Financial Data and Technology Association
c/o The University of Edinburgh
13-15 South College Street
Edinburgh
EH8 9AA

5 October 2020

Helene Oger-Zaher,
Payments Policy
Financial Conduct Authority
12 Endeavour Square
London E20 1LJ

Sent via email to:

Cc:
cp20-18@fca.org.uk

Dear Helene,

On behalf of the membership of FDATA Europe, please find our response to the Quarterly Consultation 29 CP20-18, specifically Chapter 3: Proposal to amend the open banking identification requirements (eIDAS certificates) below.

Should you have any questions relating to this response, please do not hesitate to ask.

Warmest regards,

Ghela Boskovich
Regional Director, Head of FDATA Europe

FDATA Europe Response to FCA's Quarterly Consultation 29 CP20-18
Chapter 3: Proposal to amend the open banking identification requirements (eIDAS certificates)

Q3.1: Do you agree with the proposed changes to Article 34 of the UK-RTS?

In principle, FDATA agrees with the proposed changes to UK-RTS Article 34. However, we do feel compelled to note the following points:

Proxy Certificates

FDATA strongly suggests that the existing 'proxy certificate' option, detailed under the FCA's SCA rules[1], published 02 September, 2019, be allowed to continue. Under this rule, ASPSPs can enable TPPs to use a certificate obtained from a provider of an API programme, so long as that provider only issues the alternative identification certificate to a TPP that has enrolled with the API programme using its eIDAS certificate to identify itself. This requires TPPs to voluntarily obtain that alternative identification certificate, and the API programme provider to continue checking, on behalf of the ASPSP, the status of the TPP's eIDAS certificate with the Qualified Trust Service Provider ('QTSP').

Using the OBIE API programme as an example, an eIDAS validation check is done during enrollment on the Open Banking Directory. If the ASPSP and TPP agree to use an OB issued certificate, then the API programme (the OBIE) does the validation on behalf of the ASPSP, and routinely checks its validity. The OB issued certificates then act as a proxy for eIDAS within this trust framework.

Many TPPs in the UK market already use this identification process with many ASPSPs. Allowing this scheme to continue would mean no interruption of service to a large portion of the market; however, it would require the FCA to support accredited TPPs enrolling with the OBIE without an eIDAS certificate if they are unable to source one, provided the OBIE continue to ensure that participants are duly authorised. We would also suggest the FCA's rule on SCA be updated to reflect the new proposed alternative to eIDAS certificates: that the requirement for OBIE to confirm a British TPP has an eIDAS certificate be removed from the rules.

FDATA recommends the FCA amend the proposed changes to the UK RTS to enable OB legacy certificates to continue to be used; if that cannot be achieved, we advocate for some form of allowance to enable a managed switch over from the legacy certificates. We also recommend that the FDA amend its proposal to permit the use of OBWAC/OBSeals certificates, which are already in line with the ETSI PSD2 eIDAS specifications.

[1] https://www.fca.org.uk/firms/strong-customer-authentication

For those ASPSPs who sit outside of the OBIE trust framework, Directory enrollment is always an option, however it is also possible for an ASPSP to leverage the OBIE trust framework for free without enrolling themselves. By designating OB issued certificates as acceptable proxies, this would enable banks to have an alternative authorised source of participant identity and trust, thereby avoiding a cliff edge come 1 January, 2021.

There are essentially two types of ASPSPs in the UK market:

1. Those ASPSPs who accept OB legacy or OBWAC certificates as proxy certificates (OBTransport and OBSigning certificates issued by the OBIE Directory, using a non-ETSI standard) . For these, we anticipate minimal interruption and changes. In this instance, TPPs would simply need to register replacement certificates with the OB Directory. However, for those TPPs using an OB legacy certificate, PSUs will be required to re-connect their accounts if the ASPSP ties bearer tokens to certificates. According to the results of the OBIE's surveys to industry, they can confirm that the feedback from TPPs and TSPs, who together account for approximately 75% of all long lived PSU consents across the UK based ASPSP, that migration away from OB legacy certificates would require the majority of their PSUs to have to re-authenticate for each service in order to maintain access. This is likely to affect in excess of 1.5 million customers and could cause significant detriment to those TPPs' business models and end users.

2. ASPSPs who only accept eIDAS certificates. For those ASPSPs, a migration plan is crucial. We anticipate the safest option in this instance is for TPPs to re-register with the Bank using an OB issued certificate. For an ASPSP, extending their services to trust the OB PKI is a technically trivial exercise. The OBWAC certificate profile is technically identical to the eIDAS QWAC profile precisely to make the adoption of eIDAS certificates technically simple. Likewise for ASPSPs that currently support eIDAS only, the adoption of OBWAC certificates is technically trivial. However, this must be done 90 days before the EBA cut-off date in order to "naturally" and invisibly transition PSUs over to the new system at the time of the customer-expected 90-day SCA reauthentication. As such, it is not possible to guarantee a smooth migration due to time constraints, and the need for custom technical changes required on the ASPSP side to accept OB issued certificates.

FDATA requests that the FCA provide clarity that OB issued certificates, and any other extant certificates, meet the FCA's requirements, and that the FCA work with OBIE to ensure that ASPSPs and TPPs that do not currently use OBIE services are able to access these certificates in a proportional, objective, and non-discriminatory manner.

New Certificates Should match OBWAC/OBSealC certificates

FDATA recommends that any new certificate not inadvertently invalidate existing OB Legacy or OBWAC/OBSealC certificates by requiring additional information, for example the proposed inclusion of a physical address. Requiring this sort of additional information by the 1st of January risks customer disruption.

