Trustis FPS

HMRC SET Certificate Service

Glossary of Terms

The following terminology shall have the definitions as given below:

Activation Data	Private data, other than keys, that are required to access cryptographic modules.
Asymmetric Cryptosystem	A system which generates and employs a secure key consisting of a Private Key for creating a Digital Signature and a Public Key to verify a Digital Signature. Also known as Public Key Cryptography.
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.
Certificate	A collection of data that at a minimum: 1. Identifies the Issuing Authority 2. Names or identifies its Subject 3. Contains the Subject's Public Key 4. Identifies the operational period of Certificate 5. Bears the Digital Signature of the Issuing Authority Also known as Digital Certificate
Certificate Authority (CA) Certificate Authority (CA) System	The software and hardware system used by the Issuing Authority or it's designated Certificate Manufacturer to issue and manage the full lifecycle of certificates.
Certificate Authority Certificate (CA-Certificate)	See Issuing Authority Certificate.
Certificate Authority Key (CA-Key)	The Private Key used by the CA for signing Certificates and other objects.
Certificate Discovery	The process of obtaining a subscribers 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 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 CP may be supported by one or more CPSs.
Certificate Profile	Defines the usage of the Certificate and is formally approved by the Policy Authority and the Issuing Authority.
Certificate Revocation List (CRL)	A list maintained by, or on behalf of, an Issuing Authority of the Certificates that it has issued, that have been Revoked or Suspended before the expiry stated in the Certificate.
Certificate Status Discovery	The process of ascertaining the Operational Status of a Certificate. Typically via a controlled mechanism from a Repository. Also known as Certificate Status Checking
Certificate Status Information	Information that indicates whether Certificates have been Revoked or Suspended; commonly provided via Certificate Revocation Lists, or individually through specific online enquiries (e.g. OCSP).
Certificate Service Provider (CSP)	See also Participant. The term CSP is used in connection with the EU Electronic Signatures Directive and Supporting ETSI Standards.
Certificate User	See Relying Party
Certification Authority	See Issuing Authority
Certification Path	A logical and ordered sequence of Certificates which, together with the Public Key of the initial object in the Certification Path, can be processed to obtain that of the final object in the Certification Path.
Certification Practice Statement (CPS)	A statement of the procedures and practices employed in the issuing, managing, revoking, and renewing of certificates. A CPS may support of one or more Certificate Policies.
Confirm	Ascertain through appropriate inquiry and investigation.
Content Commitment	An action whereby a signer of a message commits to the content being signed by them. This term is sometimes used synonymously with Non-Repudiation, however, in any specific context the detailed definition may result in its legal standing differing from that of Non-Repudiation. See also Non-Repudiation
Corresponding Private Key	Given a public key taken from a key pair, the corresponding private key is the private key from that same key pair, (and vice-versa for corresponding public key).
Cross-certificate	A Certificate used to establish a trust relationship

	between two Issuing Authorities.
Digital Certificate	See Certificate
Digital Signature	The result of a transformation of a message by means of a cryptographic system and a Hash Function, using keys such that a person who has the initial Message can determine: 1. Whether the transformation was created using the Private Key that corresponds to the signer's Public Key, and 2. Whether the initial Message has been altered since the transformation was made.
End-Entity	Those using Digital Certificates. See Subscriber and Relying Party
Hash Function	An algorithm mapping or translating one sequence of bits into another, generally smaller, set (the Hash or Message Digest) such that: 1. A Message yields the same Hash result every time the algorithm is executed using the same Message as input; 2. It is computationally infeasible that a Message can be derived or reconstituted from the Hash result provided by the algorithm; and 3. It is computationally infeasible that two Messages can be found that produce the same hash result using the algorithm
Hash	The output produced by a Hash Function upon processing a Message (see also Message Digest).
High Security Zone	An area to which access is controlled through an entry point and is limited to authorised, appropriately screened personnel and properly escorted visitors. High-Security Zones should be accessible only from Security Zones, and are separated from Security Zones and Operations Zones by a perimeter built to the specifications recommended in a threat risk assessment. High-Security Zones are monitored 24 hours a day and 7 days a week by security staff, other personnel or electronic means.
Hold a Private Key	To use or to be able to use a Private Key.
Incorporate by Reference	Make one Message a part of another Message by:- 1. Identifying the Message to be incorporated; 2. Providing information which enables the Receiving Party to access and obtain the incorporated Message in its entirety; and 3. Expressing the intention that it be part of the incorporating Message. The incorporated Message shall have the same effect as if it had been fully stated in the incorporating Message to the extent permitted by law.

