OPEN BANKING CERTIFICATE POLICY

CONTENTS

1 INTRODUCTION

1.1 OVERVIEW

This Open Banking Certificate Policy defines the requirements for the Issuance and management of Certificates by Open Banking (http://ob.trustis.com/production/policies/).

A Certificate Policy is a named set of rules that indicates the applicability of a Certificate to a particular community and/or class of application with common security requirements and is further supported by a Certification Practice Statement.

The responsibility for this Open Banking Certificate Policy lies with a body within Open Banking Limited known as the Open Banking Policy Authority, and any queries regarding the content of this Open Banking Certificate Policy should be directed to the Open Banking Policy Authority.

This Open Banking Certificate Policy is structured according to the guidelines provided by IETF RFC 3647 (https://tools.ietf.org/html/rfc3647) with extensions and modifications defined where appropriate.

The Open Banking Issuing Authority which Issues Certificates in accordance with this Open Banking Certificate Policy has made its own stipulations regarding Parties, further restrictions on usage of Certificates, additional liability provisions, etc. These stipulations are published by the Open Banking Issuing Authority in a document termed the Open Banking PKI Disclosure Statement, which serves as the highest-level vehicle by which provisions affecting Subscribing PKI Participants and Relying PKI Participants are defined. The Open Banking PKI Disclosure Statement supporting this Open Banking Certificate Policy incorporates this Open Banking Certificate Policy by reference. All Certificates Issued under this Open Banking Certificate Policy shall contain a reference to where the Open Banking PKI Disclosure Statement published by the Open Banking Issuing Authority that Issued the Certificate may be found.

This Open Banking Certificate Policy defines a Public Key Infrastructure and in conjunction with the Open Banking PKI Disclosure Statement, specifies:

- Who can participate in the Public Key Infrastructure defined by this Open Banking Certificate Policy.
- The primary rights, obligations and liabilities of the Parties governed by this Open Banking Certificate Policy.
- The purposes for which Certificates Issued under this Open Banking Certificate Policy may be used.
- Minimum requirements and guidance for the Issuance, management, usage and Reliance upon Certificates.

The various terms used throughout this document are explained in the Open Banking Definitions of Terms at http://ob.trustis.com/production/policies/.

1.2 DOCUMENT NAME AND IDENTIFICATION

This Open Banking Certificate Policy is registered with Entrust Limited operating in an authorised administrative role for Open Banking Limited. Entrust Limited is registered with the Internet Address Naming Authority (IANA) and has been assigned an object identifier ("OID") of 1.3.6.1.4.1.5237. This Open Banking Certificate Policy has also been assigned an OID as defined in Section 12 of the associated Open Banking PKI Disclosure Statement located at http://ob.trustis.com/production/policies/.

1.3 PKI PARTIES

The Open Banking Issuing Authority has an obligation to operate the Public Key Infrastructure in accordance with the defined and published Open Banking Certificate Policy. The Open Banking Issuing Authority does not however conduct all aspects of Public Key Infrastructure operations itself. There are sets of functions that are logically and conveniently grouped and delegated. This allows Public Key Infrastructure services to align with the Open Banking Ecosystem business model including the outsourcing of some of the Public Key Infrastructure services to other Parties.

Each Party operates to fulfil clearly defined roles which are described further in the following sections. These roles are:

- Policy Authority
- Trust Service Providers:
    - Issuing Authority
    - Certificate Manufacturer
    - Registration Authority
    - Repository
- End Entities:
    - Subscribing PKI Participants
    - Certificate Subjects
    - Relying PKI Participants

For the avoidance of doubt, Subscribing PKI Participants and Relying PKI Participants only have a contractual relationship with Open Banking Limited and not each other. These relationships are defined by the Open Banking Subscribing PKI Participant Agreement and Open Banking Relying PKI Participant Agreement.

Certificate Subjects hold Certificates on behalf of Subscribing PKI Participants. In all cases however, the contractual relationship with Open Banking Limited is held by the Subscribing PKI Participant.

The requirements placed upon Parties providing Trust Services which support the Open Banking Issuing Authority are controlled by the provisions of this Open Banking Certificate Policy and any contractual arrangements between them and Open Banking Limited.

In any case of non-compliance with this Open Banking Certificate Policy, the Open Banking Issuing Authority will determine the steps to be taken. It may refer matters to the Open Banking Policy

Authority who has overall and final control over the content of this Open Banking Certificate Policy and related documentation.

1.3.1 CERTIFICATION AUTHORITIES

IETF RFC 3647 (https://tools.ietf.org/html/rfc3647) defines Certification Authorities as the entities that Issue Certificates. Within the scope of the model outlined a "Certification Authority consists of the two elements described in 1.3.1.1 and 1.3.1.2.

1.3.1.1 ISSUING AUTHORITY

By definition, the Issuing Authority is the entity listed in the issuer field of a Certificate.

The Open Banking Issuing Authority has the ultimate responsibility for deciding who may be issued with a Certificate carrying its name as the Open Banking Issuing Authority. Whether Public Key Infrastructure services are provided by internal resources or are contracted out to external Parties, the provisions of this Open Banking Certificate Policy apply. This Open Banking Certificate Policy may be complemented by a contract between the Open Banking Issuing Authority and Parties providing services where applicable.

For the benefit of Subscribing PKI Participants and Relying PKI Participants, the Open Banking Issuing Authority publishes a summary of important provisions that form a part of this Open Banking Certificate Policy, together with any further provisions affecting Subscribing PKI Participants and Relying PKI Participants, in the Open Banking PKI Disclosure Statement.

The Open Banking Issuing Authority ensures that all Certificates Issued by it under this Open Banking Certificate Policy shall contain a reference to where the Open Banking PKI Disclosure Statement and this Open Banking Certificate Policy document are published.

1.3.1.2 CERTIFICATE MANUFACTURER

The Certificate Manufacturer provides operational Certificate management services for the Open Banking Issuing Authority.

The Certificate Manufacturer is approved by the Open Banking Issuing Authority to manage Certificates on behalf of the Open Banking Issuing Authority or other Parties in the Public Key Infrastructure governed by this Open Banking Certificate Policy. It has no authority to make decisions on the Issuance of Certificates, or other aspects of certificate management; it operates under the direct control of the Open Banking Issuing Authority.

The Certificate Manufacturer must demonstrate compliance with this Open Banking Certificate Policy. Compliance is documented and controlled via a Certification Practice Statement.

1.3.2 REGISTRATION AUTHORITIES

A Registration Authority is responsible for ensuring the eligibility of Subscribing PKI Participants to be Issued with Certificates together with the accuracy of the information presented during the Certificate request procedure.

Within the Open Banking Limited Public Key Infrastructure, the Registration Authority functions are split across the following:

- Open Banking Enrolment: This team are responsible for carrying out the enrolment onto the Open Banking Directory. This includes Authentication of organisations and their named individuals (Primary Technical Contact, Primary Business Contact and any other additional technical and business contacts) by the Open Banking enrolment team or other third party approved by Open Banking Limited to establish their identity.
- Open Banking Local Registration Authority: This is the Open Banking Limited technical system that Subscribing PKI Participants and Open Banking Manual Registration Authority staff use to apply for, Renew/Re-key and Revoke Certificates. It also allows the Open Banking Issuing Authority to Revoke Subscribing PKI Participant Certificates programmatically, independent of the Subscribing PKI Participant.
- Open Banking Manual Registration Authority: This is the Open Banking Limited team responsible for the manual Revocation of Subscribing PKI Participant Certificates.
- Registration Authority Server: This is a technical system located at the Certificate Manufacturer that accepts, processes and responds to Certificate Issuance and Certificate lifecycle management requests from the Open Banking Local Registration Authority.

Where the term Open Banking Registration Authority is used it shall refer to all of the Registration Authority functions listed above with the exception of the Registration Authority Server.

A Public Key Infrastructure may operate with a single or multiple Registration Authorities. Each must demonstrate compliance with this Open Banking Certificate Policy. Compliance is documented and controlled via a Certification Practice Statement. Such procedures may vary between Registration Authorities. However, in each case they must support the Certification Practice Statement and fully comply with this Open Banking Certificate Policy.

The Open Banking Issuing Authority has approved the Registration Authorities listed in section 13 of the Open Banking PKI Disclosure Statement with respect to Certificates governed by this Open Banking Certificate Policy.

1.3.3 SUBSCRIBING PKI PARTICIPANTS

A Subscribing PKI Participant is an End Entity organisation that has applied for, and received a Certificate. It is the Subscribing PKI Participant that has a relationship with the Open Banking Issuing Authority for the Issuance of Certificates.

The Subscribing PKI Participant bears responsibility for the use of a Private Key associated with a Certificate.

A Subscribing PKI Participant is contractually bound to the terms of this Open Banking Certificate Policy and operates in accordance with this Open Banking Certificate Policy, Open Banking Subscribing PKI Participant Agreement and associated Public Key Infrastructure practices.

Certificate Applicants eligible to be authorised by the approved Registration Authorities as Subscribing PKI Participants, are identified in section 15 of the Open Banking PKI Disclosure Statement.

1.3.4 CERTIFICATE SUBJECTS

Where a Certificate is Issued for an application or device, the application or device does not directly contract with Open Banking Limited. The Subscribing PKI Participant therefore agrees to the terms of this Open Banking Certificate Policy on behalf of the Certificate Subject and operates in accordance with this Open Banking Certificate Policy, Open Banking Subscribing PKI Participant Agreement and associated Public Key Infrastructure practices

1.3.5 RELYING PKI PARTICIPANTS

A Relying PKI Participant is an End Entity that does not necessarily hold a Certificate but even so, may rely on a Certificate and/or Digital Signature(s) created using that Certificate.

Eligible Relying-Parties for Certificates Issued under this Open Banking Certificate Policy are specified in Section 16 of the Open Banking PKI Disclosure Statement.

1.3.6 OTHER PARTIES

1.3.6.1 POLICY AUTHORITY

The Open Banking Policy Authority has ultimate responsibility for governance and control over the Issuance, management and usage of Certificates issued under this Open Banking Certificate Policy. Simply stated, the Open Banking Policy Authority is the entity that sets the rules under which the Public Key Infrastructure is to be operated.

The Open Banking Policy Authority is identified in Section 1 of the Open Banking PKI Disclosure Statement.

1.3.6.2 REPOSITORY

A Repository is a Party that holds data in support of Public Key Infrastructure operations. This includes Certificate Policy and related documentation, Certificates and Certificate Status information.

The Open Banking Repository provides a community-wide accessible mechanism by which primarily Subscribing PKI Participants and Relying PKI Participants can obtain and validate information on Certificates Issued under this Open Banking Certificate Policy.

The Open Banking Issuing Authority has approved the Repositories identified in section 14 of the Open Banking PKI Disclosure Statement to provide these services.

1.3.6.3 CERTIFICATE USAGE

Certificate usage is controlled by the Certificate Profile. This is a function of the issuing Certificate Authority and each profile is formally approved by the Open Banking Policy Authority before implementation.

1.4 CERTIFICATE USAGE

1.4.1 APPROPRIATE CERTIFICATE USES

The categories of transactions, applications, or purposes for which Certificates Issued under this Open Banking Certificate Policy may be used are defined in Section 2 of the Open Banking PKI Disclosure Statement.

