UTSP Trust Service PKI Definitions

Document Version Control			
Version	Date	Author	Changes
1.1	11-12-2017	Tom Jerrard	Original Document
1.2	03-03-2020	Praveen Jain	UTSP (Part of pay.UK) logo updated

Copyright © UTSP Limited 2017

This document is the master list of UTSP defined terms and acronyms. These terms are used in the Certificate Policy and elsewhere. The intention is that all terms in UTSP contracts and other documents should be consistent. If any inconsistency is noticed please inform: UTSP@wearepay.uk

No.	Term	Meaning
1.	Activation Data	Private data, other than keys, that are required to access cryptographic modules.
2.	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. See also: Message
3.	Bacs	means Bacs Payment Schemes Limited or any organisation/company that is a successor to Bacs Payment Schemes Limited.
4.	Bacs Payment Services Website	**"Bacs Payment Services Website"** or **"Bacs PSW"** means the website owned and operated by Bacs and used for the purposes described in the Websites section of IPL00114, the live version of this website having the URL: paymentservices.bacs.co.uk and the "customer readiness" version having the URL: testservices.bacs.co.uk. See also IPL00114.
5.	Bacstel-IP	**"Bacstel-IP"** means the mechanism and processes adopted by Bacs to enable a user of the payment system operated by Bacs to authenticate, sign and submit payment messages to such payment system and to validate, confirm receipt and report on the processing of such payment messages.
6.	Bacs Service	**Bacs Service** means the end-to-end payment scheme for the processing and settlement of Bacs direct debit and direct credit transactions.

No.	Term	Meaning
7.	Central Infrastructure	means the infrastructure and systems which undertake or otherwise enable the automated clearing and settlement of payments for the Faster Payments Service and Bacs as administered by Pay.UK Limited.
8.	Certificate	Certificate means a data structure containing information which: (a) identifies the Certification Authority issuing that data structure; (b) unambiguously names or identifies the Certificate Subject of it; (c) contains the Certificate Subject's Public Key; and (d) is digitally signed by the Certification Authority issuing it.
9.	Certificate Authority ("CA")	means the technical system component operated by the Certification Authority that issues Certificates and maintains information about their status. See also Certification Authority.
10.	Certificate Discovery	The process of obtaining a Subscribers certificate. Typically, from a directory or database.
11.	Certificate Manufacturer	The entity providing certificate management services and facilities for an Issuing Authority. These services are currently provided by Trustis.
12.	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 Relying Party 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. See also: Certification Practice Statement (CPS)
13.	Certificate Profile	means a specification of the fields and format of those fields contained within a Certificate.
14.	Certificate Re-key (Re-key)	The process by which an existing Certificate has its Public Key value changed by issuing a new certificate with a different Public Key (and therefore a new Private Key). The content of the Certificate is unchanged apart from the Public Key, the serial number and effective date information.

No.	Term	Meaning
15.	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.
16.	Certificate Service Provider (CSP)	CSP is a provider of the following services: 1. Certificate manufacturer services 2. Repository services 3. Validation authority (OCSP responder provider) services Trustis Limited *(contracted to UTSP)* provides the above services to Participants as part of the Trust Service.
17.	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). See also Online Certificate Status Protocol (OCSP)
18.	Certificate Subject (or Subject)	means, in respect of a Certificate, the person or device (such as a HSM) named in the Subject field of that Certificate or 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 Certificate Subscriber. A Subject must always be either a Certificate Subscriber or formally bound under the jurisdiction of a Certificate Subscriber. For example, a Participant's employee will have a contract of employment and a Certificate Subject Agreement with the Participant.
19.	Certificate Subject Agreement	An agreement between a Certificate Subscriber and a Certificate Subject that establishes the rights and responsibilities of the parties regarding the issuance and management of Certificates and associated Private Keys.
20.	Certificate Subscriber	Means an organisation, including a Participant or a Participant's Customer or a Participant's Supplier who requests or holds one or more Certificates. Usually the Certificates will be held by the Certificate Subject acting on behalf of the Certificate Subscriber. The Certificate Subscriber will access the Scheme

