Land Registry

Version 3.1 09/12/2008

Certification Practice Statement:

A Guide to the operation of the Land Registry Certificate Authority

1. Introduction

The following is a guide to the way in which Land Registry will operate as a Certificate Authority (hereafter referred to as CA). It outlines the processes and procedures that have been put in place in order for Land Registry, as CA, to operate securely; and aims to answer any questions that an individual may have who is issued with a Certificate, or is required to rely upon a Certificate, issued by the CA. Its intention is to ensure transparency, which will enable all interested parties to have full confidence in the practices of the CA.

If you have been issued a Digital Certificate by Land Registry you will be obliged to use it in accordance with either the Full Network Access Agreement and associated Technical Manual in force, or the current Signature Network Access Agreement. This document is for guidance only. It is subject to change in accordance with Section 10 of both Network Access Agreements.

2. What is a Certificate and how does it work?

2.1 What a Certificate is

A Certificate (or digital Certificate) is a means of electronically proving your identity when carrying out an electronic transaction, in much the same way as using your driving licence or passport when carrying out a face-to-face interaction. Certificates can be used for a variety of electronic transactions, such as email, e-commerce, and electronic funds transfers. They allow the person you are interacting with to trust your identity. A Certificate itself consists of an electronic file containing the publicly available half of what is known as a *key pair*[1]. This key pair is used to create e-signatures and safeguard access to computer systems. A Certificate is signed by a CA, rendering it unforgeable (see Section 2.2), and it is issued to a user and published in a *public repository*.

The purpose of a Certificate is to bind you to your *public key*, which is embedded in your Certificate and made publicly available, and also to bind you to your *private key* that is available only to you. By activating your private key you prompt the system to verify it against the public key embedded in the Certificate. If the two keys match then the Certificate has verified the link between you and the key pair, which acts to prove your identity. This allows the other party involved in the transaction to trust your identity and can also be used to verify an e-signature.

[1] Words shown in Italics are glossary terms and are italicised the first time they are used only.

2.2 What a Certificate does

A Certificate enables you to identify the owner of a public key (known as the subject) and, therefore, the corresponding key pair. This allows you to verify the identity of the subject that activates a private key. It also tells you which body issued the Certificate and against which *Certificate policy*. This enables you to ascertain the level of trust and confidence you might have in the identity of the subject by accessing the relevant Certificate policy under which the Certificate and key pair were generated. The Certificate also provides information as to the time period within which the Certificate is valid and how the Certificate may be used. Certificates are used for two main purposes. The first is for identity verification. It allows a system to verify that the individual who is attempting to gain access is who they purport to be.

The second main purpose is for creation of an *e-signature*, which verifies both the identity of the signer and the integrity of the document being signed. In this process the private key of the user is used to *encrypt* a document. *Decryption* and validation of this e-signature can only be carried out, if the public key of the user matches the private key that was used to create the e-signature. This verification of the e-signature also helps protect an electronic transaction by providing a method of detecting tampering.

3. What is a CA and why is it required?

3.1 What a CA is

A CA is a trusted body that creates, issues and manages Certificates. The CA confirms the identity of the Certificate holder and binds them to a particular key pair.

3.2 What a CA does

The CA holds a repository for all of the Certificates issued and decides what they may be used for. It also arranges for the necessary checks to be carried out on the identity of the applicant before issuing the Certificate. Each time a user attempts to use their Certificate, the CA confirms whether or not the Certificate is valid to be used for the particular transaction. It also arranges renewal of Certificates when necessary and revokes them when there is a problem, such as they have been misused, or the user cannot remember their PIN to initiate use of their private key. It publishes what is known as a '*Certificate revocation list*' on a regular basis. This is a regularly updated list of Certificates that have been revoked and allows any party relying on a Certificate to check that it has not been revoked.

3.3 Land Registry as CA

In many cases one would expect Certificates to be issued by an independent third party CA. However, Land Registry, operating as the land registration authority, will be the party relying most heavily on the Certificates issued for the purposes specified in this document. Therefore it has chosen to act as its own CA, issuing Certificates to the users of the Land Registry *portal*, and publishing its own Certificate revocation list.

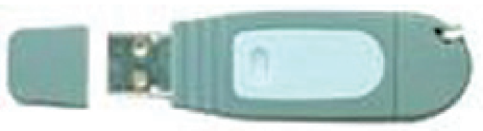
4. What will Certificates issued by the CA be used for?

Certificate holders will use Certificates issued by the CA for the following two purposes.