1.4.2 PROHIBITED CERTIFICATE USES

All other application use and any other usage categories for Certificates Issued under this Open Banking Certificate Policy is prohibited as described in Section 2 of the Open Banking PKI Disclosure Statement

1.5 POLICY ADMINISTRATION

1.5.1 ORGANISATION ADMINISTERING THE DOCUMENT

The Open Banking Policy Authority is responsible for approving rights, obligations, liabilities and all other terms and conditions contained in this Open Banking Certificate Policy.

The Open Banking Issuing Authority is responsible for this Certification Policy, its management and change control. Contact details are listed in Section 1 of the Open Banking PKI Disclosure Statement.

Entrust Limited is authorised by Open Banking Limited to administer this Open Banking Certificate Policy.

1.5.2 CONTACT PERSON

In the first instance, Open Banking Limited should be contacted regarding the contents of this Open Banking Certificate Policy.

Contact details are provided in Section 1 of the Open Banking PKI Disclosure Statement.

1.5.3 PERSON DETERMINING CPS SUITABILITY FOR THE POLICY

The Open Banking Policy Authority determines the suitability of any Certification Practice Statement operating under this Open Banking Certificate Policy.

In the first instance, Open Banking Limited should be contacted regarding the inclusion of additional Certification Authorities to operate within this Public Key Infrastructure or interoperation with other PKIs.

Contact details are provided in Section 1 of the Open Banking PKI Disclosure Statement.

1.5.4 CPS APPROVAL PROCEDURES

The Open Banking Policy Authority determines the suitability and approves the use of any Certification Practice Statement which is used to support this Open Banking Certificate Policy.

1.6 DEFINITIONS AND ACRONYMS

Definitions of the terms used in this Open Banking Certificate Policy are detailed in the Open Banking Definitions of Terms at http://ob.trustis.com/production/policies/.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 REPOSITORIES

An information Repository shall be made available under the terms of this Open Banking Certificate Policy. Details of this Open Banking Repository are set forth in this Open Banking Certificate Policy. The Open Banking Issuing Authority makes Certificate Status Information available via an Open Banking Repository in accordance with this Open Banking Certificate Policy.

2.2 PUBLICATION OF CERTIFICATION INFORMATION

The Open Banking Repository publishes the following information on behalf of the Open Banking Issuing Authority:

- This Open Banking Certificate Policy with its associated Open Banking PKI Disclosure Statement.
- Any supporting policy documents and agreements.
- The information that will allow the authenticity of the Certificate of the Open Banking Issuing Authority to be verified.
- All Certificate Authority Certificates Issued by the Open Banking Issuing Authority.
- Certificate Status Information for Certificates Issued under this Open Banking Certificate Policy.

The location for electronic access to information published by the Open Banking Repository is included in the Certificates issued in accordance with this Open Banking Certificate Policy.

2.3 TIME OR FREQUENCY OF PUBLICATION

Information as listed in 2.2 shall be published promptly upon its creation, with the exception that if Certificate Revocation Lists are used to provide Revocation information, they shall be published according to section 4.9.7 and 4.9.8 of this Open Banking Certificate Policy.

2.4 ACCESS CONTROLS ON REPOSITORIES

The Open Banking Repository must make available the information specified in section 2.2. However, the Open Banking Repository may control access to information and restrict access to those Parties with specific need for the information.

The Open Banking Repository shall not prevent access by Parties where required by this Open Banking Certificate Policy.

3 IDENTIFICATION AND AUTHENTICATION

3.1 NAMING

3.1.1 TYPES OF NAMES

Each Certificate Subject must have a clearly distinguishable and unique X.501 Distinguished Name (DN) in the Certificate subjectName field of Certificates Issued under this Open Banking Certificate Policy and in accordance with IETF RFC 5280 (https://tools.ietf.org/html/rfc5280).

3.1.2 NEED FOR NAMES TO BE MEANINGFUL

The contents of each Certificate Subject name field must have an association with the authenticated name of the Certificate Subject. The natural identity of the Certificate Subject is required to be hidden.

3.1.3 ANONYMITY OR PSEUDONYMITY OF SUBSCRIBING PKI PARTICIPANTS

Pseudonymity of Subscribing PKI Participants is required under this Open Banking Certificate Policy. The anonymity of Subscribing PKI Participants is not permitted.

3.1.4 RULES FOR INTERPRETING VARIOUS NAME FORMS

The interpretation for any entity shall be as follows:

Element	Description
Common Name	For Subscribing PKI Participants, the Common Name shall consist of a random value generated automatically by Open Banking Limited. For Certificate Authority Certificates the

	Common Name field shall contain the name of the Certificate Authority.
Organisational Unit	For Subscribing PKI Participants the Organisational Unit field shall consist of a pseudonymous random value generated automatically by Open Banking Limited to represent the Subscribing PKI Participant organisation. For Certificate Authority Certificates the Organisational Unit Name field shall not be used.
Organisation	The Organisation field shall contain text to identify this Certificate as part of the Open Banking Ecosystem.

3.1.5 UNIQUENESS OF NAMES

Name uniqueness will be interpreted as per section 3.1.4 of this Open Banking Certificate Policy.

3.1.6 RECOGNITION, AUTHENTICATION, AND ROLE OF TRADEMARKS

Open Banking Limited is not liable for the inclusion of trademarks, trade names or other information under restricted use.

The Open Banking Subscribing PKI Participant Agreement shall require Subscribing PKI Participants to warrant legitimacy of their registration details provided to the Open Banking Issuing Authority as part of the Open Banking Enrolment and Certificate request processes.

3.2 INITIAL IDENTITY VALIDATION

3.2.1 METHOD TO PROVE POSSESSION OF PRIVATE KEY

The registration and/or Issuance process shall involve a stage in which the Subscribing PKI Participant demonstrates possession of the Private Key. Technical means employed to ensure possession of Private Keys will be PKCS#10 (https://tools.ietf.org/html/rfc2986), other equivalent cryptographic mechanism or using a process specifically approved by the Open Banking Issuing Authority.

3.2.2 AUTHENTICATION OF ORGANISATION IDENTITY

All Subscribing PKI Participant organisations shall be subject to specific checks by Open Banking Limited or other party approved by Open Banking Limited to establish their identity to a substantial degree of assurance.

Open Banking Limited shall define and document or otherwise approve the mechanisms used to support the level of organisation identity Authentication assurance required.

3.2.3 AUTHENTICATION OF INDIVIDUAL IDENTITY

All Subscribing PKI Participant Primary Technical Contacts with responsibility for Certificate management activities shall be subject to face-to-face Authentication by the Open Banking Enrolment team or other party approved by Open Banking Limited to establish their identity.

Individual identity Authentication shall be carried out in accordance with UK Government GPG 45 (https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual) Level of Assurance 2.

Open Banking Limited shall define and document or otherwise approve the mechanisms used to support the level of individual Authentication assurance required.

3.2.4 NON-VERIFIED SUBSCRIBING PKI PARTICIPANT INFORMATION

Non-verified information shall not be included in Certificates governed by this Open Banking Certificate Policy.

3.2.5 VALIDATION OF AUTHORITY

Validation of authority (i.e. the determination of whether a Subscribing PKI Participant has specific rights, entitlements, or permissions, including the permission to act on behalf of an organisation to obtain a Certificate) is the responsibility of Open Banking Limited or other party approved by Open Banking Limited.

Open Banking Limited shall define and document or otherwise approve the mechanisms used to validate authority.

3.2.6 CRITERIA FOR INTEROPERATION

The criteria by which another Certification Authority wishing to operate within, or interoperate with the Public Key Infrastructure governed by this Open Banking Certificate Policy, will be defined by the Open Banking Policy Authority. The Open Banking Policy Authority will also determine whether any specific Certification Authority is approved for interoperation.

Requests for interoperation must be directed in the first instance to Open Banking Limited, whose contact details are given in Section 1 of the Open Banking PKI Disclosure Statement**.**

3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1 IDENTIFICATION AND AUTHENTICATION FOR ROUTINE RE-KEY

Re-key of Certificates governed by this Open Banking Certificate Policy is permitted.

For Subscribing PKI Participants, Re-key requests shall be under the control of Subscribing PKI Participant Primary Technical Contacts Authenticated in accordance with 3.2.3 and holding authorisation to submit such requests.

3.3.2 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY AFTER REVOCATION

Where a Certificate has been Revoked by a Subscribing PKI Participant, a Certificate Re-Key request may be submitted if the Subscribing PKI Participant's Primary Technical Contact Authentication status made in accordance with 3.2.3. is valid and they retain authorisation to submit such requests.

Where a Certificate has been Revoked by the Open Banking Issuing Authority, the Open Banking Issuing Authority has the sole discretion to remove the Subscribing PKI Participant's Primary Technical Contact's authorisation to submit further Certificate requests. Re-key after such an event must at a minimum include the Identification and Authentication of the requester to at least the Authentication standards defined in section 3.2.3.

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

Revocation requests must at a minimum include the Identification and Authentication of the requester and sufficient information to uniquely identify the Certificate to be Revoked. Valid proof of possession of the Private Key associated with the Certificate to be Revoked is permitted as Authentication.

The risk for fraudulent misuse of a Private Key associated with a Certificate to be Revoked must be recognised.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 CERTIFICATE APPLICATION

4.1.1 WHO CAN SUBMIT A CERTIFICATE APPLICATION

Certificate applications may be made by Subscribing PKI Participant's Primary Technical Contacts Authenticated in accordance with 3.2.3. and holding authorisation to submit such requests.

Subscribing PKI Participants must comply with the procedures described in this document. Eligible Subscribing PKI Participants are specified in Section 15 of the Open Banking PKI Disclosure Statement.

4.1.2 ENROLMENT PROCESS AND RESPONSIBILITIES

The Open Banking Registration Authority shall define the specific processes associated with a particular Certificate enrolment mechanism. In all cases enrolment processes shall include:

- Provision of accurate information in support of Authentication (and validation of a Certificate Subject or representative of an organisation if applicable).
- Acceptance of the Open Banking Subscribing PKI Participant Agreement by the Subscribing PKI Participant.
- Compliance with this Open Banking Certificate Policy and obligations of Subscribing PKI Participants as defined in Section 4 of the Open Banking PKI Disclosure Statement.

4.1.2.1 REGISTRATION AUTHORITIES AND THEIR REPRESENTATIVES

The Issuance of Certificates to Open Banking Registration Authority staff for the purpose of accessing any Open Banking Registration Authority facilities shall require approval by the Open Banking Issuing Authority or other party approved by the Open Banking Issuing Authority. See section 3.2.3.

4.2 CERTIFICATE APPLICATION PROCESSING

4.2.1 PERFORMING IDENTIFICATION AND AUTHENTICATION FUNCTIONS

The Open Banking Local Registration Authority is permitted to conduct Authentication of Certificate Applicants.

4.2.2 APPROVAL OR REJECTION OF CERTIFICATE APPLICATIONS

The Open Banking Local Registration Authority shall verify that each Certificate Applicant has a right to obtain that Certificate and, if the Certificate identifies that the Certificate Subject has particular attributes or privileges, that they are valid.

The Open Banking Issuing Authority shall define and document the mechanisms used to support the level of Authentication assurance.

The Open Banking Local Registration Authority will either approve or reject a Certificate application.

Where an application fails to achieve the specified Authentication requirements or the level of assurance of Authentication cannot be met a Certificate application will be rejected.

Where approved, the Certificate application will be digitally signed for processing by the Certificate Manufacturer.

Where a Certificate application is rejected, the reasons for rejection may be given to the prospective Applicant.

4.2.3 TIME TO PROCESS CERTIFICATE APPLICATIONS

No stipulation.

