Australian Government
Department of Finance and Deregulation
Australian Government Information Management Office

Gatekeeper PKI Framework

February 2009

Relationship Certificate Guidebook

ISBN 1 921182 25 3

Department of Finance and Deregulation

Australian Government Information Management Office

CONTENTS

1. EXECUTIVE SUMMARY

Relationship Certificates are issued to Clients of a Relationship Organisation according to business rules local to the Community of Interest (COI) of which the Relationship Organisation is a part, and intended for use in applications only within the same Community.

Relationship Certificates are a departure from historical Gatekeeper identity certificates. The rationale for adding Relationship Certificates to Gatekeeper is well grounded in real world experience of Public Key Infrastructure (PKI), including the fact that successful PKIs tend to be "closed" and therefore subject to localised business rules rather than global identification rules. Relationship Certificates will be easier to obtain and deploy, and will be better matched to their intended applications, meaning that PKI enabled software should be easier to use.

Since Relationship Certificates are novel, care is needed in how they are selected and deployed. This Guidebook is intended to help organisations plan for and deploy Relationship Certificates, under the Gatekeeper PKI Framework (the Framework).

Instead of the Subscriber undergoing any particular Evidence of Identity (EOI) check (e.g. the existing 100-point EOI check required under Gatekeeper policy), Relationship Certificates represent that the Subscriber has an established ***relationship*** with a Relationship Organisation within a defined COI.

A COI in general is a set of individuals and/or entities (Subscribers and Relying Parties) which all agree to transact online according to a defined set of rules (such rules might be in the form of an explicit membership agreement, or they might be enshrined in legislation).

The Relationship Organisation requests (or authorises) issuance of a Relationship Certificate to the Subscriber, who may use that Certificate only within the COI.

The details of these relationships may vary from one COI to another. Confidence in Relationship Certificates is context dependent: it is determined by what the relationship is, how the relationship is attained and maintained, and what applications the Certificate is intended to support across the COI.

The deployment of Relationship Certificates should therefore be closely linked to the design of the associated PKI enabled services, applications and business processes (particularly in relation to maintenance of the accuracy and integrity of Client databases). The major part of this Guidebook describes activities that should be undertaken as part of the design process, in order to deliver robust certificate registration processes, clarity for management of the legal implications of their Community PKI, and improved awareness on the part of developers as to how Relationship Certificates ought to be integrated into software applications.

About this document

This document is a Guidebook to assist Service Providers, Organisations and their Clients, as appropriate, issue, manage and use Relationship Certificates. It is intended to provide an overview of policy issues; implementation issues and light touch regulatory oversight relevant to Relationship Certificates.

This Guidebook should be read in conjunction with other information relevant to Relationship Certificates. In particular the following documents will be relevant:

- the Certificate Policy (CP) template for Relationship Certificates; and
- the Threat and Risk Assessment (TRA) template.

All Gatekeeper documents referenced in this document are available at www.gatekeeper.gov.au

2. INTRODUCTION

2.1. Background

The Australian Government's vision is to make greater use of Information and Communications Technology (ICT) to enable a transformation of the business of government. Increasingly individuals and business are choosing to utilise electronic authentication to participate in electronic Transactions. A critical element of enabling electronic service delivery is having the means to authenticate and secure online Transactions.

Simplified sign-on procedures to access connected government services in an environment of privacy and security may reduce the cost and complexity of interacting with government.

One of the initiatives taken by Government to achieve this vision has been the development of the Gatekeeper Framework for the use of PKI by individuals and businesses in their interactions with government. The Framework:

- facilitates the deployment of a broader range of digital certificates designed to meet specific business requirements of agencies and their Clients;
- facilitates adoption of a risk management approach aligned to the National e-Authentication Framework (NeAF) and Government Security Standards;
- facilitates increased use of PKI by both business and the broader community through reducing the cost and complexity of producing, acquiring and using digital certificates; and
- fosters a competitive market for digital certificates.

The Framework comprises three Certificate categories (Special, General and High Assurance). Digital certificates issued under the Framework will be X.509 compliant and all Service Providers (Certification Authorities (CAs), Registration Authorities (RAs) and Registration Authorities Extended Services (RAES)) must be Gatekeeper Accredited or Recognised.

Using risk assessment processes, Agencies will select the type of digital certificate appropriate for their Clients to use in conducting Transactions.

2.2. Structure of this document

This Guidebook assists organisations issue, manage and use Relationship Certificates under the Special Category.

This Guidebook contains:

- **an overview of the role and characteristics of Relationship Certificate**

  (Refer to *Section 3 – Description of Relationship Certificates.)*

- **guidelines on deploying Relationship Certificates**

  (Refer to *Section 4 – Deployment of Relationship Certificates)*

- **a list and summary of Listing and Evaluation Criteria for relevant participants in a Relationship Certificate deployment.**

  (Refer to *Section 5 – Listing and Evaluation Criteria)*

3. DESCRIPTION OF RELATIONSHIP CERTIFICATES

3.1. What is a Relationship Certificate?

A Relationship Certificate, issued under the Special Category, is a digital certificate issued by or on behalf of a Relationship Organisation (using a Gatekeeper Accredited or Recognised Certification Authority to generate the digital certificates[1]) to Individuals and/or Organisations for the purpose of conducting Transactions within a closed COI[2]. A Relationship Certificate provides some or all of the following as agreed by the members of the COI: authentication, confidentiality, integrity and non-repudiation in Transactions within that specific COI.

Some of the key elements of Relationship Certificates include:

- the strategic intent of Relationship Certificates to provide a flexible structure with minimum and less complex administrative formalities for users within a closed PKI, without compromising the trust placed in the digital certificates generated by Gatekeeper Accredited or Recognised CAs;

---

[1] A Gatekeeper accredited RAES may also be involved in the Key Generation process.