We understand, based on information from the OBIE, that the vast majority of certificates in use at the moment are the original OB certificates (not eIDAS, nor OBWAC), which do not include the address field.

FDATA understands that requiring the new certificates to carry specific information fields, particularly the address fields of the issuer and holder of the certificate, will require technical changes for the current certificate providers. Moreover, there is no business use for the information to be contained in the certificate. It is also unnecessarily redundant, as the FCA holds the data relating to the TPP's registered address in its Financial Services Register, which is a publicly available data base, which can be used to cross-reference the firm's registration number.

However, should the FCA wish to proceed with the inclusion of this information in new certificate profiles, the incorporation of the address information in new certificates that are issued is again technically trivial for the OBIE and other providers to adopt. Our ask would be that this be phased in over a 12-month period which would keep the existing OB Certificates valid, provide sufficient time for TPPs and Banks to plan the migration to a new certificate profile which could be performed safely.

It is for these reasons that FDATA therefore recommends that clauses 7(c)(i) and (ii) be removed from the proposed draft text. We also recommend the FCA designate the alternative certificate provider be the OBIE for the immediate future, or for a set amount of time that allows for a smooth transition.

No Break in 90-Day Consent

ASPSPs who do not currently accept 'proxy certificates' are very unlikely to be ready to accept new certificates by the 31 December deadline, should the required change freeze be enforced. Were additional information fields such, then it is almost certain that ASPSPs will need to make minor technical changes. Given the looming change freeze that all ASPSPs would prefer to keep, this almost certainly guarantees that payment service users will not only experience disrupted service, but that existing viable consent will also be interrupted.

As mentioned above, any migration from OB issued certificates has the potential detrimentally affect upwards of 1.5 million PSUs, as well as significantly harm TPP business models.

This will fundamentally ruin any seamless transition or migration of users via a 'new registration' with the ASPSP. FDATA firmly backs the objective that there be no interruption in PSU end-user service.

In order to achieve a seamless transition, we propose two routes forward: 1) The ASPSP adds the new certificate to the existing 'software' that the TPP has registered;

2) The ASPSP requires the TPP to register a new ‘software’ with a different certificate; once registered, the ASPSP migrates user consents to the new software.

FDATA members strongly support the first route: adding a new certificate to existing registered software. Member experience with some ASPSPs who opted to migrate customers to a new software when transitioning to a new platform has proven that this is needlessly complex, requires extensive testing, and takes an inordinate amount of time. In some instances, it is technically not viable for the banks to register new software; it also has proven to lead to significant loss of access for TPPs. Considering the short amount of time the UK market has to ensure no end-user service is disrupted, the second route becomes a highly risky choice.

Length of time for Transition

FDATA members note that they need at least 30 days notice to customers that there may be a need to reconfirm consent. As this particular consultation ends 5 October, and the close out date for 90 Day reauthorization to be met before 31 December is in fact 2 October, the timeline for migration is too narrow to manage a seamless transition before the FCA officially determines an alternative certificate provider, as well as changes the text of the legislation.

We therefore argue that the use of the most ubiquitous certificates already in market be the solution; use of OB issued certificates, (legacy and OBWAC/OBSealC), would mitigate the risk window for interrupted 90 Day consent, as well as mitigate much of the need to notify customers in a timely manner of the transition, and resulting need to re-consent. This ‘proxy certificate’ solution would solve for the transition timeline risks.

Competitive Certificate Market

FDATA is in support of a competitive certificate market, but not as a first priority; ensuring no disruption to end-user service is of the highest priority, and it requires adoption of alternative certificates already in use in the market. In this case, the OB issued certificates – as indicated in the consultation – are already widely adopted, in use, and are relatively easy to obtain for TPPs. For TPPs, onboarding to the Directory is free, and requires a single API call. A single supplier of identification certificates is a rational and practical solution up against such a tight timeline; any federated alternatives do not seem viable given the exigent circumstances.

This eIDAS certificate cliff edge requires a pragmatic approach, and a single supplier to the market is a viable solution, especially in the short term. The Open Banking Directory as the third party issuing certificates is the preferred FDATA member solution.

That being said, and once the UK market has stabilised, FDATA does encourage the FCA to explore promoting competition in the market for certificates that meet the requirements of the FCA’s amended text, bearing in mind the functional differences between the requirements of the FCA’s proposed alternative certificate and the benefits to firms using an eIDAS certificate.

Over time, FDATA believes it is important to consider how existing alternative certificate providers can ensure they issue certificates that support the industry during a volatile transition period, while the wider Trust Service Provider industry responds to the enablement of a competitive market for those certificates.

One suggestion for how we can transition from a single issuance model to a competitive market model would be to take the existing providers of the National Trust List under eIDAS (administered by tScheme on behalf of the ICO[2]) and have this entity create a non-eIDAS National Trust List for the UK certificate regime.

This root-of-trust could then be expanded beyond a single entity (the OBIE) in due course if and when there is a requirement for a competitive market for trust. API programmes like the Open Banking Implementation Entity would then change their "proxy validation" endpoints to accept any certificates on this trust list, not just those directly issued by themselves. The actual implementation of these or other competitive market steps are out of scope for this consultation but provided as an example to demonstrate the potential for expanding OBWAC/OBSealC single issuer models into federated competitive models.

[2] https://www.tscheme.org/tsl/uk-tsl