4.1 Identity verification

In the future, all Land Registry *E-services* will be accessed through a new Land Registry portal. In order to gain access to those services for which a user must be registered, users will need to be provided with an account that will allow them access to the relevant Land Registry systems. They will log into their account through the portal by supplying the *security credentials* that were issued to them when their account was created. In most cases this will consist of only a Username and Password. However, each *organisation* making use of Land Registry E-services must nominate at least one administrator. The job of the administrator will be to create and manage the accounts of all of the users within their organisation. (This delegation of account administration by Land Registry is explained further in section 5.1.2.)

The added level of responsibility associated with the *role* of administrator will mean that they will require additional higher level verification of their identity before accessing their account to carry out their administrator duties. This will be achieved by adding the additional security associated with a second authentication method. In addition to their User ID and Password, the administrator will be issued with a Certificate and associated key pair. In real terms this will mean that when a request is made for an administrator to be issued with a Certificate, the CA generates a key pair. The public key is then sent to a *registration authority* where additional information about the subject is collected and checks carried out. Once these identity checks have been completed successfully, this information along with the public key is used to complete the Certificate. This Certificate and the private key will both be housed in a device held in the sole control of the administrator. For administrators, this device will be in the form of a USB token, as shown below:



When administrators are required to verify their identity at log in, they will enter their USB token and the system will request the corresponding PIN that was issued separately to them. By entering their PIN correctly they will activate their private key, and once the system has verified that their private key matches the public key that forms part of the Certificate, and that their Certificate is valid, they will be allowed to access those e-services for which they have the necessary permissions.

4.2 Creation and verification of an electronic signature

As some Land Registry documents start to become available online as e-documents, and it becomes possible to create e-charges, this will result in the need for users to be able to apply e-signatures to documents, which will identify the signer and verify the integrity of the document.

4.2.1 Creating an e-signature

An e-signature is created using a process of encryption, which uses a specific *algorithm* to create what is known as a *hash-value* of a document. This hash-value is in turn encrypted with the private key of the signatory, which creates another hash value known as an e-signature. This process is shown in figure 1 below:

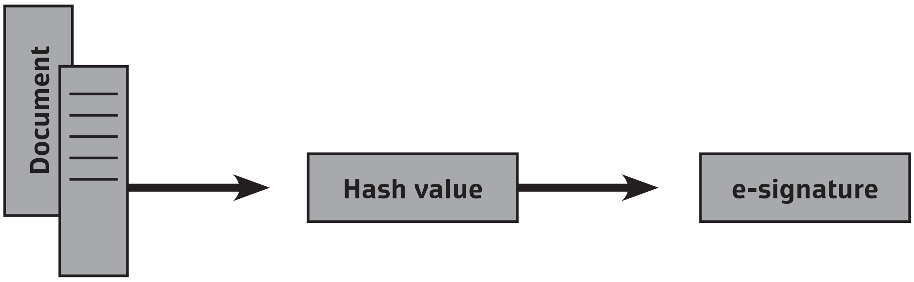


Figure 1

4.2.2 Verification of an e-signature

On receipt of the e-signature, the hash-value of the document is calculated. This hash-value is known as the current hash-value, because it is calculated from the current state of the document. The e-signature is then decrypted using the public key of the signatory and using the same algorithm as was used for signing the document. As a result, the original hash-value that was created during the first step of the signing process is obtained. The current hash value is then compared with the original hash value. If they are identical this proves that the private key of the user that corresponds with the public key has signed the document. This acts as evidence that the document has not been changed since it was signed. The process is shown in Figure 2 below:

