# UTSP Trust Service PKI

# Privacy Policy

Date: 13th July 2017

Revision: 001



## 1. INTRODUCTION

A. A Participant, Subscriber, Relying Party or Subject *(each referred to as a Relevant Party or REP as defined in the Certificate Policy Definitions)* is responsible for observing these terms and for administering or flowing through these terms to a party (including to another REP) or their respective individual users to the extent such party or individual share their Personal Data in relation to or for the purpose of the Trust Service.

B. The Privacy Policy and its terms shall form a binding agreement between (i) a REP and another REP ( where relevant); or (ii) a REP and its respective individual users. Further in either case each party shall require the other party to flow down these terms to their respective individual users.

## 1.1 DEFINITIONS

Capitalised terms that are not defined in this Privacy Policy are defined in the Certificate Policy Definitions at https://utsp.trustis.com/policy

**"Data Protection Law"** means the (UK) Data Protection Act 1998 and such provisions of the EU Data Protection Directive 95/46/EC as implemented in the UK and as amended or replaced from time to time; and "Controller", "Consent", "Processor", "Data Subject", "Personal Data, "Personal Data Breach" and "Processing" shall have the same meanings as in the Data Protection Law and "Processed" and "Process" shall be construed in accordance with the definition of "Processing".

A party or individual to whom this Privacy Policy is issued to is referred to herein as "**You**".

Parties to each issue of the Privacy Policy agreement will be identified in the cover page of the Privacy Policy.

## 2. WHAT INFORMATION IS COVERED BY THIS PRIVACY POLICY

This Privacy Policy covers Personal Data that is voluntarily supplied by You *(or on behalf of a REP or respective individual user(s))* as part of an enrolment process to, or for using or accessing the Trust Service *(or any part thereof)* plus any additional information about You, a REP *(and or their respective individual users)* that is supplied by any third party 'information source' at the request of a relevant REP, an Issuing Authority, a Registration Authority or a Policy Authority but excluding PINs, password, passphrases, challenge phrases and other information that may create a security risk if divulged.

## 3. PURPOSE OF USE

The Personal Data that You supply under Section 2 is used for the following purpose:

a) To bind some of the Personal Data into the Certificate itself. For example, a personal e-mail address or web server URL and personal names may form part of a Certificate and identify it to other Relying Parties;

b) To establish certain facts about the relevant REP or its user(s) whether at an individual and or company/organisational level. For example, an individual's name, company name and/or department name supplied may be used:
   i. To check with a third party agent that the individual, company and/or department is a real entity, is eligible to receive a certificate and is still active; and
   ii. To check that the application for a Certificate is legitimately made by the individual, company and/or department.

c) In order to verify old documents signed with a Private Key that corresponds to the Public Key in a Certificate that may have lapsed some time before, the Personal Data may be retained by the Registration Authority beyond the expiry date of the Certificate. Details of this period can be found in Section 5.4.3 read with Section 5.5.2 of the Certificate Policy.

d) In order to: (a) validate Certificate application information; (b) issue the Certificate and publish it to potential Relying Parties, the Registration Authorities acting on its behalf may need to communicate Your Personal Data to one or more of:

   i. Authorised and trusted service providers that are involved in the management of Certificates.

   ii. Third party information providers, where external corroboration of applicant data is required to provide adequate confidence in that data.

All of these external agents are bound by contract to the relevant Trust Service Provider to observe the same or a substantially equivalent privacy policy.

## 4. CONSENT

4.1 You hereby give Your explicit consent to the REP issuing the Certificate *(including the right to give instructions/authorisations to other parties on Your behalf)* to use and or Process Your Personal Data in order to:

a) enable the REP or relevant Trust Service Provider (s) to confirm, verify, validate Your identity in connection with the provision of the Trust Service and or store, share Your Personal Data with such parties or carry out all such activities that are set out Section 3 above; and

b) (where relevant) in addition to the above use/or Process Your Personal Information for reporting, billing, conducting security checks and auditing the Trust Service.

(“**the Authorised Purpose”).**

4.2 If You are not happy with a REP or Trust Service Provider holding Your Personal Data, You may request relevant REP in writing to deactivate or delete Your Personal Data as per in accordance with and subject to Section 7 below.

