Open Banking

PKI Disclosure Statement

Important Notice

The full Certificate Policy under which Certificates are issued is defined by two documents:

- The Open Banking PKI Disclosure Statement (this document).
- The Open Banking Certificate Policy.

The purpose of this document is to:

- Summarise the key points of the Open Banking Certificate Policy for the benefit of Subscribing PKI Participants and Relying PKI Participants.
- Provide additional detail and further provisions that apply to the Open Banking Certificate Policy and which are incorporated in it by reference.

Certificates issued by the Open Banking Issuing Authority reference the Open Banking Certificate Policy located at http://ob.trustis.com/production/policies/, and consequently this document.

Terms used in this document are defined in the Open Banking Definitions of Terms located at http://ob.trustis.com/production/policies/.

1. Policy Authority & Issuing Authority Contact Info

Open Banking Policy Authority and Open Banking Issuing Authority:

Open Banking Limited

8th Floor,

100 Bishopsgate,

London,

EC2N 4AG Tel: +44 (0) 203 2178188

email: servicedesk@openbanking.org.uk

2. Certificate Type, Validation procedures and usage

The Certification Services provided by Open Banking Limited implement a Public Key Infrastructure wherein Certificates will only be issued to those who both satisfy eligibility criteria and are enrolled by the Open Banking Issuing Authority. Those Relying PKI Participants that have not been enrolled by the Open Banking Issuing Authority and which are outside of the Open Banking Ecosystem, may however rely on Certificates provided that they do so on the terms of the Open Banking Limited Policy

Documents. The Parties providing Trust Services and End Entities entitled to issue, obtain, use, and/or Rely upon Certificates that reference the Open Banking Certificate Policy are clearly defined. Receipt, possession or use of a Certificate constitutes acceptance of the Open Banking Certificate Policy and related documents

The services provided by the Open Banking Issuing Authority support secure operations and interactions in the direct pursuit of participation in the Open Banking Ecosystem. Certificates provided by this service are supported by the use of strong cryptography and highly robust registration mechanisms to a defined and assured level of trust and security.

Permitted usages are:

- Digital Signing.
- Authentication.

Certificates do not verify the regulatory status of a Subscribing PKI Party and should not be relied on for this purpose. A Relying PKI Participant should consult the Open Banking Directory or the register of the relevant national competent authority or suitable alternative directory to obtain this information. Applicants for Certificates are required to submit to the Validation of identity credentials and their eligibility to hold such a Certificate

3. Reliance Limits

The Open Banking Issuing Authority does not set reliance limits for Certificates it issues. Reliance limits may be set by applicable law or by agreement.

4. Obligations of Subscribing PKI Participants

Subscribing PKI Participants must comply with the requirements defined in the Open Banking Subscribing PKI Participant Agreement located at http://ob.trustis.com/production/policies/, and those set out below.

It is the responsibility of the Subscribing PKI Participant to:

- Ensure all information submitted in support of a Certificate application is true, accurate and they hold such rights as necessary to any trade marks or other such information submitted during the application for a Certificate.
- Review the issued Certificate to confirm the accuracy of the information contained within it before installation and first use.
- Use a trustworthy system for generating or obtaining a Key Pair and to prevent any loss, disclosure, or unauthorised use of the Private Key.
- Keep Private Keys confidential.
- Keep confidential, any passwords, pass-phrases, PINs or other personal secrets used in obtaining authenticated access to Certificates and PKI facilities.

- Make only true and accurate representations to the Open Banking Registration Authority and/or Open Banking Issuing Authority as to the information required to determine eligibility for a Certificate and for information contained within the Certificate.
- In accordance with the Open Banking Certificate Policy at http://ob.trustis.com/production/policies/, exclusively use the Certificate for purposes permitted by law and restricted to those authorised purposes detailed by the Open Banking Certificate Policy.
- Revoke a Certificate upon suspected or known compromise of the Private Key associated with a Certificate.

For a device or application, the individual responsible for the device or application must also accept these responsibilities.

WARNING: If a Subscribing PKI Participant's Private Key is compromised; unauthorised persons could decrypt or sign messages with the Key and commit the Subscribing PKI Participant to unauthorised obligations.

5. Certificate Status checking Obligations of Relying PKI Participants

Relying PKI Participants must comply with the requirements defined in the Open Banking Relying PKI Participant Agreement located at http://ob.trustis.com/production/policies/, and those set out below.