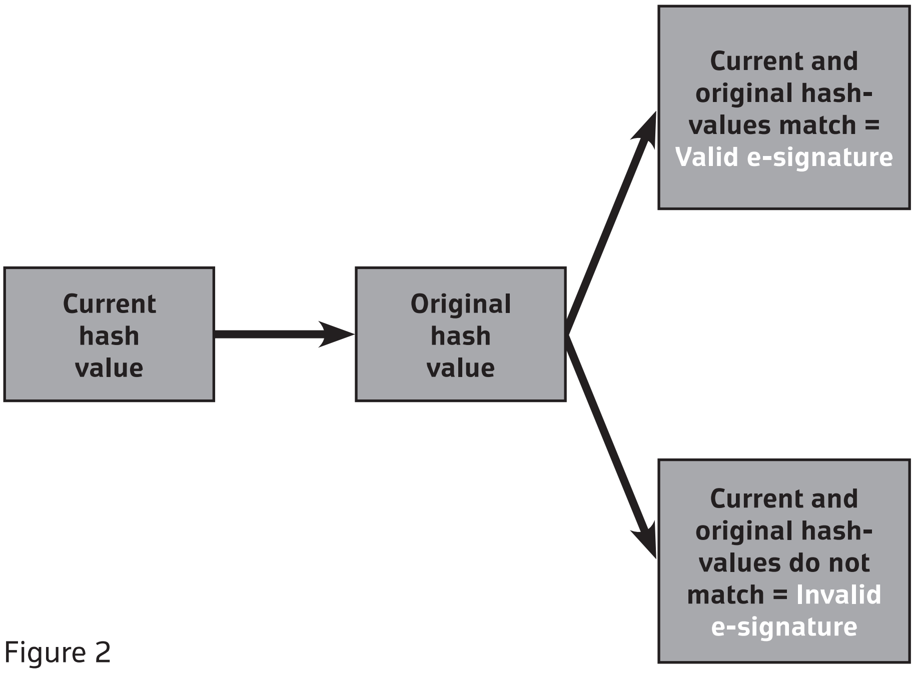

Current and original hash-values match = Valid e-signature
Current hash value
Original hash value
Current and original hash-values do not match = Invalid e-signature

Figure 2

4.3 E-signature methods

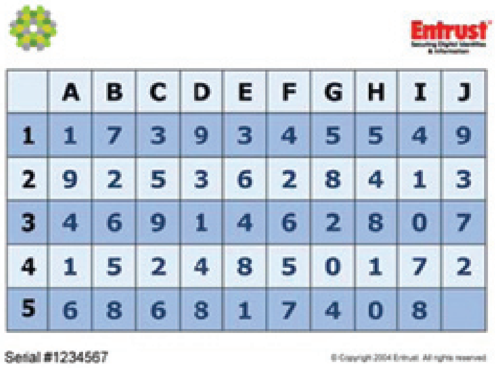
For Land Registry electronic signing, there will be two possible ways that the Certificate and key pair might be housed and accessed to apply an e-signature. This is in order to provide for the differing technical capabilities of potential e-signers.

4.3.1 Local signing

Local signing works in much the same way as for identity verification. The key pair is generated on a USB token; in order to activate their private key, the user enters the USB token into their PC and is asked for the associated PIN. If they enter the PIN correctly they will be allowed to apply their e-signature using their private key. Only if their private key matches the public key contained in their Certificate can their e-signature be decrypted and validated.

4.3.2 Central signing

For clients of conveyancers; or for any citizen involved in an electronic transaction; or for those users who do not have a USB port on their PC or would simply rather use a different method, there is a further option, known as central signing. Using this method, the Certificate and key pair are not stored on a device held by the user. Instead, they are stored on a central Land Registry server. In order for the user to activate their private key, they are issued with an *Authentication Grid* (see example below).



	A	B	C	D	E	F	G	H	I	J
1	1	7	3	9	3	4	5	5	4	9
2	9	2	5	3	6	2	8	4	1	3
3	4	6	9	1	4	6	2	8	0	7
4	1	5	2	4	8	5	0	1	7	2
5	6	8	6	8	1	7	4	0	8	

Serial #1234567

© Copyright 2004 Entrust. All rights reserved

The Authentication Grid will be printed with a unique assortment of characters. The card is identifiable by a serial number, which will be linked to the account of the user and their Certificate. When the user wishes to apply their e-signature, they are prompted for information from the grid to demonstrate that they are in possession of it. If the user enters the information correctly this activates their private key stored on the central server, allowing them to apply their e-signature. In order for the signature to be decrypted and validated, their Certificate, which is also held on the central server, checks the private key against the corresponding public key.

4.4 Parties that rely upon Land Registry-issued Certificates

The party that will ultimately be relying on Land Registry issued Certificates is Land Registry itself, operating as the land registration authority. Each time a user performs a function requiring use of a Certificate, such as logging in as an administrator, or lodging a document where an e-signature has been applied, Land Registry will employ an automatic process of checking the keys associated with the Certificate to verify the identity of the user, and the validity of any signature that has been applied. In addition, Land Registry will also be responsible for checking the validity of the Certificate itself. (More details of the checks required to be made by relying parties in relation to Certificates can be found at section 13.) Although the party that will ultimately be reliant upon these Certificates is Land Registry, operating as the land registration authority, chargees will also be reliant upon the Certificates issued by the CA. However, in the early stages, since the conveyancer acting for the chargee will also be the conveyancer who makes the Certificate request and carries out the registration checks, then although they will have access to the Certificate revocation list, only Land Registry operating as the land registration authority will have the facility to make checks in relation to content of the Certificate itself.

5. How does the process of issuing Certificates work?

Sections 5.1 and 5.2 below detail the processes involved in the issuing of a Certificate to a user. The sequence of events is further set out in Figure 3 and Figure 4 that follow these sections.

