

* Chamber SimplySign - PKI Disclosure Statement

Chamber SimplySign PKI Disclosure Statement (v1.1 06-Jun-2007)

This document does not substitute or replace the full **Chamber SimplySign Certificate Policy** under which **Chamber SimplySign Digital Certificates** are issued. You must read the full **Chamber SimplySign Certificate Policy** before you apply for or rely on a Chamber SimplySign Certificate.

The full **Chamber SimplySign Certificate Policy** is defined by two documents:

- This document, the 'Chamber SimplySign PKI Disclosure Statement', and
- The '[Trustis FPS Certificate Policy](#) (CP).

Certificates issued by this Issuing Authority directly reference this document and consequently the **Chamber SimplySign Certificate Policy**.

1. Policy Authority & Issuing Authority Contact Info:

Policy Authority: Trustis FPS

email: sspa@trustis.com
Mailing Address:
Trustis FPS Policy Authority
Trustis Limited
Building 273
New Greenham Park
Thatcham
Newbury
RG19 6HN
UK

Issuing Authority: Trustis FPS

email: ssia@trustis.com
Mailing Address:
Trustis FPS Issuing Authority
Trustis Limited
Building 273
New Greenham Park
Thatcham
Newbury
RG19 6HN
UK

Note: This contact may be used for information regarding the suitability of Certification Practice Statements to support this Policy.

2. Certificate Type, validation procedures and usage

The Digital Certification Services provided by Chamber SimplySign implement what is known as a closed Public Key Infrastructure ("PKI") in the sense that access and participation is only open to those who both satisfy eligibility criteria and are approved by Chamber SimplySign. The only Trust Service Providers and End-Entities authorised and approved to issue, obtain, use, and/or rely upon Certificates that reference this Policy are clearly defined, conditional upon their first agreeing to be bound by the terms of this Policy.

The Digital Certification Services provided by Chamber SimplySign support secure operations in its interactions with the

general public, agent organisations and external contractors, in the direct pursuit of Government Gateway business or in the authorised usage of services provided by Chamber SimplySign. Certificates provided by this service, deemed Level-2, include authentication of individuals, and where applicable organisations, to HMG Government Authentication Framework Level 2 or equivalent. Additionally, data submitted as part of the certificate application are subject to corroboration and verification; see Section 4, Obligations of Subscribers.

Certificates are supported by the use of strong cryptography and highly robust Registration mechanisms and thus support a level of trust and security comparable with the highest level of Certificate available from many public schemes.

3. Reliance Limits

Chamber SimplySign 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

It is the responsibility of the Subscriber to:

- 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 PKI or Government Gateway 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 Chamber SimplySign Certificate Policy, exclusively use the Certificate for legal purposes and restricted to those authorised purposes detailed by the Chamber SimplySign Certificate Policy
- Immediately notify the Registration Authority of a suspected or known key compromise in accordance with the procedures laid down in the Chamber SimplySign Certificate Policy

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

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.

See 'Private Key Protection' for further information and guidance on this topic.

5. Certificate Status Checking Obligations of Relying Parties

If a Relying Party is to reasonably rely upon a Certificate it shall:

- Verify the validity, suspension or revocation of the Certificate using current revocation status information available at the location specified in the Certificate to be relied upon (<http://www.trustis.com/pki/simplysign/crl/ee.crl>).
Note: due to the Issuing Authorities practices and the mechanism used to provide revocation status information, there may be a delay of up-to 1 day in disseminating revocation status information.
- Ensuring that reliance on Certificates issued under this Policy is restricted to appropriate uses (see "Certificate Type, validation procedures and usage", above for a summary of approved usages).
- Ensuring that the Certificate has not Expired
- Ensuring that the Certificate has not been Revoked by accessing any and all relevant Certificate Status information
- Determining that such Certificate provides adequate assurances for its intended use
- Take any other precautions prescribed in agreements or elsewhere.

Note: The liability of Issuing Authorities applies to parties who "Reasonable Rely" on a Certificate.

6. Limited Warranty & Disclaimer/Limitation of Liability

By signing a Certificate containing a Policy identifier which indicates the use of this Policy, the Issuing Authority certifies to all who reasonably rely on the information contained in the Certificate, that the information in the Certificate has been checked according to the procedures laid down in this Policy.

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

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 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 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

- A Subscriber Agreement can be found at:
http://www.simplysign.co.uk/subscriber_agreement.shtml
- A Relying Party Charter can be found at:
http://www.simplysign.co.uk/relying_party_charter.shtml
- This document (PKI Disclosure Statement) can be found at:
http://www.simplysign.co.uk/pki_disclosure_statement.htm
- The Base Certificate Policy can be found at:
http://www.simplysign.co.uk/downloads/T_FPS_CP_V1_04.pdf
- Guidance in the use of certificates can be found at:
<http://www.simplysign.co.uk/onlinehelp.html>

8. Privacy Policy

Chamber SimplySign strongly believes in an individual's rights to privacy. Chamber SimplySign operates this Digital Certification Service according to an extensive Privacy Charter which can be found at:
http://www.simplysign.co.uk/privacy_charter.shtml

9. Refund Policy

Not applicable for this Policy. Chamber SimplySign do not offer refunds.

10. Applicable Law & Dispute Resolution

Disputes shall be handled in accordance with Chamber SimplySign Certificate Services Complaints and Grievance Procedures, a copy of which can be obtained by applying to the Issuing Authority contact listed in section 1 of this document.

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

11. Certificate Authority & Repository Licences Trust Marks & Audit

The topics of Licensing and Trust Marks are currently still under discussion in the UK. Every effort will be made to comply with their requirements once such schemes are underway.

Audit shall be carried out on an annual basis. The following Auditors have been approved under this policy:

- Audit resources of Chamber SimplySign
- Audit resources of contracted Trust Service Providers
- A Certified Public Accountant ("CPA") with demonstrated expertise in computer security or an accredited computer security professional

12. Identification of this Certificate Policy

This Policy has been registered with Trustis FPS and 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 Policy:

- Trustis FPS

14. Approved Repositories

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

- Trustis FPS
- Chamber SimplySign
- British Chambers of Commerce

15. Eligible Subscribers

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

- End-Entities required to be identified in the provision of the Government Gateway services, provided they are also approved by the Registration Authority.

A Subscriber Agreement can be found at: http://www.simplysign.co.uk/subscriber_agreement.shtml

16. Eligible Relying Parties

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

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

A Relying Party Charter can be found at: http://www.simplysign.co.uk/relying_party_charter.shtml

17. CRL publication Frequency

Certificate Revocation Lists (CRLs) shall be published at least every 24 hours.