No.	Term	Meaning
		Services in order to execute some business or operational function. The Certificate Subscriber has a contractual relationship with UTSP in the case of a Participant or with the Participant in the case a Participant's Customer or a Participant's Supplier. The Certificate Subscriber bears ultimate responsibility for the use of the Private Key associated with the Certificate.
21.	Certification Authority (or CA)	means the entity responsible for the certification of Public Keys, the issuance of Certificates and the maintenance of Certificate status information.
22.	Certification Practice Statement (CPS)	A statement of practices that a Certification Authority (CA) employs in issuing, managing, revoking, and renewing or re-keying Certificates.
23.	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
24.	Cross-certificate	A Certificate used to establish a trust relationship between two Issuing Authorities. Note that Cross-certificates are not used by the UTSP Trust Service in order to maintain compliance with the Bacs Trust Service Code of Conduct.
25.	Credentials	The Certificate, Private Key and Public Key used to establish the claimed identity of a Certificate Subject.
26.	Digital Certificate	See Certificate.
27.	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 receives a 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 Message has been altered since the transformation was made. See also Message.

No.	Term	Meaning
28.	Distinguished Name	The meaning given to it in X.501 version November 2008, as updated, amended and replaced from time to time.
29.	End-Entity	Means: 1. Certificate Subscribers 2. Certificate Subjects 3. Relying Parties using UTSP Digital Certificates.
30.	Enrolment Officer	Means a person nominated by a Participant to carry out the Enrolment Procedures on behalf of the Participant and authorised by the Issuing Authority to do so.
31.	Enrolment Procedures.	Means the business processes defined and used by each Participant for the issuing of Certificates.
32.	Faster Payments Service	Faster Payments Service has the meaning given to it in the FPS Rules.
33.	Faster Payments Website	Means the website owned and operated by FPSL and used the Participant for the purposes described in the Websites section of IPL00114, the live version of this web site having the URL: iplservices.voca.com and the "customer readiness" version having the URL: member.testservices.voca.co.uk.
34.	FPSL	"FPSL" means Faster Payments Scheme Limited, a company incorporated and registered in England and Wales (company no. 07751778) having its registered office at 2 Thomas More Square, London, E1W 1YN (or any organisation/company that is a successor in title to FPSL)
35.	FPSL Rules	"FPS Rules" means the rules of the Faster Payments Service, as updated, amended and replaced from time to time, the current version of which are published at: http://www.fasterpayments.org.uk/membership/access-options/direct-membership/scheme-documentation.

No.	Term	Meaning
36.	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
37.	Hold a Private Key	To use or to be able to use a Private Key.
38.	IPL00114	IPL00114 means the document published by VocaLink titled "FPS Reference data maintenance Member, agency and scheme guide" version 2.60 dated 12 June 2015 with reference IPL00114.
39.	Issuance (Issue a Certificate)	The acts of an Issuing Authority in creating a Certificate which is bound to a Certificate User. The process requires Authentication of the Certificate Subscriber and/or Certificate User.
40.	Issuing Authority	By definition, an Issuing Authority is the entity listed in the issuer field of a Digital Certificate. For the UTSP Trust Service, being the Issuing Authority is a role of UTSP Limited.
41.	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.
42.	Local Registration Authority (LRA)	That part of the overall Registration Authority that is delegated to a Participant and operated by their Enrolment Officers.
43.	Message	means data being transmitted. In the context of payment systems a Message will be sent by or received by the Central Infrastructure.
44.	Non-repudiation	means 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.
45.	Notify	Communicate or make available information to another person as required under the circumstances
46.	Online Certificate Status	Means the Online Certificate Status Protocol as defined

No.	Term	Meaning
	Protocol (OCSP)	in RFC 6960.
47.	OCSP Certificate Status Information	See Certificate Status Information.
48.	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.
49.	Participant	Participant means an organisation that has entered into an Agreement with UTSP for the provision of PKI Services. See also: UTSP UTSP Trust Service Participant Agreement UTSP RtP Heads of Terms Agreement
50.	Participant Process Definitions	Means the process definitions supplied by UTSP to the Participants that specify the business processes that are to be implemented by each Participant in connection with the use and operation of the Trust Service.
51.	Payment Schemes	UK payment or payment related systems provided by Pay.UK Limited including but not limited to the services of Bacs, the Faster Payments Service, RtP and the services of its subsidiary Mobile Payments Service Company Limited (Paym) (or any organisation/company that is a successor in title to these companies) See also: Scheme Services.
52.	Personal Data	This has the meaning set out in the UK Data Protection Act 2018.
53.	Public Key Infrastructure (PKI)	Public Key Infrastructure or PKI means the technical infrastructure required to provide and support the management of Private Keys and Public Keys and the provision of related authentication, encryption, integrity or non-repudiation services.
54.	PKI Card	means any handheld hardware device or card that is able to hold a Private Key in a secure fashion.
55.	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). Being the Policy Authority is a role of UTSP.