5.1 Application for a Certificate

Initial applications for Certificates will be made by:

- ***Land Registry CA on behalf of its own business administrators, who will be required to administer the accounts of those organisations that sign up for e-services***
- ***organisations on behalf of intended administrators***
- ***administrators on behalf of their users who require an e-signing capability***
- ***conveyancers who have been granted the necessary permissions to request an e-signing capability on behalf of their clients, or any citizen involved in an electronic transaction.***

5.1.2 Delegation of Administration

Although the actual issuance of Certificates is carried out by the CA, the registration process involved in the creation of a Certificate will be delegated to fit in with the account administration processes that have been put in place. The delegation of administration for Land Registry account holders works as follows.

- ***A dedicated team of Land Registry business administrators create accounts for the organisations themselves and for the administrators who will carry out account administration on behalf of that organisation.***
- ***Administrators within these organisations create accounts for their users.***
- ***Conveyancers who are users create accounts for their clients, or for any citizen involved in an electronic transaction when required.***

Registration checks must be carried out before a request is made for an individual to become an administrator, or for a user to be provided with an e-signing capability. Therefore, when a user requires a Certificate for e-signing, those individuals with the correct permissions to create and manage the account of that user will also be required to carry out the necessary registration checks in order for the user to be granted a Certificate.

The process of delegating these checks elsewhere is normal practice for a CA, since although many do choose to carry out their own checks, others arrange for what are known as *Registration Authorities* to carry out these identity verification checks on their behalf. It is, however, imperative that the necessary checks on the identity of the individual applying for the Certificate are carried out by those responsible in each organisation. The responsibility for checking the identity of the individual applying for a Certificate lies solely with the organisation itself, and is not the responsibility of the CA.

5.1.3 Identity verification

Registration checks are vital for those relying on the Certificates to have full trust in the validity of the Certificate. In the case both of applications for an administrator to be provided with a Certificate, and of administrators requesting an e-signing Certificate on behalf of their users, the organisation as land registration authority must carry out identity verification checks on the applicant in line with the Money Laundering Regulations 2007, or any legislation that replaces them. These checks should also satisfy the 'Registration and Authentication e-Government Strategy Framework Policy and Guidelines' set out by the Office of the e-Envoy. These can be viewed at **www.archive.cabinetoffice.gov.uk/e-envoy/frameworks-authentication**.

In the case of conveyancers registering their clients, or any citizen involved in an electronic transaction for a Certificate, as well as the above regulations and guidelines, solicitors should ensure that they follow the latest Anti-Money Laundering Practice Note issued by the Law Society, and other professional conveyancers should follow their equivalent guidance.

5.2 Issuance of Certificates

When a user is allocated with a role that requires additional identity verification or an e-signature capability, and in turn a Certificate, this triggers a Certificate request. The CA issues a Certificate, and a key pair is generated and linked to the user via the Certificate. The type of Certificate being requested and the requirements of the user dictate the housing of the key pair. For those requiring or requesting a local USB device, the keys will be housed on that device and the device itself will be despatched to the user. If the keys are stored on the Land Registry central server, then issuance of the Certificate and generation of the key pair will also take place on the Land Registry central server.

Figure 3 below shows the end-to-end process for the issuance of a Certificate to an administrator.

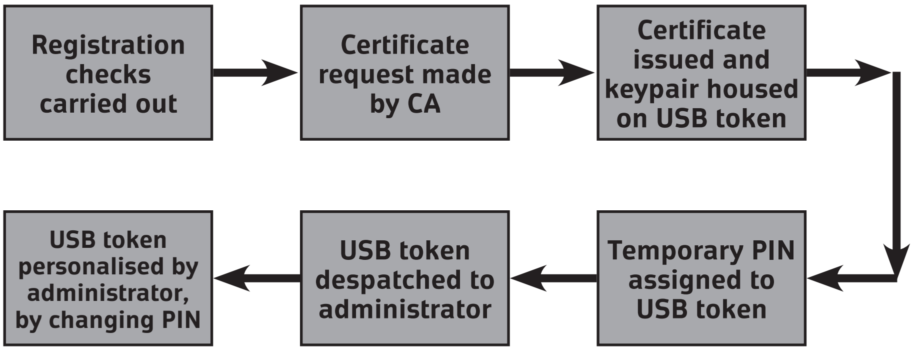

Registration checks carried out
Certificate request made by CA
Certificate issued and keypair housed on USB token
Temporary PIN assigned to USB token
USB token despatched to administrator
USB token personalised by administrator, by changing PIN

Figure 3

Figure 4 below shows the end-to-end process for the issuance of a Certificate to a user requiring an e-signature.

