FINANCIAL CONDUCT AUTHORITY

Amendments to the open banking identification requirements (eIDAS certificates)

Policy Statement
PS20/13

November 2020

This relates to

Consultation Paper 20/18
which is available on our website at
www.fca.org.uk/publications

Email:
cp20-18@fca.org.uk

How to navigate this document

returns you to the contents list

takes you to helpful abbreviations

takes you to the previous page

takes you to the next page

prints document

email and share document

Contents

1 Summary 3

2 Open Banking Identification Requirements 8

Annex 1
List of non-confidential respondents 14

Annex 2
Abbreviations used in this paper 15

Appendix 1
Made rules (legal instrument)

1 Summary

1.1 On 4 September 2020, in CP20/18 (chapter 3), we consulted on the proposal to amend Article 34(1) of the UK regulatory technical standards for strong customer authentication and secure communication (UK-RTS). It aimed to address issues caused by the European Banking Authority (EBA) announcing the revocation of the certificates UK third-party providers (TPPs) rely on to access customer account data and initiate payments under the system known generally as 'Open Banking'. The consultation closed on 5 October.

1.2 This Policy Statement (PS) summarises the responses we received.

1.3 This PS also confirms that Article 34 of the UK-RTS will be amended, with only minor changes to the proposed amendment we consulted on. It will come into force, along with the UK-RTS, immediately after the end of the transition period for Brexit at 11pm on 31 December 2020 (referred to as Implementation Period (IP) Completion Day).

1.4 Our aim is to minimise disruption to the UK's open banking ecosystem, and its end users, post Brexit. We want to ensure that the UK's open banking ecosystem continues to serve over 2 million customers. To that end, we have also decided to provide a short transition period until 30 June 2021. We cannot delay the revocation of eIDAS certificates and do not support a period where certificates would not be exchanged. This transition is therefore limited in scope. The transition period allows firms to make the necessary technical changes, while continuing to rely on certificates in order to access customer's online payment account data and initiate payments.

Who this affects

1.5 This PS will affect:

- firms that provide and maintain a payment account with online access for a payer (ASPSPs)
- firms that provide online services that consolidate customers' payment account data (AISPs)
- firms that provide online services that allow users to initiate payments (PISPs)
- firms that provide services that initiate card-based payments from payment accounts held by an ASPSP (CBPIIs)

The wider context of this policy statement

1.6 Under the Payment Services Regulations 2017 (the PSRs), which implement the second payment services directive (PSD2), providers of account information and payment initiation services (also known as third-party providers (TPPs)) are required under paragraph 70(3)(c) and paragraph 69(3)(d) respectively, to identify themselves to account servicing payment service providers (ASPSPs) to access customer's online payment account data and initiate payments from such accounts.

1.7 The Regulatory Technical Standards on strong customer authentication and common and secure communication (SCA-RTS) set out the standards of communication required and regulate access by TPPs to customer accounts held with their ASPSPs. Article 34(1) of the SCA-RTS requires TPPs to rely on eIDAS certificates for identification to ASPSPs. eIDAS certificates are issued by qualified trust service providers (QTSPs) under Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market (the eIDAS Regulation).

1.8 The requirement to rely on an eIDAS certificate for identification will be carried across into the UK regulatory technical standards for strong customer authentication and secure communication (UK-RTS). The eIDAS Regulation, as amended by the Electronic Identification and Trust Services for Electronic Transactions (Amendment etc.) (EU Exit) Regulations 2019, will also be onshored, at the end of the Transitional Period agreed with the European Union.

1.9 On 29 July 2020, the EBA published a press release on Brexit stating that eIDAS certificates issued by EU QTSPs to UK-based TPPs will be revoked on IP Completion Day.

1.10 While eIDAS certificates issued by EU QTSPs remain valid under UK law, the revocation of individual certificates under EU law means that, after IP Completion Day, TPPs will no longer hold a valid certificate for use in the UK. We understand that at present there is no scope within the European eIDAS regime to issue UK-only certificates. In addition, there are no UK QTSPs qualified to issue eIDAS certificates under the UK eIDAS Regulation.

