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

Gatekeeper PKI Framework

February 2009

Gatekeeper Public Key Infrastructure Framework

Department of Finance and Deregulation

Australian Government Information Management Office

CONTENTS

1 EXECUTIVE SUMMARY

Public Key Infrastructure (PKI) is a system of cryptographic technologies, standards, management processes and controls governing the use of digital certificates. The Gatekeeper Strategy governs the use of PKI in government for the authentication of external clients (Organisations, Individuals and other entities). The Strategy ensures a whole-of-government framework that delivers integrity, interoperability, authenticity and trust for Agencies and their Clients.

The Gatekeeper PKI Framework (the Framework) incorporates the Gatekeeper Strategy while introducing new flexibility that better aligns the application of PKI to the way government interacts with external stakeholders. These new features reduce the cost and complexity of Gatekeeper for both business and government.

The Framework:

- retains the objective of a competitive government market for digital certificates at a "wholesale" rather than "retail" level. It does this by encouraging Certification Authorities (CAs) to operate as "service bureaus" for Agencies. This will allow Agencies to request digital certificates which meet their requirements rather than accepting standard digital certificates issued by Accredited CAs;
- incorporates existing certificate types into the Framework, under three new classification categories - Special, General, and High Assurance;
- retains the existing Government security standards for all Service Providers;
- introduces a risk management approach broadly aligned to the National e-Authentication Framework (NeAF)[1];
- introduces greater flexibility through the ability to leverage Known Customer (KYC) data and by enabling Service Providers to issue a range of Supplementary Certificates within security, privacy and transparency parameters;
- introduces Supplementary Certificates (designed to meet Agency business needs) including:
    - Hosted Certificates which enables a third party (Host) to digitally sign (or encrypt) messages on behalf of a small business for the purpose of interacting electronically with other Organisations;
    - Corporate Certificates where the certificate identifies the Organisation rather than an individual to facilitate wider use of PKI within a business enterprise;
    - Digital Credentials Certificates which combines a digital certificate with verified credentials of an Individual or Organisation such as an

[1] The NeAF recognises a range of risk levels for transactions and provides a methodology for assessing the risk level of the transaction and matching appropriate e-authentication mechanism to mitigate those risks.

Individual's profession or other qualifications, for example, lawyer, doctor or engineer;

- introduces the concept of sectoral Communities of Interest (COI) where Agencies or sectors will be able to rely on the identity established between a nominated Relationship Organisation and its clients within a COI;
- introduces streamlined administrative processes (including in particular a reduction in the paper burden on Service Providers) that have the potential to reduce the cost and complexity of generating, managing and using digital certificates for Agencies, Service Providers and business; and
- allows for the Framework to evolve to a national Framework, if appropriate.

1.1 Purpose of this Document

This document provides a high level overview of the Gatekeeper PKI Framework (the Framework). The document is the product of an administrative review of the Gatekeeper accreditation program and as such has been prepared as a high-level policy summary of the key features of the Framework.

1.2 Gatekeeper Documentation

The Department of Finance and Deregulation (Finance) has developed a suite of documentation to give operational effect to the Framework. All Gatekeeper documents referenced in this document are available at www.gatekeeper.gov.au.

The document suite listed below, when read in conjunction with the Commonwealth Protective Security Manual (PSM) and the Australian Government Information and Communications Technology Security Manual (ISM) will provide all the relevant information required for an entity to:

- obtain Gatekeeper Accreditation
- maintain its Gatekeeper Accreditation;
- be Listed as either a Known Customer or Threat and Risk Organisation; and
- be Listed as a Relationship Organisation in a Community of Interest.

The documents are logically arranged in the following diagrams to facilitate their use by Gatekeeper stakeholders (both current and new).