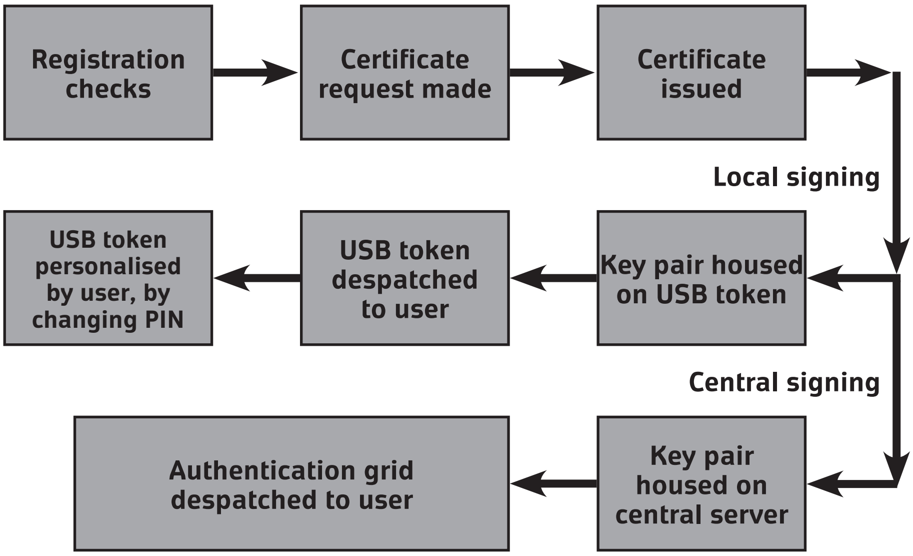

Registration checks
Certificate request made
Certificate issued
Local signing
Key pair housed on USB token
USB token despatched to user
USB token personalised by user, by changing PIN
Central signing
Key pair housed on central server
Authentication grid despatched to user

Figure 4

5.3 Acceptance of Certificates

Acceptance of a Certificate is deemed to have occurred when one of the following occurs.

- ***Installation and use of the Certificate. This could mean use of the USB token or authentication grid.***
- ***Failure to object to the Certificate or its content.***

5.4 How will Certificates be managed?

The CA will manage Certificates as follows:

5.4.1 Certificate renewal

The Certificates issued by the CA will be valid for a specific period. At the end of this period, they will need to be renewed. If this point is reached without the user renewing their Certificate, then the Certificate expires. In the case of an electronic signing Certificate this period is 18 months. In the case of an identity verification Certificate, this period is 12 months. The user will be contacted two months before expiry of the Certificate and asked if they wish to renew. If the user confirms that they wish to renew the Certificate, then it will be renewed for the same period. This process, instigated by the CA, allows the CA to minimise the number of unused Certificates that remain active. Certificate renewal does not apply to Certificates issued under Signature Network Access Agreements.

5.4.2 Certificate suspension or revocation

Certificate suspension or revocation will follow as a consequence of suspension or deletion of the account access or e-signing capability of a user. The Certificate suspension/revocation process is as follows:

5.4.2.1 Permission to request Certificate suspension or revocation

Suspension or revocation of a Certificate can be requested by:

- a Land Registry business administrator on behalf of the Certificate of any user in an organisation
- an administrator in a firm on behalf of themselves or any other user in their organisation
- a user (if they are a conveyancer) on behalf of themselves or on behalf of a client, or any citizen involved in an electronic transaction.
- a client, or any citizen involved in an electronic transaction on behalf of themselves.

5.4.2.2 Reasons for suspension or revocation

Appropriate reasons for suspension or revocation would be:

- ***following an actual or suspected compromise of the PIN or private key of the user***
- ***following an actual or suspected breach of the terms and conditions associated with the applicable agreement that was signed on behalf of the organisation, allowing the user access to the services for which their Certificate has been issued***
- ***the user has ceased to exist***
- ***the Certificate has been used in a faulty or improper way, that is, not in accordance with the uses and practices detailed in this document***
- ***the Certificate information becomes inaccurate in a manner material to the trustworthiness of the Certificate***
- ***the CA ceases to operate.***

5.4.2.3 Applicability of and procedure for Certificate suspension

Suspension of a Certificate will take place as a result of one of the following.

- ***Access to the Land Registry portal is suspended for one of the reasons listed in section 5.4.2.2 above. Account suspension will trigger automatic suspension of the Certificate. Once the Certificate is suspended the CA will promptly add it to the Certificate revocation list as being on 'hold'. If account access is subsequently reinstated, then the Certificate will also be reinstated. (This is the most common circumstance whereby a Certificate will be suspended.)***
- ***Suspension of the e-signing capability allocated to the user is requested, but their account access is to be retained. In this circumstance a request will be made by the CA for the Certificate to be suspended and a Land Registry system administrator will trigger suspension of the signing Certificate. The CA will add the Certificate to the Certificate revocation list as on 'hold'. If the e-signing capability is subsequently reinstated, then the Certificate will also be reinstated.***

5.4.2.4 Procedure for and applicability of Certificate revocation

Certificate revocation will take place as a result of one of the following.

