Trustis FPS

Certificate Policy

trustis®

trustis®

Trustis FPS Certificate Policy

1 INTRODUCTION

1.1 Overview

A Certificate Policy is a named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements and is further supported by a Certification Practice Statement ("CPS"). The responsibility for this Certificate Policy lies with a body known as the Policy Authority, and any queries regarding the content of this policy should be directed to the Policy Authority.

Various terms are used throughout this document to define parties, processes, technology elements and applicable legal and regulatory requirements. These terms are explained in Appendix A.

This Certificate Policy is structured according to the guidelines provided by IETF RFC 2527 with extensions and modifications defined where appropriate. Further guidance in the preparation of this policy has been taken from the National Automated Clearing House Association (NACHA) Certification Authority Rating and Trust (CARAT) Task Force "Guidelines for Constructing Policies Governing the Use of Identity-Based Public Key Certificates" and the American Bar Association's draft "PKI Assessment Guidelines".

Each Issuing Authority that undertakes to issue certificates according to this policy may make its own decisions with regard to use of service providers, further restrictions on usage of certificates, additional liability provisions, etc. These decisions shall be published by the Issuing Authority in a document that shall henceforth be termed a **PKI Disclosure Statement.** The **PKI Disclosure Statement** shall serve as the highest-level vehicle by which provisions affecting Subscribers and Relying Parties are defined and shall incorporate this Certificate Policy by reference. All certificates issued under this policy shall contain a reference to where the **PKI Disclosure Statement** published by the Issuing Authority that issued the certificate, may be found.

This Policy defines a closed public key infrastructure and in conjunction with the **PKI Disclosure Statement,** specifies:
- Who can participate in the public key infrastructure defined by this Policy
- The primary rights, obligations and liabilities of the parties governed by this Policy
- The purposes to which certificates issued under this Policy may be put
- Minimum requirements to be observed in the issuance, management, usage and reliance-on certificates

1.2 Identification

This policy document is registered with Trustis Limited operating in an authorised administrative role for the Policy Authority defined in section 1 of **PKI Disclosure Statement** and remains the property of Trustis Limited at all times. Trustis Limited is registered with the Internet Address Naming Authority (IANA) and has been assigned an object identifier ("OID") of 1.3.6.1.4.1.5237. The Certificate Policy based on this document has also been assigned an OID as defined in section 12 of **PKI Disclosure Statement**

1.3 Community and Applicability

As described in the National Automated Clearing House Association (NACHA) Certification Authority Rating and Trust (CARAT) Task Force "Guidelines for Constructing Policies Governing the Use of Identity-Based Public Key Certificates", early thinkers conceived of a Certification Authority as not only the piece of software used to generate and manage the lifecycle of digital certificates, but also as the single party responsible for performing all PKI functions.

However, these same early thinkers recognised that a Certification Authority may delegate a certain set of functions to a Registration Authority. In practice, there are other sets of functions that can be logically and conveniently grouped and delegated. In business models, such sets of functions are those that are often outsourced or that have some other heightened significance

There is not necessarily a one-to-one correlation between roles and parties participating in a PKI. Any single party may perform one or more roles in any particular PKI. However, the decomposition of the parties participating in a PKI into clearly defined roles, enables organisations to flexibly construct the business relationships between themselves that takes advantage of both outsourcing and in-house capabilities where appropriate. Existing PKI deployments around the world, have tended to include the following roles with individual organisations taking up various combinations of those roles:

- Policy Authority
- Trust Service Providers
    - Issuing Authority
    - Certificate Manufacturer
    - Registration Authority (or Registrar)
    - Repository
- End Entities
    - Subscriber
    - Relying Party

Under such a role-based scheme, regardless of how organisations may decide to allocate the roles, whether to take on multiple roles, or to outsource one or more roles to one or more third party organisations, End-Entities need only have a business relationship with the Issuing Authority. Subscribers may see this instantiated in a Subscriber Agreement – a contract to be agreed-to at the time of the subscriber taking up the service. Relying Parties may see this through documentation explaining the rights, obligations and liabilities of both the Relying Party and the Issuing Authority. Should any end-entity need to dispute some issue or event, it is taken up with the Issuing Authority. If the Issuing Authority discovers that the dispute results from some lapse in a particular Trust Service, it is taken up by the Issuing Authority with that Trust Service Provider. If the Trust Service Provider is also part of the Issuing Authority organisation, then the matter is resolved internally, allowing the Issuing Authority to respond to the End-Entity. If however, the Trust Service Provision is out-sourced, then the Issuing Authority must rely on the contract between itself and the Trust Service Provider to resolve the matter. In either case, the Issuing Authority is responsible for resolving any potential dispute with End-Entities, according to rules and conditions defined in the Certificate Policy.

These relationships are shown diagrammatically in Figure 1.
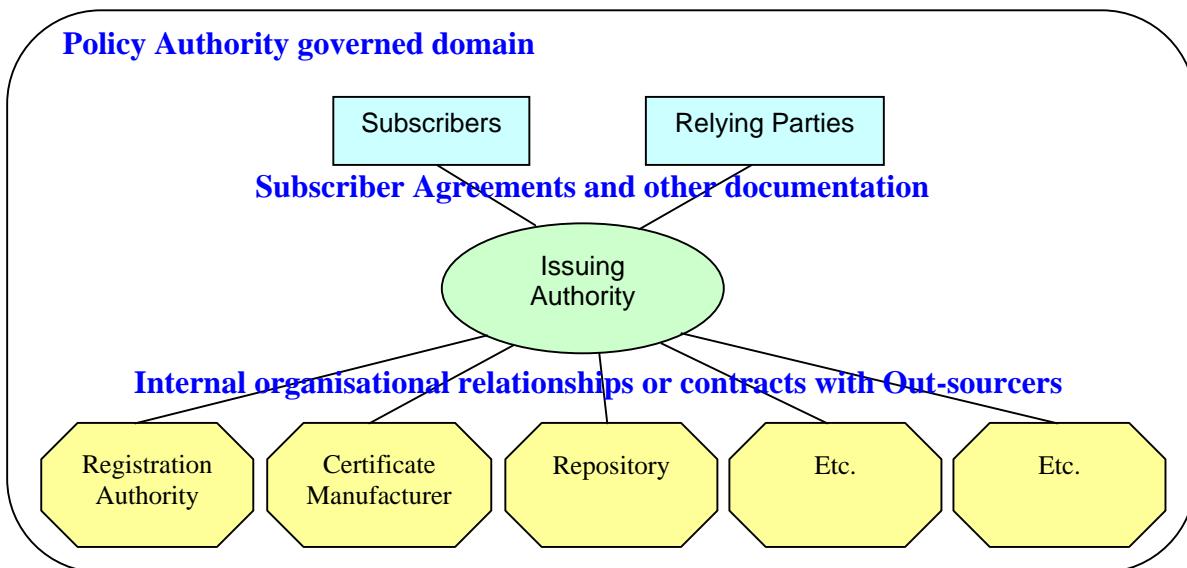
Figure 1. Roles & Business Relationships

These roles, that together comprise the PKI community governed by this Certificate Policy, are defined in the rest of section 1 of this document.

1.3.1   Policy Authority

The Policy Authority has ultimate responsibility for governance of the control, issuance, management and usage of digital certificates issued under this policy. The Policy Authority can be described as the governing body or the designee thereof, that is tasked with promulgating the Certificate Policy in a manner that supports and reflects the needs of the underlying relationships and transactions to be supported by a public key infrastructure. Simply stated, the Policy Authority is the entity that sets the rules under which the PKI is to be operated

The Policy Authority is identified in section 1 of **PKI Disclosure Statement.**

The only trust service providers and end entities authorised and approved by the Policy Authority to participate (i.e., issue, obtain, use, and/or rely upon certificates that reference this Policy) are detailed in the rest of section 1 of this document, conditional upon their first agreeing by contract to be bound by the terms of this Policy.

1.3.2   Trust Service Providers

1.3.2.1   Issuing Authority

By definition, an Issuing Authority is the entity listed in the issuer field of a digital certificate.

The Issuing Authority has the ultimate responsibility for deciding who may be issued with a certificate carrying its name and is the only entity with which End-Entities have any form of direct or indirect contractual relationship. Whether its digital certification services are provided by internal resources or are contracted out to external service providers, the provisions of this Policy shall apply. These may be reinforced by contract between the Issuing Authority and any service providers.

For the benefit of Subscribers and Relying Parties, the Issuing Authority shall publish a summary of important provisions that form a part of this Certificate Policy, together with any further provisions

affecting Subscribers and Relying Parties, in a document known as **PKI Disclosure Statement.** These provisions include, but are not limited to the following:
1. Policy Authority & Issuing Authority Contact Info
2. Certificate Type, validation procedures and usage
3. Reliance Limits:
4. Obligations of Subscribers:
5. Certificate Status checking obligations of Relying Parties:
6. Limited Warranty & Disclaimer/Limitation of Liability
7. Applicable Agreements, Certification Practice Statement, Certificate Policy
8. Privacy Policy
9. Refund Policy
10. Applicable Law & Dispute Resolution
11. CA & Repository Licences Trust Marks & Audit
12. Identification of this Certificate Policy
13. Approved Registration Authorities
14. Approved Repositories
15. Eligible Subscribers
16. Eligible Relying Parties
17. Certificate Status Information

Issuing Authorities shall ensure that all certificates issued by it under this Certificate Policy shall contain a reference to where its **PKI Disclosure Statement** and this Certificate Policy document may be found.

1.3.2.2   Certificate Manufacturer

The Certificate Manufacturer provides certificate management operational services for the Issuing Authority as detailed elsewhere in this policy.

The Certificate Manufacturer is approved by the Issuing Authority to manage certificates on behalf of other entities participating in the public key infrastructure governed by this policy.

1.3.2.3   Registrar (Registration Authority)

The Registrar or Registration Authority is responsible for ensuring the eligibility of applicants to be issued with certificates together with the accuracy and integrity of required information presented by applicants. The Registration Authority is a delegated function of the Issuing Authority and whose role is to approve requests from applicants for the issuance of certificates or for their revocation as detailed elsewhere in this policy.

The Issuing Authority has approved the Registration Authorities listed in section 13 of **PKI Disclosure Statement** with respect to certificates governed by this policy.