A Relying PKI Participant may justifiably rely upon a Certificate only after:

- Ensuring that reliance on Certificates issued under this Open Banking Certificate Policy is restricted to permitted usages (see "Certificate Type, validation procedures and usage", above for a summary of approved usages).
- Ensuring, by accessing any and all relevant Certificate Status Information, that the Certificate remains valid and has not been Revoked.
- Ensuring, by accessing any and all relevant OSCP Certificate Status Information Services, that the Certificate remains valid and has not been Revoked.
- Determining that such Certificate provides adequate assurances for its intended use.
- Taking any other precautions prescribed in the Open Banking Certificate Policy,

and only in accordance with the terms of the Open Banking Limited Policy Documents.

6. Limited Warranty & Disclaimer/Limitation of Liability

Open Banking Limited assumes no liability whatsoever in relation to the use of Certificates or associated Public/Private Key Pairs Issued under the Open Banking Certificate Policy for any use other than in accordance with the Open Banking Certificate Policy

Subscribing PKI Participants will immediately indemnify 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) as further set out in paragraph 9 of the Open Banking Certificate Policy.

Open Banking Limited shall not be liable for any consequential, indirect or incidental 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 the 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 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 the 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 the Open Banking Certificate Policy.

7. Applicable Agreements, Certification Practice Statement, Certificate Policy

The Open Banking Certificate Policy, Open Banking Subscribing PKI Participant Agreement and Open Banking Relying PKI Participant Agreement are published by the Open Banking Issuing Authority and available at the locations referenced in this Open Banking PKI Disclosure Statement.

8. Privacy Policy

Open Banking Limited operates this service according to the Privacy Policy which is located at https://www.openbanking.org/privacy-policy/.

9. 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.

10. Applicable Law & Dispute Resolution

Disputes arising between Subscribing PKI Participants or Relying PKI Participants and Open Banking Limited shall be handled in accordance with the Open Banking Limited Complaints and Dispute Resolution Procedure which can be obtained by contacting Open Banking Limited. Contact details are provided in Section 1 of this document.

The provision of Open Banking Issuing Authority Certification Services shall be governed by and constructed in accordance with the laws of England and Wales and all parties shall submit to the exclusive jurisdiction of the courts of England and Wales

11. Trust Marks & Audit

Certificates are manufactured under the Open Banking Certificate Policy through the use of an Entrust Limited service which is both accredited to ISO 27001 and has attained tScheme approval.

Audit shall be carried out on a periodic basis as required by the relevant accreditation bodies to maintain security and trust accreditations. The audit shall be undertaken by auditors approved for this purpose by the relevant accreditation bodies.

12. Identification of this Open Banking Certificate Policy

The Open Banking Certificate Policy has been assigned an Object Identifier (OID) of 1.3.6.1.4.1.5237.134.1.1.

13. Approved Registration Authorities

The following Registration Authorities have been approved by the Open Banking Issuing Authority to register Subscribing PKI Participants under the Open Banking Certificate Policy:

- Open Banking Registration Authority

14. Approved Repositories

The following Repositories have been approved by the Open Banking Issuing Authority under the Open Banking Certificate Policy:

- Open Banking Repository provided by Entrust Limited.

15. Eligible Subscribing PKI Participants

The following types of Subscribing PKI Participants are eligible to be issued with Certificates under the Open Banking Certificate Policy:

- TPPs, ASPSPs, CD ASPSPs and CD TPPs enrolled in the Open Banking Directory.

The Open Banking Subscribing PKI Participant Agreement can be found at http://ob.trustis.com/production/policies/.

16. Eligible Relying PKI Participants

The following types of Relying PKI Participants are eligible to rely on Certificates issued under the Open Banking Certificate Policy:

- TPPs enrolled in the Open Banking Directory.
- ASPSPs (whether or not enrolled in the Open Banking Directory).
- CD ASPSPs and CD TPPs enrolled in the Open Banking Directory

The Open Banking Relying PKI Participant Agreement can be found at http://ob.trustis.com/production/policies/.

17. Certificate Status Information

Certificate Status information confirming the validity of Certificates is made available via an Online Certificates Status Protocol service. The service location is identified via an AIA entry in Subscribing PKI Participant Certificates.

A new Certificate Revocation List is published every 4 hours, and immediately upon a Certificate Revocation. CRLs are valid for 8 days.

Document History

Version	Date	Author(s)	Status
0.1	16/10/2017	Gerry Hay	Working draft for OB internal use only
0.2	02/11/2017	Gerry Hay	Updated following OB internal review.
0.3	02/11/2017	Gerry Hay	Updated to align with CP changes.
0.4	06/11/2017	Gerry Hay	Updated to align with CP changes
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).
1.3	10/06/2021	Entrust, Open Banking	Version updated to align with CP version.

1.4	08/10/2021	Entrust, Open Banking	Version updated to include new address and issuance of certificates for Crown Dependencies
1.5	19/09/2024	Open Banking	Removal of CoP Participants from Section 15 (Eligible Subscribing PKI Participants) and Section 16 (Eligible Relying PKI Participants)