No.	Term	Meaning
56.	Policy Qualifier	Policy dependent information that may accompany a CP identifier in an X.509 certificate.
57.	Pre-Authorisation (Pre-Authentication)	A Registration Authority process whereby Certificate Applicants have their identity authenticated prior to submitting a Certificate application. Also known as Pre-Authentication
58.	Private Key	Private Key means the private key of an asymmetric cryptographic key pair. The Private Key is typically used for signing Digital Signatures or for decrypting Messages.
59.	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.
60.	Public Key Cryptography	See Asymmetric Cryptosystem
61.	Registration Authority (RA)	Registration Authority or RA means the entity that manages the registration and certificate lifecycle processes for Certificate Subscribers and Relying Parties. For example: 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. Some of the functions of the RA are delegated to the Participant's Local Registration Authority function, for example, the Participant aspects of the processes listed above. An RA does not have responsibility for signing or issuing Certificates or providing Certificate Status Information.
62.	Registration Authority Operator (RAO)	Means a Registration Authority staff member with approvals to conduct a full set of Certificate management functions
63.	Registration Policy and Procedures	Means the policies and procedures established by UTSP acting as Registration Authority and also the procedures recommended by UTSP for use by Participants which are then embodied in the Participant's Local Registration Authority procedures.

No.	Term	Meaning
64.	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 Public Key. See Certificate Re-key.
65.	Relying Party	Relying Party means the person that relies on the identity (of a Certificate Subject) to undertake specified business actions such as accepting and processing a payment request.
66.	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.
67.	Relevant Party or REP	Shall mean to include any Participant, Certificate Subscriber, Relying Party (each referred to as a "Relevant Party" or "REP") who is/are responsible for observing the terms of the Certificate Policy and for administering or flowing through its terms to a party (including to another REP) or their respective individual users to the extent such party or individual is involved in an activity of Relying or using a UTSP Certificate. See also: Trust Service Terms
68.	Renew a Certificate	The process by which an existing Certificate that is bound to a Certificate User is replaced by issuing a new Certificate to that Certificate User.
69.	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.
70.	Request Form (UTSP Request Form) (for RtP this may be referred to as an Enrolment Form)	The form that is used to complete the details of those entities wishing to use the Trust Services or such other services as may be offered from time to time by UTSP.
71.	Revocation (Revoke a Certificate)	Permanently end the Operational Period of a Certificate from a specified time.
72.	Revocation Information	Information required before enacting a Certificate Revocation (or Suspension). It must include evidence of the authenticity of the requestor.
73.	RFC 3647	Means the document published by the Internet Engineering Task Force with reference RFC 3647 titled "X.509 Internet Public Key Infrastructure Certificate

No.	Term	Meaning
		Policy and Certification Practices Framework" and available at: https://tools.ietf.org/html/rfc3647.
74.	RFC 6960	Means the document published by the Internet Engineering Task Force with reference RFC 6960 titled "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP" and available at: https://tools.ietf.org/html/rfc6960.
75.	RtP	Means Request to Pay which is a secure messaging service.
76.	RtP Participant	Means an organisation that has signed an agreement with Pay.UK to participate in the RtP service.
77.	Secure-IP	"Secure-IP" means the mechanism and processes adopted by FPSL to enable a user of the payment system operated by FPSL to authenticate, sign and submit payment messages to such payment system and to validate, confirm receipt and report on the processing of such payment messages.
78.	Scheme Services	Means services provided by the Payment Schemes to their respective Participants and when appropriate to the Participant's Customers. The Scheme Services include but are not limited to the following: a) the Bacs Payment Services; b) the Faster Payments Service; c) Bacstel-IP; d) Secure-IP. e) RtP
79.	Subject	See Certificate Subject.
80.	Subject Agreement	See Certificate Subject Agreement
81.	Subscriber	See Certificate Subscriber. See also Participant.
82.	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.
83.	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 a 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.
84.	Entrust (Europe) Limited (also defined as"Trustis")	a company incorporated in England and Wales (registered no. 03613613) that carries on the business of building, operating and supplying PKIs and related products and services to enable the end-to-end