1.3.2.4   Repository

The Repository provides a community-wide accessible mechanism by which primarily subscribers and relying parties can obtain and validate information on certificates issued under this policy. The Issuing Authority has approved the Repositories identified in section 14 of **PKI Disclosure Statement** to provide these services.

1.3.3   End entities

1.3.3.1   Subscribers

A Subscriber is an entity (such as a person or organisation) that has applied for, and received a digital certificate. Certificate Applicants, eligible to be authorised by the approved Registration Authorities as subscribers, are identified in section 15 of **PKI Disclosure Statement.**

1.3.3.2 Relying Parties

A Relying Party is an entity that does not necessarily hold a certificate as a subscriber does, but even so, during the course of a transaction, may be a recipient of a certificate and who therefore relies on that certificate and/or digital signatures verified using that certificate. The right to rely on certificates issued under this policy is limited to the entities that are identified in section 16 of **PKI Disclosure Statement.**

1.3.4 Applicability

The categories of transactions, applications, or purposes for which certificates issued under this policy may be used are set forth in section 2 of **PKI Disclosure Statement.**

1.4 Contact Details

1.4.1 Specification administration organisation

The Policy Authority, responsible for approving rights, obligations, liabilities and all other terms and conditions contained in this policy, is listed in section 1 of **PKI Disclosure Statement.**

Trustis Limited is authorised by the Policy Authority to administer this policy. Trustis Limited may be contacted as follows:

Trustis Limited.	Email: info@trustis.com
Building 273	Web: http://www.trustis.com
New Greenham Park	
Greenham Common	Tel: +44 (0) 1865 736780
Thatcham,	Fax: +44 (0) 1865 736 782
Berkshire, RG19 6HN	
UK	

1.4.2 Contact person

Specific personnel who can be contacted regarding the contents of this policy are listed in section 1 of **PKI Disclosure Statement** under **Policy Authority.**

1.4.3 Person determining CPS suitability for the policy

Specific personnel who can be contacted regarding the suitability of Certificate Practice Statements to support this policy are listed in section 1 of **PKI Disclosure Statement** under **Issuing Authority.**

2 GENERAL PROVISIONS

2.1 Obligations

2.1.1 Trust Service Provider Obligations

2.1.1.1 Issuing Authority Obligations

An Issuing Authority that issues Certificates under this Certificate Policy shall as a minimum undertake to:
* Observe the rights of the Subscribers and Relying Parties who use Certificates in accordance with applicable laws and regulations
* Ensure that access is provided to a high availability certificate status information repository
* Ensure that Certificates are issued to Subscribers in accordance with the Certificate Policy
* Provide on-line customer service and guidance with respect to the location of services, authorities participating in the public key infrastructure, and good practice associated with subscriber and relying party behaviour

- Publish this Certificate Policy in a manner that is accessible by all parties participating in the public key infrastructure governed by this policy

2.1.1.2 Certificate Manufacturer Obligations

A Certificate Manufacturer that operates under this Certificate Policy shall as a minimum undertake to:
- Keep any private signature keys held by them confidential
- Keep confidential, any passwords, pass-phrases, PINs or other personal secrets used in obtaining authenticated access to PKI facilities and maintain proper control procedures for all such personal secrets
- Keep any tokens used in the performance of Certificate Manufacturer operations, and their related authentication information, separate in such a way that unauthorised possession of one of these items does not enable use of the other
- Use the private key created for the purpose of managing certificates that conform to this Certificate Policy, only for signing certificates and, certificate status information
- On authenticated request from the Registration Authority, manufacture certificates for Subscribers in accordance with the Certificate Policy
- On authenticated request from approved parties (section 4.4.2), revoke certificates that are created by this Certificate Manufacturer
- Supply public certificate information to the Repository
- Supply certificate status information to the Repository
- Notify the Issuing Authority of any breaches or suspected breaches of security or other circumstances that would affect the trust of certificates issued under this Certificate Policy

2.1.1.3 Registration Authority Obligations

A Registration Authority that operates under this Certificate Policy shall as a minimum undertake to:
- Keep confidential, any private signature keys held by them
- Keep confidential, any passwords, pass-phrases, PINs or other personal secrets used in obtaining authenticated access to PKI facilities and maintain proper control procedures for all such personal secrets
- If issued with a smart card or other hardware token, must keep the token and the related authentication information separate in such a way that unauthorised possession of one of these items does not enable use of the other
- Use a Registration Authority private signature key for all activities associated with the Registration Authority function
- Make only true and accurate representations to the Issuing Authority as to the information required to determine eligibility as a Registration Authority
- Make only true and accurate representations to the Issuing Authority for information contained within certificates used as part of Registrar operations
- In accordance with this Certificate Policy, authenticate Certificate Applicant and Subscriber requests for certificate management operations
- In accordance with this Certificate Policy, exclusively use their certificate for legal purposes and restricted to those authorised purposes detailed in section 1.3.4
- Immediately notify the Issuing Authority and/or the Certificate Manufacturer (if required to do so by the Issuing Authority), of a suspected or known key compromise

2.1.1.4 Repository Obligations

The Repository shall be obligated to:
- Provide access to a high availability information repository
- Provide notification to parties affected by certificate issuance, renewal, suspension and revocation via the publication of public key certificate information and certificate revocation information, through the use of an information repository
- Ensure that the information repository is maintained with the most current information available on certificates issued under this policy

- To the best of its abilities, protect information in the information repository from unauthorised modification

2.1.1.5 Time Stamping Authority Obligations

No stipulations.

2.1.1.6 Other Trust Services Obligations

No stipulations.

2.1.2 End Entity Obligations

2.1.2.1 Subscriber Obligations

It is the responsibility of the Subscriber to:
- Review his/her issued certificate to confirm the accuracy of the subscriber information contained within it before 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 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 this Certificate Policy exclusively use their certificate for legal purposes and restricted to those authorised purposes detailed in section 1.3.4
- Immediately notify the Registration Authority of a suspected or known key compromise in accordance with the procedures laid down in this Certificate Policy

2.1.2.2 Relying party Obligations

It is the responsibility of the Relying Party to:
- In accordance with the Certificate Policy, restrict reliance on certificates issued under this policy to appropriate uses as detailed in section 1.3.4
- Before relying on a certificate, ensure that the certificate has not expired and has not been revoked or suspended by accessing all relevant certificate status information repositories
- Before relying on a certificate, determine that such certificate provides adequate assurances for its intended use

2.2 Liability

2.2.1 Trust Service Provider Liability

2.2.1.1 Issuing Authority Liability

By signing a certificate containing a policy identifier which indicates the use of this policy, an 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/private key pairs issued under this policy for any use other than in accordance with this 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,

trustis®

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 Digital 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 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.

2.2.1.1.1   Limits of Liability

Notwithstanding the operation of section 2.2.1.1 above, the Issuing Authority limits any liability of any kind whatsoever for any award, damages or other claim or obligation of any kind arising from tort, contract or any other reason with respect to any service associated with the issuance, use of, or reliance upon certificates or associated public/private key pairs issued under this policy, in excess of that specified in section 6 of **PKI Disclosure Statement.**

Those utilising this PKI to protect their services or transactions may establish their own liability limits for prescribed transaction types under their control. Where this is done, the revised limits shall be published and available to all affected parties.

2.2.1.2   Certificate Manufacturer Liability

The Certificate Manufacturer, in providing a service for and on behalf of the Issuing Authority, is liable only to the Issuing Authority and does not accept any liability to others, including Subscribers and Relying Parties. Any liabilities of the Certificate Manufacturer are governed by the contract between the Certificate Manufacturer and the Issuing Authority.

2.2.1.3   Registration Authority Liability

The Registration Authority, in providing a service for and on behalf of the Issuing Authority, is liable only to the Issuing Authority and does not accept any liability to others, including Subscribers and Relying Parties. Any liabilities of the Registration Authority are governed by the contract between the Registration Authority and the Issuing Authority.

2.2.1.4   Repository Liability

The Repository, in providing a service for and on behalf of the Issuing Authority, is liable only to the Issuing Authority and does not accept any liability to others, including Subscribers and Relying Parties. Any liabilities of the Repository are governed by the contract between the Repository and the Issuing Authority.

2.2.1.5   Time Stamping Authority Liability

No Stipulations.

2.2.1.6   Other Trust Services Liability

No Stipulations.

2.3   Financial responsibility

2.3.1   Indemnification by Subscribers and Relying Parties

Subscribers and Relying Parties will be bound to accept the validity, terms and conditions for use of a key and its corresponding certificate unless Revocation has occurred.

The Issuing Authority assumes no liability whatsoever in relation to the use of certificates or associated public/private key pairs issued under this policy for any use other than in accordance with this policy and any other agreements. Subscribers and Relying Parties will forthwith indemnify the Issuing Authority from and against any such liability and any costs and claims arising therefrom

2.3.2   Fiduciary relationships

Issuance of certificates in accordance with this certificate policy does not make any of the Trust Service Providers listed, an agent, fiduciary, trustee, or other representative of Subscribers or Relying Parties. Neither Subscribers nor Relying Parties have any authority to bind Trust Service Providers, by contract or otherwise, to any obligation. Trust Service Providers will make no representations to the contrary, either expressly, implicitly, by appearance, or otherwise.

2.3.3   Administrative processes

No stipulations.

2.4   Interpretation and Enforcement

2.4.1   Governing law

This Certificate Policy shall be governed by the law of England and Wales and the parties submit to the exclusive jurisdiction of the courts of England and Wales. In the event of any dispute (other than one relating to the infringement of intellectual property rights, for which an injunction would be the appropriate remedy) arising from or concerning this Certificate Policy, then such matter shall be settled by mediation between the parties according to 2.4.3.

2.4.2   Severability, survival, merger, notice

2.4.2.1   Severability

In the event that any one or more of the provisions of this Certificate Policy shall for any reason be held to be invalid, illegal, or unenforceable at law, such unenforceability shall not affect any other provision, but this Certificate Policy shall then be construed as if such unenforceable provision or provisions had never been contained herein, and insofar as possible, construed to maintain the origin intent of the Certificate Policy.

2.4.2.2   Survival

This Certificate Policy shall be binding upon, and inure to the benefit of all parties hereto. The rights and obligations detailed in this Certificate Policy are not assignable by the parties and any purported assignment without such consent shall be void.