1.11 Without intervention, TPPs in the UK will no longer be able to access their customer's account data held with ASPSPs in line with UK law after the transition period ends on IP Completion Day. To avoid disruption to open banking services, we proposed in CP20/18 (Chapter 3) an amendment to the regulatory requirements to allow for the use of an alternative form of identification.

Is this of interest to consumers?

1.12 Our amendment to Article 34 of the UK-RTS ensures the same level of consumer protection remains by continuing to require TPPs to identify themselves securely. In particular, it defines the criteria an alternative certificate must meet that are equivalent to those of an eIDAS certificate.

1.13 Our amendment will continue to promote competition in the market. Indeed, it will allow continued access by TPPs to customers' payment account data, with the consumer's explicit consent, meaning consumers continue to be provided with a range of products and services.

What we are changing

1.14 Under Regulation 106A of the PSRs, from IP Completion Day, the FCA is able to make changes to the UK-RTS. We are amending Article 34 of the UK-RTS to require ASPSPs to accept at least one other electronic form of identification issued by an independent third party. This is in addition to continuing to accept eIDAS certificates.

1.15 The additional form of identification must meet certain criteria. It must be a digital certificate issued by an independent third party upon identification and verification of the payment service provider's identity. The certificate must be revoked as soon as the TPP is no longer authorised to conduct TPP activities. Further, it requires ASPSPs to verify the authorisation status of the TPP, in a way that would not create any obstacles to TPP access, and to satisfy itself of the suitability of the independent third party issuing the certificate. ASPSPs are also required to specify publicly which means of identification it accepts to ensure TPPs are aware (eg on the Open Banking Implementation Entity (OBIE) transparency calendar or on their website).

1.16 The certificate must include the name of the TPP as well as information on the competent authority the TPP is authorised or registered with, and the corresponding registration number (Firm Reference Number (FRN)).

1.17 We are not prescribing any further detailed attributes for certificates. Nor are we prescribing a specific alternative certificate that should be used.

1.18 In so doing, we hope to minimise the potential for disruption to existing market practice, and maximise the options available for ASPSPs and TPPs.

1.19 The UK-RTS, with these amendments, will be made under Regulation 106A to come into effect immediately after IP Completion Day.

Outcome we are seeking

1.20 The amendment seeks to ensure that TPPs can continue to serve their 2 million customers post IP Completion Day. This means ensuring TPPs can continue to access their customers' payment accounts data or initiate payments and that any transition to a new certificate will have minimal impact on end users. The amendment is designed to limit the risk of disruption and ensure the continuity of open banking.

1.21 We aim to achieve this by requiring ASPSPs to accept eIDAS certificates and at least one alternative form of certificate.

Measuring success

1.22 We will know this intervention has been successful if open banking continues to function for its 2 million users, with minimal disruption.

1.23 We will evaluate the success of our changes through firm supervision and monitoring of information provided by firms. We may also engage with API programme providers, such as the OBIE, to assess the impact of these changes, including consumer outcomes.

Summary of feedback and our response

1.24 We received 22 responses from trade bodies, regulated and unregulated firms and consumer representatives. Most responses welcomed the FCA's action and were broadly supportive of our proposal.

1.25 Some respondents expressed minor concerns about some of the detailed requirements mandated on the additional form of identification. In addition, many responses were concerned that the time allocated to make changes ahead of the new requirement becoming applicable was too short and queried whether some form of transition period could be envisaged. A respondent also stated they would prefer the regulation to define specifically the alternative certificate to ensure inter-operability and standardisation, while another thought that less detail should be provided in the proposed amendment to ensure providers have varied options and choices.

1.26 Following the responses, we have made minor changes to a few of the detailed requirements under Article 34(8) of the UK-RTS. Those changes include removing the need for the certificate to include the address of the TPP and issuer and the need for revoking the certificate if identity information is unverifiable as those are not required for eIDAS certificates and not common practice. We have also removed the need for a certificate to be amended as, technically, a certificate can only be revoked and not amended.

