Land Registry

Version 2.0 23/07/2008

PKI Disclosure Statement

1. Introduction

Land Registry has created an e-security platform for its customers to facilitate role-based access, authentication and electronic signatures within its e-services. The security services include a Public Key Infrastructure, which has a Certification Authority operated by Land Registry (CA). The policy requirements on the operation and management of the CA issuing Certificates are defined in the Land Registry Certificate Policy (CP) document such that Subjects certified by the CA and Relying Parties may have confidence in the reliability of the Certificates.

The purpose of this document is to summarise the key points of the CP for the benefit of Subscribers, Subjects and Relying Parties.

NB. The terms used in this document are defined in the CP.

2. Certificate Authority Contact Information:

The Registrar

Head Office

Trafalgar House

1 Bedford Park

Croydon CR0 2AQ

Contact: certificate_policies@landregistry.gov.uk

3. Certificate type, validation procedures and usage

The CA issues four types of Certificate:

1. **Land Registry Local Signing** – for use only where End Users create Electronic Signatures using Private Keys held on Tokens attached to their local machines.

2. **Land Registry Central Signing** – for use only where End Users create Electronic Signatures using Private Keys held centrally by Land Registry.

3. **Land Registry Individual Authentication** – for use only where End Users need to perform Administration functions within the e-Security service, using identity-based authentication.

4. **Land Registry Device Authentication** – for use only where Devices with software key storage need to communicate securely within the Land Registry Network.

The CA shall ensure that evidence of Subjects' identification and the accuracy of their names and associated data are either properly examined as part of the defined service or, where applicable, concluded through examination of attestations from appropriate and authorised sources.

4. Reliance Limits:

The CA does not set reliance limits for the Certificates it issues, but see Section 7 below for limitation of liability.

5. Obligations of Subscribers:

It is the responsibility of Subscribers to:

- only use the Key Pairs for the purposes defined in Section 3 above and in accordance with any other limitations that may be notified to the Subscriber
- submit accurate and complete information to the CA during Subject registration in accordance with the requirements of the CP
- exercise reasonable care to avoid unauthorised use of the Subject's Private Key
- notify the CA, without any unreasonable delay, if any of the following occurs up to the end of the validity period indicated in the Certificate:
  - the Subject's Private Key has been potentially or actually lost, stolen or compromised
  - control over the Subject's Private Key has been lost due to potential or actual compromise of activation data (eg PIN code) or other reasons
  - inaccuracy or changes to the Certificate content, as notified to the Subscriber.
- ensure that if the Subscriber or Subject generates the Subject's Key Pair, only the Subject holds the Private Key
- ensure that Private Keys are generated within the hardware key storage device (Token).

6. Certificate status checking obligations of Relying Parties:

The obligations of the Relying Party, if it is to reasonably rely on a Certificate, are to:

- verify the validity, suspension or revocation status of the Certificate using current revocation status information as indicated to the Relying Party in the CP
- take account of any limitations on the usage of the Certificate indicated to the Relying Party either in the Certificate or the terms and conditions (see Section 3 above for usage)
- take any other precautions prescribed in the Certification Practice Statement (CPS).

7. Limited warranty & disclaimer/ limitation of liability:

The liability taken by the CA is limited to the correct application of procedures as declared in the CPS (incorporated into the Technical Manual); these procedures relate to the issue and management of digital Certificates. Therefore any failure of transaction that utilises the digital Certificate is out of scope.

In essence the liability will include the correct identification of Subjects according to the declared practices. If a transaction is found to be in error through the incorrect identification of the Subject through failing to follow the declared practices, then the CA is liable. If the Subject is incorrectly identified, but the error was within the documents used to support the Subject's claim to an identity, then the CA shall not be liable.

The CA shall include any limitation of liability within the Certificate, providing the relevant information within an easily accessible statement both on its web site and within the CPS.

8. Applicable agreements, Certification Practice Statement, Certificate Policy:

The Network Access Agreement (NAA), the CP, and the CPS (incorporated into the Technical Manual) are published in full on the Land Registry website, **www.landregistry.gov.uk** and are also available upon application in writing to the CA (see Section 1 above).

9. Privacy policy:

The CA shall safeguard the privacy of Subject information as prescribed by the Data Protection Act. It will also ensure that all relevant information concerning a Certificate is recorded for an appropriate period of time, in particular for the purpose of providing evidence of certification for the purposes of legal proceedings.

10. Refund policy:

Not applicable.

11. Applicable law, complaints and dispute resolution:

The CA has policies and procedures for the resolution of complaints and disputes received from customers or other parties about the provisioning of CA services or any other related matters. Details can be obtained by applying to the CA (see Section 2 above).

English Law shall govern the provision of CA services. All parties shall submit to the exclusive jurisdiction of the courts of England and Wales.

12. Certificate Authority and Repository Licences, Trust Marks and Audit:

The CA issues Certificates using Entrust products that have been accredited to the relevant Common Criteria EAL 3 and/or EAL 4 augmented requirements. The CA service operation has been designed and built to attain tScheme approval.

Audit is an integral part of the CA services whereby all significant events shall be logged to provide a trail, as documented in the CPS.

Audit of the CA services themselves shall be carried out on a periodic basis in accordance with Land Registry security policies and procedures.

For alternative formats please contact the customer contact centre on 0844 892 1111.

Issued by Land Registry Corporate Marketing Services Janary 2016