2.4.2.3   Merger

It is expressly agreed that the provisions set forth herein constitute all understanding and agreements between the parties. Any prior agreements, promises, negotiations, or representations not expressly set forth in this Agreement are of no force and effect. No term or provision of this Certificate Policy directly affecting the respective rights and obligations of any party may be orally amended, waived, supplemented, modified, or terminated, except by an authenticated message or document of such affected party, except to the extent provided otherwise herein.

If the Private Key corresponding to the Public Key that is specified in a Certificate to which this Certificate Policy applies is Compromised or the Expiration date of a Certificate to which this Certificate Policy applies is reached or passed then all rights and obligations except those that are identified in 2.4.2.2 shall merge.

2.4.2.4 Notice

Whenever any subscriber hereto desires or is required to give any notice, demand, or request with respect to this Certificate Policy, such communication shall be made either by using digitally signed messages consistent with the requirements of this Certificate Policy, or by paper-based communications. Electronic communications shall be effective upon the sender receiving a valid, digitally signed acknowledgment of receipt from recipient. Such acknowledgement must be received within five working (5) days, or else notice must then be given by paper-based communications. Such paper-based communications must be delivered by a service that confirms delivery in writing or via certified or registered mail, postage prepaid, return receipt requested, addressed to the Issuing Authority as detailed in section 1 of the **PKI Disclosure Statement** under **Issuing Authority.** All such communications shall be effective upon receipt.

A Subscriber requiring receipt of notice under this Certificate Policy is required to provide notice of:
- Changes in address including postal and e-mail addresses
- Changes in financial or other status, which would change the basis upon which the Certificate has been granted
- Any other notice pertinent to the maintenance of the provisions of this Certificate Policy.

Notice may be given to Relying Parties by digitally signed or unsigned messages, or by making such notice accessible online in a similar manner as that used for the publication of this Certificate Policy.

Notice requirements with regard to termination of Issuing Authority operations are specified in 4.9

Notice requirements with regard to changes in this Certificate Policy are specified in section 8.

2.4.3 Dispute resolution procedures

All disputes shall be referred in writing to the Issuing Authority. The Issuing Authority shall deal with such disputes in accordance with its dispute resolution process referred-to in section 10 of the **PKI Disclosure Statement**.

2.5 Fees

2.5.1 Certificate issuance or renewal fees

An Issuing Authority may establish its own fees for the issuance of certificates issued under this policy. If fees are charged, the fee schedule shall be published and available to all affected certificate applicants at the time of application for a certificate.

2.5.2 Certificate access fees

The Issuing Authority or Repository may charge fees for access to information on certificates issued under this policy, including certificates and certificate status information, in accordance with a fee schedule approved by the Issuing Authority. If such fees are charged, the fee schedule shall be published and available to all affected Relying Parties at the time of reliance on a certificate.

2.5.3 Revocation or status information access fees

As detailed in the section entitled "Certificate access fees".

2.5.4　Fees for other services such as policy information

A Trust Service Provider operating under this policy shall not impose any fees on the availability or distribution of this policy, or any document incorporated by reference in any certificate issued under this policy.

Fees for services such as access to archived information may be charged. If such fees are charged, the fee schedule shall be published and available to all affected parties.

2.5.5　Refund policy

An Issuing Authority may establish its own refund policy in respect of any fees charged for certificates issued under this policy. If fees are charged, the refund policy shall be published and available to all affected certificate applicants at the time of application for a certificate.

2.6　Publication and Repository

2.6.1　Publication of Trust Service Provider information

Issuing Authorities operating under this policy shall ensure the following items are made available to all parties participating in the public key infrastructure:
- Certificate revocation information
- This certificate policy with its associated **PKI Disclosure Statement**
- The Issuing Authority's public signature verification key
- All CA-certificates issued by the Issuing Authority (including those for sub-ordinate and superior Issuing Authorities, and cross certificates for cross certified Issuing Authorities)

2.6.2　Frequency of publication

Information as listed in 2.6.1 shall be published promptly upon its creation, with the exception that if CRLs are used to provide revocation information, they shall be published according to section 4.4.9 of this Certificate Policy.

2.6.3　Access controls

There may be access controls on information contained in the information repository. The Repository shall not prevent access by entities where required by this policy.

2.6.4　Repositories

An information repository shall be made available under the terms of this Certificate Policy, the Certificate Practice Statement and any relevant contract.

2.7　Compliance audit

2.7.1　Frequency of entity compliance audit

Services of Trust Service Providers operating under this policy and those of any designated authorised agents shall be audited at least annually.

2.7.2　Identity/qualifications of auditor

Approved Auditors are as defined in section 11 of **PKI Disclosure Statement** and may include internal auditing resources of Trust Service Providers.

2.7.3　Auditor's relationship to audited party

There are no restrictions on the auditor's relationship to the audited party provided that the auditor can demonstrate adequate independence from the audited party to ensure that the audited party cannot influence the audit process.

2.7.4   Topics covered by audit

Audit is required to ensure a Trust Service Provider is operating in accordance with its CPS, and may be required to attest to CPS conformity with this Certificate Policy.

Where the Trust Service Provider uses any designated authorised agents in order to provide the service, the audit shall also consider the operations of such designated authorised agents.

Audit will address all aspects of Trust Service Provider operations (whether or not directly in support of its CPS) to ensure overall standards of operation are commensurate with the risk assessment for certification according to this Certificate Policy.

2.7.5   Actions taken as a result of deficiency

If irregularities are found in the audit:
- On advice from the Policy Authority, other certifying Issuing Authorities may immediately revoke cross certification Certificates
- The Policy Authority may allow the Trust Service Provider to continue operations under conditions to be defined at that time by the Policy Authority in writing, pending correction of any problems before a decision to revoke or allow continuance of operations is taken
- The Policy Authority may require correction of minor shortcomings, but allow the Trust Service Provider to continue operations until the next audit without suspension or revocation.

The Policy Authority has responsibility for deciding what actions are to be taken. The decision regarding what actions to take will be based on previous responses to problems, the severity of the irregularities, and the recommendations of the auditor.

If a Cross-Certificate of another Issuing Authority is revoked, the Issuing Authority shall immediately update the appropriate certificate status information.

2.7.6   Communication of results

Trust Service Providers operating under this Certificate Policy must make a statement to Relying Parties that their practices fully comply with this Certificate Policy. It is strictly prohibited for any person or organisation to falsely claim compliance with this policy. The Policy Authority will take legal action against those making false statements.

2.8   Confidentiality

2.8.1   Types of information to be kept confidential

Any personal or corporate information held by Trust Service Providers that does not appear on issued Certificates is considered confidential and shall not be released without the prior consent of the Subscriber, unless required otherwise by law.

All private and secret keys used or otherwise handled by Subscribers and Trust Service Providers operating under this policy are to be kept confidential unless required otherwise by law.

Audit logs and records shall not be made available as a whole, except:
- As required by law
- Or as part of audit, (in which case only to an approved auditor)
- For verification of audit logs (see section 4.6.7.). Only records of individual transactions may be released.

2.8.2   Types of information not considered confidential

Certificates and certificate status information are not considered confidential unless special agreements so dictate.

2.8.3 Disclosure of certificate revocation/suspension information

See 2.8.2

2.8.4 Release to law enforcement officials

As stated in 2.8.1

2.8.5 Release as part of civil discovery

No stipulations.

2.8.6 Disclosure upon owner's request

As stated in 2.8.1

2.8.7 Other information release circumstances

No stipulations.

2.8.8 Requirements for Data Protection

Trust Service Providers, Subscribers, Relying Parties and all others using or accessing any personal data in connection with matters dealt with by this Certificate Policy shall comply with the Data Protection Act 1998, and any other relevant legislation relating to data protection, and any equivalent legislation or regulations in any relevant jurisdiction. Unless specified by special agreement, in the course of accepting a certificate, all Subscribers have agreed to allow their personal data submitted in the course of registration to be processed by and on behalf of the Trust Service Providers, and used as explained in the registration process, and have been given an opportunity to opt out of having their personal data used for particular purposes. They have also agreed to let certain personal data appear in publicly accessible directories and be communicated to others.

2.9 Intellectual Property Rights

All copyright and other intellectual property rights in this Certificate Policy and any Certification Practice Statement ('the Materials'), provided or made available by Trustis Limited, shall remain the property of Trustis Limited. Trustis Limited grants the Policy Authority and those Trust Service Providers, Subscribers, Relying Parties and other parties operating under this Certificate Policy, a non-exclusive licence to make use of the Materials only for the purposes and in compliance with the terms of this Certificate Policy, relevant Certification Practice Statements and any applicable contract, and in particular may only be used in conjunction with a public key infrastructure in which Trustis Limited is an approved Trust Service Provider.

Trust Service Providers, Subscribers, Relying Parties and other parties operating under this Certificate Policy shall ensure that all information supplied to other parties operating under this Certificate Policy, does not infringe upon any rights including intellectual property rights.

All parties operating under this Certificate Policy shall ensure that in using the services provided under this Certificate Policy they will do nothing illegal or in infringement of any third party rights and in particular will ensure that any material that they supply or transmit is not illegal, libellous, and does not infringe any intellectual property right.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Initial Registration

3.1.1 Types of names

Each Entity must have a clearly distinguishable and unique X.501 Distinguished Name (DN) in the certificate subjectName field of certificates issued under this Certificate Policy and in accordance with

IETF PKIX RFC 2459. Each Entity may in addition, use an alternative name via the SubjectAlternate Name field, which must also be in accordance with IETF PKIX RFC 2459.

3.1.2   Need for names to be meaningful

The contents of each certificate Subject name field must have an association with the authenticated name of the Entity. This association may be direct, or where the natural identity of a subscriber is required to be hidden, may be recorded elsewhere by the Registration Authority. The Relative Distinguished Name (RDN) may also identify an organisational position or role, provided that a person responsible for the oversight of that role, is recorded.

A certificate issued for a device or application must include within the DN the name of the person or organisation responsible for that device or application.