- ***Deletion of the account of a user***
- ***Permanent removal of the e-signing capability of the user.***

On receipt of a revocation request the CA will authenticate the validity of the request. Once its validity has been confirmed the Certificate will be revoked. Revocation requests will be processed immediately upon receipt during normal business hours, or on the next working day at other times. Once a Certificate has been revoked it will be promptly added to the Certificate revocation list, as permanently revoked.

5.4.2.5 Certificate revocation list

The Certificate revocation list detailing all revoked and suspended Certificates will be updated at least once a day, so that any relying party does not rely on a Certificate that has been revoked by the CA. Information leading to a decision to revoke keys and Certificates will not be made publicly available. Once a Certificate has been revoked it cannot be reinstated, so a new Certificate must be applied for if required. The Certificate revocation list can be accessed at **www.landregistry.gov.uk/crl/issuing.crl**

6. What else do I need to know about Certificates?

6.1 Cost of a Certificate

There is no direct cost for the issue of a Certificate. The cost of maintaining the overall e-security system associated with user accounts, which includes the issuance of Certificates, is spread between all of the electronic transactions processed through Land Registry portal. In addition, the cost of applying e-signatures, which again includes Certificate issuance, is to be recovered from the fees charged for the processing of e-documents that require e-signatures.

6.2. What personal information will be stored about a Certificate holder?

The personal information stored about the Certificate holder in their Certificate is limited to their name, organisation name and email address. This is linked in the Certificate to their security details, which are also contained there.

7. How will the CA ensure that a Certificate can be trusted?

7.1 CA Key Signing Ceremony

It is vitally important that the CA can ensure trust in its operations, since Land Registry electronic transactions will be taking place through the open and often hostile environment of the internet. Both the Certificate holder and Land Registry, as the land registration authority, must be confident that Certificates issued by the CA can be trusted. In order for this to be the case, it is necessary for the CA to be established with its own Certificate and key pair, so that it can verify its authenticity as a Certificate issuer to anyone who might question the validity of a Certificate it issues. Once this process has been completed the private key held by the CA is known as the *root key*, as it represents the root from which trusted Certificates can be issued.

The root key pair is established in much the same way as lower level keys are generated. However, the actual key generation must take place under extremely secure circumstances, as part of a formal ceremony, which is recorded on video, runs to a script and must be witnessed and fully audited. This is to create confidence in the authenticity and security of the key pair that is generated. The Land Registry key signing ceremony has already taken place and a root key pair has been established. Both keys were generated and housed inside a *hardware security module* and a back-up of this module was created. These modules act as a secure storage device for the private key, meaning that the keys cannot be copied from the device and that the key cannot be stolen and used to create fake Certificates. In order to ensure that the private key is not compromised, the only way that the private key can be accessed is by use of an additional set of physical keys. These keys have been stored in a safe at a secure location and can only be accessed by designated key holders using a PIN that they have been allocated. A number of key holders are required in order to access the private key and all of the PINs are stored safely in tamper-evident envelopes held with the key holders.

7.2 Action to be taken on compromise of private key

If a user believes that their private key has been compromised, they should notify Land Registry or their administrator immediately. In many cases this would be due to loss of the USB token containing the Certificate and key pair, but any suspected compromise should be reported, as it is likely that the Certificate will need to be revoked. In the circumstances of a lost USB token the CA would revoke the Certificate promptly and the account of the user would be reset. A new Certificate and key pair would then be generated, along with new activation data.

7.3 Action to be taken on loss or compromise of activation data

If the user loses their PIN or believes that it has been compromised in any way, there is a process in place that allows the user to reset their PIN. This is an online self-service process and allows the user to delete their old PIN and create a new one. The process relies on *shared secret* questions and answers that the user was asked to create on the first occasion that they logged into their account. If the user needs to reset their PIN they are asked for the answers to two randomly selected shared secrets from those they created, and if they answer correctly, then they are asked to insert their USB token and create a new PIN on the token. This ensures that only the valid Certificate holder can reset the PIN that activates their private key. If the user does not answer the questions correctly the account is locked and only their administrator is in a position to unlock it.

7.4 Action to be taken on compromise of the CA

If the CA suspects that its own private key has been compromised, or if the installation housing the CA becomes damaged or inoperative due to disaster, then there are business continuity arrangements in place. The CA will arrange for the continued retention of the keys and information it holds. All Certificate application data, audit data, the database of the Certificates issued and the private keys are backed up in case of this situation. Land Registry will also use all reasonable efforts to notify all users immediately.

