UTSP PKI Disclosure Statement

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

The purpose of this document is to summarise the key points of the UTSP Certificate Policy for the benefit of Subscribers and Relying Parties.

The Certificate Policy under which Certificates are issued is defined by the UTSP Certificate Policy. You must read the Certificate Policy at www.trustis.com/pki/utsp before you apply for or rely on a Certificate issued by the UTSP Issuing Authority.

Terms used in this document are defined in the UTSP Glossary located at www.trustis.com/pki/utsp.

1. Policy Authority & Issuing Authority Contact Info:

1. **Policy Authority:**
   UTSP Policy Authority

   Mailing Address:
   UTSP Limited,
   2, Thomas More Square,
   London,
   E1W 1YN,
   UK
   email: UTSP@wearepay.uk

2. **Issuing Authority:**
   UTSP Issuing Authority

   Mailing Address:
   UTSP Limited,
   2, Thomas More Square,
   London,
   E1W 1YN,
   UK
   email: UTSP@wearepay.uk

2. Certificate Type, validation procedures and usage:

The Certification Services provided by UTSP implement a closed public key infrastructure in the sense that access and participation is only open to those who both satisfy eligibility criteria and are approved by UTSP. The Participants providing trust services and End-Entities authorised and approved to issue, obtain, use, and/or rely upon Certificates that reference the Certificate Policy are clearly defined. Participation is conditional upon agreeing to be bound by the terms of the Certificate Policy.

The Certification Services provided by the UTSP Issuing Authority support secure operations and interactions with the general public, agent organisations, partners, customers and external contractors in the direct pursuit of UTSP related business, or in the authorised usage of services provided by UTSP. 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.

Certificates issued under this Certificate Policy may only be used for the following purposes:

- Authenticated access to UK payment or payment related systems of Pay.UK Limited including but not limited to the services of The Payment Schemes.
- Digital signing of payment transactions and payment files and other submissions to the Payments Schemes' Central Infrastructure provider(s) by Payment Scheme participants and their authorised customers.

- Digital signing of data to be sent by the Payments Schemes' Central Infrastructure provider(s) to Payment Scheme participants.

Applicants for Certificates are required to submit to the validation of identity credentials and their eligibility to hold such a Certificate as detailed in the certificate enrolment procedures detailed at www.trustis.com/pki/utsp.

Acceptable documentary evidence that can be provided in support of an application for a Certificate is detailed in www.trustis.com/pki/utsp.

3. Reliance Limits:

UTSP does not set reliance limits for Certificates it issues. Reliance limits may be set by applicable law or by agreement. See Limitation of Liability below.

4. Obligations of Subscribers:

Subscribers must comply with the requirements as defined in the Subscriber Agreement at www.trustis.com/pki/utsp.

It is the responsibility of the Subscriber 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 Registration Authority and/or Issuing Authority as to the information required to determine eligibility for a Certificate and for information contained within the Certificate
- In accordance with the UTSP Certificate Policy, exclusively use the Certificate for legal purposes and restricted to those authorised purposes detailed by the UTSP Certificate Policy
- Immediately notify the Registration Authority of a suspected or known compromise of Certificate security in accordance with the procedures laid down in the UTSP Certificate Policy.

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

For Subjects holding Certificates and acting on behalf of Subscribers, the Subscriber must ensure all responsibilities are met.

WARNING: If a Subscriber's Private Key is compromised, unauthorised persons could decrypt or sign messages with the key and commit the Subscriber to unauthorised obligations.

5. Certificate Status checking Obligations of Relying Parties:

Relying Parties must comply with the requirements as defined in the UTSP PKI Relying Party Agreement at www.trustis.com/pki/utsp.

A Relying Party may justifiably rely upon a Certificate only after:

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

6. Limited Warranty & Disclaimer/Limitation of Liability:

The Issuing Authority assumes no liability whatsoever in relation to the use of Certificates or associated Public/Private Key pairs issued under the Certificate Policy for any use other than in accordance with the Certificate Policy and any other agreements. Subscribers will immediately indemnify the Issuing Authority from and against any such liability and costs and claims arising therefrom.

The Issuing Authority 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 Issuing Authority's negligence, wilful misconduct, or where otherwise required by applicable law.

Nothing in the Certificate Policy excludes or restricts liability for death or personal injury resulting from negligence or the negligence of its employees, agents or contractors.

The Issuing Authority excludes all liability of any kind in respect of any transaction into which an End-Entity may enter with any third party.

The Issuing Authority 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 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.

7. Applicable Agreements, Certification Practice Statement, Certificate Policy:

Copies of the Certificate Policy, Certificate Subscriber Agreement, Certificate Subject Agreement, Relying Party Agreement and the Definitions document that are updated from time to time are published by the Issuing Authority at http://utsp.trustis.com/.

The Certification Practice Statement is confidential to Trustis and UTSP.

8. Privacy Policy:

UTSP strongly believes in an individual's rights to privacy, and operates the Certification Service according to the Privacy Policy which man be found at www.trustis.com/pki/utsp.

9. Refund Policy:

The UTSP Issuing Authority does not provide refunds for issued Certificates.

10. Applicable Law & Dispute Resolution:

Disputes between Participants and UTSP shall be handled in accordance with the UTSP Trust Service Participant Contract.

11. CA & Repository Licences Trust Marks & Audit:

Certificates are manufactured under the Certificate Policy through the use of a Trustis Limited service which is both accredited to ISO 27001:2013 and has attained tScheme approval.

Audit is carried out on a periodic basis required to maintain security and trust accreditations. The Auditors that have been approved under the Certificate Policy are:

- Audit resources of contracted Participants providing trust services.
- A certified public accountant with demonstrated expertise in computer security or an accredited computer security professional

12. Identification of this Certificate Policy:

All Certificates issued under the Certificate Policy with the exception of Certificates issued for the RtP Service have been assigned an Object Identifier (OID) of 1.3.6.1.4.1.5237.131.1.1.

All Certificates issued under the Certificate Policy for the RtP Service have been assigned an Object Identifier (OID) of 1.3.6.1.4.1.5237.131.1.2.

13. Approved Registration Authorities

The following Registration Authorities have been approved by the Issuing Authority to register Subscribers under the Certificate Policy:

- UTSP Issuing Authority
- UTSP PKI Participant LRA Enrolment Officers

14. Approved Repositories

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

- Trustis Limited
- UTSP Limited

15. Eligible Subscribers

A Certificate Subscriber must be a Participant who has signed a UTSP Trust Service Participant Agreement with UTSP or a Participant's Customer or Participant's Supplier who has a contract with the Participant that requires them to abide by the obligations set out in the Certificate Policy. The Subscriber Agreement can be found at www.trustis.com/pki/utsp.

16. Eligible Relying Parties

Relying Parties who are eligible to Rely on Certificates Issued under the Certificate Policy are specified below:

- Participant (s) of the Trust Service provided by UTSP and their customers.

- UK payment or payment related systems of Pay.UK Limited including but not limited to the services of the Payment Schemes.
- The Central Infrastructure provider(s) to the Payment Schemes.

The Relying Party Agreement can be found at www.trustis.com/pki/utsp.

17. Certificate Status Information

Certificate Status information confirming the validity of certificates is updated every 2 - 2½ hours through the generation of a new CRL, or immediately upon a Certificate revocation. The Certificate Status information is made available via a Trustis OCSP Service. The OCSP service location is identified via an AIA entry in Subscriber Certificates.