Open Banking
Definitions of Terms

This Definitions of Terms supports Public Key Infrastructure (PKI) policy documents issued by Open Banking Limited.

Activation Data	Private data, other than Keys, that are required to access cryptographic modules.
Agreement	Refers to the Subscribing PKI Participant Agreement or Relying PKI Participant Agreement.
Applicant	The Subscribing PKI Participant is sometimes also called an "Applicant" after applying to a Certificate Authority for a Certificate, but before the Certificate Issuance procedure is completed.
ASPSP	Means a payment service provider providing and maintaining a payment account for a payer as defined by PSD2
Authenticate/Authentication	The process of establishing that individuals, organisations, or devices are who or what they claim to be. In the context of a PKI, Authentication can be the process of establishing that an individual or organisation applying for or seeking access to something under a certain name is, in fact, the proper individual or organisation. Authentication can also refer to a security service that provides assurances that individuals, organisations, or things are who or what they claim to be or that a Message or other data originated from a specific individual, organisation, or device. Thus, it is said that a Digital Signature of a Message Authenticates the Message's sender.
Card Based Payment Instrument Issuer (CBPII)	A Card Based Payment Instrument Issuer is a payment services provider that issues card-based payment instruments that can be used to initiate a payment

	transaction from a payment account held with another payment service provider.
CD ASPSP	means a Crown Dependency account servicing payment service provider
CD TPP	means Crown Dependency AISP (“CD AISP”) or Dependency (“CD PISP”) that has successfully completed the enrolment process on the Open Banking Directory for Crown Dependencies.
Certificate	A collection of data that at a minimum: 1. Identifies the Issuing Authority 2. Names or identifies its Certificate Subject 3. Contains the Certificate Subject's Public Key 4. Identifies the operational period of the Certificate 5. Bears the Digital Signature of the Issuing Authority
Certificate Authority	An entity that is responsible for the generation, Issuance, management, Suspension and Revocation of Certificates
Certificate Discovery	The process of obtaining a Subscribing PKI Participant’s Certificate, typically from a directory or database.
Certificate Manufacturer	The entity providing Certificate management services and facilities for an Issuing Authority.
Certificate Policy (CP)	A named set of rules that indicate the applicability of a Certificate to a particular community and/or class of application with common security requirements. A Certificate Policy (CP) may be employed by a Certificate user to help in deciding whether a Certificate (and the binding therein), is sufficiently trustworthy for a particular purpose. A Certificate Policy (CP) may be supported by one or more Certification Practice Statements (CPS).
Certificate Profile	Defines the usage of the Certificate and is formally approved by the Open Banking Policy Authority and the Issuing Authority.
Certificate Revocation List (CRL)	A list maintained by, or on behalf of, the Issuing Authority of the Certificates that it has issued, that

	have been Revoked or Suspended before the expiry stated in the Certificate.
Certificate Status	Current status of a Certificate – Issued, valid, Suspended, Revoked, expired.
Certificate Status Discovery	The process of ascertaining the operational status of a Certificate. Typically, via a controlled mechanism from a Repository.
Certificate Status Information	Information that indicates whether Certificates have been Revoked or Suspended; commonly provided via Certificate Revocation Lists (CRL), or individually through specific online enquiries e.g. Online Certificate Status Protocol (OCSP).
Certificate Subject	The Certificate Subject is the entity listed in the subject field of a Certificate. For Subscribing PKI Participants, the Certificate Subject is the software statement identified in the Certificate DN.
Certification Practice Statement (CPS)	A statement of the procedures and practices employed in Issuing Certificates, managing Certificates, Revoking and Certificate Renewal. A Certification Practice Statement (CPS) may support of one or more Certificate Policies.
Certification Services	The Certificate services provided by the Open Banking PKI (Authentication of Subscribing PKI Participants, Issuing Certificates, managing Certificates, Revoking, and Certificate Renewal/Certificate Re-keys.)
Common Name (CN)	Common Name component of a Distinguished Name.
CRL Distribution Point	Indicates how Certificate Revocation List (CRL) information may be accessed.
Data Protection Laws	Means the Data Protection Act (1998), EU Data Protection Directive 95/46/EC and the EU Privacy & Electronic Communications Directive 2002/58/EC, any amendments and replacement legislation including the EU General Data Protection Regulation (EU) 2016/679, European Commission decisions, binding EU and national guidance and all national implementing legislation.