No.	Term	Meaning
		provision of a Trust Service.
85.	Trustis Service	Trustis is contracted by UTSP to provide the following services that form part of the Trust Service: (a) establish and maintain a Public Key Infrastructure that is accredited against and complies with the Bacstel-IP Rules, Bacs TSCoC, FPS Rules and FPSL Security Code of Conduct; (b) provide certification authority services to the standards and requirements set out in the Bacstel-IP Rules, Bacs TSCoC, FPS Rules and FPSL Security Code of Conduct; (c) provide and maintain a Certificate Practice Statement in conformance with RFC 3647; and (d) maintenance and support of IT systems and related infrastructure that is used by UTSP to provide the Trust Service (including the Certification Authority, Registration Authority and related components); and (e) supply of resale products (e.g. Gemalto software and hardware)
86.	Trustis Service Contract	Means the agreement that governs the provision of the Trustis Service provided by Trustis to UTSP.
87.	Trust Service	Trust Service means a Public Key Infrastructure (PKI) service consisting of a Certification Authority (CA), Registration Authority (RA) and a Validation Authority (VA) that in combination are able to issue, manage and certify Certificates to enable the authentication and encryption of digital communications. This definition shall also include where the context so permits such roles and services provided by parties participating in a PKI as more specifically set out in Section 1.3 of the Certificate Policy *("Parties in the PKI Trust Service").*
88.	Trust Service Provider (TSP)	An entity that acts as a supplier of Trust Services and shall be interpreted to include all such parties and roles that are identified in Section 1.3 of the Certificate Policy *("Parties in the PKI Trust Service")*. Trustis Limited *(contracted to UTSP)* provides CSP and such services that are identified in Section 1.3 of the Certificate Policy to Participants as part of the Trust Service. See also: Participant. Relevant Parties (REP)

No.	Term	Meaning
		Trustis UTSP
89.	Trust Service Terms	Means to include all terms and conditions that is/are applicable to parties that are participating in a PKI including terms of the Certificate Policy and any other Policy Document referenced therein including contractual arrangements by and between REPs to observe or flow through or promulgate the terms of the Certificate Policy. See also: Relevant Parties (REP)
90.	tScheme	Means tScheme Limited, a company incorporated and registered in England and Wales (company no. 04000985). See http://www.tscheme.org for further information.
91.	UTSP	Means UTSP Limited, a company incorporated and registered in England and Wales (company no. 10281396) and having its registered office at 2 Thomas More Square, London, E1W 1YN or such organisation or company that may be a successor in title from time to time
92.	UTSP RtP Heads of Terms Agreement	Means the agreement signed between UTSP and Pay.UK Limited under which UTSP provides Trust Service to Pay.UK.
93.	UTSP Trust Service Participant Agreement	Means the agreement between UTSP and the Participant under which the UTSP provides a Trust Service to it. See also: Participants
94.	Validation	See Authentication
95.	Validation Authority	Means the entity checking the status of digital certificates.
96.	Validity Period	The period that is defined within a Certificate, during which that Certificate is intended to be valid. See also Operational Period
97.	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

No.	Term	Meaning
		2. That the Message has not been altered since its Digital Signature was created.
98.	Vettor	Registration Authority staff member with approvals to conduct a limited set of Certificate management functions
99.	VocaLink	Means VocaLink Limited
100.	X.501	Means Recommendation ITU-T X.501 | ISO/IEC 9594-2 titled "Information technology – Open Systems Interconnection – The Directory: Models".
101.	X.509	Means Recommendation ITU-T X.509 | ISO/IEC 9594-8 titled "Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks".
102.	X.509 Certificate	Means a Certificate that complies with X.509.