[2] The deployment of Hosted Certificates is restricted to Communities of Interest under the Special category of the Framework. Where a Relationship Organisation intends to deploy Hosted Certificates reference must be made to the Hosted Certificate Policy Specification

- Relationship Certificate deployments use Gatekeeper Accredited or Recognised CAs or Accredited RAES to generate Keys and Certificates. Subscribers are enrolled by administrators in the COI, which can communicate Certificate requests and other lifecycle management requests to the CA by a variety of means;

- Relationship Certificates are intended to be used for specific purposes, tightly coupled to defined applications, and are not to be used outside the COI;

- Relationship Certificates must be uniquely identifiable so Relying Party software can readily identify the digital certificates it expects to see; and

- a critical issue in establishing a Relationship Certificate COI is to understand the registration, end user and application related risks (as these are under the control of the Community either in whole or in terms of specific members).

3.2. The purpose of Relationship Certificates

Relationship Certificates address the needs of members of a defined COI who wish to transact securely online with government without the need to undergo an in-person EOI check at a Gatekeeper accredited RA. Clients are issued with digital certificates on the basis of their "relationship" with the Relationship Organisation, the exact nature of which will vary from one Community to another, depending on what the digital certificate is intended to be used for. Relationship Certificate deployments allow autonomy and discretion on the part of each COI. The basic role of the Relationship Certificate is therefore to represent or provide evidence of a specific relationship between the Relationship Organisation and the Subscriber.

In addition to the information that may be encapsulated in a Relationship Certificate (see below), they remain "identity" digital certificates, with the Subscriber being identified on the basis of their relationship with the Relationship Organisation.

Relationship Certificate Subscribers may be Individuals or Organisations, or other types of entities such as a computer server at a designated location.

Relationship Certificate Profiles will be highly flexible, which will allow them to usefully encapsulate (often in custom extensions) stable attribute and authority information associated with the Subscriber and relevant to the class of Transactions for which the digital certificate has been designed. Nevertheless, all Relationship Certificates shall fully comply with X.509.

Attribute and authority information may be included in the digital certificate in various ways. The design decision as to what information to include in a digital certificate must be made on a case-by-case basis. The inclusion of attributes with relatively short lifetimes can result in high churn rates and administration overheads that might outstrip the potential business benefits.

Experience shows that useful Relationship Certificates can be used to represent relatively long-lived authority information (and encapsulate such special data). Examples include:

- formal membership of an association;
- the fact of employment within the COI;
- standing as a registered professional or business licensee; or
- standing as a customer.

3.3. Assumptions about the use of Relationship Certificates

The following sections list and discuss some key assumptions that underpin the Relationship Certificate construct.

3.3.1. A "Community of Interest" will be defined

For the purposes of Relationship Certificates, a Community of Interest is *a defined population of users – Subscribers and Relying Parties – that agree to use Relationship Certificates according to an agreed set of rules*. A COI may therefore range from a single Relying Party that is also the Relationship Organisation with multiple digital certificate holders, through to multiple Relying Parties and Subscribers.

The rules governing the COI might centre on explicit membership agreements signed when users receive their Relationship Certificates. Alternatively the rules might be embodied in over-arching legislation or regulations as can apply to members of certain professions (e.g. doctors or lawyers).

The following examples of potential COIs are provided to assist in explaining some of the key concepts of Relationship Certificates:

Hypothetical Scenario 1: Company COI

The employees of a company could form a COI, with the fact of their employment represented by Relationship Certificates. The "agreed set of rules" would be enacted through employment contracts managed by the Human Resources department. Such digital certificates could be used to authenticate staff accessing online Human Resources records and services. In some cases, with the express agreement of the company, outside organisations could rely upon certain Transactions such as Purchase Orders originated using employee Relationship Certificates. To enable Transactions outside the company, arrangements need to be put in place to enlarge the COI.

Hypothetical Scenario 2: University COI

The enrolled students of a university could be issued Relationship Certificates under enrolment rules, with which online examinations and similar applications could be authenticated. If other institutions have arrangements in place with the university that recognise their students for certain purposes (such as borrowing privileges for online intellectual property) then the Relationship Certificates could be relied upon for associated applications.

Hypothetical Scenario 3: Professional Body COI

The members of a professional body could form a COI, together with the entities and other individuals which recognise the professionals' qualifications. The rights and responsibilities of certain chartered professions, such as accountants, are codified in legislation. If such professionals were issued Relationship Certificates by or on behalf of their body, they could exercise their rights and responsibilities online, under existing arrangements. Note that the COI for accountants is bigger than the set of accountants themselves, for it includes all business people who rely upon accountants, under the rules laid down by legislation and the profession.

Each COI is represented by a management entity referred to as the "Relationship Organisation" able to enter into agreements (with CAs in particular) on behalf of the Community's members.

3.3.2. Relationship Certificates will not be used outside their defined Community of Interest

For various reasons, "closed" PKI deployments to date have proved to be generally the most effective in Australia and around the world. Closed PKI deployments restrict the use of digital certificates to a known set of Relying Parties where these parties are usually contractually bound. "Open" PKI deployments anticipate the widespread acceptance of digital certificates where Relying Parties may not be known and where the parties are not generally contractually bound.

There are several reasons for the success of closed PKI, including the fact that risks are easier to manage (and general liabilities are correspondingly reduced) when there are constraints on what a digital certificate can be used for. In light of this, a defining principle of Relationship Certificates is that they will not be used outside their COI. This principle in particular will help commercial CAs provide streamline services into a variety of Communities, because they will find their liabilities for misuse of digital certificates easier to characterise and control. The Gatekeeper Core Obligations Policy provides guidance in this regard.

There are varying degrees to which this principle can be enforced (and different Communities will have to assess for themselves the risks of the principle breaking down). At a minimum, Relationship Certificates will have as a strict condition of use that Subscribers not use their digital certificates beyond the Community. This should be explicitly stated in the applicable Certificate Policy and terms and conditions for participation.

An alternative measure to constrain outside use can be to populate the Digital Certificate with an X.509 V3 Critical Extension.