7.5 Audit Procedures

All transactions that involve the CA will be audited. This includes administrative user logins and logouts, use of activation data, account activation, key updates and any system failures. The key signing ceremony, which creates the Root CA, is also fully audited. (Further information as to the detailed audit procedures can be found at section 9.)

8. What standards will the CA adhere to?

In order to further ensure the security of Certificates issued by the CA, its procedures will adhere to a number of relevant industry standards. The generation of Certificates and key pairs themselves will meet the recommended standards set out for Government security procedures. The way that e-signatures are generated and managed will also comply with the EU Digital Signature Directive and relevant Internet Engineering Task Force (IETF) standards. The Land Registry e-security policies follow the code of conduct associated with the relevant British Standards in Information Security Management (BS ISO/IEC 27001:2005 and BS ISO/IEC 27002:2005), which require that the CA ensure that it stays in line with industry requirements year upon year. Land Registry is also following the guidelines specified by 'tScheme', which is an independent body that sets out the required security standards for the trusted operation of e-business transactions conducted by an organisation. When the CA is externally audited it will be assessed against these guidelines.

In addition to the above, the CA will also fully observe the Data Protection Act 1998 and the Freedom of Information Act 2000, when dealing with individual Certificate information. (This is discussed further in section 10.)

9. What Governance procedures will be in place for the CA?

9.1 Internal Audit Policy

9.1.1 Types of event recorded

All actions undertaken by the CA, and transactions undertaken by Land Registry (as the land registration authority) that involve the CA, will be fully audited so that an accurate record is kept of all Certificate-related information. It is critical that Land Registry audit procedures are unambiguous, easily interpreted and tamperproof, and as such, Land Registry seeks to ensure compliance at all times with the provisions of the British Standard 'BIP 0008', which is a code of practice for legal admissibility and evidential weight of information stored electronically. A summary will be kept of audit log activity and a description of each transaction providing further details, such as an explanation of the event that the audit log is related to, and the severity of the transaction. The audit procedures that are in place are designed around ensuring that the CA can provide assurance that the guidelines set out by the independent body 'tScheme' are being followed.

9.1.2 Frequency of audit examination

Audit logs will be examined at least once a week for significant security and operational events. Further daily, monthly and annual vulnerability assessments will be performed and reviewed following examination of monitored events. In addition, audit logs will be reviewed in response to any alerts generated by irregularities and incidents within the CA systems. Any action taken in response to these examinations is also documented.

9.1.3 Protection, backup and retention of audit logs

Incremental back ups of audit logs are created daily and full backups are performed weekly. Audit logs will be retained long enough to validate any Land Registration transactions they are associated with before they are archived.

9.2 Records archival

9.2.1 Types of event recorded

The CA will archive all Certificate related audit information, as referred to in section 9.1.1, as well as Certificate application information, documentation supporting Certificate applications, and information regarding any renewal or revocation of a Certificate.

9.2.2 Protection, backup and retention of archive information

The archive is protected against unauthorised viewing, modification and deletion, or other tampering through a stringent security authorisation regime. The CA also incrementally backs up its electronic archives every day of Certificates that have been issued, and performs full back ups weekly. Records will be retained for at least five years following the date of Certificate revocation or expiry.

9.2.3 Procedure for obtaining archive information

Only authorised Land Registry personnel are able to obtain access to the archive. The integrity of the information is verified when it is restored.

9.3 External Compliance Audit

The CA will be audited every year by an external auditor who assesses the information security procedures carried out by Land Registry, both in reference to its general e-security practices as the land registration authority, and more specifically its operating procedures as a CA. The auditor will look at the environmental, key management controls, and Certificate management controls of the CA. The auditor will be responsible for making recommendations relating to the guidelines set out for information security, to ensure that Land Registry both as the land registration authority, and as CA, is in line with the necessary industry standards.

10. Will my Certificate information be kept confidential?

10.1 Types of information to be kept confidential

Personal information that is provided to or by the CA is covered by the principles set out in the Data Protection Act 1998. The CA is required to operate fully within the requirements of the Act. Such information collected or held by the CA may only be released to a third party in accordance with the Official Secrets Act 1989 and the Freedom of Information Act 2000. All private keys will be kept private and never disclosed.

10.2 Types of information not considered confidential

Non-personal Certificate information is not confidential and is deemed to be public knowledge where the Certificate is used for its intended purpose, and where the information appears in a public directory.

10.3 Release to law enforcement officials

Land Registry may make Certificate information available to law enforcement officials, notwithstanding the confidentiality obligations referred to in section 10.1.