Issuance (Issue a Certificate)	The acts of an Issuing Authority in creating a Certificate which is bound to a Subscriber. The process requires Authentication of the Subscriber and/or Subject.
Issuing Authority	By definition, an Issuing Authority is the entity listed in the issuer field of a Digital Certificate. The Issuing Authority may obtain benefit in return for taking on the risks associated with transactions secured by Digital Certificates, for example, risk of fraud. The Issuing Authority has the responsibility for deciding who may be issued with a Certificate carrying its name.
Issuing Authority Certificate	A Certificate for an Issuing Authority's Public Key, and for use in signing Certificates created by certificate authority software under its control.
Key Pair	In an Asymmetric Cryptosystem - 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.
Local Registration Authority (LRA)	See Registration Authority
Message	A digital representation of information.
Message Digest	The output produced by a Hash Function upon processing a Message.
Message Integrity	The assurance of the unaltered status of a Message.
Non-repudiation	Strong and substantial evidence of the identity of the Signer of a Message and of Message Integrity, sufficient to prevent a party from successfully denying the original submission or delivery of the Message and the integrity of its contents. See also Content Commitment
Notify	Communicate or make available information to another person as required under the circumstances
Online Certificate Status Protocol (OCSP)	A network protocol used to ascertain the current validity status of a Certificate.
Operational Period of Certificate	The Operational Period of a Certificate begins on the date and time it is issued by an Issuing Authority (or on a later date and time certain if stated in the Certificate), and ends at the completion of its Validity Period unless it is earlier Revoked or Suspended.
Operations Zone	An area where access is limited to personnel who work there and to properly escorted visitors. Operations Zones should be monitored at least periodically, based on a threat risk assessment, and should preferably be accessible from a Reception Zone.
Participant	An individual or organisation that plays a role within a given a PKI, typically as a Subscriber, Relying Party, CA, RA or Certificate Manufacturer. Entities other than Subscribers, Subjects and Relying Parties (i.e. not End Entities) may also be known as a Trust Service Provider

	(TSP) or a Certificate Service Provider (CSP).
Public Key Infrastructure (PKI)	A system of Digital Certificates, Certificate Authorities, and other components that verify and authenticate the validity of parties involved in electronic transactions.
PKI Disclosure Statement (PDS)	An instrument that supplements a CP or CPS by disclosing critical information about the policies and practices of a CA/PKI. A PDS is a vehicle for disclosing, summarising and emphasizing information normally covered in detail by associated CP and/or CPS documents. A PDS is not intended to replace a CP or CPS.
Policy Authority	The entity that has ultimate responsibility for governance and control over the issuance, management and usage of a specified set of Digital Certificates. It uses a Certificate Policy as the mechanism to exercise control over all Participants in a PKI. Also known as Policy Management Authority (PMA).
Policy Qualifier	Policy dependent information that may accompany a CP identifier in an X.509 certificate.
Post-Authorisation	A Registration Authority process whereby Certificate Applicants have their identity authenticated during the Certificate application process. Also know as Post-Authentication
Pre-Authorisation	A Registration Authority process whereby Certificate Applicants have their identity authenticated prior to submitting a Certificate application. Also know as Pre-Authentication
Private Key	The private part of an asymmetric key pair used for public key encryption techniques. The Private Key is typically used for signing Digital Signatures or for decrypting Messages.
Public Key	The public part of an asymmetric 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 Cryptography	See Asymmetric Cryptosystem
Public-access Zone	An area in which there is no personnel access control. Generally surrounds or forms part of a security facility. Examples include the grounds surrounding a building, and public corridors and elevator lobbies in multiple-occupancy buildings. Boundary designators such as signs and direct or remote surveillance may be used to discourage unauthorised activity.
Reception Zone	The entry to a facility where the initial contact between the public and the facility occurs, where services are provided, information is exchanged and access to restricted (Operations, Security and High-security) zones

