it was applied to non-card payments.The EBA have wisely decided that behavioural data cannot be used as the “inherence” factor for secure authentication, but it can and should be used for fraud detection. Article 1e(iii) says the fraud detection and prevention mechanism must take into account “an adequate transaction history of the payer to evaluate its typical spending behavioral patterns, information about the customer device used and a detailed risk profile of the payee and/or the payees device.”

8. Sensitive payment data

There is no definition of “sensitive payment data” in the primary legislation, and the EBA have explicitly avoided providing one. The draft says that ASPSPs must provide AIS with “the same information from designated payment accounts and associated payment transactions made available to the payment service user when directly accessing the information online”, which is quite clear. Unfortunately, it then adds the proviso “provided that this information does not include display of sensitive payment data”.

ASPSPs have to be careful not to breach rules around data protection and personally identifiable information, so the least-risk strategy is to redact all data that could conceivably be classed as “sensitive”. This could include the name of the party to whom payments are made, the names of parties making payments into an account, and so on. Of course, account information and transaction history with those details redacted is of little or no use.

9. The role of eIDAS

eIDAS is the European regulation covering electronic identification and trust services for electronic transactions. It creates standards for electronic signatures, qualified digital certificates, electronic seals, timestamps and other proof for authentication mechanisms to give electronic transactions the same legal standing as transactions performed on paper.

The EBA has taken the bold decision to mandate the use of eIDAS certificates for authentication of ASPSPs, AISPs and PISPs. The use of PKI certificates to allow payment system participants to identify each other is definitely the right approach, and indeed probably the only one that will permit parties with no prior trust relationship to interact with an appropriate level of security.

The decision is bold because it’s not clear whether there will even be any eIDAS certification authorities in time for the implementation deadline of October 2018. The consultation invites respondents to suggest a “Plan B” to mitigate this risk.

10. Card Not Present requires Secure Customer Authentication

The draft RTS says that "card acquiring PSPs should require payees to support secure customer authentication for all payment transactions, in order to allow the payer's PSP to perform SCA in compliance with PSD2."

> **...a blow particularly to Amazon's brilliant one-click model, which would have to be changed to support something like 3D Secure**

This looks like a blow particularly to Amazon's brilliant one-click model, which would have to be changed to support something like 3D Secure - the dialog box that appears in the middle of some card transaction asking the customer for additional information. Customers hate this because it often looks like a phishing attack, and often asks for information the customers have forgotten anyway. The result is a significant rate of abandoned transactions, which of course merchants hate. At least this levels the playing field between card payments and non-card payments, forcing both to make the same trade-offs of security versus ease of use.

From theory to practice

It's one thing to discuss the RTS, but how will it work in the real world? Icon Solutions have put together a demonstration of how merchants, PISPs and ASPSPs can interact using web screens, APIs and back office systems to support e-commerce according to the draft RTS. If you would like to see the demonstration for yourself, please contact Icon using the details below and we will be delighted to arrange a convenient time.

If you would like to learn more about how Icon help your organisation with any specific PSD2 or payment challenges, please contact;

Tom Hay, Head of Payments at Icon Solutions Ltd

020 7147 9955

tom.hay@iconsolutions.com,

uk.linkedin.com/in/tomhay