11. What are the responsibilities of the CA?

The CA will be responsible for:

- ***ensuring that all administrators in organisations who perform registration activities for the CA in connection with Certificates are, as a minimum, supplied with the information contained in this document***
- ***producing Certificates correctly, maintaining evidence that due diligence was exercised in validating the information contained in the Certificate***
- ***managing suspected and actual key compromise, revoking Certificates as appropriate***
- ***publishing all Certificates and Certificate revocation lists in a publicly available location and in a timely manner***
- ***establishing effective business continuity arrangements to ensure that the CA is adequately prepared for a potential compromise***
- ***carrying out effective identity verification checks on organisations that apply for Certificates, on behalf of their administrator.***

12. What are the responsibilities of the Certificate holder?

The Certificate holder will be responsible for:

- ***submitting accurate and complete registration information to the Registration Authority or CA (as appropriate) during registration***
- ***ensuring that if they are in possession of a device that contains their private key, they keep it in their sole control at all times***
- ***exercising reasonable care to avoid unauthorised use of their private key***
- ***notifying the CA without unreasonable delay if their private key or activation data is lost, stolen or compromised in any way, or if the content of their Certificate becomes inaccurate***
- ***ensuring that Certificates are only used in accordance with this document***
- ***ensuring that the Certificate is not used after it has been revoked or has expired***
- ***not tampering with any aspect of the security credentials, Certificate or keys issued.***

13. What are the responsibilities of parties relying on a Certificate?

Parties relying on a Certificate issued by the CA will be responsible for:

- ***ensuring that the Certificate has been used for the purpose for which it has been issued***
- ***taking account of any limitation on the usage of the Certificate that has been indicated in the Certificate***
- ***verifying the validity and revocation status of the Certificate, using the current revocation status as indicated by the CA***
- ***establishing trust in the Certificate by verifying the Certificate path back to Land Registry's root CA***
- ***verifying that any e-signature has been generated using the associated private key***
- ***preserving the original signed data for as long as it takes to verify the signature of the data when the Certificate is used for e-signing.***

14. How can I obtain more information relating to Certificates issued by the CA?

Queries, comments and requests for additional information should be addressed to:

Certificate Policies
Business Development Board
HM Land Registry
Head Office
Lincoln’s Inn Fields
London
WC2A 3PH

Or alternatively can be emailed to:

certificate.policies@landregistry.gsi.gov.uk

15. Glossary

Term	Description
Algorithm	A specific set of instructions for carrying out a procedure or solving a problem.
Authentication Grid	A grid containing an assortment of characters, which is linked to the account of an individual. When the individual is required to authenticate they will be prompted for information from the grid, which they should have in their possession.
Certificate Policy	The administrative policy for the management of a particular type of Certificate. Land Registry issues different types of Certificate, each being associated with a different use, for example 'identity verification' Certificates, or 'local signing' Certificates.
Certificate Revocation List (CRL)	A time-stamped list of revoked Certificates that have been signed by the CA.
Cryptography	The science of protecting information from unauthorised access through the use of numeric keys and special mathematical functions.
Encrypt[ion]	The use of *cryptography* to make a message unreadable, to prevent unauthorised access.
Electronic Signature	Data in electronic form, affixed to or logically associated with a message, used to identify the originator, and the integrity of the message.
E-services	Electronically delivered Services
Decryption	The application of a cryptographic key to encrypted information in order to make it readable.
Hardware Security Module (HSM)	A cryptographic device that is used to store a private key and perform cryptographic tasks. Once generated, the private key can never leave the HSM apart from for the creation of back ups of the HSM.
Hash-Value	A number generated from a string of text. The hash is substantially smaller than the text itself, and is generated by a mathematical formula in such a way that it is extremely unlikely that some other text will produce the same hash value.

Term	Description
Key Pair	Two mathematically related keys. One key is used to encrypt messages created by the other key (see also private key and public key).
Organisation	A legal entity that has signed up to a User Agreement with Land Registry.
PIN	Personal Identification Number
Portal	A website that is a gateway to a number of different types of information and services.
Private Key	The key of a key pair that is kept secret and used to create an e-signature.
Public Key	The publicly available key of a key pair that is used to verify an e-signature purportedly sent by the holder of a corresponding private key.
Public Repository	A public database where Certificates and revocation status information is stored. The designation of a database as a repository is taken to signify that it is trustworthy and reliable.
Registration Authorit[y] (RA)	A company or individual delegated by a CA to verify the identity of a Certificate applicant.
Role	A grouping of 'permissions' to use particular functionality that may be allocated to an individual.
Root Key	The private key used by the CA to sign the Certificates it issues (see also private key).
Security Credentials	A secure detail or details allocated to a user in order for them to verify their identity when accessing a system account. This may take the form of details such as a user ID, password or PIN.
Shared Secret	Information not in the public domain and known only to a particular user. Often a shared secret consists of a question and answer pair, where the question is in the public domain, but only the user knows the answer to the question.

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

Issued by Land Registry Corporate Marketing Services July 2008.