3.3.3. Backend CA Service Providers will be Gatekeeper Accredited /Recognised

Relationship Certificate deployments allow a COI to use digital certificates to represent a relationship, the inherent acceptability of which will not always be apparent outside the community, because of the varying visibility of the registration process. However, another aspect of acceptability has to do with the possibility that a given digital certificate has been counterfeited. While the Framework seeks not to codify or specify what any COI's internal processes should be, nevertheless Gatekeeper requires that all issuers of Relationship Certificates meet Australian Government security and technology requirements that improve resistance to counterfeiting.

In this regard, all Relationship Certificates will be required to be produced by a Gatekeeper Accredited or Recognised CA. Where Key Generation (or other functions normally performed by a CA) is undertaken by an organisation other than the CA or Subscriber, that organisation will also be required to be Gatekeeper Accredited. The suite of personnel, physical, logical and technological security controls – evidenced by Defence Signals Directorate (DSD) Highly Protected, Australian Security Intelligence Organisation (ASIO) T4 Group and Common Criteria EAL4 benchmarks – represents a broadly accepted level of protection against counterfeiting[3].

3.3.4. Relationship Certificates are not restricted to identity Digital Certificates

Relationship Certificates can be utilised for very specific purposes. They are not purely "identity" digital certificates. This means that a Relationship Certificate may in some cases grant the holder particular authority or access to an application or system. The digital certificate itself may contain information that enables a Relying Party to determine the authority or access rights of the digital certificate holder. In addition, the digital certificate itself may contain information about an "attribute" of the digital certificate holder.

3.4. Characteristics of Relationship Certificates

Requirement	Relationship Certificate Characteristic
NeAF Assurance Level	Level 1 - 4 (with restrictions) Can provide from a minimal to high level of assurance[4] concerning the identity of the Subscriber depending on the nature of the relationship and the "source of truth" that is accepted in the defined COI. Provides authentication of identity within a COI.
Certificate Purposes	• Authentication • Non-repudiation • Integrity • Confidentiality (As agreed within the defined COI)

[3] It is worth noting that Gatekeeper's historical choice of personnel, physical, logical and technological security benchmarks is not dissimilar to such international regimes as tScheme in the UK, WebTrust for CAs, and IdenTrust.

[4] More information on NeAF is available at http://www.finance.gov.au/e-government/security-and-authentication/authentication-framework.html.

Requirement	Relationship Certificate Characteristic
Transaction Types	Defined by agency/business as part of a risk assessment.
Certificate Issuer	Relationship Certificates will be generated and issued by a Gatekeeper Accredited/Recognised CA or Accredited RAES. Alternative issuance mechanisms may be considered by the Gatekeeper Competent Authority on a case by case basis.
Key Pairs	All digital certificates will operate with fully functional Key Pairs able to provide authentication and/or confidentiality services. The Certificate Policy under which the Relationship Certificate is issued must specify Key Usage within the Certificate Profile.
Government Information Security Levels[5]	A Relationship Certificate is suitable for supporting the transmission of information up to and including X in Confidence (but not Cabinet-In-Confidence) as defined by an agency in accordance with the Commonwealth Protective Security Manual (PSM). (Within the defined COI)
Evidence of Identity (EOI)	Threshold EOI requirements are determined by each COI on a case-by-case basis, in accordance with the COI's business practices, intended use of the digital certificates, and the Threat and Risk Assessment to be conducted on each Relationship Certificate implementation, as described in this Guidebook.
EOI Refresh	As defined by the COI.
Certificate Life	Certificate life will be based on ISM minimum standards and structure of PKI deployment (currently neither greater nor equal to 10 years). Digital certificate renewal will require use of the unexpired digital certificate to request renewal. There is no stipulation as regards re-key.
Technical Specification (key length, algorithms)	In accordance with ISM (SIC) edition.
Certificate Medium	Medium can be selected at agency/business discretion subject to compliance as appropriate with ISM or other internationally accepted

[5] Concerns information transmitted across a public network only (in accordance with the PSM).

Requirement	Relationship Certificate Characteristic
	standards (e.g. FIPS140-2) and provided the choice of medium and applicable standards have been subject to a risk assessment process.
Certificate Profiles	There are no mandatory Certificate Profiles for Relationship Certificates. The only requirement is that Relationship Certificates must contain an Object Identifier (OID) that links to the Certificate Policy and that Key Usage is specified.
Supplementary Certificates	Scope exists, dependent on COI requirements, for the deployment of Supplementary Certificates (Device Certificate, Hosted Certificate, Digital Credential and Corporate Certificate) within a COI.
Certification Authority (CA) and Registration Authority Extended Services (RAES) Accreditation Requirements	CA/RAES Gatekeeper accreditation to meet the requirements for the Highly Protected security level. No Gatekeeper accreditation is required of the Subscriber enrolment related functions unless Key generation (or other CA-like function) is performed by the Relationship Organisation, in which case RAES Accreditation is required.
Operational Security Requirements – CA	CA/RAES security requirements for Relationship Certificates are the same as for other Gatekeeper categories; that is, IT products implementing CA functions must be accredited to EAL4, operations personnel must be cleared to Highly Protected, and CA physical security is required at SR1.
Operational Security Requirements – Subscriber Enrolment Administration	The Relationship Organisation is responsible for implementing security measures that are fit for purpose, informed by the Threat and Risk Assessment, and by existing operational requirements. Consideration must be given to physical security and access controls at any workstation from which Certificate lifecycle operations are administered.

4. DEPLOYMENT OF RELATIONSHIP CERTIFICATES

One of the objectives of Relationship Certificates is to provide autonomy and flexibility for Agencies and other organisations. There is no one model for Relationship Certificate deployment. This Guidebook strives not to codify or specify what any Community of Interest's internal processes should be in detail, so as not to limit their scope for choice. Yet it may be possible to characterise at a higher level what a sound Relationship Certificate deployment "looks like" and to document a repeatable project management approach for creating effective COI.

This section presents a series of activities that should be undertaken by Agencies / Organisations (in particular the Relationship Organisation but also other prospective members of the COI) at design time, to help ensure that best use is made of Relationship Certificates. The Guidelines are presented as if the business application in question is still in its formative stages. In cases where significant components of the business application are already in place, then management will need to decide how best to "retrofit" the activities presented here.

