

ARTL PKI

Certificate Policy PKI Disclosure Statement

Important Notice:

This document (PKI Disclosure Statement, PDS) does not by itself constitute the Certificate Policy under which Certificates governed by this Certificate Policy are issued. You must read the Certificate Policy at http://www.ros.gov.uk/artl/pki/pki_policy.html before you apply for or rely on a Certificate issued by the ARTL Issuing Authority.

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

- PKI Disclosure Statement (this document).
- ARTL PKI Base Certificate Policy.

The purpose of this document is to;

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

Certificates issued by this Issuing Authority, reference this document and consequently the ARTL PKI Base Certificate Policy at http://www.ros.gov.uk/artl/pki/pki_policy.html

Terms used in the document are defined in the Registers of Scotland Glossary of PKI Terms.

1. Policy Authority & Issuing Authority Contact Info:

Policy Authority:

The Keeper of the Registers of Scotland is the Policy Authority for the ARTL PKI. Day-to-day responsibility for the Policy Authority role is delegated to the ARTL Policy Authority Function Group.

Mailing Address:
ARTL Policy Authority Function Group
Business Development
Registers of Scotland
Meadowbank House
153 London Road
Edinburgh
EH8 7AU
Tel: +44 (0)131 200 3943
Fax: +44 (0)131 479 3671

email: PAFG@ros.gov.uk

Issuing Authority:
ARTL Issuing Authority.

Mailing Address:
ARTL Issuing Authority
Business Development
Registers of Scotland
Meadowbank House
153 London Road
Edinburgh
EH8 7AU
Tel: +44 (0)131 200 3943
Fax: +44 (0)131 479 3671
email: PKI.IA@ros.gov.uk

2. Certificate Type, validation procedures and usage:

The Certification Services provided by the ARTL Issuing Authority implement a closed public key infrastructure in the sense that access and participation are only open to those who both satisfy eligibility criteria and are approved by the ARTL Issuing Authority. The Participants providing trust services and End-Entities authorised and approved to issue, obtain, use, and/or rely upon Certificates that reference the ARTL PKI 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 ARTL Issuing Authority support secure operations and interactions with agent organizations and customers in the direct pursuit of ARTL related business, or in the authorised usage of services provided the ARTL Issuing Authority. 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 the ARTL PKI Certificate Policy may only be used in conjunction with the Automated Registration of Title to Land (ARTL) system.

Permitted Certificate use includes secure interaction with the ARTL system and electronic signature of documents, applications and transactions processed via the system.

Note - Certificates used for creating electronic signatures may not be used for other purposes.

No other usages are permitted for Certificates issued under the ARTL PKI Certificate Policy.

Applicants for Certificates are required to satisfy the requirements of HMG's Minimum Requirements for the Verification of the Identity of Individuals - Version 2.0 - January 2003 at level 2. This means that applicants must submit to the validation of identity credentials and their eligibility to hold such a Certificate as detailed in

www.ros.gov.uk/artl/pki/regpolicyandprocedures.pdf

3. Reliance Limits:

The ARTL Issuing Authority does not set reliance limits for Certificates it issues (see 6.Limitation of Liability).

4. Obligations of Subscribers:

Subscribers must comply with the requirements as defined in the Subscriber Agreement which can be found at http://www.ros.gov.uk/artl/pki/pki_policy.html

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 only the Approved Trustworthy System(s) for generating or obtaining a Key Pair.
- Use only the Approved Trustworthy System(s) for storing a Private Key to prevent any loss, disclosure, or unauthorised use.
- 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.
- Exclusively use the Certificate for legal purposes and restricted to those authorised purposes detailed in accordance with the ARTL PKI 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 ARTL PKI Certificate Policy.

Approved Trustworthy Systems : Two factor Authentication Systems that are certified as in conformance with Common Criteria for Information Technology Security Evaluation at EAL 4+

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 ARTL PKI Relying Party Agreement at http://www.ros.gov.uk/artl/pki/pki_policy.html

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 when used for transactions and signatures the Certificate is valid and has not been Revoked.
- 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 the ARTL PKI Certificate Policy for any use other than in accordance with the ARTL PKI 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, delict, 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 ARTL PKI Base 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 ARTL PKI 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 the locations referenced in this PKI Disclosure Statement.

Such information is also made available upon application in writing to the Issuing Authority.

8. Privacy Policy:

The ARTL Issuing Authority strongly believes in an individual's rights to privacy, and operates this Certification Service according to the Registers of Scotland Digital Certification Services Privacy Charter which may be found at http://www.ros.gov.uk/artl/pki/pki_policy.html

9. Refund Policy:

Not Applicable.

10. Applicable Law & Dispute Resolution:

Disputes shall be handled in accordance with the Registers of Scotland Complaints Procedure, details of which can be obtained by applying to the Issuing Authority. Contact details are provided in Section 1 of this document.

The provision of ARTL Issuing Authority Certification Services shall be governed by Scottish law and all parties shall submit to the exclusive jurisdiction of the courts of Scotland.

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 ISO17799 and has attained tScheme approval.

Audit shall be carried out on a periodic basis to maintain security and trust accreditations. The Auditors that have been approved under this policy are:

- Audit resources of contracted Participants providing trust services.
- An auditor or assessor organization that is approved by the ARTL Policy Authority Function Group.

12. Identification of this Certificate Policy:

This Certificate Policy has been assigned an Object Identifier (OID) of:
1.3.6.1.4.1.5237.116.1.1

13. Approved Registration Authorities

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

- Registers of Scotland.
- Participants in the ARTL PK.I
- Trustis Limited.

14. Approved Repositories

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

- Registers of Scotland.
- Trustis Limited.

15. Eligible Subscribers

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

- Registers of Scotland staff and other End-Entities under the management of the Registers of Scotland, including approved users of the ARTL system.
- Users of the Automated Registration of Title to Land (ARTL) system, if first authorised and approved by registration agents operating on behalf of the Registers of Scotland.

The Subscriber Agreement can be found at
http://www.ros.gov.uk/artl/pki/pki_policy.html

16. Eligible Relying Parties

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

- Registers of Scotland.

The Relying Party Agreement can be found at:
http://www.ros.gov.uk/artl/pki/pki_policy.html

17. Certificate Status Information

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

Copyright © Trustis Limited 2006
All Rights Reserved

This document is licensed for use only in conjunction with the use of Trustis Trust Services