3.1.3   Rules for interpreting various name forms

The inclusion of Common name in a Distinguished Name is mandatory. All other fields that may be included are optional. Their interpretation for any entity shall be as follows:

Element	Description
Common name	Where the entity is a natural person, Common name may consist of a pseudonym established to hide the natural identity of the entity. In this case, the fact that the Common name is a pseudonym must be made obvious, either by the style of the pseudonym or by explicit indication in Common name. Where this hiding is not required, Common name shall consist of the given name, middle name or middle initial (if the entity has a middle name), and the family name of the entity, in that order, separated by space characters. Where the entity is a device or application, Common name shall consist of whatever information is required to identify the entity. These name forms may be followed by any other optional information required for identification or for uniqueness of RDN.
Street address	The physical location where the entity resides or conducts business or where the entity can receive paper mail.
Locality name	The city or town or other recognised locality where the entity resides or conducts business.
Country name	The country where the entity resides or conducts business.
Organization name	An organisation with which the entity has a significant relationship. The organization name serves only as an additional identifier of the entity and does not imply employment or any authority to act on behalf of the organisation unless the certificate and/or its policy specifically provide otherwise.
SubjectAlternate Name	Specified only in accordance with IETF PKIX RFC 2459. Where this specifies an email address, it is the electronic mail address at which the entity can receive electronic mail via the Internet.

3.1.4   Uniqueness of names

Distinguished names must be unique for all End-entities of an Issuing Authority. For each End-Entity any other optional information may be appended to the Distinguished Name as required for identification or to ensure it's uniqueness.

3.1.5   Name claim dispute resolution procedure

The Issuing Authority reserves the right to make all decisions regarding Entity names in all assigned certificates. A party requesting a certificate may be requested to demonstrate its right to use a particular name.

trustis®

3.1.6 Recognition, authentication and role of trademarks

No stipulations.

3.1.7 Method to prove possession of private key

The registration and/or issuance process shall involve a stage in which the applicant demonstrates possession of the private key.

3.1.8 Authentication of organisation identity

This process may include face-to-face authentication with a duly authorised and authenticated representative of the organisation, but not require it, provided that alternate mechanisms of commensurate reliability and trust are in place for authenticating the validity of the application and the identity of both the applicant organisation and the representative making the application. The Issuing Authority in section 2 of **PKI Disclosure Statement** or other community-wide accessible document, shall define the mechanisms to be used that support the level of confidence required in the identity asserted by a digital certificate issued under this Certificate Policy. The Registration Authority shall note the method used in an audit log.

The Registration Authority shall verify that each certificate applicant has a right to obtain that certificate and, if the certificate will imply that the subscriber has particular attributes or privileges, that the applicant has the corresponding attributes or privileges.

3.1.9 Authentication of individual identity

The Issuing Authority shall undertake face-to-face authentication of one or more initial Registration Authority Administrators. A nominated Registration Authority Administrator may undertake face-to-face authentication of subsequent Registration Authority Administrators.

Authentication and validation of Subscriber applicants may include face-to-face authentication, but not require it, provided that alternate mechanisms of commensurate reliability and trust are in place for authenticating the validity of the application and the identity of the applicant. The Issuing Authority in section 2 of **PKI Disclosure Statement** or other community-wide accessible document, shall define the mechanisms to be used that support the level of confidence required in the identity asserted by a digital certificate issued under this Certificate Policy. The Registration Authority shall note the method used in an audit log..

The Registration Authority shall verify that each certificate applicant has a right to obtain that certificate and, if the certificate will imply that the subscriber has particular attributes or privileges, that the applicant has the corresponding attributes or privileges.

3.2 Routine Rekey

Applications for renewal or replacement of Subscribers' keys and Certificates prior to any revocation or time expiry shall be via a renewal request. Provision of registration information or undergoing a new registration process is not required.

3.3 Rekey after Revocation

Applications for renewal or replacement of Subscribers' keys and associated certificates after revocation shall require full registration.

3.4 Revocation Request

An Issuing Authority, or Registration Authority acting on its behalf, must undertake to authenticate a request for revocation of a certificate. An Issuing Authority must establish and make available to all parties participating in the public key infrastructure, the process by which it addresses such requests and the means by which it will establish the validity of the request. If there is a recognised risk for fraudulent misuse of the private key associated with the certificate to be revoked, and reliable

authentication of the revocation request isn't possible, the Issuing Authority, or Registration Authority acting on its behalf, shall give priority to revocation of the certificate even if this requires the means of authentication to be reduced, or even omitted. In such case the Issuing Authority or Registration Authority acting on its behalf shall seek confirmation of the request to the greatest extent possible by practical means.

Requests for revocation of certificates must be logged.

4 OPERATIONAL REQUIREMENTS

4.1 Certificate Application

An Issuing Authority, or Registration Authority acting on its behalf, must ensure that all procedures and requirements with respect to an application for a certificate are set out in a document that is made available to the community to be served. Bulk applications on behalf of End-Entities, if supported, are permitted to be made only by persons authorised by the Issuing Authority to make such applications.

An applicant for a certificate (which may be an authorised person in the case of organisations, organisational units, roles, devices or applications) shall complete the following procedures for each certificate application:

- Apply for a certificate by use of an application procedure approved by the Issuing Authority. This may be in an on-line format.
- Present personal information to be validated and/or to be filed along with the certificate application.
- Present a public key and prove possession of the corresponding private key, which must be generated using a PSE according to this policy, or consent to having a new private key generated, protected and stored on a PSE according to this policy. In addition in the latter case, be informed how he/she will obtain the initial PSE activation data and how this can be changed into personally chosen activation data.
- Authenticate himself/herself either in person or by alternative methods of equivalent reliability to the Registration Authority according to requirements specified in the section entitled "Identification and Authentication".
  - In cases where the intended subscriber generates the private key, this may take place at the time of initial application.
  - In cases where the private key is generated and protected by an entity approved by the Issuing Authority for this task (e.g. an authorised Registrar of a Registration Authority), this authentication must at least take place in conjunction with the delivery of the PSE and/or activation data.

An application for a certificate does not oblige an Issuing Authority to issue a certificate.

4.2 Certificate Issuance

The issuance of a certificate by an Issuing Authority indicates a complete and final approval of the certificate application by the Issuing Authority.

Registration of the information necessary for issuing certificates and any associated tokens shall be performed in a system with high-level integrity protection. The registration routine shall ensure no compromise or confusion of personal data, can occur.

The private key used for signing approved certification requests shall as a minimum meet the security requirements for Registration Authority private keys according to this policy.

4.3 Certificate Acceptance

A subscriber shall explicitly indicate acceptance of a certificate to the Issuing Authority. The Issuing Authority shall make certain that the subscriber in connection with the acceptance of a certificate

acknowledges that it agrees to the terms and conditions stipulated in the certificate policy and any other applicable contractual documents prior to first use of the certificate.

For a device or application, the individual responsible for the device or application may give this acknowledgement.

The Issuing Authority shall undertake to clearly inform the subscriber, that by accepting a certificate issued under this certificate policy, a subscriber agrees to, and certifies, that at the time of certificate acceptance and throughout the operational period of the certificate, until notified otherwise by the subscriber:

- No unauthorised person has ever had access to the subscriber's private key
- All information given by the subscriber to the Issuing Authority or Registration Authority relevant for the information in the certificate are true
- The private key associated with the certificate is being consciously used in consistence with usage restrictions in the certificate

The above stipulations may be integrated with the certificate application process and the PSE delivery process as appropriate.

4.4   Certificate Suspension and Revocation

The Issuing Authority is formally responsible for ensuring that certificate status information is provided.

The certificate status information service shall enable Relying Parties to obtain status information on all revoked and/or suspended certificates; at least until their assigned validity period expires.

Upon revocation or suspension of a subscriber's certificate, the Issuing Authority shall undertake to inform the subscriber.

4.4.1   Circumstances for revocation

A certificate must be revoked:

- When any of the information in the certificate is known or suspected to be inaccurate
- Upon suspected or known compromise of the private key
- Upon suspected or known compromise of the media holding the private key
- When the Subscriber withdraws from or is no longer eligible to participate in the public key infrastructure governed by this certificate policy

The above use of the term "compromise" is intended to include:

- Unauthorised access
- Loss
- Theft
- Irrecoverable corruption
- Destruction

The Issuing Authority may revoke a certificate when an Entity fails to comply with obligations set out in this certificate policy, any additional published documents defining practices to be followed by the entity, any other relevant agreement or any applicable law.

4.4.2   Who can request revocation

The revocation of a certificate may be requested by any entity, authenticated according to section 3.4 of this Certificate Policy that presents reliable information indicating a valid circumstance for revocation according to 4.4.1. Approval of a revocation request may only be granted by:

- The Policy Authority
- The Issuing Authority

- Authorised and authenticated administrators of the Issuing Authority
- Authorised and authenticated Registrars of a Registration Authority acting on behalf of the Issuing Authority

Upon revocation of a subscriber's certificate, the Issuing Authority shall undertake to inform the subscriber.

4.4.3   Procedure for revocation request

Revocation shall be requested promptly after detection of a compromise or any other event giving cause for revocation.

A revocation request may be generated in the following ways, in order of preference:
- Electronically by a digitally signed message
- By personal representation to the Issuing Authority or a Registration Authority
- By a signed fax message
- Electronically by a non-signed message
- By telephone call to the Issuing Authority or a Registration Authority

Authentication of the revocation request shall meet the requirements in 3.4 of this Certificate Policy.

The Issuing Authority or Registration Authority acting on its behalf may seek independent confirmation, for example, by making a phone call to the subscriber's employer, prior to initiating the revocation of a certificate.

The Issuing Authority, or Registration Authority acting on its behalf, shall archive all revocation requests, the cause for revocation, the means of authenticating the requester and the resulting actions taken.

4.4.4   Revocation request grace period

None. If the revocation request is approved, it must be reflected in the next scheduled publication of certificate status information.

4.4.5   Circumstances for suspension

This Certificate Policy does not support suspension of subscriber certificates.

4.4.6   Who can request suspension

Not applicable.

4.4.7   Procedure for suspension request

Not applicable.

4.4.8   Limits on suspension period

Not applicable.

4.4.9   CRL issuance frequency (if applicable)

Where CRLs are used to provide revocation information, the Issuing Authority shall ensure that publication of valid certificate status information is scheduled at least every twenty-four (24) hours.

4.4.10 CRL checking requirements

A Relying Party must check the status of all certificates in the certificate validation chain against the current CRLs or other pertinent revocation information before relying on them. A Relying Party must verify the authenticity, validity and integrity of CRLs or any other pertinent certificate status information used.

If no valid certificate status information can be obtained, due to system or service failure, then no certificates should be accepted or relied-upon. Any acceptance or reliance-on a certificate without conformance to this requirement is done at the Relying Party's own risk.