The main tasks recommended in a Relationship Organisation deploying Relationship Certificates include:

- conduct a digital certificate needs analysis;
- examine in detail the relationships between stakeholders in the COI;
- develop a business case, typically in cooperation with a CA Services Provider;
- conduct a Threat and Risk Assessment (this is not a mandatory step but it does represent best practice);
- design digital certificate registration process (which to a greater or lesser extent will be arranged to be a by-product of the way the Relationship Organisation established its relationship with the Subscriber), Key and Certificate lifecycle management, and Certificate Profile;
- analyse legal implications of the community PKI and any new arrangements as necessary, including obtaining legal advice and compliance with the Gatekeeper Core Obligations Policy;
- negotiate Services Agreement (see Services Agreement Template) with CA Services Provider;

- sign off on an agreed Certificate Policy with the CA. A Relationship Certificate CP (see Relationship Certificate CP Template) must be developed by or on behalf of the Relationship Organisation, based on the major outputs of the above activities; and

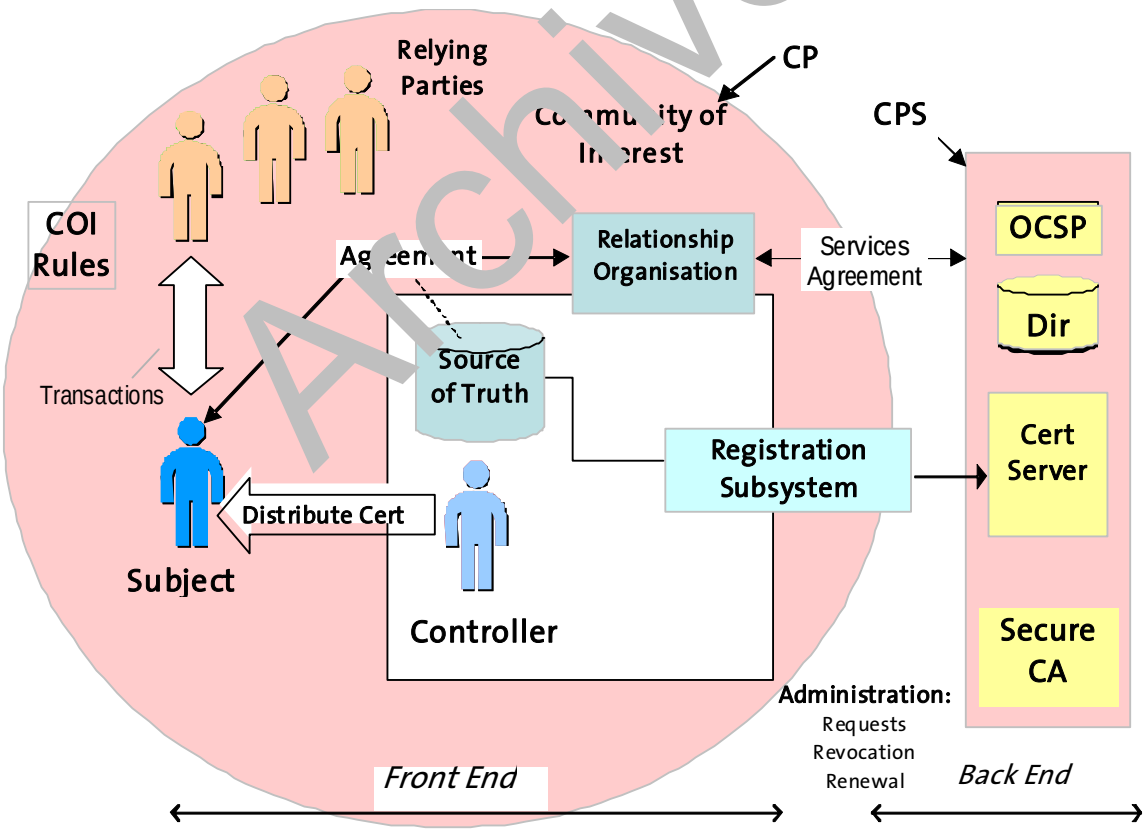
- document the operational procedures for the designated Certificate Controller, such as step-by-step instructions for how to use a Card Management System or Web RAO workstation as applicable, and including any new EOI or quality control requirements that are determined to be necessary over and above existing administrative procedures.

4.1. Operational Issues

The following sections provide an overview of operational issues.

4.1.1. Generalised operational model

The diagram below illustrates a generalised operational model for the registration, production and distribution of Relationship Certificates[6].



[6] Note – the Subject in the above diagram is equivalent to a Subscriber

The central operational concepts common across all Relationship Certificate deployments are as follows:

- Certificate Subscribers (Subjects) belonging to a defined COI may be individuals, or other entities, including "machines" as in the case of Device Digital Certificates and other embedded digital certificates. An agreed set of rules governs the rights and responsibilities of all members (Subscribers and Relying Parties), and all Transactions carried out between them;

- each COI has a "Source of Truth" (typically a database maintained by a Relationship Organisation) about its Clients, being a definitive register of all legitimate Subscribers, together with applicable authority information, membership conditions and other status data;

- each COI will have a Relationship Organisation (RO) being an administrative function within the community responsible for managing the relationship between members of the community and the community itself. The RO may in some circumstances also administer a Membership Agreement, through which members become represented in the Source of Truth;

- Subscribers are registered (or equivalently, "enrolled") for their Relationship Certificates by a Certificate Controller in the Relationship Organisation. A core administrative process translates relationship information held in the Source of Truth into a form suitable for issuing a digital certificate. Further, the Controller ensures that the right person (or entity) gets the right digital certificate. The Controller is a person in a trusted position, responsible for making the determination that a given member of the COI is eligible for a Relationship Certificate;

- subsequently, a digital certificate request message needs to be sent in some form (see below) to a Gatekeeper Accredited or Recognised Certification Authority (CA) contracted to generate digital certificates for the COI;

- the Certificate Controller is also responsible for instigating other Certificate lifecycle actions with the CA, such as digital certificate renewal and certification revocation. Lifecycle actions might be automated to a greater or lesser extent, such that human intervention is minimized. For example, Relationship Certificates can in some cases be produced in bulk from a file of existing members. Nevertheless, in all cases there must be a designated Certificate Controller in the Relationship Organisation responsible for the distribution of digital certificates to Subscribers; and

- Relying Parties may or may not themselves be Subscribers. In some instances, the Relationship Organisation itself may be a Relying Party (perhaps the only Relying Party) to Transactions originated using Relationship Certificates.