Digital Signature	A digital code attached to an electronic communication that distinctly identifies the sender of that communication and confirms that its contents have not been altered during transmission.
Distinguished Name (DN)	The meaning given to it in X.501. See X.501.
End Entity (Entities, when more than one Entity)	End Entity have certificates that can only be used for authentication, confidentiality, or message integrity. End Entity cannot themselves issue certificates. End Entity include: • Subscribing PKI Participants • Certificate Subjects • Relying PKI Participants
FIPS 140-2	Federal Information Processing Standard – Security Requirements for Cryptographic Modules
Guidelines for Read/Write Participants	This means the guidelines produced and maintained by Open Banking Limited applicable to participants in the Open Banking Ecosystem, including any annexes or documentation referred to therein, as may be updated, amended or modified from time to time.
Identification	The process of establishing the identity of an individual or organization, i.e., to show that an individual or organization is a specific individual or organization. In the context of a Public Key Infrastructure (PKI), identification refers to two processes: 1. Establishing that a given name of an individual or organization corresponds to a real-world identity of an individual or organization, and 2. Establishing that an individual or organization applying for or seeking access to something under that name is, in fact, the named individual or organization. A person seeking identification may be a Certificate applicant, an applicant for
	employment in a trusted position within a Public Key Infrastructure (PKI) Party, or a person seeking access to a network or software application, such as a Certificate Authority administrator seeking access to Certificate Authority systems.

IETF	Internet Engineering Task Force
ISO 27001	ISO/IEC 27001:2013 Information Security Management Standard.
Issuance/Issues/Issuing (Issue a Certificate)	The act of signing a Certificate request with the Private Key of a Certificate Authority to create a Certificate.
Issuing Authority	By definition, an Issuing Authority is the entity listed in the issuer field of a Certificate. The Issuing Authority has the responsibility for deciding who may be issued with a Certificate carrying its name.
Key	A cryptographic key.
Key Pair	In Public Key Cryptography a Private Key and its mathematically related Public Key having the property that the Public Key can verify a Digital Signature that the Private Key creates.
Object Identifier (OID)	An object identifier is a string, of decimal numbers, that uniquely identifies an object. These objects are typically an object class or an attribute.
Online Certificate Status Protocol (OCSP)	A network protocol used to ascertain the current validity status of a Certificate.
Open Banking Certificate Authority	The Open Banking Limited entity that is responsible for the generation, Issuance, management, Suspension and Revocation of Certificates
Open Banking Certificate Policy	The Certificate Policy governing the Open Banking PKI Services.
Open Banking Directory	The directory system used to support Open Banking PKI Services.
Open Banking Limited	A company incorporated and registered in England with company number 10440081 whose registered office is at 8th Floor, 100 Bishopsgate, London EC2N 4AG.

Open Banking Limited Policy Documents	The suite of Public Key Infrastructure (PKI) policy documents issued by Open Banking Limited available here: http://ob.trustis.com/production/policies/
Open Banking Ecosystem	Means the open banking environment implemented by Open Banking.

Open Banking Issuing Authority	Open Banking Limited acting as an Issuing Authority.
Open Banking Manual Registration Authority	Open Banking Limited manually carrying out Certificate lifecycle activities.
Open Banking Enrolment	Open Banking Limited carrying out the procedures required for joining the Open Banking Ecosystem.
Open Banking PKI Services	The services provided by Open Banking Limited to Subscribing PKI Participants and Relying PKI Participants.
Open Banking Repository	The Open Banking Limited provided community-wide accessible mechanism by which Parties can obtain Certificate or Certificate Status information to validate Certificates, and obtain Certificate Policy (CP) and other controlling information for the Public Key Infrastructure (PKI).
Open Banking Registration Authority	Open Banking Limited carrying out the practices and procedures for the following: 1. The Identification and Authentication of Certificate applicants (via Open Banking Enrolment) 2. The approval or rejection of Certificate applications (via Open Banking Local Registration Authority) 3. Initiating Certificate Revocations under certain circumstances (via Open Banking Local Registration Authority & Open Banking Manual Registration Authority) 4. Approving or rejecting requests for the Renewal or Certificate Re-Key (via Open Banking Local Registration Authority).
Open Banking Relying PKI Participant Agreement	An agreement between the Open Banking Issuing Authority and a Relying PKI Participant that

	establishes the rights and obligations between those Parties regarding the verification of Digital Signatures or other uses of Certificates.