DIAGRAM 1: GATEKEEPER PKI FRAMEWORK DOCUMENTATION

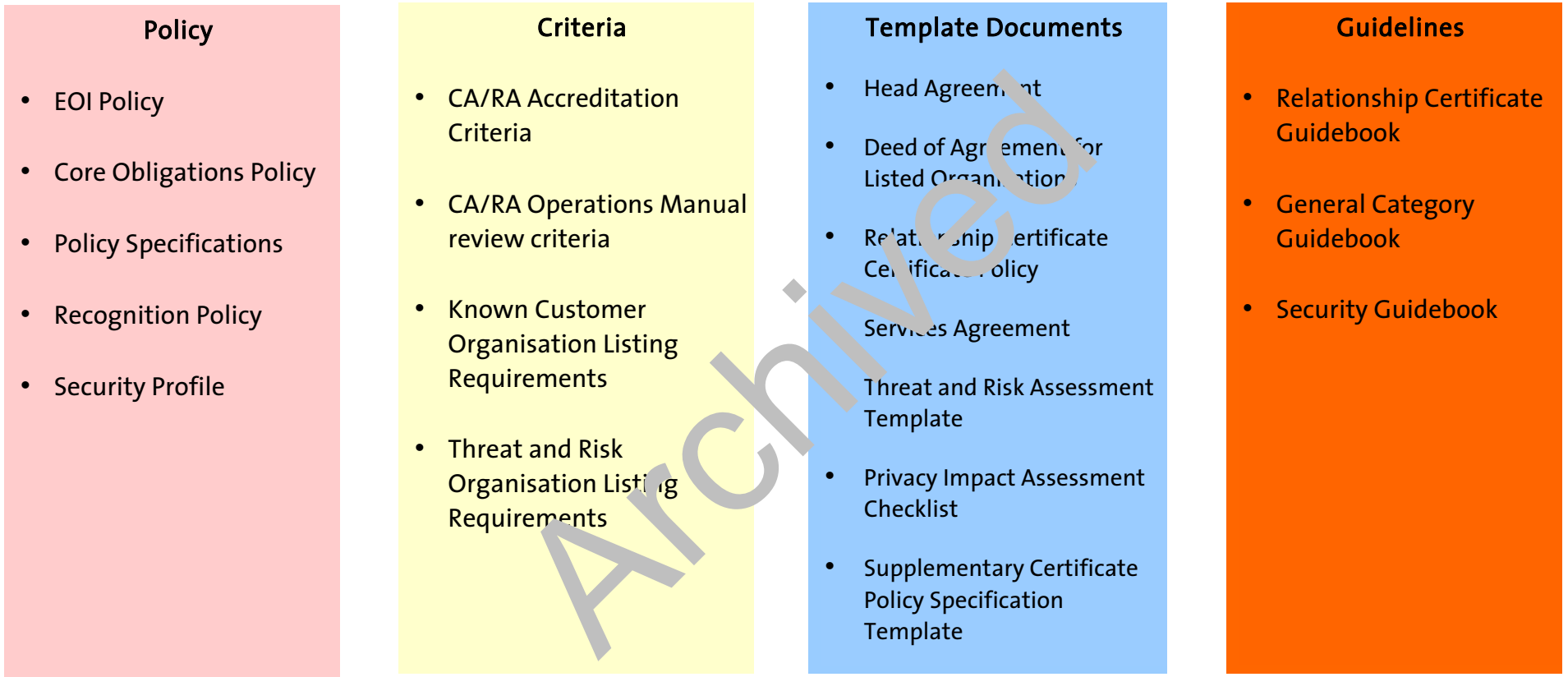
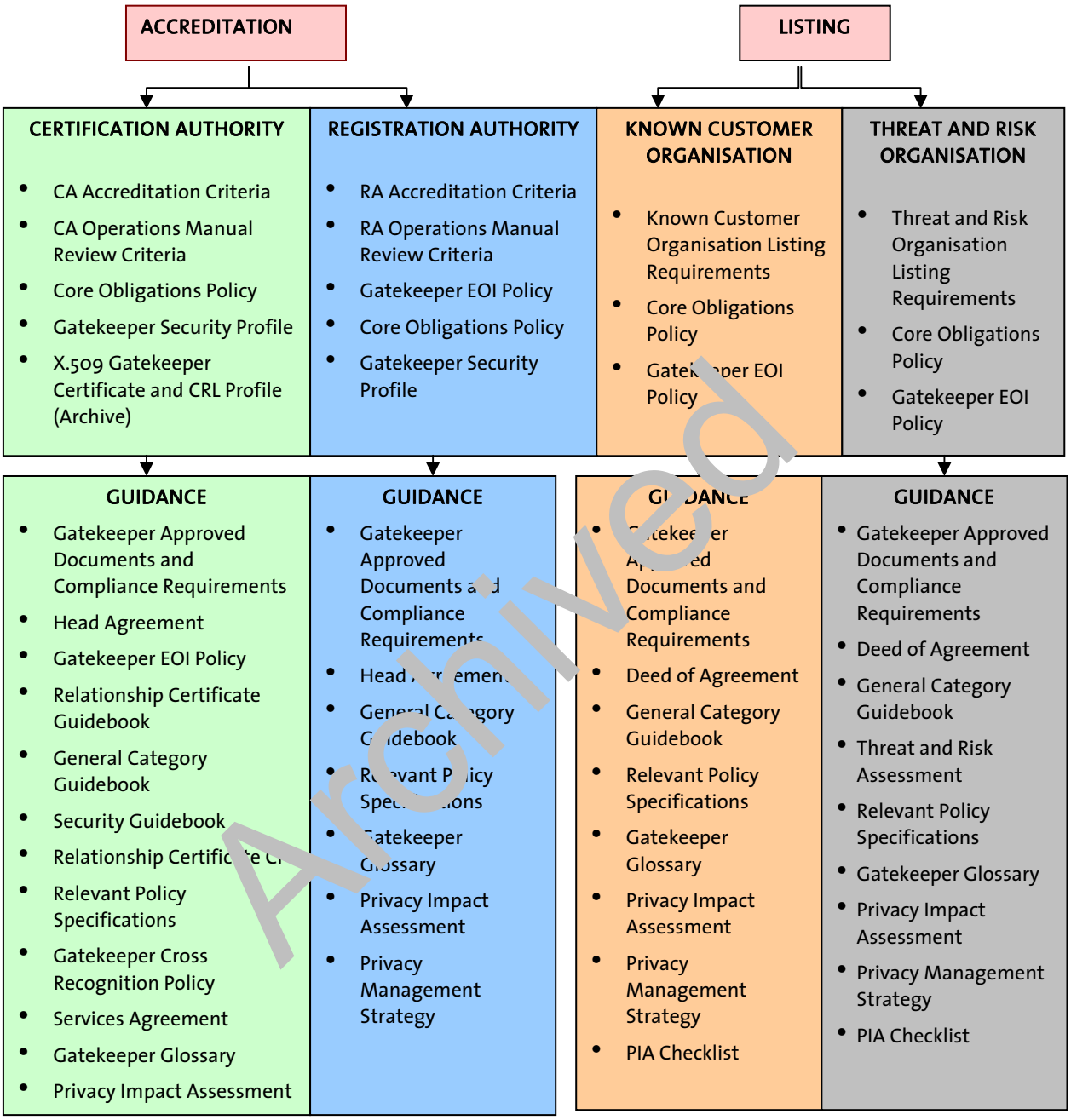