4.3 CERTIFICATE ISSUANCE

4.3.1 CA ACTIONS DURING CERTIFICATE ISSUANCE

Certificates shall be Issued automatically by the Certificate Manufacturer only in response to a properly constructed, signed and validated Certificate request from the Open Banking Local Registration Authority. Only an approved Open Banking Local Registration Authority system can communicate with the associated Certificate Authority to submit a Certificate request.

4.3.2 NOTIFICATION TO SUBSCRIBING PKI PARTICIPANT BY THE CA OF ISSUANCE OF CERTIFICATE

The Certificate Manufacturer (or Certificate Authority) does not communicate with the Subscribing PKI Participant (Certificate Subject) regarding Certificate Issuance. The Local Registration Authority is responsible for such notification where applicable.

4.4 CERTIFICATE ACCEPTANCE

4.4.1 CONDUCT CONSTITUTING CERTIFICATE ACCEPTANCE

The Issuing Authority shall ensure that the terms and conditions stipulated in this Open Banking Certificate Policy, associated Open Banking Subscribing PKI Participant Agreement and any other applicable obligations are made available to the Subscribing PKI Participant during or prior to the application for a Certificate, or during the delivery of a Certificate.

A Subscribing PKI Participant must acknowledge that it agrees to the terms and conditions stipulated in this Open Banking Certificate Policy and associated Open Banking Subscribing PKI Participant Agreement upon acceptance of a Certificate.

The Open Banking Issuing Authority shall inform the Subscribing PKI Participant that upon receipt of a Certificate Issued under this Open Banking Certificate Policy, a Subscribing PKI Participant agrees to, and warrants, that at the time of Certificate acceptance and throughout the operational period of the Certificate, until notified otherwise by the Subscribing PKI Participant:

- No unauthorised person has ever had access to the Subscribing PKI Participant's Private Key.
- All information given by the Subscribing PKI Participant to the Open Banking Issuing Authority or Open Banking Local Registration Authority is true and accurate.

The above stipulations may be integrated with the Certificate application process.

4.4.2 PUBLICATION OF THE CERTIFICATE BY THE CA

The Certificate Manufacturer may publish the Issued Certificate in a Repository at the location specified by the Issuing Authority. This repository may be subject to access restrictions.

Further “publication” of the Certificate is permitted. Details of approved Repositories are provided in Section 14 of the Open Banking PKI Disclosure Statement.

4.4.3 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

The Certificate Manufacturer does not directly inform any other parties of the Issuance of a Certificate.

Notification of Certificate Issuance, by inclusion into a directory or other mechanism for Certificate Discovery is permitted.

4.5 KEY PAIR AND CERTIFICATE USAGE

4.5.1 SUBSCRIBING PKI PARTICIPANT PRIVATE KEY AND CERTIFICATE USAGE

Subscribing PKI Participants must ensure that use of the Private Key associated with the Certificate is consistent with the usage restrictions in the Certificate as stipulated and published by the Open Banking Issuing Authority.

4.5.2 RELYING PKI PARTICIPANT PUBLIC KEY AND CERTIFICATE USAGE

A Relying PKI Participant may only rely on a Subscribing PKI Participant’s Public Key and Certificate for the specific functions stipulated and published by the Open Banking Issuing Authority.

Relying PKI Participants must satisfy the requirements for reliance on a Certificate defined in Section 5 of the Open Banking PKI Disclosure Statement.

4.6 CERTIFICATE RENEWAL

4.6.1 CIRCUMSTANCE FOR CERTIFICATE RENEWAL

Certificates may be Renewed at any time during their Operational Period.

Renewal of Revoked certificates must involve Re-key and shall be carried out in accordance with 3.3.2.

Unless specifically and expressly approved by the Open Banking Issuing Authority Renewal shall incorporate Re-key of the Certificate.

4.6.2 WHO MAY REQUEST RENEWAL

Renewal requests may be made by Subscribing PKI Participant Primary Technical Contacts Authenticated in accordance with 3.2.3. and holding authorisation to submit such requests.

Renewal requests shall be made via the Open Banking Local Registration Authority.

4.6.3 PROCESSING CERTIFICATE RENEWAL REQUESTS

The Open Banking Local Registration Authority will either approve or reject an application for Certificate Renewal.

Certificate renewals are automatically processed by the Certificate Manufacturer in response to a properly constructed and signed Certificate request from the Open Banking Local Registration Authority.

Extension of validity of a Key Pair beyond the initial validity period of the Key Pair, as defined by the expiry date field of the Issued Certificate is not permitted.

4.6.4 NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBING PKI PARTICIPANT

As specified in Section 4.3.2.

4.6.5 CONDUCT CONSTITUTING ACCEPTANCE OF A RENEWAL CERTIFICATE

As specified in Section 4.4.1.

4.6.6 PUBLICATION OF THE RENEWAL CERTIFICATE BY THE CA

As specified in Section 4.4.2.

4.6.7 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

As specified in Section 4.4.3.

4.7 CERTIFICATE RE-KEY

4.7.1 CIRCUMSTANCE FOR CERTIFICATE RE-KEY

Re-key of Certificates is permitted at any time during their Operational Period.

Re-key of revoked certificates shall be carried out in accordance with 3.3.2.

4.7.2 WHO MAY REQUEST CERTIFICATION OF A NEW PUBLIC KEY

Re-key requests may be made by Subscribing PKI Participant Primary Technical Contacts Authenticated in accordance with 3.2.3. and holding authorisation to submit such requests.

4.7.3 PROCESSING CERTIFICATE RE-KEYING REQUESTS

The Open Banking Local Registration Authority will either approve or reject an application for Re-key of a Certificate.

Certificate Re-key requests are automatically processed by the Certificate Manufacturer in response to a properly constructed and signed Certificate request from the Open Banking Local Registration Authority.

4.7.4 NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBING PKI PARTICIPANT

As specified in Section 4.3.2.

4.7.5 CONDUCT CONSTITUTING ACCEPTANCE OF A RE-KEYED CERTIFICATE

Acceptance of a Re-keyed Certificate is the same as that for Issued Certificates. See Section 4.4.1.

4.7.6 PUBLICATION OF THE RE-KEYED CERTIFICATE BY THE CA

As specified in Section 4.4.2.

4.7.7 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

As specified in Section 4.4.3.

4.8 CERTIFICATE MODIFICATION

4.8.1 CIRCUMSTANCE FOR CERTIFICATE MODIFICATION

Certificate modification is not permitted. Changes to Certificates must be enacted via Issuance of a new Certificate or one of the approved processes specified in this Open Banking Certificate Policy.

4.8.2 WHO MAY REQUEST CERTIFICATE MODIFICATION

See Section 4.8.1.

4.8.3 PROCESSING CERTIFICATE MODIFICATION REQUESTS

See Section 4.8.1.

4.8.4 NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBING PKI PARTICIPANT

See Section 4.8.1.

4.8.5 CONDUCT CONSTITUTING ACCEPTANCE OF MODIFIED CERTIFICATE

See Section 4.8.1.

4.8.6 PUBLICATION OF THE MODIFIED CERTIFICATE BY THE CA

See Section 4.8.1.

4.8.7 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

See Section 4.8.1.

4.9 CERTIFICATE REVOCATION AND SUSPENSION

Certificate Status Information services shall identify all Revoked Certificates at least until their assigned Validity Period expires.

Upon Revocation of a Subscribing PKI Participant's Certificate, the Open Banking Issuing Authority shall undertake to inform the Subscribing PKI Participant.

4.9.1 CIRCUMSTANCES FOR REVOCATION

The circumstances under which Certificate Revocation may be requested (and carried out) is defined by the Open Banking Issuing Authority and published as appropriate. The Open Banking Local Registration Authority is responsible for the implementation of the decision of the Open Banking Issuing Authority.

The Open Banking Local Registration Authority must conduct verification of Revocation requests in accordance with this Open Banking Certificate Policy. See Section 3.4.

A Certificate must be Revoked:

- When any of the information in the Certificate is known or suspected to be inaccurate.
- Upon suspected or known compromise of the Private Key associated with the Certificate.
- Upon suspected or known compromise of the media holding the Private Key associated with the Certificate.
- When the Subscribing PKI Participant withdraws from or is no longer eligible to participate in the Public Key Infrastructure governed by this Open Banking Certificate Policy.

A Certificate may be revoked by the Open Banking Issuing Authority:

- Upon suspected or known misuse or fraudulent use of the Certificate.
- For reasons related to regulatory or legal requirements including but not limited to changes in legislation.

4.9.2 WHO CAN REQUEST REVOCATION

Manually initiated Revocation requests will only be accepted from Subscribing PKI Participants Authenticated in accordance with section 3.4 of this Open Banking Certificate Policy.

Automated Revocation requests are initiated by Open Banking Limited via the Open Banking Local Registration Authority.

4.9.3 PROCEDURE FOR REVOCATION REQUEST

Revocation must be requested promptly after detection of a compromise or any other event giving cause for Revocation.

An automated revocation request initiated by the withdrawal of a Subscribing PKI Participant's authority to hold a Certificate shall be processed automatically by the Open Banking Local Registration Authority.

A manual Revocation request may be initiated by a telephone call to the Open Banking Manual Registration Authority. Any such request shall be subject to strong Authentication using a mechanism defined by the Open Banking Issuing Authority.

Certificate Revocations are automatically processed by the Certificate Manufacturer in response to a properly constructed and signed Revocation instruction from the Open Banking Local Registration Authority.

4.9.4 REVOCATION REQUEST GRACE PERIOD

None. If the Revocation request is approved, it must be reflected in the next publication of Certificate Status Information.

4.9.5 TIME WITHIN WHICH CA MUST PROCESS THE REVOCATION REQUEST

The time to process a Certificate Revocation request is made up of two elements:

- The time for the Certificate Revocation request to be validated, approved and action taken by the Open Banking Manual Registration Authority or Subscribing PKI Participant. This time is not constrained but the Open Banking Manual Registration Authority or Subscribing PKI Participant must take all reasonable steps to conduct the Revocation procedure expeditiously.
- The time taken for the Certificate Manufacturer to respond to the authorised Certificate Revocation request. The Certificate Manufacturer must respond promptly to authorised Revocation requests. The maximum time taken for this element is determined by the Open Banking Issuing Authority in its contract with the Certificate Manufacturer.

4.9.6 REVOCATION CHECKING REQUIREMENT FOR RELYING PKI PARTICIPANTS

The mechanisms, if any, that a Relying PKI Participant may use (or where defined in Section 5 of the Open Banking PKI Disclosure Statement) in order to check the Certificate Status Information of the Certificate upon which they wish to rely, must be via a Certificate Revocation List or equivalent on-line protocol that permits authenticity and integrity of the Status Information to be verified. Specific mechanisms are defined in Section 17 of the Open Banking PKI Disclosure Statement.

4.9.7 CRL ISSUANCE FREQUENCY (IF APPLICABLE)

The frequency of Certificate Revocation List Issuance is defined in Section 17 of the Open Banking PKI Disclosure Statement.

4.9.8 MAXIMUM LATENCY FOR CRLS (IF APPLICABLE)

No stipulation.

4.9.9 ON-LINE REVOCATION/STATUS CHECKING AVAILABILITY

The availability of on-line Certificate Status checking is published by the Open Banking Issuing Authority in Section 17 of the Open Banking PKI Disclosure Statement.

4.9.10 ON-LINE REVOCATION CHECKING REQUIREMENTS

The requirements on Relying PKI Participants to perform on-line Certificate Status checking are defined in Section 5 of the Open Banking PKI Disclosure Statement.