1.27 In relation to a possible transition period, we do not have the ability to delay the revocation of eIDAS certificates. We also do not support the functioning of open banking without TPPs presenting certificates to account providers, as this is a key security measure. So, we have decided to provide a short transition period that keeps the fundamental obligations in place, but allows some extra time for technical changes to be processed in the background. During the transition period, we will allow ASPSPs to accept a certificate obtained from a provider of an API programme that does not meet the requirements of the revised Article 34. The use of these certificates is only valid when TPPs have also presented a compliant certificate to that API programme. The provider of the API programme should validate the certificate and continue checking, on behalf of the ASPSP, the status of the TPP's compliant certificate. This transitional arrangement will end on 30 June 2021.

1.28 Feedback and our responses are set out in detail in Chapter 2.

Equality and diversity considerations

1.29 We have considered the equality and diversity issues that may arise from the proposals in this PS, in light of the feedback we received to our consultations.

1.30 We do not consider that the proposals in the PS will have a negative impact on any of the groups with protected characteristics - age, disability, sex, marriage or civil partnership, pregnancy and maternity, race, religion and belief, sexual orientation and gender re-assignment.

What you need to do next

1.31 If your firm is an ASPSP, you need to assess the need for any changes in your systems and processes and implement any necessary changes as soon as possible ahead of IP Completion Day. We also expect you to tell TPPs which alternative certificate you will accept as early as possible. We continue to encourage you to use existing certificates where possible.

1.32 If your firm is a TPP and your eIDAS certificate is likely to be revoked, you must have an alternative certificate(s) as soon as possible ahead of IP Completion Day.

2 Open Banking Identification Requirements

2.1 In this chapter, we summarise and respond to the feedback received to our proposed amendments to Article 34 of the UK-RTS.

Amendments to Open Banking Identification Requirements

2.2 Article 34 of the SCA-RTS specifies that TPPs must identify themselves to ASPSPs using eIDAS certificates when accessing customer payment accounts data and initiating payments. eIDAS certificates are issued by QTSPs under the eIDAS Regulation. This requirement was carried across into the UK-RTS and the eIDAS Regulation was also onshored, with some amendments.

2.3 On 4 September, we consulted on an amendment to Article 34 of the UK-RTS aiming to address issues caused by the EBA announcing the revocation of the certificates UK TPPs rely on to access customer account data and initiate payments. The amendment requires ASPSPs to accept at least one other electronic form of identification issued by an independent third party, in addition to eIDAS certificates.

We asked:

Q1: ***Do you agree with the proposed changes to Article 34 of the UK-RTS?***

2.4 Respondents were broadly supportive of our proposal and welcomed our action to minimise harm and disruption to the UK's open banking ecosystem. Respondents provided feedback and raised concerns about some specific aspects of our proposal. Responses included feedback and concerns about:

- specific requirements proposed for the alternative form of identification
- existing alternatives and practical challenges to making required changes ahead of IP Completion Day

2.5 A few respondents provided general feedback and points for further considerations.

Specific requirements within the alternative form of identification

2.6 In our consultation, we proposed that the alternative certificate must include specific identity information (eg name and address of the TPP and issuer) as well as information on the competent authority the TPP is authorised or registered with, and the corresponding registration (FRN) number. We also highlighted certain other criteria the alternative certificate should meet including the requirement to amend the certificate when identity information changes and revoke the certificate where that information is unverifiable.

2.7 While respondents were generally supportive and acknowledged the underlying principles on which the proposed requirements were based, many raised concerns about the feasibility of timings.

2.8 Many respondents disagreed with including the address on the certificate, explaining that this is an optional field under the eIDAS Regulation and that no certificate in use in the industry currently included that information.