Open Banking Subscribing PKI Participant Agreement	An agreement between the Open Banking Issuing Authority and a Subscribing PKI Participant that establishes the rights and responsibilities of the parties regarding the Issuance and management of Certificates and associated Private Keys.
Open Banking Policy Authority	Open Banking Limited carrying out governance and control over the Issuance, management and usage of a specified set of Certificates. It uses a Certificate Policy (CP) as the mechanism to exercise control over all Parties in a Public Key Infrastructure (PKI).
Open Banking Local Registration Authority	The Open Banking system component that performs a subset of the functions undertaken by a Registration Authority. This includes Key/Certificate life-cycle management functions such as initiating a Revocation request or a Certificate Renewal on behalf of a Subscribing PKI Participant.
Open Banking PKI Disclosure Statement (PDS)	The Open Banking Limited PKI Disclosure Statement.
Organisation (O)	Organisation component of a Distinguished Name.
Organisational Unit (OU)	Organisation Unit component of a Distinguished Name.
Party (Parties, when referring to more than one Party)	Certificate Manufacture; Certificate Authority; Issuing Authority; Local Registration Authority; Open Banking Registration Authority; Open Banking Policy Authority; Relying PKI Participant; and Subscribing PKI Participant.
PKCS#10	Certification Request Syntax Specification

PKI Disclosure Statement (PDS)	An instrument that supplements a Certificate Policy (CP) or Certification Practice Statement (CPS) by disclosing critical information about the policies and practices of a Certification Authority. A PKI Disclosure Statement (PDS) is a vehicle for disclosing, summarising and emphasizing information normally covered in detail by associated Certificate Policy (CP) and/or Certification Practice Statement (CPS) documents. A PKI Disclosure Statement (PDS) is not intended to replace a Certificate Policy (CP) or Certification Practice Statement (CPS).
Policy Qualifier	Policy dependent information that may accompany a Certificate Policy (CP) identifier in an X.509 Certificate.
Primary Technical Contact	An individual nominated by an ASPSP, TPP, CD ASPSP or CD TPP to have access to the Open Banking Directory and will be able to nominate other Open Banking Directory technical users. This should be a main point of contact for technical configuration and a senior member of staff with responsibility for the management of the Open Banking Limited digital identity.
Primary Business Contact	An individual nominated by an ASPSP, TPP, CD ASPSP, or CD TPP to have access to the Open Banking Directory and will be able to nominate other Open Banking Directory business users. This should be a formal business point of contact and a senior member of staff responsible for systems and controls related to Open Banking Limited.
Private Key	The private part of a Public Key Cryptography key pair used for Public Key encryption techniques. The Private Key is typically used for creating Digital Signatures or for decrypting Messages.
Public Key	The public part of a Public Key Cryptography Key Pair used for Public Key encryption techniques. The Public Key is typically used for verifying Digital Signatures or to encrypt messages to the owner of the Private Key.

Public Key Infrastructure (PKI)	A system of Certificates, Certificate Authorities, and other components that verify and authenticate the validity of parties involved in electronic transactions.
Registration Authority	An entity that is authorised or licensed by an Issuing Authority to carry out the practices and procedures for one or more of the following functions: 1. The Identification and Authentication of Certificate applicants; 2. The approval or rejection of Certificate applications; 3. Initiating Certificate Revocations or Suspensions under certain circumstances; 4. Processing requests to Revoke or Suspend Certificates; 5. Approving or rejecting requests by for the Renewal or Re-Key of Certificates. A Registration Authority does not have responsibility for signing or issuing Certificates or Certificate Status Information.
Registration Authority Server	The 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.
Rely/Reliance	Act as a Relying PKI Participant.
Relying PKI Participant	A recipient of a Certificate who acts in reliance on that Certificate and/or any Digital Signatures verified using that Certificate.
Repository	The entity provided community-wide accessible mechanism by which Parties can obtain Certificate or Certificate Status information to validate Certificates, and obtain Certificate Policy (CP) and other controlling information for the Public Key Infrastructure (PKI).
Revocation/Revoke/Revoked/Revoking	Permanently end the Operational Period of a Certificate from a specified time.