4.4.11 On-line revocation/status checking availability

As an alternative to CRL-checking, an on-line status-checking service, if available, may be used. The details of any support for on-line certificate status information shall be published for the benefit of relying parties.

4.4.12 On-line revocation checking requirements

As specified in 4.4.10 of this Certificate Policy.

4.4.13 Other forms of revocation advertisements available

No stipulations.

4.4.14 Checking requirements for other forms of revocation advertisements

No stipulations.

4.4.15 Special requirements re key compromise

In the event of the compromise, or suspected compromise, of any Entity's private key, an Entity must notify the Issuing Authority or Registration Authority immediately and must indicate the nature and circumstances of the compromise, to the fullest extent known.

4.5 Security Audit Procedures

4.5.1 Types of event recorded

Audit logs of all transactions pertinent to Certificate lifecycle management shall be securely maintained to provide an audit trail. The precise list of events audited for each Trust Service Provider shall be recorded in its CPS.

4.5.2 Frequency of processing log

A Trust Service Provider must ensure that its personnel review its audit logs at least once every two weeks and all significant events are explained in an audit log summary. Such reviews shall involve verifying that the log has not been tampered with, and then inspecting all log entries, with a thorough investigation of any alerts or irregularities in the logs.

Actions taken following these reviews must be documented.

4.5.3 Retention period for audit log

Audit logs are to be retained for a period of no less than seven (7) years

4.5.4 Protection of audit log

The electronic audit log system must include mechanisms to protect the log files from unauthorised viewing, modification, and deletion. Manual audit information must be protected from unauthorised viewing, modification and destruction.

4.5.5 Audit log backup procedures

Audit logs and audit summaries must be backed up or if in manual form, must be copied.

4.5.6 Audit collection system

No stipulations.

4.5.7 Notification to event-causing subject

No stipulations.

4.5.8 Vulnerability assessments

No stipulations.

4.6 Records Archival

4.6.1 Types of event recorded

The records to be recorded for an individual Trust Service provider shall include all relevant evidence in the Trust Service Provider's possession, for example:

- Certificate requests and all related messages exchanged with Trust Service Providers
- Registration agreements from Subscriber's applications for Certificates, PSEs and activation data, including the identity of the person responsible for accepting the application
- Signed acceptance of the delivery of PSEs and any activation data
- Contractual agreements regarding Certificates and associated tokens
- Contents of issued Certificates
- Certificate renewals and all Messages exchanged with the Subscriber
- Records on CA rekeying including key identifiers and cross Certificates
- Records on cross certification including the decision basis for cross certification and the performed actions
- Revocation requests and all recorded messages exchanged with the originator of the request and/or the Subscriber
- CRLs posted to the directory and/or any other relevant revocation checking information
- Audit journals including records of annual auditing of a Trust Service Provider's compliance with its CPS.
- Current and previously implemented Certificate Policy documents and their related CPSs.

The precise list of records to be archived for each individual Trust Service provider shall be recorded in the CPS.

Records of all digitally signed electronic requests made by Trust Service Provider personnel (trusted staff) shall include the identity of the administrator responsible for each request together with all information required for non-repudiation checking of the request for as long as the record is retained.

4.6.2 Retention period for archive

Archives shall be retained for a period as specified in the CPS, or for seven (7) years, whichever is the greater.

4.6.3 Protection of archive

Archives shall be protected from unauthorised viewing, modification, and deletion. At least one copy of the archive must be adequately protected from environmental threats such as temperature, humidity and magnetism.

4.6.4 Archive backup procedures

No stipulations.

4.6.5 Requirements for time-stamping of records

No stipulations.

4.6.6 Archive collection system

No stipulations.

trustis®

4.6.7   Procedures to obtain and verify archive information

Trust Service Providers shall comply with the confidentially requirements specified in this Certificate Policy (see section 2.8).

Records of individual transactions may be released upon request by any of the entities involved in the transaction, or their recognised representatives.

Trust Service Providers shall ensure availability of their archives and that archived information is stored in a readable format during its retention period, even if the Trust Service Provider's operations are interrupted, suspended or terminated.

In the event that the services of a Trust Service Provider providing services for or on behalf of the Issuing Authority are to be interrupted, suspended or terminated, the Issuing Authority shall ensure the continued availability of the archive. All requests for access to such archived information shall be sent to the Issuing Authority or to the entity identified by the Issuing Authority prior to terminating its service.

4.7   Key changeover

A Subscriber may only renew or replace a certificate and key pair prior to the expiration of the keys, provided that the current certificate remains valid and has not been revoked. A Subscriber, the Issuing Authority, or the Registration Authority may initiate this key changeover process. Automated notification of an impending required key changeover is permitted, but not required to be supported.

Subscribers without valid keys must be re-authenticated in the same manner as the initial registration.

Where a Subscriber's certificate has been revoked as a result of suspected or actual non-compliance, whichever of the Issuing Authority or the Registration Authority that intends to initiate the key changeover process, must verify that any reasons for non-compliance have been addressed to its satisfaction prior to certificate re-issuance.

New Issuing Authority CA signing keys shall be generated and a new CA-certificate corresponding to these keys shall be issued at least three months prior to the expiration of the old CA-certificate.

After generation of the new Issuing Authority signing keys, the Issuing Authority shall cross certify according to the following:
* The Issuing Authority holding the new private CA-key shall issue one certificate for the old public CA-certificate signed with the new private CA-key and
* The Issuing Authority holding the old private CA-key shall issue one certificate for the new public CA-certificate signed with the old private CA-key

All CA-certificates shall be made available in a repository accessible to all participants in the PKI.

All copies of old Issuing Authority private CA-keys shall be:
* Destroyed such that the private keys cannot be retrieved; or
* Retained in a manner such that they are protected against being put back into use

4.8   Compromise and Disaster Recovery

A business continuity plan shall be in place to protect critical public key infrastructure processes from the effect of major compromises, failures or disasters. These shall enable the recovery of all Issuing Authority services. Business continuity plans shall be specified in the CPS. Trust Service Providers must provide evidence that such plans have been exercised. In any such case the Issuing Authority shall as a minimum provide the following undertakings:
* Immediately cause the suspension of the certificate status checking service for all issued Certificates affected by a compromise, failure or disaster. This will stop any of these certificates

trustis®

from being accepted by any relying party who follows proper revocation checking procedures according to 4.4.10

4.8.1 Computing resources, software, and/or data are corrupted

Trust Service Providers must establish business continuity procedures that outline the steps to be taken in the event of the corruption or loss of computing resources, software and/or data. Where an individual Trust Service Provider is not under the control of the Issuing Authority, the Issuing Authority must ensure that any agreement with the Trust Service Provider ensures that business continuity procedures be established and documented by the Trust Service Provider.

4.8.2 Entity public key is revoked

See section 4.8

4.8.3 Entity key is compromised

See section 4.8

4.8.4 Secure facility after a natural or other type of disaster

A backup facility used for relocation following a disaster shall maintain compliance with this Certificate Policy. During any relocation/transition, the provisions of this certificate policy shall be maintained.

4.9 CA Termination

Termination of a CA is regarded as the situation where all service associated with an Issuing Authority is terminated permanently. It is not the case where the service or elements of the service is transferred, such as between or to Certificate Manufacturers, or responsibility for certificates is transferred between Issuing Authorities, even if there is a change of CA-Keys.

Before terminating its service, an entity approved as an Issuing Authority under this policy must undertake the following actions in the sequence as shown below:
1. Inform the Policy Authority
2. Provide a notice period of 90 days to Subscribers with valid certificates and all other Issuing Authorities with whom it is cross-certified, that certificate revocation will take place at the end of that period
3. Make available for viewing by Relying Parties, a similar notification
4. Revoke all certificates at the end of 90 days without prejudice to any claims, rights or obligations that any Subscribers or Relying Parties may have up to the date of revocation.
5. Ensure preservation and storage of records in the manner and for the time indicated in 4.6
6. Arrange for the continued retention of the logical CA's keys in the manner and for the time indicated in 4.6

In the event of failure to comply by the Issuing Authority, the Policy Authority shall make best endeavours to notify affected subscribers.

In the event of a change in management of an Issuing Authority's operations, the Issuing Authority must notify all Entities for which it has issued certificates and other Issuing Authorities with whom it has cross-certified.

In the event of a transfer of an Issuing Authority's operations to another Issuing Authority operating at a lower level of assurance, the certificates issued through the Issuing Authority whose operations are being transferred must be revoked prior to the transfer.

5 PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS

5.1 Physical Controls

5.1.1 Site location and construction

See section 5.1.2

5.1.2 Physical access

Sites where certificate manufacture or time-stamping operations are carried out must:
- Satisfy at least the requirements for a Security Zone
- Be manually or electronically monitored for unauthorised intrusion at all times
- Ensure unescorted access to the CA or time-stamping server is limited to those personnel identified on an access list
- Ensure that access to the CA or time-stamping server, shall require the simultaneous presence of at least two persons on the access list
- Ensure personnel not on the access list are properly escorted and supervised
- Ensure a site access log is maintained and inspected periodically
- Ensure all removable media and paper containing sensitive plain text information are stored in secure containers.

Under this policy, the detailed functionality of a Registration Authority may vary. In some scenarios, the Registration Authority is simply a data gatherer that assists the Issuing Authority in gathering registration or revocation information from users, authenticating users, and forwarding the results to the Issuing Authority and/or Certificate Manufacturer. In other scenarios the Registration Authority may additionally initialise and load certificates and private keys into protected stores or tokens. The physical security controls for the various types of Registration Authority will be different.

In the case where Registration Authorities act only as information verifiers/forwarders
- Registration Authority sites must be located in areas that at least satisfy the controls required for a Reception Zone
- If a Registration Authority is permitted to submit on-line requests for certificate issuance, the Issuing Authority will ensure the operation of the Registration Authority site provides appropriate security protection of the cryptographic module and the Registration Authority Administrator's private key
- A security container should be utilised for storing records of subscriber registration requests and tokens used to gain access to the Registration Authority workstation

In the case where Registration Authorities' workstations may hold confidential subscriber information (including subscriber key materials), then the Registration Authority's physical security controls shall be equivalent to those required for certificate manufacture as described in this section 5.1

All Repository sites must be located in areas that at least satisfy the requirements for an Operational Zone, and in addition, must:
- Ensure unescorted access to the Repository server is limited to those personnel identified on an access list;
- Ensure personnel not on the access list are properly escorted and supervised;
- Ensure a site access log is maintained and inspected periodically

Where PINs, pass-phrases or passwords are recorded, they must be stored in a security container accessible only to authorised personnel.