4.1.2. The CA – Registration function interface

There are several options for interfacing the front-end registration function to the backend digital certificate production function, and exchanging Certificate lifecycle requests. The four parallel grey boxes in the diagram above depict some of the options, as follows:

- A registration sub-system can receive "out of band" instructions from the RO (by hand, by telephone and so on), generate formal request messages in a format such as PKCS#12, and pass them to the Certificate Server. Typically the registration sub-system and the CA server will come from the same PKI product vendor and be designed to work in concert.

- A Web Registration sub-system can provide a direct Internet based interface between the RO and the CA server at the back-end. Typically the Web Registration sub-system will present a form to the user.

- Certificate lifecycle management can be integrated within a Smart Card Management System (CMS).

- In principle, Certificate lifecycle management functions can be integrated into human resources, customer management or similar software systems (although at the time of writing, no good examples of such a deep level of integration are known).

Note that no matter what type of interface connects the front-end registration function to the Gatekeeper Accredited or Recognised CA, some sort of access control is necessary to mitigate the possibility of digital certificate requests being launched by someone other than an authorized controller. The appropriate level of access control needs to be decided on a case by case basis, with due regard to the potential risks arising from unauthorized Certificate lifecycle management requests being launched from the RO workstation.

4.1.3. Legal documents

Four significant legal documents govern the interactions between major players in the Relationship Certificate PKI:

1. **Certification Practices Statement (CPS)**

   The CPS fundamentally specifies the operations behind production of digital certificates, in particular the physical, logical, personnel and technological security controls implemented to ensure the integrity and reliability of digital certificates;

2. **Certificate Policy (CP)**

   The CP fundamentally describes what the Relationship Certificates are for, the conditions for their use, and the precise contents of the Certificate Profile;

3. **Services Agreement**

   A Services Agreement between the Relationship Organisation and the Gatekeeper Accredited or Recognised CA/RA/CSP will govern such matters as the performance and availability of Certificate production services, standards conformance, commercial arrangements and legal liabilities; and

4. **COI Agreement**

   A general tenet of the Relationship Certificate approach in the Gatekeeper PKI Framework is that since Relationship Certificates merely represent existing or "real world" relationships, there should be no need in general for additional rules to be imposed in managing the use of such digital certificates. All necessary terms and conditions should be present in regular agreements or arrangements struck with members of the Community. If the introduction of PKI involves new obligations (such as Key Usage conditions, or requirements to revoke under prescribed circumstances), then these should be systematically built into regular arrangements like employment agreements, contracts and other sources of terms and conditions.

4.2. Business Case

To help create a robust business case for establishing a Relationship Certificate system, the real need for digital certificates should be analysed, and a clear business model developed, as described below. Additional guidance on developing business cases can be found at http://www.finance.gov.au/budget/ict-investment-framework/index.html.

4.2.1. Digital Certificate needs analysis

Digital certificates and PKI in general have proved to be a relatively complex, even controversial technology. Many projects around the world have struggled to make best use of digital certificates, and frequently project managers have reverted to more "traditional" authentication approaches such as username and password. It is therefore essential that any new project contemplating the use of digital certificates commence with a clear needs analysis, to ensure that PKI will deliver real business benefits in the context of the intended application.

Suitable applications for digital certificates (or to put it another way, applications that stand to gain the most from digital certificate based security) tend to involve users applying *signatures* to Transactions, in order to explicitly denote their intention to be bound to the Transaction (i.e. signing for legal effect). While PKI offers a range of security functions, many are common to other technologies. But digital signatures supported by digital certificates are unique in that they provide a *lasting indelible binding* between a user and Transactions. Digital signatures are persistent over long periods of time, remaining readily verifiable without resorting to costly and involved investigations.

Successful Relationship Certificate deployments will tend to characteristically involve Transactions that require their senders to be authorised in some formal way, under the auspices of the Community of Interest.

At this early stage the proposal should also consider practical matters that will influence the ability to effectively integrate PKI technologies, including digital signature toolkits.