2.9 Several respondents also raised concerns around the requirement to include the TPP's registration (FRN) number within the certificate. Respondents highlighted that while eIDAS certificates included that field and that other alternative certificates also did (giving the examples of Open Banking Certificates for Website Authentication (OBWACs) and Open Banking Certificates for Electronic Seals (OBSeals)), not all alternative certificates did. They argued that ASPSPs and certificate issuers can satisfy this requirement through others means, without the need to include that field. Other respondents, by contrast, supported its inclusion.

2.10 Concerns were expressed regarding the requirement to amend the certificate where the identity information changes. Some respondents explained that it is not technically possible to make amendments to existing certificates once issued and that certificates could only be revoked. They also highlighted that this was not a requirement for current eIDAS certificates.

2.11 Some respondents expressed confusion around the reference to information being unverifiable and sought clarity around the requirement to revoke the certificate where the TPP is unverifiable. They wanted to understand how certificate issuers were expected to comply. Others highlighted that it was not a requirement for eIDAS certificates and that it would likely have implications for certificate issuers and TPPs.

Our response

We have considered the feedback and made minor amendments.

Our objective when proposing to amend Article 34 was to limit the risk of disruption to the market and its end users. We did not intend to introduce any changes that would likely lead to customer disruption and require the market to go above the existing requirements under the eIDAS Regulation.

Respondents have explained that including the physical address is not information that is included in any existing certificate (including eIDAS). They also thought it would constitute a significant change (described as a 'breaking change' by respondents) leading to likely customer disruption. So, we have removed that requirement from Article 34(8).

We have also decided to remove the requirement to revoke a certificate if information is 'unverifiable'. We think the requirement to revoke a certificate when the TPP no longer has the appropriate authorisation or registration to carry out its activities is sufficient. We are also satisfied that this is aligned with the eIDAS regulations.

We have also removed the reference to amending a certificate when identity information changes as respondents explained that a certificate cannot technically be amended and will instead be revoked where applicable.

We are satisfied that those changes provide an adequate balance between maintaining strong security standards and aligning with existing requirements under the eIDAS Regulation and, from IP Completion Day, the UK eIDAS regulation while ensuring that we can achieve our objective of limiting the risk of disruption.

We acknowledge the concerns raised around the requirement to include FRN in the alternative certificates and the practical downsides caused as existing legacy certificates do not contain this information. Despite this, we think this information is important and should be included to ensure an adequate level of security. The purpose of the FRN is to allow the unique identification of the TPP and to facilitate verification of the authorisation status of the TPP. The inclusion of the FRN allows for more secure identification and is a key requirement for eIDAS certificates.

Existing alternatives and practical challenges to making required changes ahead of IP Completion Day

2.12 In CP20/18, we proposed that the ASPSPs should accept at least one other electronic form of identification in addition to eIDAS certificates. We also encouraged firms to consider using existing solutions that are currently available in the UK.

2.13 Many respondents highlighted that there were alternatives available in the market, referencing in particular the new OBIE certificates (OBWACs and OBSeals), which are aligned to eIDAS certificates. However, they also explained that many firms continue to rely on legacy certificates, citing in particular those legacy certificates issued by the OBIE before eIDAS certificates became available. As a result, respondents expressed concerns around the feasibility of migrating to the newer types of certificates in the very short time available to them before IP Completion Day. They highlighted the time needed to reconfigure their systems to allow another form of certificate and mentioned the limitations they face on making any significant change around Christmas, citing IT 'change freezes' around that period.

2.14 One respondent also explained that ASPSPs who only accept eIDAS certificates will be more impacted than ASPSPs that already accept alternatives.

2.15 In addition, a number of respondents highlighted that TPPs need to obtain the relevant certificate(s), and then need to integrate and test them in their systems. It was suggested that they would need 3 months to do that.

2.16 Further, other respondents explained that the transition of a TPP from eIDAS certificate to an alternative will require a change of the existing consents. They suggested that the best way to do so would be by ensuring that those changes can take place using the 90-day reauthentication cycle, rather than by requiring all customers to re-authenticate on 1 January. They argued that some flexibility around timings would be very beneficial to end users.