Subscribers must not leave their workstations unattended when the cryptography is in an unlocked state

trustis ®

(i.e., when the PIN, pass-phrase or password has been entered). A workstation that contains private keys on a hard drive must be physically secured or protected with an appropriate access control product:

5.1.3   Power and air conditioning
No Stipulations

5.1.4   Water exposures
No Stipulations

5.1.5   Fire prevention and protection
No Stipulations

5.1.6   Media storage
No Stipulations

5.1.7   Waste disposal
All media used for the storage of information such as keys, activation data, confidential subscriber information or CA files is to be sanitised or destroyed before released for disposal.

5.1.8   Off-site backup
As required by the business continuity plan specified in 4.8

5.2   Procedural Controls

5.2.1   Trusted roles
A Trust Service Provider must ensure a separation of duties for critical functions to prevent single person from maliciously using the Trust Service Provider system without detection.

A Trust Service Provider should provide for the separation of distinct PKI personnel roles, distinguishing between day-to-day operation of the Trust Service Provider system and the management and audit of those operations. To the greatest extent possible, differing levels of physical and systems access control based on roles and responsibilities should be employed to reflect the requirements of those roles and responsibilities. Only those personnel responsible for the duties required for Trust Service Provider operations should have access to the software that controls the Trust Service Provider operation.

An Issuing Authority must ensure that Registration Authority personnel are adequately trained and understand their responsibility for the identification and authentication of prospective Subscribers and perform the following functions:
* Acceptance of subscription, certificate change, certificate revocation and key recovery requests
* Verification of an applicant's identity and authorisations
* Transmission of applicant information to the Issuing Authority and/or Certificate Manufacturer
* Provision of authorisation codes for on-line key exchange and certificate creation

An Issuing Authority may permit all roles and duties for Registration Authority functions to be performed by one individual.

5.2.2   Number of persons required per task
Multi-user control is required for CA key generation as outlined in 6.2.2.

All other duties associated with Issuing Authority or Certificate Manufacturer roles may be performed by an individual operating alone, however, it must be ensured that any verification process employed provides for oversight of all activities performed by privileged role holders.

5.2.3   Identification and authentication for each role

All Trust Service Provider personnel must have their identity and authorisation verified before they are:
- Included in the access list for the Trust Service Provider site
- Included in the access list for physical access to the Trust Service Provider system
- Given a certificate for the performance of their Trust Service Provider role
- Given an account on the Trust Service Provider system

Each of these certificates and accounts (with the exception of CA signing certificates) must:
- Be directly attributable to an individual
- Not be shared
- Be restricted to actions authorised for that role through the use of Trust Service Provider software, operating system and procedural controls

Trust Service Provider system operations must be secured, using mechanisms such as token-based strong authentication and encryption, when accessed across a shared network.

5.3   Personnel Controls

5.3.1   Background, qualifications, experience, and clearance requirements

A Trust Service Provider must ensure that all personnel performing duties with respect to its operation must:
- Be appointed in writing
- Be bound by contract or statute to the terms and conditions of the position they are to fill
- Have received training with respect to the duties they are to perform
- Be bound by statute or contract not to disclose sensitive Trust Service Provider security-relevant information or Subscriber information
- Not be assigned duties that may cause a conflict of interest with their Trust Service Provider duties
- Not have been, as far as known, previously relieved of a past assignment for reasons of negligence or non-performance of duties

Trust Service Providers may also specify additional criteria for security clearance of personnel, such as requirements for citizenship, rank, qualifications, satisfactory credit check, and absence of a criminal record. Any such additional requirements shall be stated in the CPS.

5.3.2   Background check procedures

As stated in 5.3.1

5.3.3   Training requirements

No stipulations.

5.3.4   Retraining frequency and requirements

No stipulations.

5.3.5   Job rotation frequency and sequence

No stipulations.

5.3.6   Sanctions for unauthorised actions

No stipulations.

5.3.7   Contracting personnel requirements

A Trust Service Provider must ensure that contractor access to its facilities is in accordance with this Certificate Policy. Individuals not security cleared must be under supervision by security cleared personnel at all times.

5.3.8   Documentation supplied to personnel

A Trust Service Provider must make available to its personnel the certificate policies it supports, its CPS, and any specific statutes, policies or contracts relevant to their position.

6   TECHNICAL SECURITY CONTROLS

6.1   Key Pair Generation and Installation

6.1.1   Key pair generation

Subscribers' key pairs may be generated by anyone approved by the Issuing Authority for the purpose, including the subscriber, with the recommendation that Subscribers' or other Entities' key pairs for signing use should preferably be generated only by the entity owning them.

Should a Subscriber's key pairs not be generated by the Subscriber, then sufficiently trusted and audited procedures requiring multi-person control should be invoked to ensure that the private key is protected from access or use by unauthorised entities.

Input to the key generation process shall be a random number, created in such a way and with such length as to make it computationally infeasible to regenerate it, even given knowledge about when and in which equipment it was generated.

The generation procedure and storage of the Private Key shall prevent it from being exposed outside of the system that created it. Furthermore, it shall be erased from the system immediately after having been transferred to a Personal Security Environment (PSE) that is approved by the Issuing Authority and satisfying the requirements of 6.2.1.

6.1.1.1   Specific requirements regarding Issuing Authority's issuing keys

The Issuing Authority's keys shall be generated and protected within a protected environment complying with sections 6.2.1 and 5.1 of this Certificate Policy.

6.1.2   Private key delivery to entity

If the private key is not generated by the prospective certificate holder, which in any case must only be accomplished according to 6.1.1, it must be delivered to the Entity via the use of a PSE approved by the Issuing Authority and satisfying the requirements of 6.2.1. In this case:

- The PSE containing the private key, protected with its initial activation data, shall be distributed to the subscriber in a way that prevents it from being found together with the activation data, until it has been delivered to the subscriber. This can be achieved by using separate channels of distribution for PSEs and their associated activation data, or by clearly separating their distribution in time
- The PSE issuer may supply the activation data directly at the time of ordering of the PSE by handing it over in a sealed envelope, or in a separate letter to the intended certificate holder's permanent address
- Delivery of a PSE, containing a private key that is (or will be) associated with a certificate according to this policy, is only allowed to be effected to the subscriber in person through a face to face meeting with the Issuing Authority, or other authorised representative of the Issuing Authority. A sufficiently trusted representative of the Issuing Authority for this purpose would normally be the Registration Authority, but in any case will be identified to the subscriber at the time of application. To obtain the PSE, the subscriber shall present valid identification that at least

meets the requirements for initial registration (3.1.9). The means of identification is noted on the receipt, which is also signed by the person, who hands over the PSE

- The receipt of the PSE shall be acknowledged by the subscriber's signature on a special form, which is filed by the PSE issuer
- The subscriber shall be clearly instructed to replace the initial activation data with personally chosen activation data at the first suitable occasion

6.1.2.1   Requirements for distribution and safekeeping of cryptographic token

Where cryptographic tokens are used by Trust Service Providers for trusted roles, before key and application initialisation:
- Deliveries of tokens from manufacturers shall be checked to see that they comply with their corresponding orders regarding properties and quantities
- Delivered consignments shall be kept together until key and application initialisations have been performed
- Two persons shall supervise all handling of the tokens, and the tokens shall be kept in a space equipped with burglar alarm and protected against break-in by a security container

After key and application initialisation, but before personalisation:
- Tokens shall be delivered to personalisation in packets, in such a way that one packet is used up before tokens are taken from the next. Unopened packets, as well as not yet finished packets of key and application initialised cards, shall be kept in security containers and be handled under the supervision of two persons.
- All deliveries between processes shall be documented. Documented routines shall be established for the handling of exceptional events, including loss of or damage to tokens

After personalisation:
- Immediately after the moment a token containing a private key has been associated with a specific subscriber the token shall – individually or bundled – be wrapped in a sealed parcel together with information about name and address of the token delivery-place and the associated subscriber, unless this personalisation is carried out by the Registration Authority and the token can be handed over immediately to the subscriber according to 6.1.2.
- Personalised tokens shall be immediately transferred to the place where they are to be delivered to the subscriber
- The personalisation shall be scheduled so as to minimise the time that the personalised tokens require safekeeping before delivery to the subscriber. Storage over night requires safekeeping in a vault or security container. Documented routines shall exist for exception handling, including disturbances in the production process, failure of delivery, and loss of or damage to tokens
- Personalised tokens shall always be kept separated from non-personalised tokens.

6.1.3   Public key delivery to Issuing Authority

If the Issuing Authority or Certificate Manufacturer acting under its authorisation does not generate the public encryption key, it must be delivered to the Issuing Authority and/or Certificate Manufacturer via the use of secure methods that protect key material and any associated personal information data from unauthorised access, modification and use.

On delivery of a public key for which it is intended that a certificate be issued, then prior to certificate issuance:
- Either the intended certificate holder or a Registration Authority must prove possession of the corresponding private key; or
- The public key must be proven to match the private key that will eventually be delivered to the intended certificate holder, using other methods documented in the CPS.

6.1.4   CA public key delivery to users

No stipulations.

6.1.5 Key sizes

The size of CA-Keys keys shall be at least 2048 bit modulus (m) for RSA.
The size of Subscribers Private Keys shall be at least 1024 bit modulus (m) for RSA.

6.1.6 Public key parameters generation

Public Key exponents shall be of values and lengths that make known attacks (e.g. low exponents attacks) infeasible.

6.1.7 Parameter quality checking

No stipulations.

6.1.8 Hardware/software key generation

Keys may be generated in hardware or software provided the requirements of this Certificate Policy are met.

6.1.9 Key usage purposes (as per X.509 v3 key usage field)

The key usage extension in X.509 v3 certificates defines the purpose (e.g., encipherment, signature, certificate signing) of the key contained in the certificate.

A usage restriction may be employed when a key that could be used for more than one operation is to be restricted. For example, when a key should be used only for non-repudiation services the nonRepudiation bit would be asserted. Likewise, when a key should be used only for key management, the keyEncipherment bit would be asserted.

Certificates issued under this policy may be used in applications and services as listed in section 1.3.4.1. Accordingly a certificate will typically embrace one or more of those security services with the exception that a certified key for use in non-repudiation service shall solely be used for that purpose and shall not be used for any other service.