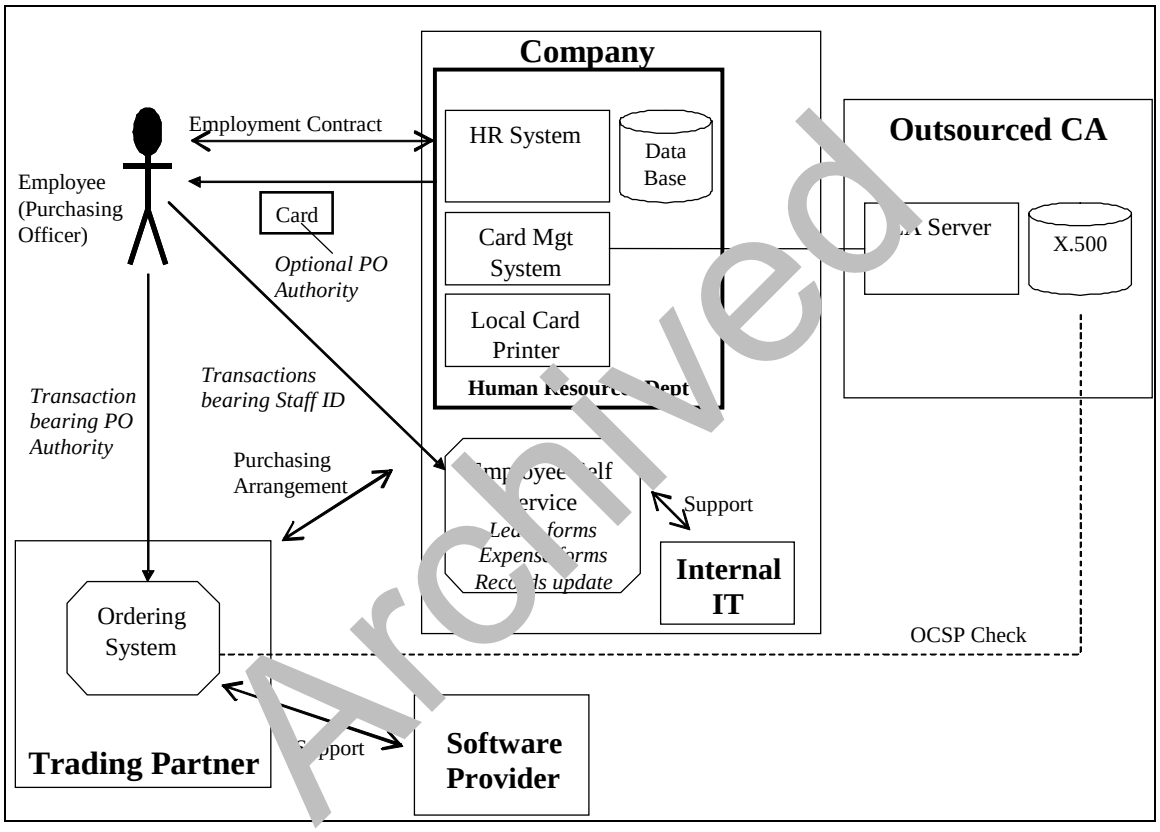
4.2.2. Business Model

At an early stage in any Relationship Certificate project, the envisaged deployment should be described in terms of a "block diagram" level description of all the major elements. These will include management processes, management functions and IT sub-systems, such as:

- Transaction systems, including applicable servers and/or Client side installations;
- client processes including databases and/or relevant "sources of truth";
- the designated Certificate Controller within the Relationship Organisation responsible for distributing digital certificates to members;

- the high level process by which Subscribers and the RO will interact, including any "automatic registration" interface between the RO workstation and "sources of truth" controlled by the COI;
- backend CA; and
- smart card or other token management systems if applicable.

The Figure below illustrates the sort of block diagram that is typically useful during this business modelling stage. Note that the diagram is entirely fictitious, and is intended for illustrative purposes only.



These block diagrams help to identify a range of practical issues, such as the mechanics of distributing digital certificates and managing them through their lifecycle, and implementing and supporting digital certificate enabled software applications. Block diagrams can be developed in a workshop mode with important project stakeholders, to help engender a common understanding of the deployment, and can be used as a crucial educative tool for other interested parties, such as executive managers.

The diagram can be maintained as a "living document" through the early stages of the Relationship Certificate project, to aid discussion. Its technical accuracy and completeness at any instance is of secondary importance compared with its value as a communication tool and discussion aid.

Note that the business model developed at this stage needs ideally to be iterated in parallel with the Threat and Risk Assessment (see below).

4.3. EOI Model

The EOI threshold for the Relationship Certificate category is variable from one COI to another. The Framework requires the Relationship Organisation to have "knowledge of, and history of its dealings with the individual or organisation to authorise the issuance of a digital certificate" that is sufficiently rigorous to provide assurance to COI members. In practice, Relationship Certificates may be produced utilising user information (including EOI) compiled and maintained by the Relationship Organisation under existing procedures. The way a Relationship Organisation compiles user information will depend primarily on the nature of its business, and will involve EOI processes that are fit for purpose.

4.3.1. Defining the Community of Interest

An important step in considering EOI for the issuance of Relationship Certificates is for the Relationship Organisation to review precisely how it is it knows its Clients. That is, what is the precise formal basis for establishing a relationship between the Clients and the COI?

> A Relationship Certificate COI is a group of digital certificate users – Subscribers and Relying Parties, where the latter may or may not be Subscribers themselves – that transact amongst one another according to a set of defined and accepted rules. The rules may come in various forms. In some cases, rules will be set by contracts such as customer terms and conditions, employee agreements, or membership agreements; in others, rules might be laid down in legislation or regulation.

There will be important hybrid situations especially in the professions where a combination of membership contracts and legislation control large and diverse COI, such as professional engineers plus all those who rely on engineers' work. Engineers enter into membership arrangements with recognised professional associations, which in turn are often recognised in law as being authoritative over certain domains and types of Transactions (such as building inspection reports).

To make sure that the project understands its particular COI, it should examine the following:

- Can all members of the COI be clearly defined or characterised? How tightly closed is it? Can all stakeholders in the Community's Transactions be counted as members of the Community?

- Can all Transactions being undertaken amongst COI members be characterised? Is it clear which Transactions are being targeted for digital certificate security?

- Is there an existing clearly recognised authoritative body or administrative function for the Community that can take on the role of Relationship Organisation?

- Does such an existing body/function govern all users, both senders and receivers of Transactions (i.e. Subscribers and Relying Parties)? Does it govern the Transaction systems that are used amongst members?

- If a natural Relationship Organisation does not presently exist, can the role be created to oversee the creation of digital certificates from relationship data?

- What formal membership/relationship processes already exist? Are the processes well documented? Is there a change management process?

- Are all members bound by clear Terms and Conditions for participating in the Community?

4.3.2. Quality and integrity of Client EOI processes

In orthodox PKI, clear-cut EOI rules are applied. With Relationship Certificates, Gatekeeper will allow Relationship Organisations within COIs to distribute (or authorise issuance of) digital certificates to their members/Clients under registration processes and EOI rules that are developed by and specific to each COI. The quality and integrity of these local registration processes – and by extension, the acceptability of the COI's Relationship Certificates is a matter for determination by the COI. However, it will still be important for the Relationship Organisation to assess whether its Client EOI processes are in fact adequate for distributing digital certificates.

Not all COIs will involve multiple agencies or organisations – many will be Agency/Organisation specific. In these cases the risks are simplified and so the internal administrative processes may therefore be simpler.