4.9.11 OTHER FORMS OF REVOCATION ADVERTISEMENTS AVAILABLE

The availability of other forms of Revocation advertisement is published by the Open Banking Issuing Authority in Section 17 of the Open Banking PKI Disclosure Statement.

4.9.12 SPECIAL REQUIREMENTS RE KEY COMPROMISE

In the event of the compromise, or suspected compromise, of any End Entity's Private Key, an End Entity must notify the Open Banking Issuing Authority immediately and must indicate the nature and circumstances of the compromise, to the fullest extent known.

4.9.13 CIRCUMSTANCES FOR SUSPENSION

This Open Banking Certificate Policy does not support Suspension of Subscribing PKI Participant Certificates.

4.9.14 WHO CAN REQUEST SUSPENSION

See Section 4.9.13.

4.9.15 PROCEDURE FOR SUSPENSION REQUEST

See Section 4.9.13.

4.9.16 LIMITS ON SUSPENSION PERIOD

See Section 4.9.13.

4.10 CERTIFICATE STATUS SERVICES

4.10.1 OPERATIONAL CHARACTERISTICS

The types of Certificate Status checking services made available to the Subscribing PKI Participant by the Open Banking Repository are defined in Section 17 of the Open Banking PKI Disclosure Statement.

4.10.2 SERVICE AVAILABILITY

The availability of any Certificate Status checking services that are available to Relying PKI Participants is, if applicable, published in Section 17 of the Open Banking PKI Disclosure Statement.

4.10.3 OPTIONAL FEATURES

The optional features of any Certificate Status checking services that are available to the Relying PKI Participants, if applicable, are published in Section 17 of the Open Banking PKI Disclosure Statement.

4.11 END OF SUBSCRIPTION

Subscribing PKI Participants - at the end of Certificate subscription, the relevant Certificates may either be Revoked or permitted to expire. The decision on which action to take is made by and implemented by the Open Banking Issuing Authority.

Service Termination - The actions to be taken in the event of the termination of the service will be defined in the contract between the Open Banking Issuing Authority, Certificate Manufacturer and any other Parties providing the Service.

4.12 KEY ESCROW AND RECOVERY

4.12.1 KEY ESCROW AND RECOVERY POLICY AND PRACTICES

Parties providing Trust Services shall not offer or support any form of Key escrow.

Subscribing PKI Participants may facilitate Key escrow or recovery mechanisms locally.

4.12.2 SESSION KEY ENCAPSULATION AND RECOVERY POLICY AND PRACTICES

This Open Banking Certificate Policy does not prescribe or control session Key management for applications. Use of session Key management is a matter for Subscribing PKI Participants.

The Open Banking Issuing Authority does not offer or support any form of session Key encapsulation.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

Where “no stipulation” is stated in this section of this Open Banking Certificate Policy it indicates there are no specific prescribed requirements for the controls, configuration or security requirements.

Where not stipulated, specific details on controls operated for components of the Public Key Infrastructure must be detailed in the Certification Practice Statement and/or supporting documentation.

Controls must be approved by the Open Banking Issuing Authority.

5.1 PHYSICAL CONTROLS

5.1.1 SITE LOCATION AND CONSTRUCTION

Sites where Certificate manufacture or Time-stamping operations are carried out must:

- Satisfy the requirements specified by tScheme for Certificate Generation.
- Be manually or electronically monitored for unauthorised intrusion at all times.
- Apply controls such that unescorted access to Certificate Authorities or Time-stamping servers is limited to authorised personnel.
- Ensure unauthorised personnel are properly escorted and supervised.
- Ensure a site access log is maintained and inspected periodically.
- Ensure all removable media and paper containing sensitive plain text information is stored in secure containers.

For Open Banking Registration Authorities permitted to submit on-line requests for Certificate Issuance, Renewal/Re-key or Revocation, the Open Banking Issuing Authority shall ensure they provide appropriate security protection for credentials involved in the Authentication and authorisation of the request.

All Open Banking Repository sites must be located in areas that at a minimum satisfy the requirements for ISO 27001.

Where PINs, pass-phrases or passwords are recorded, they must be stored in a security container accessible only to authorised personnel.

5.1.2 PHYSICAL ACCESS

See section 5.1.1.

5.1.3 POWER AND AIR CONDITIONING

No stipulation.

5.1.4 WATER EXPOSURES

No stipulation.

5.1.5 FIRE PREVENTION AND PROTECTION

No stipulation.

5.1.6 MEDIA STORAGE

Controls must be placed on all media used for the storage of information such as Keys, Activation Data, confidential Subscribing PKI Participant information or Certificate Authority information. Controls must be detailed in the Certification Practice Statement and/or supporting documentation.

5.1.7 WASTE DISPOSAL

All media used for the storage of information such as Keys, Activation Data, confidential Subscribing PKI Participant information or Certificate Authority files is to be sanitised or destroyed before released for disposal.

5.1.8 OFF-SITE BACKUP

Off site backup arrangements must be in place as required by the business continuity arrangements outlined in Section 5.7

Where data and facilities are removed from primary locations or in support of business continuity activities, controls must be applied which are at least comparable with those of the primary location.

5.2 PROCEDURAL CONTROLS

5.2.1 TRUSTED ROLES

A Party providing Trust Services must ensure a separation of duties for critical functions to prevent a single person from maliciously using Certificate Authority systems and supporting systems without detection.

The Certificate Manufacturer shall provide for the separation of distinct Public Key Infrastructure personnel roles by named personnel, distinguishing between day-to-day operation of the system and the management and audit of those operations. To the greatest extent possible, differing levels of physical and systems access control based on roles and responsibilities shall be employed to reflect the requirements of those roles and responsibilities. Controls must be detailed in the Certification Practice Statement and/or supporting documentation.

Open Banking Registration Authorities must ensure that all personnel are adequately trained and understand their responsibility for the Identification and Authentication of prospective Subscribing PKI Participants and related Certificate management tasks. Open Banking Registration Authorities shall document arrangements for trusted roles in their policy and procedures and/or supporting documentation. Arrangements must be approved by the Open Banking Issuing Authority or auditors acting on its behalf.

An Open Banking Registration Authority may permit all roles and duties for that Registration Authority to be performed by one individual.

5.2.2 NUMBER OF PERSONS REQUIRED PER TASK

Multi-person control is required for Certificate Authority Key generation.

Multi-person controls must be established for the performance of critical functions associated with the build and management of Certificate Authority systems, including the software controlling Certificate Manufacturer operations.

All other duties associated with Certificate Manufacture or Parties providing other Trust Services may be performed by an individual operating alone, however, verification processes employed must provide for oversight of all activities performed by trusted role holders.

5.2.3 IDENTIFICATION AND AUTHENTICATION FOR EACH ROLE

All Parties providing Trust Services shall ensure personnel in trusted roles have their identity and authorisation verified before they are:

- Included in the access list for the site of the Party providing Trust Services.
- Included in the access list for physical access to the Trust Service provider systems.
- Given a credential for the performance of their Trust Service provider role.
- Given an access on Trust Service provider systems.

Credentials issued to personnel in trusted roles must be:

- Managed so that their use can be detected and monitored.
- Managed so that their use is restricted to actions authorised for that role through applicable technical and procedural controls.
- Maintained under a prescribed and documented security policy.

5.2.4 ROLES REQUIRING SEPARATION OF DUTIES

For the Certificate Manufacturer, roles requiring the separation of duties are not specifically prescribed. The assignment of duties among personnel shall maintain appropriate separation of duties so as not to compromise the security arrangements for Certificate Manufacturing and other critical processes. The Certificate Manufacturer shall provide and maintain records of role allocation.

Other Parties providing Trust Services shall maintain appropriate separation of duties so as not to compromise the security arrangements for critical processes.

5.3 PERSONNEL CONTROLS

5.3.1 QUALIFICATIONS, EXPERIENCE, AND CLEARANCE REQUIREMENTS

A Party providing Trust Services must ensure that all personnel performing duties with respect to its operation must:

- Be appointed in writing.
- Be bound by contract or statute to the terms and conditions of the position they are to fill.
- Have received training with respect to the duties they are to perform.
- Be bound by statute or contract not to disclose sensitive security-relevant information or Subscribing PKI Participant information and maintain required protection of personal information.
- Not be assigned duties that may cause a conflict of interest with their service provision duties.
- Not have been, as far as known, previously relieved of a past assignment for reasons of negligence or non-performance of duties.

Parties providing Trust Services may also specify additional criteria for security clearance of personnel, such as requirements for citizenship, rank, qualifications, satisfactory credit check, and absence of a criminal record. Any such additional requirements shall be stated in the Certification Practice Statement and/or supporting documentation.

5.3.2 BACKGROUND CHECK PROCEDURES

See Section 5.3.1.

5.3.3 TRAINING REQUIREMENTS

See Section 5.3.1.

5.3.4 RETRAINING FREQUENCY AND REQUIREMENTS

No stipulation.

5.3.5 JOB ROTATION FREQUENCY AND SEQUENCE

No stipulation.

5.3.6 SANCTIONS FOR UNAUTHORIZED ACTIONS

No stipulation.

5.3.7 INDEPENDENT CONTRACTOR REQUIREMENTS

A Party providing Trust Services must ensure that contractor access to its facilities is in accordance with this Open Banking Certificate Policy. Individuals not security cleared must be under supervision by approved personnel at all times.

The actions of contracting staff are subject to the same audit arrangements and requirements as those of the personnel of the Party providing Trust Services.

5.3.8 DOCUMENTATION SUPPLIED TO PERSONNEL

All personnel associated with Trust Service provision shall be provided access to all documentation relevant to their position. This will include the Certificate Policies and associated Certification Practice Statements relevant to the service, together with any specific supporting documentation, statutes, policies or contracts relevant to the position and role of the personnel.

5.4 AUDIT LOGGING PROCEDURES

5.4.1 TYPES OF EVENTS RECORDED

Certificate Manufacturer - Audit logs of all transactions relevant to Certificate creation, Certificate lifecycle management and the operation of trusted systems and services must be maintained to provide an audit trail. The event types are at a minimum:

- Messages received from authorised sources requesting an action on the part of the Certificate Authority.
- All actions taken in response to requests.
- Trusted system installation and any modifications.
- Receipt, servicing and shipping of hardware cryptographic modules.
- Creation and issuance of Certificate Revocation Lists.
- All error conditions and anomalies associated with the operation of trusted systems and services.
- Any known or suspected violations of physical security.
- Any known or suspected violations of network and/or trusted system security.
- All Certificate Authority and trusted application start-up and shutdown.
- All usage of the Certificate Authority signing Key.
- All personnel/role changes for trusted roles.

Registration Authority Server – must record for audit purposes, at a minimum the event types listed below:

- Any log on/off attempts by Registration Authority Server operators
- All messages from authorised sources requesting an action of the Registration Authority Server and the subsequent actions taken by the Registration Authority Server in response to such requests.
- All messages to the Certificate Authority requesting an action of the Certificate Authority and the subsequent action taken by the Certificate Authority.
- All physical accesses to Registration Authority Server systems (including components) and locations.
- Registration Authority Server application start-up and shut down.
- All use of the Registration Authority Server signing key(s).
- Any suspected or known violations of physical security.
- Any suspected or known violations of network and system security.
- All checks made for the registration of Registration Authority Server staff.
- All personnel/role changes for trusted roles.