2.17 Respondents therefore queried whether the FCA would consider providing a transition period to ensure a smooth switch from one type of certificate to another. Suggestions on timings varied from 3 to 12 months.

Our response

It is important to highlight that we are not able to provide flexibility or additional time when it comes to the revocation of eIDAS certificates. The eIDAS certificates of UK TPPs will be revoked as a result of the UK's departure from the EU.

We also think that the presentation of such certificates by TPPs to account providers is an essential protection for consumers within open banking.

However, we acknowledge the challenges faced by TPPs and ASPSPs to implement changes, as explained by respondents. To ensure continuity of service and enable TPPs to use the existing 90-day reauthentication cycle, we have decided to provide a short transition period. During this period, we will allow ASPSPs to accept a certificate obtained from a provider of an API programme that does not meet the requirements of the amended Article 34. The use of these certificates will only be valid on the following conditions: 1) TPPs have also presented a compliant certificate, as described under the revised Article 34, to that API programme, 2) that API programme verifies the certificate and 3) continues checking, on behalf of the ASPSP, the status of the TPP's compliant certificate. For example, a legacy OBIE certificate may be used during that period, provided that the TPP has presented a valid certificate to the OBIE. This provisional arrangement will end on 30 June 2021.

We consider this approach to be proportionate as it should limit the risks of disruption while ensuring adequate protection.

Other feedback

2.18 A few respondents highlighted general feedback and points for further consideration.

2.19 Some respondents requested further clarity on how they should interpret our proposal of requiring ASPSPs to accept at least one other electronic form of identification in addition to eIDAS certificates. One respondent wanted to understand whether ASPSPs are required to accept both eIDAS certificates and an alternative certificate.

2.20 One respondent highlighted the need for an alternative certificate which ensures the impact on end-users is minimal, and that disruption is limited and open banking continues to develop in the UK.

2.21 Others highlighted the need for ASPSPs to share the additional means of identification they are willing to accept to ensure that TPPs are aware in a timely manner. Once ASPSPs have confirmed which alternative certificates they will accept, TPPs can

migrate to these alternatives and inform their customers of the need to re-consent. One respondent also suggested ways that ASPSPs can share this information with TPPs within the ecosystem.

2.22 One respondent highlighted that in the medium to long term there is a risk of fragmentation due to the lack of standardisation. It was highlighted that the market should adopt interoperable standards and processes for ease of implementation and to minimise fragmentation. By contrast, another respondent suggested that competition was needed within the market in the future to ensure that the market can withstand future changes.

2.23 Some respondents highlighted the possible risk of lack of equivalence with the EU due to a possible divergence of identification requirements. One respondent expressed the view that identification requirements prescribed in the consultation may not be entirely equivalent to those under eIDAS requirements.

Our response

We note that respondents have requested clarity on what is expected from them regarding the acceptance of eIDAS and alternative certificates. As explained in CP20/18 (Chapter 3), ASPSPs are required to accept eIDAS certificates and at least one additional certificate issued by an independent third party. We are not prescribing which alternative certificate should be used.

ASPSPs must continue accepting valid eIDAS certificates. This includes for UK firms until their certificates are revoked, including post IP Completion Date where applicable, as well as for European firms that benefit from the Temporary Permission Regime.

We agree with the respondent who stated that the disruption to end users should be minimal. Our objective when proposing to amend Article 34 was to limit the risk of disruption to the market and its end users, while ensuring adequate levels of security. We have, as highlighted above, amended our rules and provided a short transition period to ensure that this objective is met.

On the publication of the alternative forms of identification ASPSPs would accept, we agree with those respondents who have stated that ASPSPs should do so in a timely fashion. We encourage ASPSPs to do so as soon as practically possible ahead of 31 December 2020, allowing TPPs to migrate in a timely manner to alternative certificates and seek customer re-authentication

We note contrasting views on the need for standardisation that may conflict with encouraging competition for those alternative certificates. In our view, our proposed requirement provides an appropriate balance between promoting competition and minimising the risk of fragmentation. Our rules enable TPPs and ASPSPs to have multiple available alternatives to choose from while ensuring that there is a level of standardisation through our prescribed set of requirements. In

addition, our amendments do not restrict the ability for the industry to agree on an alternative certificate if they so wish.