There are clear hallmarks of a well-managed membership or registration process. Some or all of the following should form the basis of a sound Relationship Certificate issuance process (as determined by risk assessment conducted by or on behalf of the COI):

- formal documentation of administrative procedures (including information security, access control, data integrity etc);

- formal approval processes and change management of administrative procedures;
- training of administrative staff, with checks of their competence in the tasks required;
- clear-cut practices for protecting and managing sensitive information, in compliance with the *Privacy Act 1988* (Cth) and other requirements;
- formal recognition of other regulatory requirements, codes of practice and so on, as applicable to the COIs business environment, and procedural mechanisms that ensure compliance;
- redundancy, to ensure continuity when key staff become unavailable, and to limit exposure should key staff start to act inappropriately;
- regular audits and corrective action procedures;
- clear chains of command in the administrative function, to deal with disputes, ambiguities and other exceptional circumstances; and
- continuous improvement processes to learn from exceptions and enhance documentation as required.

For the Relationship Certificate concept to demonstrate or generate confidence in the adequate integrity of Client EOI processes project management can undertake its own on-site inspection of the membership processes and the functioning of the Relationship Organisation or independent assessments can be sought. Documented processes should be reviewed, and checks made to see that documented processes are in fact carried out. New memberships, renewals, terminations and relevant exception or complaint handling scenarios should all be examined.

Management functions are increasingly subject to formal standards and therefore to external certification of compliance.

4.4. Issuance Model

Developing a robust, secure, low impact and business-beneficial Digital Certificate issuance model is the core challenge of any Relationship Certificate deployment. After establishing previously that the Community has a need for digital certificates, and after confirming that the Community is well defined in respect of its direct members, other stakeholders and their inter-relationships, the project has to establish a digital certificate issuance process.

Most Relationship Certificate deployments start with the working assumption that the Relationship Organisation's existing administrative processes are well tested and accepted in their proper context.

If Relationship Certificates are to be deployed to digitally represent real world relationships, then the basic approach to designing an issuance model is to make digital certificate registration a by-product of the otherwise regular user-administration process. The ideal situation is for existing Clients to receive new digital certificates automatically (with digital certificates populated using data from an existing reliable Client databases that are already considered the authoritative source of identity information in that COI). New Clients will generally receive their digital certificates at the time they are admitted into the Community as a by-product of conventional enrolment or admission processes with the Relationship Organisation.

A Threat and Risk Assessment (TRA) is required at this stage of any Relationship Certificate project as a tool to guide the detailed design of the issuance process. This TRA approach is described at a high level in the section below.

Where the TRA and issuance model design tasks identify vulnerabilities in the Community's administrative processes in the context of digital certificate issuance review and revision of those processes will be required.

Careful consideration must also be given to handling exception scenarios including:

- what happens if the COI no longer maintains a relationship with the Subscriber?
- dissolution of the COI; and
- what happens if the Relationship Organisation (as the Source of Truth) leaves the COI?

4.4.1. Threat and Risk Assessment

Central to the Framework is the "Secure Certification Authority" model, which allows Gatekeeper Accredited or Recognised CAs to operate as "service bureaus" for COIs. This model allows a strict separation of duties between Gatekeeper Accredited or Recognised CAs and front-end registration function, and broad allocation of relevant risk to the respective ends of the digital certificate supply chain.

Three major categories of risk can be described for a Relationship Certificate deployment, and responsibility for managing these risks can be allocated as follows:

- **Risks relating to Mis-registration**

Mitigating risks relating to mis-registration of Relationship Certificate Subscribers is the responsibility of the Relationship Organisation. Threats in this category include false representations made by an impostor, deliberate fraud by a Certificate Controller to create bogus digital certificates, and erroneous user information being entered into an otherwise legitimate digital certificate.

- **Risks relating to Counterfeiting**

Mitigating the risks relating to counterfeiting of Relationship Certificates is the responsibility of the Gatekeeper Accredited or Recognised CA. Threats in this category include corrupt behaviour by CA operations personnel that have access to the CA Private Key, and submission of fraudulent digital certificate requests by an attacker taking control of the RA-CA channels.

- **Risks relating to misuse of Keys and Certificates**

Mitigating risks relating to misuse of Keys and Certificates is broadly the responsibility of Subscribers. Threats in this category include attempting to use Keys and Certificates for purposes other than those sanctioned by applicable usage agreements, and loss of control of one's Private Key through neglect.

The TRA Template is structured to separate these categories of risk. It is only necessary for Relationship Certificate projects to consider risks relating to mis-registration and risks relating to misuse of Keys and Certificates. It can generally be assumed that risks relating to counterfeiting are covered by Gatekeeper Accredited or Recognised CAs. These issues are covered in other Gatekeeper documentation (e.g. the CPS, the CP and the Services Agreement).

Threat and risk analysis should be undertaken relatively early in the issuance model design stage. The TRA document should be iterated where necessary as design proceeds. The TRA should be re-visited whenever a significant change is made to the PKI system (examples include when a Community of Interest might seek to expand the scope of use for its digital certificates, when new membership categories or processes are introduced, or when major upgrades are made to the PKI-enabled Transaction software systems).

4.4.2. Design

Relationship Certificate issuance is a direct by-product of administration processes. It is critical that the detailed Registration processes address all issues peculiar to PKI, especially the whole Certificate lifecycle. Regardless of whether or not it is obvious to end users or even Certificate Controllers, Relationship Certificates are still managed via CA sub-systems[7] through stages of issuance, renewal and revocation, in accordance with X.509 and related standards. The design of the issuance model must implement all facets of the Certificate lifecycle, usually by mapping them onto regular administrative processes.

The design process should engage all-important stakeholders in the Relationship Certificate lifecycle. In particular, those managers responsible for membership processes (or human resources, customer service and so on as applicable) must be brought into the design of the issuance model. This Guidebook does not seek to promote any particular design methodology, but some form of active participation such as collaborative workshops will be essential.