Open Banking Local Registration Authority – must record for audit purposes, at a minimum the event types listed below:

- All messages from authorised sources requesting an action of the Open Banking Local Registration Authority and the subsequent actions taken by the Open Banking Local Registration Authority in response to such requests.
- All messages to the Certificate Authority requesting an action of the Certificate Authority and the subsequent responses from the Certificate Authority.
- All physical accesses to Open Banking Local Registration Authority systems (including components) and locations.
- Open Banking Local Registration Authority application start-up and shut down.
- All use of the Open Banking Local Registration Authority signing Key(s).
- Any suspected or known violations of physical security.
- Any suspected or known violations of network and system security.
- All checks made for the registration of Open Banking Local Registration Authority staff.
- All personnel/role changes for trusted roles.

Registration Authorities must retain records of information provided in support of Certificate application and Revocation requests.

5.4.2 FREQUENCY OF PROCESSING LOG

Parties providing Trust Services shall review audit logs as appropriate to the items being recorded.

The Party shall provide details of audit log processing in the records of role allocation in the Certification Practice Statement and/or supporting documentation. Procedures must be approved by the Open Banking Issuing Authority or auditors acting on its behalf.

5.4.3 RETENTION PERIOD FOR AUDIT LOG

Audit logs are to be retained for a period of no less than six (6) years.

5.4.4 PROTECTION OF AUDIT LOG

Electronic audit log systems must include mechanisms to protect the log files from unauthorised viewing, modification, and deletion. Manual audit information must be protected from unauthorised viewing, modification and destruction.

5.4.5 AUDIT LOG BACKUP PROCEDURES

Audit logs and audit summaries must be backed up or if in manual form, must be copied.

Such backups must be provided with the same level of security as the originals and must be commensurate with the data contained within them.

5.4.6 AUDIT COLLECTION SYSTEM (INTERNAL VS. EXTERNAL)

No stipulation.

5.4.7 NOTIFICATION TO EVENT-CAUSING SUBJECT

No stipulation.

5.4.8 VULNERABILITY ASSESSMENTS

No stipulation.

5.5 RECORDS ARCHIVAL

5.5.1 TYPES OF RECORDS ARCHIVED

The event records and any accompanying data as described in section 5.4.1 of this Open Banking Certificate Policy are to be archived.

Parties providing Trust Services may also be required to retain additional information to ensure compliance with this Open Banking Certificate Policy and/or legal requirements.

All Registration Authorities must retain records of information provided in support of Certificate application and Revocation requests.

5.5.2 RETENTION PERIOD FOR ARCHIVE

Archived information is to be retained for a period of no less than six (6) years

5.5.3 PROTECTION OF ARCHIVE

Archived information is to be retained for a period of no less than six (6) years

5.5.4 ARCHIVE BACKUP PROCEDURES

No stipulation.

5.5.5 REQUIREMENTS FOR TIME-STAMPING OF RECORDS

No stipulation.

5.5.6 ARCHIVE COLLECTION SYSTEM (INTERNAL OR EXTERNAL)

No stipulation.

5.5.7 PROCEDURES TO OBTAIN AND VERIFY ARCHIVE INFORMATION

Parties providing Trust Services shall comply with the confidentially requirements specified in this Open Banking Certificate Policy (see section 9.3).

Records of individual transactions may be released upon request by any of the Parties involved in the transaction, or their recognised representatives.

Parties providing Trust Services shall ensure availability of their archives and that archived information is stored in a readable format during its retention period, even if the Trust Service Provider's operations are interrupted, suspended or terminated.

In the event that the services of a Party providing Trust Services for or on behalf of the Open Banking Issuing Authority are to be interrupted, suspended or terminated, the Open Banking Issuing Authority shall ensure the continued availability of the archive. All requests for access to such archived information shall be sent to the Open Banking Issuing Authority or to the entity identified by the Open Banking Issuing Authority prior to terminating its service.

5.6 KEY CHANGEOVER

A Certificate Authority Key Pair shall be generated and a new Certificate Authority Certificate corresponding to this Key Pair shall be Issued at least three months plus the validity period of the longest End Entity Certificate prior to the expiration of the old Certificate Authority Certificate.

After generation of the new Certificate Authority Key Pair, the Open Banking Issuing Authority shall cross certify according to any requirements for cross certification as approved by the Policy Management Authority.

All Certificate Authority Certificates shall be made available in the Open Banking Repository accessible to all Parties in the Public Key Infrastructure.

All copies of old Certificate Authority Private Keys shall be:

- Destroyed such that the Private Keys cannot be retrieved; or
- Retained in a manner such that they are protected against being put back into use.

5.7 COMPROMISE AND DISASTER RECOVERY

5.7.1 INCIDENT AND COMPROMISE HANDLING PROCEDURES

A business continuity plan shall be in place to protect critical Public Key Infrastructure processes from the effect of major compromises, failures or disasters. These shall enable the recovery of all Open Banking Issuing Authority services. Business continuity plans for Parties providing Trust Services shall be detailed in the Certification Practice Statement and/or supporting documentation. Plans must be approved by the Open Banking Issuing Authority or auditors acting on its behalf.

Parties providing Trust Services must provide evidence that such plans have been exercised.

In the case of compromise or suspected compromise of a Certificate Authority or Certificate Authority Keys, the Open Banking Issuing Authority shall assess the impact of the compromise or suspected compromise and take action as appropriate. This could include:

- Disabling the OCSP system thereby causing all Relying PKI Participant Certificate Status requests to fail.
- Notification to Public Key Infrastructure Parties of the compromise.
- Revocation of Certificates.
- Publication of Certificate Status Information.
- Rebuild of the affected systems and the re-Issuance of Certificates.
- Other action as necessary, agreed between the Open Banking Issuing Authority and Parties.

The Open Banking Policy Authority and/or Open Banking Issuing Authority shall make any determination relating to Revocation of Certificate Authority Certificates.

5.7.2 COMPUTING RESOURCES, SOFTWARE, AND/OR DATA ARE CORRUPTED

Parties providing Trust Services must establish business continuity procedures that outline the steps to be taken in the event of the corruption or loss of computing resources, software and/or data. Business continuity plans for Parties providing Trust Services shall be detailed in the Certification Practice Statement and/or supporting documentation. Plans must be approved by the Open Banking Issuing Authority or auditors acting on its behalf.

5.7.3 ENTITY PRIVATE KEY COMPROMISE PROCEDURES

See Section 5.7.1

5.7.4 BUSINESS CONTINUITY CAPABILITIES AFTER A DISASTER

The business continuity plan for the Certificate Manufacturer shall be designed to deal with any disruption to services and shall ensure managed, progressive recovery of components used to provide the service. A geographically separate alternative backup facility in order to maintain, at a minimum, Certificate Status Information must be made available.

Any backup facility used for relocation following a disaster shall maintain compliance with this Open Banking Certificate Policy. The provisions of this Open Banking Certificate Policy shall be maintained during any relocation/transition.

Open Banking Registration Authority business continuity arrangements must be approved by the Open Banking Issuing Authority or auditors acting on its behalf.

5.8 CERTIFICATE AUTHORITY OR REGISTRATION AUTHORITY TERMINATION

The specific actions relating to termination of the Open Banking Limited Public Key Infrastructure, including all Certificate Manufacturer, Certificate Authority and Registration Authority functions will be prescribed by Open Banking Limited. These could include, but may not be limited to:

- Providing appropriate notice to all affected Parties.
- Revoking all relevant Certificate Authority, Registration Authority and Subscribing PKI Participant Certificates.
- Ensuring all Certificate Authority Private Keys are destroyed or put beyond use.
- Arranging with a third party for the preservation and storage of records for the minimum period of time stipulated for the service being terminated but in any event not less than six (6) years.

6 TECHNICAL SECURITY CONTROLS

Where “no stipulation” is stated in this section of this Open Banking Certificate Policy it indicates there are no specific prescribed requirements for the controls, configuration or security requirements.

Specific details on technical controls operated for components of the Public Key Infrastructure must be detailed in the Certification Practice Statement and/or supporting documentation. Controls must be approved by the Open Banking Issuing Authority or auditors acting on its behalf.

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 KEY PAIR GENERATION

Certificate Manufacturer - Certificate Authority Keys shall be generated in a protected environment. Certificate Authority Key generation shall be multi-person control using random numbers of such length so as to make it computationally infeasible to regenerate them, even with the knowledge of when and in which equipment they were generated. See Section 6.2.1.

Private Keys used in any Open Banking Issuing Authority and/or Trust Services process that affects the outcome of Issued Certificates and Certificate Status Information services (such as signing of Certificate Revocation Lists), must be generated under controlled procedures. Parties conducting such key generation shall provide details of the procedure in the Certification Practice Statement and/or supporting documentation. Procedures must be approved by the Open Banking Issuing Authority or auditors acting on its behalf.

Subscribing PKI Participant Keys used for signing shall only be generated by the Subscribing PKI Participant.

6.1.2 PRIVATE KEY DELIVERY TO SUBSCRIBING PKI PARTICIPANT

No stipulation.

6.1.3 PUBLIC KEY DELIVERY TO CERTIFICATE ISSUER

Certificate Manufacturer – All Public Keys from Registration Authorities shall be delivered in a secure manner using a standard, recognised protocol e.g. PKCS#10 (https://tools.ietf.org/html/rfc2986).

Open Banking Local Registration Authority - The mechanism by which Subscribing PKI Participant Public Keys are delivered to the Certificate Manufacturer through the Registration Authorities is defined and described by the Open Banking Issuing Authority.

6.1.4 CERTIFICATE AUTHORITY PUBLIC KEY DELIVERY TO RELYING PKI PARTICIPANTS

The Open Banking Issuing Authority shall ensure that the delivery of Public Keys to Relying PKI Participants shall be done in a way that preserves and allows the verification of the integrity of the Public Keys.

6.1.5 KEY SIZES

The size of Open Banking Issuing Authority and any supporting Certificate Authority Keys shall be not less than 2048 bit modulus for RSA.

The size of Subscribing PKI Participant Private Keys shall be not less than 2048 bit modulus for RSA.

6.1.6 PUBLIC KEY PARAMETERS GENERATION AND QUALITY CHECKING

Public Key exponents shall be of values and lengths that make known attacks (e.g. low exponent attacks) infeasible.

6.1.7 KEY USAGE PURPOSES (AS PER X.509 V3 KEY USAGE FIELD)

Certificates Issued under this Open Banking Certificate Policy may be used in applications and services as listed in Section 2 of the Open Banking PKI Disclosure Statement. A Certificate may be used for one or more of the following Key usage services:

- Digital signature.
- Non repudiation.
- Key Encipherment.
- Data Encipherment.
- Key Agreement.
- Certificate Signature.
- CRL Signature.
- Encrypt only.
- Decrypt only.

Where a Certificate has been issued under this policy for the Key usage service of non repudiation the Private Key shall be used solely for the purpose of non repudiation.

Use of extensions in the Certificate shall be consistent with Section 7.1.2 of this Open Banking Certificate Policy.

6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1 CRYPTOGRAPHIC MODULE STANDARDS AND CONTROLS

Certificate Authority Keys shall be protected by high assurance physical and logical security controls. They must be stored in, and operated from inside a specific tamper resistant hardware based security module that complies with FIPS140-2 level 3, its equivalents and successors.

Private Keys used in any Open Banking Issuing Authority and/or Registration Authority Server process that affects the outcome of Issued Certificates and Certificate Status Information services (such as signing Certificate Revocation Lists), shall be protected by, maintained in, and restricted to, a hardware cryptographic token designed to meet the level of requirements as specified in FIPS 140-2 level 2, or its equivalents and successors.