On equivalence, the requirements the alternative certificate must meet are premised on third party authenticated identification of TPPs (like eIDAS certificates) and we think that they are therefore substantively equivalent to eIDAS certificates.

Annex 1
List of non-confidential respondents

1. We received 22 responses to CP20/18. The following organisations submitted responses that were not confidential:

Account Technologies

Crezco Limited

Hope Macy Ltd

Independent Consumer & SME Representatives to Open Banking Implementation Entity

InfoCert S.p.A.

Intuit Limited

The Coalition for a Digital Economy

The Smart Request Company Ltd

Annex 2
Abbreviations used in this paper

AISP	Account Information Service Provider
ASPSP	Account Servicing Payment Service Provider
CBPII	Card Based Payment Instrument Issuer
eIDAS Regulation	Electronic identification and trust services for electronic transactions in the internal market
EBA	European Banking Authority
FRN	Firm Reference Number
IP Completion Day	Implementation Period Completion Day
OBIE	Open Banking Implementation Entity
OBSeals	Open Banking Certificates for Electronic Seals
OBWACs	Open Banking Certificates for Website Authentication
PISP	Payment Initiation Services Provider
PS	Policy Statement
PSRs	Payment Services Regulations
QTSP	Qualified Trust Service Provider
PSD2	Second payment services directive
SCA-RTS	Regulatory technical standards on strong customer authentication and common and secure communication
TPP	Third-Party Provider
UK-RTS	UK regulatory technical standards for strong customer authentication and secure communication

Appendix 1
Made rules (legal instrument)

TECHNICAL STANDARDS ON STRONG CUSTOMER AUTHENTICATION AND COMMON AND SECURE METHODS OF COMMUNICATION (AMENDMENT OF EIDAS CERTIFICATE) INSTRUMENT 2020

Powers exercised

A. The Financial Conduct Authority ("the FCA") makes this instrument in the exercise of the power and related provisions in or under:

(1) Regulation 106A (Technical Standards) of the Payment Services Regulations as amended by the Electronic Money, Payment Services and Payment Systems (Amendment and Transitional Provisions) (EU Exit) Regulations 2018 which comes into force on exit day as defined by the EU Withdrawal Act 2018;

(2) the following sections of the Financial Services and Markets Act 2000 ("the Act") as amended by the Financial Regulators' Powers (Technical Standards etc.) (Amendment etc.) (EU Exit) Regulations 2018:

(a) section 138P (Technical Standards);
(b) section 138Q (Standards instruments);
(c) section 138S (Application of Chapters 1 and 2);
(d) section 137T (General supplementary powers);
(e) section 138F (Notification of rules); and
(f) section 138I (Consultation by the FCA).

Pre-condition to making

B. The FCA has consulted the Prudential Regulation Authority and the Bank of England as appropriate in accordance with section 138P of the Act.

C. A draft of this instrument has been approved by the Treasury, in accordance with section 138R of the Act.

Commencement

D. This instrument comes into force [on IP completion day as defined in the European Union (Withdrawal Agreement) Act 2020, immediately after the Technical Standards on Strong Customer Authentication and Common and Secure Methods of Communication Instrument 2020 (the "SCA-RTS") comes into force].

[**Note:** IP completion day is 11pm on 31 December 2020.]

Amendments to material outside the Handbook

E. The SCA-RTS (Article 34) is amended in accordance with the Annex to this instrument.

Citation

F. This instrument may be cited as the Technical Standards on Strong Customer Authentication and Common and Secure Methods of Communication (Amendment of eIDAS Certificate) Instrument 2020.

By order of the Board
[*date*]

In this instrument, underlining indicates new text and striking through indicates deleted text.