Use of extensions in the certificate shall be in consistence with section 7.

6.2 Private Key Protection

6.2.1 Standards for cryptographic module

CA-Keys shall be protected by high assurance physical and logical security controls. They must be stored in, and operated from inside a specific tamper resistant hardware based security module that complies with FIPS140-1 level 3 [1], or its equivalents and successors, and has appropriate certification of the compliance.

Private Keys used in any Issuing Authority and/or Registration Authority process that affects the outcome of issued Certificates and certificate status checking services (such as signing Certificate requests and revocation requests), shall be protected by, maintained in, and restricted to, a hardware cryptographic token designed to meet the level of requirements as specified in FIPS 140-1 level 2, or its equivalents and successors.

Subscribers' private keys shall be protected by, maintained in, and restricted to, a PSE designed to meet the level of requirements as specified in FIPS 140-1 level 1, or its equivalents and successors.

---

[1]   FIPS PUB 140-1 - Federal Information Processing Standards Publication, 11 January 1994. Security Requirements For Cryptographic Modules. U.S. Department Of Commerce & National Institute of Standards and Technology

trustis®

6.2.2 Private key (n out of m) multi-person control

For an Issuing Authority's private signature keys, at least two-person control is required. This means that no single person shall possess the means required to access the environment where the private key is stored or use it in any sense.

For Registration Authorities and Subscribers, one-person control is permitted.

6.2.3 Private key escrow

No stipulations.

6.2.4 Private key backup

Back-ups of private keys are normally considered as part of a disaster recovery plan. As part of such a disaster recovery objective, Trust Service Providers may back-up their private keys and with the consent of subscribers, the keys of subscribers. End Entities may also make their own back-ups of their keys.

In the case of separate backups of individual keys, the backed-up keys must be protected at a level commensurate with that stipulated for the primary version of the key.

In the case of aggregated backups of keys, (for example, many keys backed-up inside and protected by a single PSE), the backed-up keys must be protected at a level commensurate with that stipulated for the Issuing Authority's private signing key.

6.2.5 Private key archival

No stipulations.

6.2.6 Private key entry into cryptographic module

If the private key is not generated in the Entity's cryptographic module, it must be entered into the module via the use of secure methods approved by the Issuing Authority, that protect key material and any associated activation data from unauthorised access, modification and use.

6.2.7 Method of activating private key

An Entity must be authenticated to its cryptographic module before the activation of the private key. This authentication may be in the form of a PIN, pass-phrase or password (activation data). When deactivated, private keys must not be exposed in plaintext form.

Cryptographic modules issued to Trust Service Provider personnel and to subscribers shall block themselves after a specified number of consecutive failed attempts to authenticate to the module. The Issuing Authority shall determine this number.

Cryptographic modules issued to Trust Service Provider personnel and to subscribers may contain an unblocking function. Unblocking shall require the holder to enter the correct unblocking code (described in 6.4).

6.2.8 Method of deactivating private key

When deactivated, private keys must not be exposed in plaintext form and must be cleared from all forms of memory before the memory is de-allocated and released to the operating system. The cryptographic module may automatically deactivate the private key after a pre-set period of inactivity.

6.2.9 Method of destroying private key

Upon termination of use of a private key, all copies of the private key in computer memory and shared disk space must be securely destroyed.

trustis ®

6.3 Other Aspects of Key Pair Management

6.3.1 Public key archival

The Issuing Authority shall ensure that all public keys are archived in accordance with section 4.6.

6.3.2 Usage periods for the public and private keys

Usage periods for key pairs shall be governed by validity periods set in issued certificates. These shall have the following maximum values:
- Subscribers – up to three (3) years
- Trust Service Provider trusted roles – five (5) years
- On-line intermediate Issuing Authorities – ten (10) years
- Off-line primary Issuing Authorities – twenty (20) years

6.4 Activation Data

6.4.1 Activation data generation and installation

Any activation data must be unique and unpredictable. The activation data, in conjunction with any other access control, must have an appropriate level of strength for the keys or data to be protected. Where PINs, passwords or pass-phrases are used, an Entity must have the capability to change these at any time.

An unblocking code for a cryptographic module (if available) shall only be delivered to the legitimate holder of the module after an express request from the holder. Delivery requires strong identification of the holder (according to 3.1.9), a signed acknowledgment of receipt of the unblocking code and archiving of receipts (according to 4.6).

6.4.2 Activation data protection

Data used to gain access to cryptographic modules must be protected from unauthorised use by an appropriate combination of cryptographic and physical access controls.

6.4.3 Other aspects of activation data

No stipulations.

6.5 Computer Security Controls

6.5.1 Specific computer security technical requirements

Each Trust Service Provider system must protect its software and data from threats identified in a threat assessment and must include the following functionality where appropriate:
- Access control to Trust Services and PKI roles
- Enforced separation of duties for PKI roles
- Identification and authentication of PKI roles and associated identities
- Use of cryptography for session communication and database security
- Archival of Trust Service Provider and End-Entity history and audit data
- Audit of security related events
- Trusted path for identification of PKI roles and associated identities
- Recovery mechanisms for Trust Service Provider keys

This functionality may be provided by the operating system, or through a combination of operating system, PKI CA software, and physical safeguards.

The Trust Service Provider shall document procedures, logging and audit requirements for processes related to initialisation, resetting, shutdown or reconfiguration of Trust Services.

6.5.2 Computer security rating

Trust Service Providers' system components (with the exception of storage of CA-Keys) do not require a formal computer security rating provided that all requirements of this Certificate Policy are satisfied.

Any hardware security module or device holding CA Keys must comply with the requirements of 6.2.1 and 5.1

6.6 Life Cycle Technical Controls

6.6.1 System development controls

The development of software, that implements Trust Service functionality shall be performed in a controlled environment that, together with at least one of the following approaches, shall be used as protection against the insertion of malicious logic.

- The vendor shall have a quality system compliant with international standards or
- The vendor shall have a quality system available for inspection upon request

6.6.2 Security management controls

The configuration of Trust Service Provider systems as well as any modifications and upgrades must be documented and controlled by the Trust Service Provider. There must be a method of detecting unauthorised modification to the Trust Service Provider software or its configuration. The Trust Service Provider must ensure that it has a configuration management process in place to support the evolution of the systems under its control.

6.6.3 Life cycle security ratings

No stipulations.

6.7 Network Security Controls

Trust Service Provider systems must be protected from attack through any open or general-purpose network with which they are connected. Such protection must be provided and configured to allow only the minimal set of functions, protocols and commands required for the operation of the Trust Service. A Trust Service Provider must document such protective measures, but is not required to publish this information in its CPS.

6.8 Cryptographic Module Engineering Controls

As stated in 6.2.1

7 CERTIFICATE AND CRL PROFILES

7.1 Certificate Profile

7.1.1 Version number(s)

The Issuing Authority must issue X.509 Version 3 certificates.

7.1.2 Certificate extensions

All Entity PKI software must correctly process the extensions identified in 4.2.1 and 4.2.2 of the IETF PKIX certificate profile.

The Basic Constraints extension shall not be used in any certificate except for CA-certificates. In such cases, use of Basic Constraints is mandatory and shall specify that the certificate is a CA-certificate.

The certificatePolicies extension is mandatory and shall contain an OID indicating the use of this policy (according to 7.1.6). The Certificate Policy Qualifier Info extension shall be used to direct end-entities to where this policy and other relevant information may be found.

Where CRLs are used to produce certificate status information, the CRL Distribution Point extension is mandatory, and shall identify a location where the latest CRL issued by the Issuing Authority can be obtained.

7.1.3 Algorithm object identifiers

No stipulations.

7.1.4 Name forms

The use of name forms shall be consistent with section 3.1of this Certificate Policy.

7.1.5 Name constraints

No stipulations.

7.1.6 Certificate policy Object Identifier

This Certificate Policy has been assigned an OID as defined in section 12 of **PKI Disclosure Statement.** This shall encoded in issued certificates using the certificatePolicies extension.

7.1.7 Usage of Policy Constraints extension

No stipulations.

7.1.8 Policy qualifiers syntax and semantics

No stipulations.

7.1.9 Processing semantics for the critical certificate policy extension

Subscribers and Relying Parties, who use and or rely upon certificates issued with the Certificate Policy extension defined, whether marked critical or not, and containing the identifier of this Certificate Policy, must accept all terms and conditions stated in this Certificate Policy before using and/or relying on them.

7.2 CRL Profile

7.2.1 Version number(s)

If CRLs are issued the Issuing Authority may support X.509 version 1 or version 2 CRLs in accordance with the IETF PKIX Certificate and CRL Profile.

An alternative to CRLs is permitted. The Issuing Authority may allow for provision of an on-line certificate status checking service, which meets the requirements in this policy.

7.2.2 CRL and CRL entry extensions

Where CRLs are used to indicate certificate status, Entity PKI software must correctly process all CRL extensions identified in the IETF PKIX Certificate and CRL profile.

8 SPECIFICATION ADMINISTRATION

8.1 Specification change procedures

8.1.1 Items that can change without notification

The only changes that may be made to this specification without notification are editorial or typographical corrections, or changes to the contact details.

8.1.2 Changes with notification

8.1.2.1 List of items

1. Any item in this certificate policy may be changed by the Policy Authority with 10 days notice.
2. Changes to items that, in the judgement of the Policy Authority, will not materially impact a substantial majority of the subscribers or relying parties using this policy, may be changed with no notice.

8.1.2.2 Notification mechanism

All proposed changes that may materially impact users of this policy will be notified in writing to Issuing Authorities registered with the Policy Authority, and will be published by the Policy Authority.

Issuing Authorities shall in turn, ensure that notice of such proposed changes is published to their subscribers.

8.1.2.3 Comment period

Entities operating under this Certificate Policy may submit comments to the Policy Authority as follows:

*   For changes in accordance with (1) of 8.1.2.1, comments shall be received within 5 days of original notice.

8.1.2.4 Mechanism to handle comments

Any action taken as a result of comments submitted in accordance with 8.1.2.2 is at the sole discretion of the Policy Authority.

8.1.2.5 Period for final change notice

No stipulations.

8.1.3 Items whose change requires a new policy

If a policy change is determined by the Policy Authority to have a material impact on a significant number of users of the policy, the Policy Authority may, at its sole discretion, assign a new Object Identifier to the modified policy.