Certificate Authority Keys shall not be available in unprotected form (complete or unencrypted) except in approved cryptographic modules.

6.2.2 PRIVATE KEY (N OUT OF M) MULTI-PERSON CONTROL

For Certificate Authority Keys and Keys that affects the outcome of Issued Certificates and Certificate Status Information services, at a minimum two-person control is required.

6.2.3 PRIVATE KEY ESCROW

Subscribing PKI Participants may undertake escrow arrangements for their own Private Keys.

Parties providing Trust Services shall not provide Private Key escrow services.

6.2.4 PRIVATE KEY BACKUP

Parties providing Trust Services may backup and archive Private Keys, including Certificate Authority Keys.

Subscribing PKI Participants may backup their own Keys.

In all cases Key backups shall at a minimum be protected to the standards commensurate with that stipulated for the primary version of the Key.

6.2.5 PRIVATE KEY ARCHIVAL

No stipulation.

6.2.6 PRIVATE KEY TRANSFER INTO OR FROM A CRYPTOGRAPHIC MODULE

Trust Service Providers conducting such Key transfer shall provide details of the procedure in the Certification Practice Statement and/or supporting documentation. Procedures must be approved by the Open Banking Issuing Authority or auditors acting on its behalf. See Section 6.1.2.

6.2.7 PRIVATE KEY STORAGE ON CRYPTOGRAPHIC MODULE

For Certificate Authority Keys and Keys that affects the outcome of Issued Certificates and Certificate Status Information services and other business processes, prescribed standards are required for the cryptographic protection of Private Keys. See Section 6.2.1.

6.2.8 METHOD OF ACTIVATING PRIVATE KEY

Software or hardware access controls shall be such that only authorised computer systems or services and/or authorised personnel may activate Subscribing PKI Participant's (Certificate Subjects) Private Key(s).

Cryptographic modules used by Parties providing Trust Services which are used as components of Certificate lifecycle management shall block themselves after a specified number of consecutive failed attempts to authenticate to the module.

Cryptographic modules used by Parties providing Trust Services may contain an unblocking function. Unblocking shall require the authorised personnel to use a mechanism to authenticate to the module.

Parties conducting unblocking must provide details of the procedures in the Certification Practice Statement and/or supporting documentation. Procedures must be approved by the Open Banking Issuing Authority or auditors acting on its behalf.

6.2.9 METHOD OF DEACTIVATING PRIVATE KEY

No stipulation.

6.2.10 METHOD OF DESTROYING PRIVATE KEY

Strict controls over destruction of Certificate Authority Keys and Keys that affect the outcome of Issued Certificates and Certificate Status Information services, must be exercised.

Whether active, expired or archived, the Open Banking Issuing Authority must approve the destruction of Certificate Authority Keys.

6.2.11 CRYPTOGRAPHIC MODULE RATING

See Section 6.2.1.

6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1 PUBLIC KEY ARCHIVAL

Public keys shall be archived in accordance with Section 5.5 of this Open Banking Certificate Policy

6.3.2 CERTIFICATE OPERATIONAL PERIODS AND KEY PAIR USAGE PERIODS

Usage periods for Key Pairs shall be governed by validity periods set in Issued Certificates. These shall have the following maximum values:

- Subscribing PKI Participants – up to three (3) years.
- Trust Service Provider trusted roles – five (5) years.
- On-line intermediate Issuing Authorities – ten (10) years.
- Off-line primary Issuing Authorities – twenty (20) years.

Unless expressly approved by the Open Banking Policy Authority, the usage period of Private Keys and associated Certificates shall not be extended beyond the lifetime of the original Certificate. This means that a Renewal which would result in Certificate expiry after the expiry date for the original Certificate issued for that Key Pair is not permitted.

6.4 ACTIVATION DATA

6.4.1 ACTIVATION DATA GENERATION AND INSTALLATION

All Certificate Authority Keys and keys that affect the outcome of Issued Certificates and Certificate Status Information services shall have Activation Data that is unique and unpredictable. The Activation Data, in conjunction with any other access control, must have an appropriate level of strength for the keys or data to be protected. Where PINs, passwords or pass-phrases are used, an entity must have the capability to change these at any time.

If applicable, unblocking code for a cryptographic module (if available) shall only be delivered to the legitimate holder of the module after an express request from the holder. Delivery of the unblocking code requires strong identification of the holder. See Section 6.2.8.

6.4.2 ACTIVATION DATA PROTECTION

All Open Banking Issuing Authority, supporting Certificate Authority Keys and Keys that affect the outcome of Issued Certificates and Certificate Status Information services shall have mechanisms for the protection of Activation Data which is appropriate to the Keys being protected.

Details of protection shall be provided in the Certification Practice Statement and/or supporting documentation. Procedures must be approved by the Open Banking Issuing Authority or auditors acting on its behalf.

6.4.3 OTHER ASPECTS OF ACTIVATION DATA

No stipulation.

6.5 COMPUTER SECURITY CONTROLS

6.5.1 SPECIFIC COMPUTER SECURITY TECHNICAL REQUIREMENTS

Parties providing Trust Services shall implement security measures that have been identified through a threat assessment exercise and must cover the following functionality where appropriate:

- Access control to Trust Services and Public Key Infrastructure roles.
- Enforced separation of duties for Public Key Infrastructure roles.
- Identification and Authentication of Public Key Infrastructure roles and associated identities.
- Use of cryptography for session communication and database security.

- Archival of Party history and audit data.
- Audit of security related events.
- Trusted path for identification of Public Key Infrastructure roles and associated identities.
- Recovery mechanisms for Keys of Public Key Infrastructure Parties providing Trust Services.

This functionality may be provided by the operating system, or through a combination of operating system, Public Key Infrastructure Certificate Authority software, and physical safeguards.

Parties providing Trust Services shall document procedures in the Certification Practice Statement and/or supporting documentation. Procedures shall at a minimum include logging and audit requirements for processes related to initialisation, resetting, shutdown or reconfiguration of Certificate Authorities and any services that affect the outcome of Issued Certificates and Certificate Status Information.

6.5.2 COMPUTER SECURITY RATING

Parties providing Trust Services may use system components that do not possess a formal computer security rating provided that all requirements of this Open Banking Certificate Policy are satisfied.

Any hardware security module or device holding Certificate Authority Keys must comply with the requirements of 6.2.1 of this Open Banking Certificate Policy.

Where specific computer security rating requirements are specified in this Open Banking Certificate Policy; details of relevant components and how they satisfy the requirements must be provided in the Certification Practice Statement and/or supporting documentation.

6.6 LIFE CYCLE TECHNICAL CONTROLS

6.6.1 SYSTEM DEVELOPMENT CONTROLS

The development of software, that implements Trust Service functionality shall as a minimum be performed in a controlled environment that, together with at least one of the following approaches, shall protect against the insertion of malicious logic.

- The system developer shall have a quality system compliant with international standards or;
- The system developer shall have a quality system available for inspection and approval by the Open Banking Issuing Authority.

6.6.2 SECURITY MANAGEMENT CONTROLS

The configuration of systems operated by Parties providing Trust Services as well as any modifications, upgrades and enhancements must be documented and controlled. There must be a method of detecting unauthorised modification or configuration of the software supporting Trust Services. Parties

providing Trust Services shall ensure that it has a configuration management process in place to support the evolution of the systems under its control.

Details of security management systems shall be provided in the Certification Practice Statement and/or supporting documentation which must be approved by the Open Banking Issuing Authority or auditors acting on its behalf.

6.6.3 LIFE CYCLE SECURITY CONTROLS

No stipulation.

6.7 NETWORK SECURITY CONTROLS

Trust Service Provider systems must be protected from attack through any open or general-purpose network with which they are connected. Such protection must be provided and configured to allow only the minimal set of functions, protocols and commands required for the operation of the Trust Service.

Parties providing Trust Services shall detail the standards procedures and controls for network security in the Certification Practice Statement and/or supporting documentation which must be approved by the Open Banking Issuing Authority or auditors acting on its behalf.

6.8 TIME-STAMPING

Time recording shall be implemented for all Certificate and other related activities that require recorded time. A synchronised and controlled time source shall be used.

Parties providing Trust Services shall detail the time source used and mechanisms for its control in the Certification Practice Statement and/or supporting documentation which must be approved by the Open Banking Issuing Authority or auditors acting on its behalf.

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 CERTIFICATE PROFILE

Certificate Profiles are under the direct control of the Open Banking Issuing Authority.

Procedures for development of Certificate Profiles shall incorporate approval by the Open Banking Issuing Authority prior to implementation.

7.1.1 VERSION NUMBER(S)

Only Certificates conformant to X.509 Version 3 and IETF RFC 5280 (https://tools.ietf.org/html/rfc5280) may be Issued.

7.1.2 CERTIFICATE EXTENSIONS

All End Entity Public Key Infrastructure software must correctly process the extensions identified in sections 4.2.1 and 4.2.2 of the IETF RFC 5280 (https://tools.ietf.org/html/rfc5280) Certificate Profile specification. The following are common Certificate extensions:

- The basic constraints extension is set to TRUE for Certificate Authority Certificates only; its use is critical specifying that it is a Certificate Authority Certificate. Subscribing PKI Participant End Entity Certificates have the value set to FALSE.
- The certificate Policies extension is mandatory and shall contain an OID indicating the use of this policy (according to 7.1.6). This Certificate Policy Qualifier Info extension shall be used to direct end-entities to where this policy and other relevant information may be found.
- Where Certificate Revocation Lists are used to produce Certificate Status information, the CRL distribution point extension is mandatory, and shall identify a location where the latest Certificate Revocation List Issued by the Open Banking Issuing Authority can be obtained.

7.1.3 ALGORITHM OBJECT IDENTIFIERS

No stipulation.

7.1.4 NAME FORMS

The use of all name forms shall be consistent with section 3.1 of this Open Banking Certificate Policy. Name forms shall be approved by the Open Banking Issuing Authority.

7.1.5 NAME CONSTRAINTS

No stipulation.

7.1.6 CERTIFICATE POLICY OBJECT IDENTIFIER

This Open Banking Certificate Policy has been assigned an OID as defined in section 12 of the Open Banking PKI Disclosure Statement. This shall be included in the certificate Policies extension of all Certificates Issued under this Open Banking Certificate Policy.

7.1.7 USAGE OF POLICY CONSTRAINTS EXTENSION

No stipulation.

7.1.8 POLICY QUALIFIERS SYNTAX AND SEMANTICS

No stipulation.

7.1.9 PROCESSING SEMANTICS FOR THE CRITICAL CERTIFICATE POLICIES EXTENSION

No stipulation.

7.2 CRL PROFILE

7.2.1 VERSION NUMBER(S)

Only Certificate Revocation Lists conforming to X.509 version 2 and IETF RFC 5280 (https://tools.ietf.org/html/rfc5280) may be issued.

The Open Banking Issuing Authority shall provide an on-line Certificate Status checking service which meets the requirements in this Policy.

7.2.2 CRL AND CRL ENTRY EXTENSIONS

No stipulation.

7.3 OCSP PROFILE

7.3.1 VERSION NUMBER(S)

Online Certificate Status Protocol and other forms of Certificate Status Information provision are permitted.

Repositories shall detail the mechanisms for on line Certificate Status Information provision in the Certification Practice Statement and/or supporting documentation which must be approved by the Open Banking Issuing Authority or auditors acting on its behalf.

Mechanisms for on line Certificate Status Discovery shall be specified in Section 17 of the Open Banking PKI Disclosure Statement.