Annex

Technical standards regarding strong customer authentication and common and secure open standards of communication.

…

Article 34

Certificates

1. For the purpose of identification, as referred to in Article 30(1)(a), account servicing payment ~~Payment~~ service providers shall ~~rely on~~ accept both of the following electronic means of identification:

   (a) qualified certificates for electronic seals as referred to in Article 3(30) of the Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust service for electronic transactions in the internal market, as amended by the Electronic Identification and Trust Services for Electronic Transactions (Amendment etc.) (EU Exit) Regulations ~~2018~~ 2019 as came into force on ~~exit day~~ IP completion day as defined in the European Union (Withdrawal Agreement) Act ~~2018~~ 2020, or for website authentication as referred to in Article 3(39) of the same Regulations~~.~~;

   (b) at least one other form of identification issued by an independent third party that is not unduly burdensome for payment service providers to obtain; and

   account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments shall rely on one of the above means of identification.

2. For the purpose of these Standards, referred to in paragraph 1, the registration number as referred to in the official records in accordance with Annex III(c) or Annex IV(c) to Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust service for electronic transactions in the internal market as amended by the Electronic Identification and Trust Services for Electronic Transactions (Amendment etc.) (EU Exit) Regulations ~~2018~~ 2019 as came into force on ~~exit day~~ IP completion day as defined in the European Union (Withdrawal Agreement) Act ~~2018~~ 2020 and the registration number referred to in paragraph 8, shall be the authorisation or registration number of the payment service provider issuing card-based payment instruments, the account information service providers and payment initiation service providers, including account servicing payment service providers providing such services, available in the public register of the UK pursuant to regulation 4 of the Payment Services Regulations (SI 2017/752) or section 347 of the Financial Services and Markets Act 2000, or in the case of such payment service

providers incorporated and registered or authorised in Gibraltar, their incorporation number available in the Regulated Entities Register of the Gibraltar Financial Services Commission.

3. For the purposes of these Standards qualified certificates for electronic seals or for website authentication referred to in paragraph 1(a) shall include, in a language customary in the sphere of international finance, additional specific attributes in relation to each of the following:

   (a) the role of the payment service provider, which may be one or more of the following:

      (i) account servicing;

      (ii) payment initiation;

      (iii) account information;

      (iv) issuing of card-based payment instruments;

   (b) the name of the competent authorities where the payment service provider is registered.

4. The attributes referred to in paragraph 3 shall not affect the interoperability and recognition of qualified certificates for electronic seals or website authentication.

5. Where a form of identification under paragraph 1(b) is used, account servicing payment service providers must:

   (a) verify that the payment service provider is authorised or registered to perform the payment services relevant to its activities in a way that does not present an obstacle to the provision of payment initiation and account information services; and

   (b) satisfy itself that the independent third party issuing that form of identification is suitable and has sufficient systems and controls to verify the information contained in the digital certificate referred to in paragraph 8.

6. Account servicing payment service providers must make public the forms of identification they accept.

7. Payment service providers relying on a form of identification under paragraph 1(b) must notify the independent third party issuing that form of identification of any changes in identity information or regulatory authorisation in writing before such changes take effect or, where this is not possible, immediately after.

8. A form of identification accepted under paragraph 1(b) must be a digital certificate that:

   (a) is issued upon identification and verification of the payment service provider's name, company number (if applicable) and its principal place of business;

   (b) gives appropriate assurance to account servicing payment service providers in relation to the authenticity of the data and the identity of the payment service provider;

   (c) represents the following information:

      (i) name of the issuer of the form of identification;

      (ii) the name of the payment service provider to whom the certificate is issued; and

(iii) the registration number and competent authority of the payment service provider to whom the certificate is issued; and

(d) is revoked where the payment service provider ceases to be authorised or registered or it would be inconsistent with its authorisation to carry on the relevant payment services.

Pub ref: 7449

12 Endeavour Square London E20 1JN
Telephone: +44 (0)20 7066 1000
Website: www.fca.org.uk