8.2 Publication and notification policies

This policy definition may be obtained from the contact person defined in section 1.4.2

Issuing Authorities issuing certificates that identify this certificate policy shall prominently post copies of this certification policy that may be accessed on-line by end-entities.

8.3 CPS approval procedures

In accordance with section 2.7

trustis ®

Appendix A – Glossary

The following terminology shall have the definitions as given below:

Accept a Certificate	Demonstrate approval of a Certificate while knowing or having notice of its contents.
Activation Data	Private data, other than keys, that are required to access cryptographic modules.
Asymmetric Cryptosystem	A system which generates and employs a secure key consisting of a Private Key for creating a Digital Signature and a Public Key to verify a Digital Signature.
Authentication	A process used to ascertain the identity of a person or the integrity of specific information. For a message, authentication involves ascertaining its source and that it has not been modified or replaced in transit.
Certificate	A collection of data that at least: 1. Identifies the issuing Certification Authority 2. Names or identifies its Subscriber 3. Contains the Subscriber's Public Key 4. Identifies the operational period of Certificate 5. Bears the Digital Signature of the Issuing Certification Authority
Certificate Authority	The software and hardware system used by the Issuing Authority or it's designated Certificate Manufacturer to issue and manage the full lifecycle of certificates.
Certificate Authority Certificate	See Issuing Authority Certificate.
Certificate Authority Key (CA-Key)	The private key used by the CA for signing certificates and other objects.
Certificate Manufacturer	The entity providing certificate management operational services for the Issuing Authority.
Certificate Policy	A named set of rules that indicate the applicability of a certificate to a particular community and/or class of application with common security requirements. A certificate policy may be used by a certificate user to help in deciding whether a certificate (and the binding therein), is sufficiently trustworthy for a particular application.
Certificate Revocation Information	Information that indicates whether Certificates have been revoked, commonly provided in bulk by Certificate Revocation Lists, or individually through specific online enquiries (e.g. OCSP).
Certificate Revocation List (CRL)	A list maintained by of on behalf of an Issuing Authority of the certificates that it has issued, that are revoked before their natural expiry time.

trustis®

Certification Path	A logical and ordered sequence of Certificates which, together with the Public Key of the initial entity in the Certification Path, can be processed to obtain that of the final entity in the Certification Path.
Certification Practice Statement	A statement of the policies and practices employed in the issuance of certificates and in support of one or more Certificate Policies.
Confirm	Ascertain through appropriate inquiry and investigation.
Corresponding private key	Given a public key taken from a key pair, the corresponding private key is the private key from that same key pair, (and vice-versa for corresponding public key).
Cross-certificate	A certificate used to establish a trust relationship between two Issuing Authorities.
Digital Signature	The result of a transformation of a message by means of a cryptographic system and a Hash function, using keys such that a person who has the initial message can determine: 1. Whether the transformation was created using the Private Key that corresponds to the signer's Public Key, and 2. Whether the initial Message has been altered since the transformation was made.
Hash Function	An algorithm mapping or translating one sequence of bits into another, generally smaller, set (the Hash or Message Digest) such that: 1. A Message yields the same Hash Result every time the algorithm is executed using the same Message as input; 2. It is computationally infeasible that a Message can be derived or reconstituted from the Hash Result provided by the algorithm; and 3. It is computationally infeasible that two Messages can be found that produce the same Hash Result using the algorithm
Hash or Message Digest	The output produced by a Hash Function upon processing a Message.
High Security Zone	An area to which access is controlled through an entry point and limited to authorised, appropriately screened personnel and properly escorted visitors. High-Security Zones should be accessible only from Security Zones, and are separated from Security Zones and Operations Zones by a perimeter built to the specifications recommended in a threat risk assessment. High-Security Zones are monitored 24 hours a day and 7 days a week by security staff, other personnel or electronic means.
Hold a Private Key	To use or to be able to use a Private Key.

Incorporate by reference	Make one Message a part of another Message by:- 1. Identifying the Message to be incorporated; 2. Providing information which enables the Receiving Party to access and obtain the incorporated Message in its entirety; and 3. Expressing the intention that it be part of the incorporating Message. The incorporated Message shall have the same effect as if it had been fully stated in the incorporating Message to the extent permitted by law.
Issue a Certificate	The acts of an Issuing Authority in creating a Certificate and notifying the Subscriber identified in the Certificate, of the contents of the Certificate.
Issuing Authority	By definition, an Issuing Authority is the entity listed in the certificate in the issuer field. The Issuing Authority may obtain benefit in return for taking on risk associated with transactions secured by digital certificates, for example, risk of fraud. The Issuing Authority has the responsibility for deciding who may be issued with a certificate carrying its name.
Issuing Authority Certificate.	A Certificate for an Issuing Authority's Public Key, and for use in signing certificates created by Certification Authority software under its control.
Key Pair	In an Asymmetric Cryptosystem - a Private Key and its mathematically related Public Key having the property that the Public Key can verify a Digital Signature that the Private Key creates.
Local Registration Authority	See Registration Authority
Message	A digital representation of information.
Message integrity	The assurance of unaltered transmission and receipt of a Message from the sender to the intended recipient
Non-repudiation	Strong and substantial evidence of the identity of the Signer of a Message and of Message integrity, sufficient to prevent a party from successfully denying the original submission or delivery of the Message and the integrity of its contents.
Notify	Communicate or make available information to another person as required under the circumstances
Online Certificate Status Protocol (OCSP)	A network protocol used to ascertain the current validity status of a certificate.
Operational Period of Certificate	The Operational Period of a Certificate begins on the date and time it is issued by a Certification Authority (or on a later date and time certain if stated in the Certificate), and ends on the date and time it expires or is earlier revoked or suspended.
Operations Zone	An area where access is limited to personnel who work there and to properly escorted visitors. Operations Zones should be monitored at least periodically, based on a threat risk assessment, and should preferably be accessible from a Reception Zone.

trustis®

Policy Authority	The entity that has ultimate responsibility for approving the Certificate Policy used to govern the issuance, management and usage of a specified set of digital certificates.
Private Key	The private part of an asymmetric key pair used for public key encryption techniques. The private key is typically used for signing via digital signatures or for decrypting messages.
Public Key	The public part of an asymmetric key pair used for public key encryption techniques. The public key is typically used for verifying digital signatures or to encrypt messages to the owner of the private key.
Public-access Zone	An area in which there is no personnel access control. Generally surrounds or forms part of a security facility. Examples include the grounds surrounding a building, and public corridors and elevator lobbies in multiple-occupancy buildings. Boundary designators such as signs and direct or remote surveillance may be used to discourage unauthorised activity.
Reception Zone	The entry to a facility where the initial contact between the public and the facility occurs, where services are provided, information is exchanged and access to restricted (Operations, Security and High-security) zones is controlled. To varying degrees, activity in a Reception Zone is monitored by the personnel who work there, by other personnel or by security staff. Access by the public may be limited to specific times of the day or for specific reasons. Entry beyond the Reception Zone is indicated by a recognisable perimeter such as a doorway or an arrangement of furniture and dividers in an open office environment.
Registration Authority (RA)	An entity which is authorised or licensed by an Issuing Authority to carry out the practices and procedures for identification and Authentication of Certificate Subscribers in order to grant requests from subscribers for issuance of certificates or for their revocation, but without the responsibility for signing or issuing Certificates or Certificate Revocation Information.
Relying Party	An entity that does not necessarily hold a certificate as a subscriber does, but even so, during the course of a transaction, may be a recipient of a certificate and who therefore acts in reliance on that certificate and/or digital signatures verified using that certificate
Repository	The entity providing a community-wide accessible mechanism by which primarily subscribers and relying parties can obtain and validate information on certificates issued under the governing policy.
Revoke a Certificate	Permanently end the Operational Period of a Certificate from a specified time.

trustis®

Security Zone	An area to which access is limited to authorised personnel and to authorised and properly escorted visitors. Security Zones should preferably be accessible from an Operations Zone, and through a specific entry point. A Security Zone need not be separated from an Operations Zone by a secure perimeter. A Security Zone should be monitored 24 hours a day and 7 days a week by security staff, other personnel or electronic means.
Signer	A person who creates a Digital Signature for a Message.
Subscriber	An entity that: 1. Is the subject named or identified in a Certificate issued to such person; and 2. Holds a Private Key that corresponds to a Public Key listed in that Certificate.
Suspend a Certificate	Temporarily suspend the Operational Period of a Certificate for a specified time period.
Time-stamp	1. To create a notation that indicates, at least, the correct date and time of an action and the identity of the person that created the notation; or 2. Such a notation appended, attached or referenced.
Time-stamping Authority	The Trust Service Provider operating, controlling and issuing time-stamps for use by other entities.
Transactional Certificate	A certificate for a specific transaction incorporating by reference, one or more Digital Signatures.
Trust Service	1. A trust-enhancing service offered or performed by a Trust Service Provider that supports the assurance, integrity or security of electronically executed activities, (e.g. time-stamping, notarisation, watermarking etc.) 2. The service offered or performed by an Issuing Authority, Registration Authority, Certificate Manufacturer or other trusted intermediary relating to the issuance and control of Digital Certificates, (e.g. manufacture, issuance, revocation, publication, registration, validity-checking, policy-making, etc.)
Trust Service Provider	An entity that acts as a supplier of Trust Services.
Trustworthy System	Computer hardware, software and procedures that: 1. Are adequately secure from intrusion and misuse; 2. Provide an adequate level of availability, reliability and correctness of operation; 3. Are adequately suited to performing their intended functions; and 4. Adhere to generally accepted security principles.

trustis®

Valid certificate	A Certificate which: 1. A Certificate Authority has issued 2. The Subscriber has accepted 3. Has not been revoked or suspended 4. Has not expired In addition for a Transactional Certificate: 1. The Subscriber has accepted, but limited to the Digital Signature created pursuant to the specific transaction to which the Transactional Certificate relates.
Validity Period	The period that is defined within a certificate, during which that certificate is intended to be valid for use in protecting the certificate holder's allowable activities.
Verify a Digital Signature and message integrity	In relation to a given Digital Signature, Message and Public Key, to determine accurately:- 1. That the Digital Signature was created during the Operational Period of a Valid Certificate by the Private Key corresponding to the Public Key listed in the Certificate; and 2. The Message has not been altered since its Digital Signature was created.

trustis®