For guidance, Relationship Certificate projects should address the following design issues:

- Certificate initial issuance, Certificate renewal and Certificate revocation. This includes the development of administrative processes for reporting lost and stolen digital certificates.

- Integration of Certificate Controller functions with Client administration.
  In some models, certificate registration functionality will need to be incorporated into the Relationship Organisation's administration area. Options will range from stand alone registration or enrolment software in which user details are manually entered (suitable for small scale COIs or for initial pilot rollout) through semi-integrated registration functions where digital certificate details can be imported from user databases, to fully automatic user administration software, such as Smart Card Management Systems (CMS), which usually have native CA interfaces.

[7] RAES processes may also be relevant in some COI certificate management models.

- Certificate Profiles will be customised to some extent for each Community.
  Each Relationship Certificate must bear a unique Policy OID indicative of the applicable Community, usage conditions and so on. The Profile must also specify Key Usage. Further, applications may take advantage of the opportunity to embed special authority information into the digital certificates, especially in order to facilitate paperless e-business. Special attention must be given to the formatting of user authority information in customised profiles. Consideration should also be given at this point to the use of Critical Certificate Extensions to help constrain the inappropriate re-use of digital certificates outside the COI.

4.4.3. Registration operators procedures

Production and maintenance of an operations manual by the Relationship Organisation for its clients would be useful. The requisite detail in the registration procedures will depend to a large extent on the RA sub-systems selected and their degree of automation. Ideally it should be included as an update to documented administration manuals where applicable, although it may include certain new activities, especially where new security technologies like smartcards or other tokens are introduced as part of the project.

4.5. Legal Issues

4.5.1. Legal arrangements

Allocation of risk in a COI will effectively be determined by the Relationship Organisation and the issuing CA, subject to the over-arching legal framework for Gatekeeper, incorporating the Gatekeeper Core Obligations Policy and Liability Guidelines. Within that framework, COIs should undertake their own legal analysis of Relationship Certificate usage with the following points in mind:

- Legal arrangements for use and management of Relationship Certificate should usually start with an analysis of the intended application. Digital certificates on their own do nothing; the consequences of misuse, abuse or other misadventure are always associated with business applications and application software. Legal analysis must be grounded in the realities of how the digital certificates will be used in practice.

- With Relationship Certificates it is easier to assume that digital certificate use is constrained and the possibility of unanticipated usage is greatly reduced. Therefore the focusing questions include: What can conceivably go wrong online with the application at hand? What are the Community's exposures in the event of misadventure? How are such risks managed in the real world (that is, prior to the introduction of Relationship Certificates)?

- Analysis can then turn to any additional exposures relating to potential mishaps with digital certificates.

- Terms and Conditions expressed in existing arrangements (employment agreements, membership agreements, professional charters, legislation and so on as applicable) will need to incorporate PKI-specific rights and obligations, and ensure compliance with Gatekeeper Policies as appropriate.

4.5.2. Services Agreement

Typically a Relationship Organisation managing Relationship Certificates will engage the services – essentially on an outsourcing basis – of a Gatekeeper Accredited or Recognised CA. Relationship Certificate deployments allows clearer separation of roles between the back-end CA and the front-end registration function, compared with orthodox PKI which tends to legally join the CA more closely to liability for errors and omissions all the way through the Certificate management lifecycle.

In Relationship Certificate deployments, registration related responsibilities and liabilities are borne by the Relationship Organisation, and digital certificate production responsibilities and liabilities are borne by a Gatekeeper Accredited or Recognised CA. While a more or less conventional CPS will specify much of the CA's operation, and a Relationship Certificate CP will describe the use and management of digital certificates within the COI, an additional Services Agreement will be needed between the Relationship Organisation and the CA.

The Services Agreement is a matter to be negotiated and agreed on a case-by-case basis between the Relationship Organisation (on behalf of the COI) and the outsourced CA. In brief, the Services Agreement should cover matters including:

- responsibilities of the CA to comply with Gatekeeper Accreditation requirements;

- responsibilities of the CA to comply with any other regulatory requirements relevant to the business environment of the COI;

- service levels to be provided by the CA in respect of timeliness of digital certificate production, revocation, renewal and so on, and availability of critical functions such as the CA server, directory, and OCSP responder;

- responsibilities of the Certificate Controller in the Relationship Organisation to perform registration functions accurately;

- possible indemnification of the CA in the event of errors or omissions on the part of the Certificate Controller in the Relationship Organisation, Subscribers, Relying Parties and/or application software; and

- possible indemnification of the Relationship Organisation in the event of errors or omissions on the part of the CA, or failures of digital certificate production systems at the CA.

Further information can be found in the Services Agreement Template.

4.6. Certificate Policy

A Relationship Certificate CP Template is available at www.gatekeeper.gov.au.

5. LISTING AND EVALUATION CRITERIA

Each CA generating Relationship Certificates under the Framework is required to be Gatekeeper Accredited/Recognised. The Department of Finance and Deregulation will List Relationship Organisations to help ensure the necessary uniqueness of Policy OIDs.

Relationship Certificates may only be requested/issued by a Gatekeeper Listed Relationship Organisation (acting on behalf of a Community of Interest).

Listing Criteria	Party	Details
Gatekeeper Accredited CA/RAES	CA/RAES	A COI can only deploy Relationship Certificates where the digital certificates are generated by a Gatekeeper Accredited / Recognised CA. Where an RAES performs Key Generation services (or other CA-like functions) it must also be Gatekeeper Accredited.
Unique OID	COI / CA	Each Relationship Certificate deployment must include a unique OID in the digital certificate that points to the Certificate Policy.
Listing with Gatekeeper	COI	Each Relationship Certificate deployment must be Listed under Gatekeeper. The listing will identify the: • COI including the name of the Relationship Organisation, and a description of the Relying Parties; • CA; • Unique OID; and • CP (including Version Number).
Notification requirement	COI / CA	Gatekeeper must be informed of any significant changes to the Relationship Certificate deployment, including significant changes to the: • Community of Interest; • CA; • Unique OID; or • CP.