Revocation Information	Information required before enacting a Certificate Revocation (or Suspension). It must include evidence of the authenticity of the requestor.
RFC 3647	https://www.ietf.org/rfc/rfc3647.txt. X.509 Internet
	Public Key Infrastructure Certificate Policy and Certification Practices Framework.
RFC 5280	https://www.ietf.org/rfc/rfc5280.txt. X.509 Public Key
	Infrastructure Certificate and Certificate Revocation List (CRL) Profile
RSA	RSA is a Public Key algorithm.
Subscribing PKI Participant	A TPP, ASPSP, CD ASPSP or CD TPP entity that contracts with an Issuing Authority for the issuance of Certificates. The Subscribing PKI Participant bears ultimate responsibility for the use of the Private Key associated with the Certificate.
Suspension/Suspend/Suspended (Suspend a Certificate)	Temporarily make a Certificate non-operational from a specified time for a period up to the end of its Validity Period
Time-stamp	To create a notation that indicates, at a minimum, the correct date and time of an action or activity and the identity of the entity that created the notation; or such a notation is appended, attached or referenced as part of a data structure. Time-stamps may, but do not require derivation of chronological data from a secure time source and/or use cryptographic techniques to preserve the integrity of the Time-stamp.
Time-stamping Authority	The Trust Service Provider (Entrust Limited) controlling and Issuing time-stamps for use by other entities.
TPP	An AISP, PISP or CBPII that has successfully completed the enrolment process on the Open Banking Directory.
Entrust Limited	Entrust (Europe) Ltd, 6th Floor Abbey Gardens, 4 Abbey Street, Reading, Berkshire, RG1 3BA

Trust Service	1. A trust-enhancing service offered or performed by a Trust Service Provider (TSP) that supports the assurance, integrity or security of electronically executed activities, (e.g. Time-stamping, notarisation, watermarking etc.). 2. The service offered or performed by an Issuing Authority, Open Banking Registration Authority, Certificate Manufacturer or other trusted intermediary relating to the Issuance and control of Certificates e.g. manufacture, Issuance, Revocation, publication, registration, validity-checking or defining policy.
Trust Service Provider (TSP)	An entity that acts as a supplier of trust services. See also Party.
Validated/Validation	The process of Identification of Certificate Applications. "Validation" is a subset of "Identification" and refers to Identification in the context of establishing the identity of Certificate Applicants
Validity Period	The period that is defined within a Certificate, during which that Certificate is intended to be valid.
Verify (a Digital Signature and/or Message Integrity)	In relation to a given Digital Signature, Message and Public Key, to determine accurately: 1. That the Digital Signature was created during the Operational Period of a Valid Certificate by the Private Key corresponding to the Public Key listed in the Certificate; and 2. That the Message has not been altered since its Digital Signature was created.
X.501	Recommendation ITU-T X.501 | ISO/IEC 9594-2 titled "Information technology – Open Systems Interconnection – The Directory: Models".
X.509	Recommendation ITU-T X.509 | ISO/IEC 9594-8 titled "Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks".

Document History			
Version	**Date**	**Author(s)**	**Status**
1.0	4/12/17	Steven Lawrence	Initial Document
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	New definitions included for CD ASPSP and CD TPP
1.5	19/09/2024	Open Banking	Removal of definition for “Confirmation of Payee (CoP) Participant”; removal of reference to “CoP Participant” from the definitions of “Primary Technical Contact”, “Primary Business Contact” and “Subscribing PKI Participant”; and updating address for Open Banking Limited.