7.3.2 OCSP EXTENSIONS

No stipulation.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

The details for assessment (if any) are specified in contractual arrangements between Open Banking Limited and the Parties providing Trust Services.

For all Parties providing Trust Services, audit must be sufficient to demonstrate to Open Banking Limited that the services comply with this Open Banking Certificate Policy and any supporting policy documents applicable to their services.

For the Certificate Manufacturer, assessment shall be against prescribed criteria defined by Open Banking Limited.

For the Certificate Manufacturer, audit shall be conducted by an approved third party auditor and conducted not less than annually.

Open Banking Limited may exercise right to audit any Parties providing Trust Services at any time.

8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR

The suitability of assessors to perform assessment of the Open Banking Issuing Authority and its associated Registration Authorities is decided by the Open Banking Policy Authority.

Approved auditors are as defined in section 11 of the Open Banking PKI Disclosure Statement and may include internal auditing resources of Parties, subject to the approval of Open Banking Limited.

For the Certificate Manufacturer audit shall be conducted by an approved third party auditor, subject to the approval of the Open Banking Issuing Authority.

8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

The acceptability of auditors is decided by the Open Banking Limited.

8.4 TOPICS COVERED BY ASSESSMENT

Audit is required to ensure a Party providing Trust Services is operating in accordance with its Certification Practice Statement, this Open Banking Certificate Policy and any declared assurance or approval schemes under which Trust Services are operated.

Where the Parties providing Trust Services use any designated authorised agents in order to provide service, the audit shall include the operations of such designated authorised agents.

Audit will address all aspects of Trust Service operations (whether they directly or indirectly influence compliance with the Certification Practice Statement) to ensure overall standards of operation are commensurate with this Open Banking Certificate Policy.

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

For compliance audits of Parties providing Trust Services, where significant exceptions or deficiencies are identified, the Open Banking Issuing Authority will inform the Open Banking Policy Authority and determine action to be taken. A remedial action plan will be developed with input from the auditor. The

Open Banking Policy Authority has overall responsibility to ensure implementation of the action plan. If an immediate threat to the security or integrity of the Public Key Infrastructure services is identified a corrective action plan which may include suspension or termination of non-compliant services will be developed, approved by the Open Banking Policy Authority and implemented by the Open Banking Issuing Authority. For lesser exceptions or deficiencies, the Open Banking Issuing Authority will determine the course of action to be taken.

8.6 COMMUNICATION OF RESULTS

Where compliance with third party assurance or approval schemes under which Trust Services are operated has been audited, approval status shall be made publicly available by the Parties providing Trust Services.

In the event of identification of material non-compliance with this Open Banking Certificate Policy the Open Banking Issuing Authority shall make available to Subscribing PKI Participants and Relying PKI Participants details of action to be taken as a result of the deficiency and any remedial action required to be taken.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 FEES

9.1.1 CERTIFICATE ISSUANCE OR RENEWAL FEES

There will be no fees payable by Subscribing PKI Participants or Relying PKI Participants for the Issuance or Revocation of Certificates or access to Certificate Status Information. Open Banking Limited reserves the right to charge fees in the future.

9.1.2 CERTIFICATE ACCESS FEES

See 9.1.1.

9.1.3 REVOCATION OR STATUS INFORMATION ACCESS FEES

See 9.1.1.

9.1.4 FEES FOR OTHER SERVICES

See 9.1.1.

9.1.5 REFUND POLICY

See 9.1.1.

9.2 FINANCIAL RESPONSIBILITY

9.2.1 INSURANCE COVERAGE

No stipulation.

9.2.2 OTHER ASSETS

No stipulation.

9.2.3 INSURANCE OR WARRANTY COVERAGE FOR END-ENTITIES

No stipulation.

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

9.3.1 SCOPE OF CONFIDENTIAL INFORMATION

Open Banking Limited and all Parties providing Trust Services shall classify personal data or corporate information as confidential.

All private and secret Keys and associated Activation Data, used or otherwise handled by a Party operating under this Open Banking Certificate Policy shall be kept confidential unless required otherwise by law.

Audit logs and records shall not be made available as a whole, except:

- As required by law
- To Open Banking Limited's professional advisors
- As part of audit or forensic investigation

In all other circumstances, only records of individual transactions may be released.

This information will only be disclosed by the Certificate Manufacturer in accordance with this Open Banking Certificate Policy or as required by law under the instruction of Open Banking Limited.

9.3.2 INFORMATION NOT WITHIN THE SCOPE OF CONFIDENTIAL INFORMATION

Certificates and Certificate Status Information are not classified as confidential or as private. Identification information or other personal or corporate information appearing in Certificates is not considered confidential.

9.3.3 RESPONSIBILITY TO PROTECT CONFIDENTIAL INFORMATION

The Open Banking Issuing Authority carries overall responsibility to protect confidential information. Other responsibilities of the Parties to maintain the confidentiality of information is outlined in this Open Banking Certificate Policy and applicable supporting documentation.

9.4 PRIVACY OF PERSONAL INFORMATION

Parties and all others using or accessing any personal data in connection with matters dealt with by this Open Banking Certificate Policy shall comply with the Data Protection Law.

9.4.1 PRIVACY PLAN

All Parties shall comply with data protection and privacy legislation applicable in their jurisdiction.

9.4.2 INFORMATION TREATED AS PRIVATE

See section 9.4.1.

9.4.3 INFORMATION NOT DEEMED PRIVATE

See section 9.4.1.

9.4.4 RESPONSIBILITY TO PROTECT PRIVATE INFORMATION

The Open Banking Issuing Authority carries overall responsibility to protect privacy information. Responsibly to protect privacy information is devolved to all Parties via this Open Banking Certificate Policy and applicable supporting documentation.

Parties also carry responsibility to protect privacy information to comply with Data protection and privacy legislation for the jurisdiction in which they operate.

9.4.5 NOTICE TO USE PRIVATE INFORMATION

All personal data shall be processed in accordance with the applicable Data Protection Law.

9.4.6 DISCLOSURE PURSUANT TO JUDICIAL OR ADMINISTRATIVE PROCESS

See the Open Banking Limited privacy policy at https://www.openbanking.org.uk/privacy-policy/.

9.4.7 OTHER INFORMATION DISCLOSURE CIRCUMSTANCES

Information held by the Certificate Manufacturer may also be disclosed:

- On the owner's request. To facilitate such disclosure an authenticated request from the information owner must be provided prior to the release of the information.
- At the specific request of the Open Banking Policy Management Authority.

9.5 INTELLECTUAL PROPERTY RIGHTS

All copyright and other intellectual property rights in this Open Banking Certificate Policy, the Open Banking PKI Disclosure Statement, the Open Banking Subscribing PKI Participant Agreement, the Open Banking Relying PKI Participant Agreement, and the Definitions of Terms (the "Materials") provided or made available by Open Banking Limited and/or Entrust Limited under this Open Banking Certificate Policy shall remain the property of the party that has contributed to it. Open Banking Limited and Entrust Limited grant to each other and to those Parties operating under this Open Banking Certificate Policy, a non-exclusive, world-wide, royalty free licence to make use of the Materials (as defined above) only in compliance with the terms of this Open Banking Certificate Policy and in conjunction with a Public Key Infrastructure in which Open Banking Limited is the Party providing Trust Services.

All Parties operating under this Open Banking Certificate Policy shall ensure that all information supplied to other parties operating under this Open Banking Certificate Policy does not infringe upon any third party rights including intellectual property rights.

All Parties operating under Open Banking Certificate Policy shall ensure that in using the services provided under this Open Banking Certificate Policy they will do nothing illegal or in infringement of any third party rights and in particular will ensure that any material that they supply or transmit is not illegal, libellous, and does not infringe any intellectual property rights.

9.6 REPRESENTATIONS AND WARRANTIES

No representations or warranties are made by Open Banking Limited in respect of the Open Banking Limited Policy Documents or any Certificates.

9.7 DISCLAIMERS OF WARRANTIES

The Parties acknowledge and agree this Open Banking Certificate Policy does not rely on any undertaking, promise, assurance, statement, representation, warranty or understanding (whether in writing or not) of any person (whether party to this Open Banking Certificate Policy or not) relating to the subject matter of this Open Banking Certificate Policy, other than as expressly set out in this Open Banking Certificate Policy or otherwise agreed in writing.

9.8 LIMITATIONS OF LIABILITY

By signing a Certificate containing a policy identifier which indicates the use of this Open Banking Certificate Policy, the Open Banking Issuing Authority certifies to all who reasonably rely on the

information contained in the Certificate, that the information in the Certificate has been checked according to the procedures laid down in this Open Banking Certificate Policy.

Open Banking Limited assumes no liability whatsoever in relation to the use of Certificates and/or associated Public/Private Key pairs Issued under this Open Banking Certificate Policy.

Open Banking Limited shall not be liable for any consequential, direct, indirect or incidental loss or damages, nor for any loss of business, loss of profit or loss of management time, whether foreseeable or unforeseeable, arising out of breach of any express or implied warranty, breach of contract, tort, misrepresentation, negligence, strict liability however arising, or in any other way arising from or in relation to the use of or reliance on any Certificate except only in the case of the Open Banking Issuing Authority's negligence, wilful misconduct, or where otherwise required by applicable law.

Nothing in this Open Banking Certificate Policy excludes or restricts liability for death or personal injury resulting from negligence or the negligence of its employees, agents or contractors or liability arising from fraudulent misrepresentation,

Open Banking Limited excludes all liability of any kind in respect of any transaction into which any Party may enter with any third party.

Open Banking Limited is not liable to End Entities either in contract, tort (including negligence) or otherwise for the acts or omissions of other providers of telecommunications or Internet services (including domain name registration authorities) or for faults in or failures of their equipment.

Each provision of this Open Banking Certificate Policy, excluding or limiting liability, operates separately. If any part is held by a court to be unreasonable or inapplicable, the other parts shall continue to apply.

Open Banking Limited limits any liability of any kind whatsoever for any award, damages or other claim or obligation of any kind arising from tort, contract or any other reason with respect to any service associated with the Issuance, use of, or reliance upon Certificates or associated Public/Private Key Pairs Issued under this Open Banking Certificate Policy.

9.9 INDEMNITIES

Subscribing PKI Participants will immediately indemnify and keep indemnified Open Banking Limited from and against all costs, claims, demands, liabilities, expenses, damages or losses (including without limitation any direct or indirect consequential losses, loss of profit and loss of reputation, and all interest, penalties and legal and other professional costs and expenses) arising out of or in connection with:

- Use of Certificates and/or Public/Private Key Pairs Issued under this Open Banking Certificate Policy in a manner that is not in accordance with this Open Banking Certificate Policy; and
- Subscribing PKI Participants' negligence, default and/or breach of this Open Banking Certificate Policy in any other manner.

If the Subscribing PKI Participant(s) becomes aware that a third party may make a claim against, or notifies an intention to make a claim against Open Banking Limited which may reasonably be considered as likely to give rise to a liability, the Subscribing PKI Participant(s) shall:

- As soon as reasonably practicable give written notice of that matter to Open Banking Limited specifying in reasonable detail the nature of the relevant claim;
- Not make any admission of liability, agreement or compromise in relation to the relevant claim without the prior written consent of Open Banking Limited (such consent not to be unreasonably conditioned, withheld or delayed); and
- Give Open Banking Limited and its professional advisers reasonable access to the premises and personnel of the Subscribing PKI Participant(s) and to any relevant assets, accounts, documents and records within the power or control of the Subscribing PKI Participant(s) so as to enable the Open Banking Limited and its professional advisers to examine such premises, assets, accounts, documents and records, and to take copies at their own expense for the purpose of assessing the merits of the relevant claim.