	is controlled. To varying degrees, activity in a Reception Zone is monitored by the personnel who work there, by other personnel or by security staff. Access by the public may be limited to specific times of the day or for specific reasons. Entry beyond the Reception Zone is indicated by a recognisable perimeter such as a doorway or an arrangement of furniture and dividers in an open office environment.
Registration Authority (RA)	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. An RA does not have responsibility for signing or issuing Certificates or Certificate Status Information.
Registration Authority Operator (RAO)	Registration Authority staff member with approvals to conduct a full set of Certificate management functions
Relying Party	A recipient of a Certificate who acts in reliance on that certificate and/or any Digital Signatures verified using that Certificate. Also known as Certificate User.
Relying Party Agreement (RPA)	An agreement between an Issuing Authority and a Relying Party that typically establishes the rights and obligations between those parties regarding the verification of Digital Signatures or other uses of Certificates. Also known as Relying Party Charter.
Repository	The entity providing community-wide accessible mechanisms by which Participants can obtain Certificate or Certificate Status information to validate Certificates, and obtain Policy and other controlling information for the PKI.
Re-Key a Certificate	The process by which an existing Certificate has its Public Key value changed by issuing a new certificate with a different (usually new) Public Key. Notably all characteristics relating to the Subject of the Certificate remain unchanged unless Re-Key is combined with a Renewal or Issuance of a new Certificate.
Renewal (Renew a Certificate)	The process by which an existing Certificate that is bound to a Subscriber is replaced by issuing a new Certificate to that Subscriber. Typically this is based upon the validity of the existing Certificate. This process

	normally involves a Re-Key.
Revocation (Revoke a Certificate)	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.
Security Zone	An area to which access is limited to authorised personnel and to authorised and properly escorted visitors. Security Zones should preferably be accessible from an Operations Zone, and through a specific entry point. A Security Zone need not be separated from an Operations Zone by a secure perimeter. A Security Zone should be monitored 24 hours a day and 7 days a week by security staff, other personnel or electronic means.
Signer	A person who creates a Digital Signature for a Message.
Subject	The entity named or identified in a certificate issued to a person, organisation or device, and who holds a Private Key corresponding to the Public Key listed in the Certificate. A Subject may also be a Subscriber. A Subject must always be either: 1. a Subscriber or 2. formally bound under the jurisdiction of a Subscriber
Subscriber	An entity that contracts with an Issuing Authority for the issuance of Certificates. The Subscriber bears ultimate responsibility for the use of the Private Key associated with the Certificate. The Subscriber may be a Subject acting on its own behalf.
Subscriber Agreement	An agreement between an Issuing Authority and a Subscriber that establishes the rights and responsibilities of the parties regarding the issuance and management of Certificates and Associated Private Keys.
Suspension (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 apart 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 persevere the integrity of the Time-stamp.
Time-stamping Authority	The Trust Service Provider operating, controlling and issuing time-stamps for use by other entities.
Trust Infrastructure	See Public Key Infrastructure
Trust Service	1. A trust-enhancing service offered or performed by a Trust Service Provider 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, Registration Authority, Certificate Manufacturer or other trusted intermediary relating to the issuance and control of Digital 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 Participant. Also known as Certificate Service Provider (CSP)
Trustworthy System	Computer hardware, software and procedures that: 1. Are adequately secure from intrusion and misuse; 2. Provide an adequate level of availability, reliability and correctness of operation; 3. Are adequately suited to performing their intended functions; and 4. Adhere to generally accepted security principles.
Validation	See Authentication
Validity Period	The period that is defined within a Certificate, during which that Certificate is intended to be valid. See also Operational Period
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.
Vettor	Registration Authority staff member with approvals to conduct a limited set of Certificate management functions