4.3 If you do not agree to your Personal Date being held then You cannot be issued with a Certificate.

## 5. YOUR RIGHTS

5.1 You have a right to ensure that:

a) the Personal Data on You is accurately recorded as supplied by You.

b) Personal Data held on You is processed legally, fairly, securely and only for the Authorised Purpose for which it was originally collected.

c) You are made aware of the purposes to which your Personal Data are put and with whom it is shared.

5.2 You are entitled to object to:

a) such Processing of Your Personal Data that is not covered by the Authorised Purpose; or

b) any use of Your Personal Data for marketing purposes.

5.3 You will be able to see a copy of Personal Data held on yourself (whether originally supplied by You or by a third party) but not including PINs, passwords or passphrases and possibly certain other information that might create a security risk. You may request REP in writing for a copy in intelligible form of Your Personal Data held by the REP. The e-mail will be sent only to the individual who corresponds to the e-mail address bound into the Certificate. The individual will be required to adequately identify himself or herself as the party entitled to obtain this data before it is released the data pursuant to such request.

5.4 You have the right to request in writing that You review Your Personal Information that the REP holds and for such data to be provided in an intelligible readable form. You may check Your Personal Data for accuracy and consistency. In the unlikely event that errors are found in Your Personal Data You have the right to have it corrected. Please however see Section 7 below on the effect of amending Personal Data.

5.5 You have the right to request deletion or deactivation of Your Personal Data but You must take note of Section 3 (c) and the sub provisions of Section 7 below.

## 6. OUR COMMITMENT

6.1 REP is committed to keeping Your Personal Data is safe and to fully observe Your rights under the Data Protection Law and this Policy.

6.2 Your Personal Information is used and Processed only for the Authorised Purpose. Your Personal Data will not be used outside the Authorised Purpose.

6.3 Your Personal Information will not be used to compile user profile(s) that is not a part of the Authorised Purpose.

6.4 REP or the Trust Service will not store or use cookies in Your computer to keep track of You.

6.5 REP will not sell Your Personal Data.

6.6 None of the statements made in this Policy affect any other applicable statutory rights You may have under Data Protection Law.

6.7 Processing will be legal, fair and confidential. Any Processing carried out on Your Personal Information data will be subject to Your consent for the Authorised Purpose (Section 4 above*)* and carried out securely.

6.8 Where data needs to be transported it will done so in a secure manner, including when this is to authorised and trusted service providers.

6.9 If Your Personal Information is sent to countries outside the European Economic Area then agreements are in place which ensures that the level of protection is not diminished

## 7. CORRECTING OR DELETING PERSONAL DATA

7.1 If You are not happy with us holding Your Personal Data, You may request REP to deactivate it, thus making it unavailable for further use. Note that this may mean that You (or Your organisation) can no longer access the Trust Service and or be provided with digital certification services.

7.2 A REP or the Trust Service Provider cannot update the information contained within a Digital Certificate without destroying its integrity since each Digital Certificate is digitally signed. If any attempt is made to amend the information in the Certificate subsequently, the Digital Signature will no longer verify its content. The Certificate will no longer be capable of being relied upon by someone else wishing to verify signatures created with the Private Key portion related to the Public Key bound into that Certificate. In such cases, the existing Certificate must be revoked and a new one issued that contains corrected information.

7.2.1 Where a Certificate is held on a PKI Card then the Certificate cannot be destroyed on request without destroying the PKI Card.

7.2.2 The data held on the OCSP Responder has to be held until after the expiry of the Certificate in order to maintain the security and integrity of the Trust Service.

7.3 A REP can only update Personal Data information which is on its records and provided that is not bound into the Certificate itself. If you would like to correct or update any such information please contact the authority to whom you originally made Your Certificate application.

7.4 In order that other Relying Parties may see the status of a given Certificate at any time, all Certificates issued may be left physically present within the Repository for such time in line with the sub-provisions of this Section 7 and Section 3(c) above. During this time, physical deletion of Personal Data information pertaining to the Certificate itself may not be not carried out, since this would prevent status checking by Relying Parties wishing to look up another's Certificate before Relying upon it and would prevent the verification of Digital Signatures made whilst the Certificate was active. The Repository will however indicate the Certificate as being invalid. Any Personal Data held which is not absolutely required for these purposes will be removed or otherwise made inaccessible.

.