9.10 TERM AND TERMINATION

9.10.1 TERM

This Open Banking Certificate Policy is extant from the date of publication and shall remain in force until otherwise terminated in accordance with Section 9.10.2, replaced or withdrawn by notice provided by Open Banking Limited, or is explicitly identified by Open Banking Limited to be terminated.

9.10.2 TERMINATION

Without prejudice to any other rights to which Open Banking Limited may be entitled, this Open Banking Certificate Policy shall be terminated with immediate effect with respect to any Subscribing PKI Participant or Relying PKI Participant if such Subscribing PKI Participant or Relying PKI Participant:

- Has been withdrawn from participating in the Open Banking Directory; or
- Has had their regulatory permissions revoked by their competent authority and this has been reflected in the competent authority register; or
- Commits a material breach of any of the terms of this Open Banking Certificate Policy.

Should this Open Banking Certificate Policy be terminated as stipulated above all Issued Certificates shall be Revoked with immediate effect.

9.10.3 EFFECT OF TERMINATION AND SURVIVAL

Upon termination of this Open Banking Certificate Policy, the Parties are nevertheless bound by its terms for all Certificates issued for the remainder of the validity periods of such Certificates and this clause 9.10.3 shall survive termination.

9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTIES

9.11.1 SUBSCRIBING PKI PARTICIPANTS

Whenever any Subscribing PKI Participant hereto desires or is required to give any notice, demand, or request with respect to this Open Banking Certificate Policy, such communication shall be made in writing either by email, post or other mechanism approved by Open Banking Limited. Email communications shall be effective upon the sender receiving a valid receipt from the email address provided in Section 1 of the Open Banking PKI Disclosure Statement. Such acknowledgement must be received within five (5) working days, or else notice must then be given by post. Postal communications must be delivered by a service that confirms delivery in writing or via certified or registered mail, postage prepaid, return receipt requested and addressed to Open Banking Limited as detailed in Section 1 of the Open Banking PKI Disclosure Statement. All such communications shall be effective upon receipt.

A Subscribing PKI Participant requiring receipt of notice under this Open Banking Certificate Policy is required to provide notice of:

- Changes in address including postal and e-mail addresses
- Changes in regulatory status, which would change the basis upon which the Certificate has been granted
- Changes in the details of Primary Business Contacts and Primary Technical Contacts
- Any other notice pertinent to the maintenance of the provisions of this Open Banking Certificate Policy.

9.11.2 OPEN BANKING ISSUING AUTHORITY

All notices by Open Banking Limited shall be provided by making such notice accessible online in a similar manner as that used for the publication of this Open Banking Certificate Policy.

Notice requirements with regard to termination of Open Banking Limited operations are specified in Section 5.8.

Notice requirements with regard to changes in this Open Banking Certificate Policy may also be provided in accordance with Section 9.12.2.

9.11.3 NOTIFICATION

Any notices given in 9.11.2 shall be deemed served effective upon dispatch.

9.12 AMENDMENTS

9.12.1 PROCEDURE FOR AMENDMENT

Amendments to this Open Banking Certificate Policy fall into three categories:

- Editorial or typographical corrections, or changes to the contact details which may be made without notification or are awaiting comments.
- Changes which, in the judgement of the Open Banking Policy Authority, will not materially impact a substantial majority of the Subscribing PKI Participants or Relying PKI Participants using this Open Banking Certificate Policy.
- Changes which, in the judgement of the Open Banking Policy Management Authority, are likely to have a material impact upon a significant number of users of this Open Banking Certificate Policy.

Where the amendments are likely to have a major impact on the majority of users of this Open Banking Certificate Policy in the opinion of Open Banking Limited then a major version number should be used. For minor changes then a minor version number should be used. See Section 9.11.3.

9.12.2 NOTIFICATION MECHANISM AND PERIOD

All proposed changes that may materially impact users of this Open Banking Certificate Policy will be notified in accordance with Section 9.11 of this Open Banking Certificate Policy by the Open Banking Issuing Authority and will be posted at http://ob.trustis.com/production/policies/. The Open Banking Issuing Authority shall make commercially reasonable efforts to advise End-Entities of such proposed changes.

Impacted Parties may file comments through the Open Banking Issuing Authority. The period for comment will be as follows:

- For changes which, in the judgement of the Open Banking Policy Authority, will not materially impact a substantial majority of users of this Open Banking Certificate Policy comments shall be received within 5 days of original notice.
- Changes which, in the judgement of the Open Banking Policy Authority, are likely to have a material impact upon a significant number of users of this Open Banking Certificate Policy comments shall be received within 15 days of original notice.

Any action taken as a result of comments filed in accordance with the above is wholly at the discretion of the Open Banking Policy Authority.

If the proposed change is modified as a result of comments received notice of the modified proposed change shall be given at least 30 days prior to the change taking effect.

Approval for incorporation of any changes to this Open Banking Certificate Policy is wholly at the discretion of the Open Banking Policy Authority.

9.12.3 CIRCUMSTANCES UNDER WHICH OID MUST BE CHANGED

If amendments to this Open Banking Certificate Policy are determined by the Open Banking Policy Authority to be sufficiently significant the Open Banking Policy Authority reserves the right to assign a new Object Identifier (OID) to the modified Open Banking Certificate Policy.

9.13 DISPUTE RESOLUTION PROVISIONS

All disputes arising between Subscribing PKI Participants or Relying PKI Participants and Open Banking Limited shall be dealt with in accordance with its dispute resolution process specified in section 10 of the Open Banking PKI Disclosure Statement.

9.14 GOVERNING LAW

This Open Banking Certificate Policy and any dispute or claim arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims) shall be governed by and construed in accordance with the laws of England and Wales. Each Party irrevocably agrees that the courts of England and Wales shall have exclusive jurisdiction to settle any dispute or claim arising out of or in connection with this Open Banking Certificate Policy or its subject matter or formation (including non-contractual disputes or claims).

9.15 COMPLIANCE WITH APPLICABLE LAW

All Parties within the Public Key Infrastructure will comply with all applicable law and regulations, for example those relating to cryptographic hardware and software that may be subject to the export control laws of a given jurisdiction.

9.16 MISCELLANEOUS PROVISIONS

9.16.1 ENTIRE AGREEMENT

The parties acknowledge that, except for documents expressly referred to or incorporated by reference herein, this Open Banking Certificate Policy constitutes the entire agreement and understanding of the parties and (unless expressly provided for herein) supersedes any previous agreement between the parties relating to the subject matter of this Open Banking Certificate Policy. For the purposes of this clause, such documents shall be:

- Open Banking PKI Disclosure Statement
- Open Banking Relying PKI Participant Agreement
- Open Banking Subscribing PKI Participant Agreement
- Definitions of Terms

In the event of any ambiguity, inconsistency or incompatibility between any of the provisions of the documents set out in Section 9.16.1 and those of the agreements set out below, the provisions of the agreements set out below will prevail as far as they relate to the parties of those agreements:

- An agreement entered into between Entrust Limited and Open Banking Limited for the provision of PKI services dated 22 September 2017 (as amended or superseded from time to time); and
- The applicable Open Banking Limited terms and conditions (as amended or superseded from time to time).

9.16.2 ASSIGNMENT

Except as expressly provided below, the rights and obligations detailed in this Open Banking Certificate Policy are not assignable by the parties and any purported assignment without such consent shall be void.

For the avoidance of doubt, nothing in this Open Banking Certificate Policy will prevent Open Banking Limited from assigning, novating, sub-contracting, transferring, or sub licensing its rights and obligations hereunder to a third party.

9.16.3 SEVERABILITY

In the event that any one or more of the provisions of this Open Banking Certificate Policy shall for any reason be held to be invalid, illegal, or unenforceable at law, such unenforceability shall not affect any other provision, but this Open Banking Certificate Policy shall then be construed as if such unenforceable provision or provisions had never been contained herein, and insofar as possible, construed to maintain the original intent of this Open Banking Certificate Policy.

9.16.4 ENFORCEMENT (ATTORNEYS' FEES AND WAIVER OF RIGHTS)

No delay, neglect or forbearance on the part of one party in enforcing against any other party any term or condition of this Open Banking Certificate Policy shall either be or be deemed to be a waiver or in any way prejudice any right of that party under this Open Banking Certificate Policy. No right, power or remedy in this Open Banking Certificate Policy conferred upon or reserved for a party is exclusive of any other right, power or remedy available to that party. Each party shall bear its own legal costs and other costs and expenses arising out of or in connection with this Open Banking Certificate Policy.

9.16.5 FORCE MAJEURE

Open Banking Limited shall have no liability to the Parties under this Open Banking Certificate Policy if it is prevented from or delayed in performing its obligations under this Open Banking Certificate Policy, or from carrying on its business, by acts, events, omissions or accidents beyond its reasonable control, including, without limitation, strikes, lock-outs or other industrial disputes (whether involving the workforce of Open Banking Limited or any other party), failure of a utility service or transport network,

act of God, war, riot, civil commotion, malicious damage, compliance with any law or governmental order, rule, regulation or direction, accident, breakdown of plant or machinery, fire, flood, storm or default of suppliers or sub-contractors.

If any such events affecting the availability of or access by a Relying PKI Participant to Certificate Status Information as described in the preceding paragraph, continue for a continuous period of more than 72 hours Open Banking Limited may terminate this Open Banking Certificate Policy by written notice to the other parties.

9.17 OTHER PROVISIONS

9.17.1 CERTIFICATE POLICY CONTENT

Section and paragraph headings shall not affect the interpretation of this Open Banking Certificate Policy and the content of Section 1.3 is descriptive only for reference purposes and such section shall be interpreted accordingly.

9.17.2 THIRD PARTY RIGHTS

No term of this Open Banking Certificate Policy shall be enforceable under the Contracts (Rights of Third Parties) Act 1999 by a third party.

DEFINITIONS

Terms used in this Open Banking Certificate Policy are defined in the Open Banking Definitions of Terms which can be found at http://ob.trustis.com/production/policies/.

Document History			
Version	**Date**	**Author(s)**	**Status**
0.1	16/10/2017	Gerry Hay	Working draft for OB internal use only.
0.2	23/10/2017	Gerry Hay	Interim draft release to support review.
0.3	02/11/2017	Gerry Hay	Updated following legal review.
0.4	05/11/2017	Gerry Hay	Further updates following team review.
0.5	24/11/2017	Gerry Hay	Further updates following team review.
0.6	27/11/2017	Gerry Hay	Further updates following team review.
1.0	04/12/2017	Gerry Hay	Issued.
1.1	17/12/2020	Entrust, Open Banking	Updates to extend the scope for the use of Open Banking Certificates.
1.2	28/01/2021	Entrust, Open Banking	Updates to accommodate the issuance of certificates for confirmation of payee (CoP). tScheme requirement clarified.
1.3	10/06/2021	Entrust, Open Banking	Change in relation to consequences of revocation of certificates and circumstances for certificate revocation

1.4	08/10/2021	Entrust, Open Banking	Version number updated to retain consistent numbering across all policy documents.
1.5	19/09/2024	Open Banking	No changes
1.6	15/09/2025	Entrust, Open Banking	Updated to allow CA renewal to extend certificate validity period and private key usage period.
1.7	18/11/2025	Entrust, Open Banking	Version updated to align with PDS version.