

# Chamber Simply Sign Certificate Policy PKI Disclosure Statement

**Important Notice:**

This document (PKI Disclosure Statement) does not by itself constitute the Certificate Policy under which Certificates governed by this Certificate Policy are issued. You must read the Base Certificate Policy at [www.simplysign.co.uk/terms-conditions.asp](http://www.simplysign.co.uk/terms-conditions.asp) before you apply for or rely on a Certificate issued by the Trustis FPS Issuing Authority.

The Certificate Policy under which Certificates are issued is defined by two documents:

- PKI Disclosure Statement (this document),
- Trustis FPS Base Certificate Policy

The purpose of this document is to:

- summarise the key points of the Trustis FPS Certificate Policy for the benefit of Subscribers, Subjects and Relying Parties
- provide additional detail and further provisions that apply to the Trustis FPS Certificate Policy and which are incorporated in it by reference.

Certificates issued by this Issuing Authority reference this document, and consequently the Trustis FPS Certificate Policy at [www.simplysign.co.uk/terms-conditions.asp](http://www.simplysign.co.uk/terms-conditions.asp)

Terms used in the document are defined in Trustis Glossary of Terms which can be found at [www.simplysign.co.uk/terms-conditions.asp](http://www.simplysign.co.uk/terms-conditions.asp)

## 1. Policy Authority & Issuing Authority Contact Info:

### 1. Policy Authority:

Trustis FPS Policy Authority

Mailing Address:

Trustis FPS Policy Authority

Trustis Limited

Building 273

Greenham Business Park

Thatcham

RG19 6HN

Tel: +44 (0) 1635 231361

Fax: +44 (0) 1635 231366

email: [sspa@trustis.com](mailto:sspa@trustis.com)

### 2. Issuing Authority:

Trustis FPS Issuing Authority

Mailing Address:

Trustis FPS Issuing Authority

Trustis Limited

Building 273

Greenham Business Park  
Thatcham  
RG19 6HN  
Tel: +44 (0) 1635 231361  
Fax: +44 (0) 1635 231366  
email: [ssia@trustis.com](mailto:ssia@trustis.com)

## **2. Certificate Type, validation procedures and usage:**

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

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

Applicants for Certificates are required to submit to the validation of identity credentials. Identity shall be validated in accordance with HMG's Minimum Requirements for Verification of Identity of Individuals Version 2.0

## **3. Reliance Limits:**

Trustis FPS does not set reliance limits for Certificates it issues. See Limitation of Liability below.

## **4. Obligations of Subscribers:**

Subscribers must comply with the requirements as defined in the Subscriber Agreement which can be found at [www.simplysign.co.uk/terms-conditions.asp](http://www.simplysign.co.uk/terms-conditions.asp)

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 Trustis FPS Certificate Policy, exclusively use the Certificate for legal purposes and restricted to those authorised purposes detailed by the Trustis FPS 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 Trustis FPS Certificate Policy.

## **5. Certificate Status checking Obligations of Relying Parties:**

Relying Parties must comply with the requirements as defined in the Relying Party Agreement which can be found at [www.simplysign.co.uk/terms-conditions.asp](http://www.simplysign.co.uk/terms-conditions.asp)

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

- Ensuring that reliance on Certificates issued under this 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 Certificate Status Information, that the Certificate remains valid and has not been Revoked or Suspended.
- Determining that such Certificate provides adequate assurances for its intended use.
- Take any other precautions prescribed in this 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 this Certificate Policy for any use other than in accordance with this 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 this 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 this 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:**

The full Certificate Policy, Subscriber Agreement and Relying Party Agreement are published by the Issuing Authority and available at:  
[www.simplysign.co.uk/terms-conditions.asp](http://www.simplysign.co.uk/terms-conditions.asp)

Such information is also made available subject to a formal application in writing to the Issuing Authority.

## **8. Privacy Policy:**

Chamber SimplySign strongly believes in an individual's rights to privacy, and operates this Certification Service according to the Privacy Policy which may be found at [www.simplysign.co.uk/terms-conditions.asp](http://www.simplysign.co.uk/terms-conditions.asp)

## **9. Refund Policy:**

Chamber SimplySign does not provide refunds for issued Certificates.

## **10. Applicable Law & Dispute Resolution:**

Disputes shall be handled in accordance with the Chamber SimplySign Digital Certification Services Complaints and Grievance Procedure, documentation of which can be obtained by applying to the Issuing Authority. Contact details are provided in Section 1 of this document.

The provision of Chamber SimplySign Certification Services shall be governed by English law and all parties shall submit to the exclusive jurisdiction of the courts of England and Wales

## **11. CA & Repository Licences Trust Marks & Audit:**

Certificates are manufactured under this Certificate Policy through the use of a Trustis Limited service which is both accredited to ISO27001, and has attained Web Trust and tScheme approval.

Audit shall be carried out on an annual basis required to maintain tScheme and Web Trust for CA trust accreditations. The Auditors that have been approved under this policy are:

- Audit resources of contracted Participants providing trust services.
- A certified public accountant (CPA) with demonstrated expertise in computer security
- A tScheme approved audit body

## **12. Identification of this Certificate Policy:**

This Certificate Policy has been assigned an Object Identifier (OID) of:  
1.3.6.1.4.1.5237.110.1.1

### **13. Approved Registration Authorities**

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

- Trustis FPS

### **14. Approved Repositories**

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

- Trustis FPS
- Chamber Simplysign
- The British Chambers of Commerce

### **15. Eligible Subscribers**

The following types of Subscribers are eligible to be issued with Certificates under this Certificate Policy:

- Individuals required to be identified in the provision of the Government Gateway services.
- Individuals who have satisfied the application and identity verification requirements for Chamber SimplySign.

The Subscriber Agreement can be found at:  
[www.simplysign.co.uk/terms-conditions.asp](http://www.simplysign.co.uk/terms-conditions.asp)

### **16. Eligible Relying Parties**

The following types of Relying Parties are eligible to rely on Certificates issued under this Certificate Policy:

- Any recipient of a Chamber SimplySign issued certificate, providing they act in accordance with the Chamber SimplySign Certificate Policy

The Relying Party Agreement can be found at:  
[www.simplysign.co.uk/terms-conditions.asp](http://www.simplysign.co.uk/terms-conditions.asp)

### **17. Certificate Status Information**

Certificate Status information is made available via Certificate Revocation Lists (CRLs) shall be published, at a minimum, every 24 hours.