DIAGRAM 2: GATEKEEPER PKI FRAMEWORK



Contact:

For further information on the Framework please contact:
The Australian Government Information Management Office
Department of Finance and Deregulation
John Gorton Building
King Edward Terrace
PARKES ACT 2600
gatekeeper@finance.gov.au

2 GATEKEEPER PKI FRAMEWORK

The primary characteristics of the Framework are:

Interoperability	Digital certificates issued by Gatekeeper Accredited Service Providers will be capable for use across jurisdictions.
Transparency	Gatekeeper Policies and Criteria will be publicly available.
Accessibility	Service providers that meet the relevant Gatekeeper Accreditation requirements are able to participate.
Standards-based	Accreditation/Recognition processes are, as far as possible, based on national and international standards (where processes are not yet standardised, Gatekeeper will define its requirements).
Privacy-centred	Protection of the privacy of personal and corporate data is a major consideration with mandatory compliance with the *Privacy Act 1988* (Cth).
Security-focused	Mandatory compliance with Government security standards.
Risk-based	Agency/business selection of certificate types will be based on a thorough risk assessment of the type of online transactions that are to be facilitated (based on AS/NZS 4360).
Accountability	Accredited and Recognised Service Providers are accountable to the Gatekeeper Competent Authority for compliance with Gatekeeper Policies and Criteria.
Trust	Accreditation processes will provide end users with a sufficient degree of trust in the operations of the service provider and the PKI products used.
Light-touch	• Gatekeeper documentation has been rationalised to reduce the paper burden on Service Providers and streamline the Accreditation process. • Accreditation focuses on security requirements rather than business and legal aspects with commercial and legal aspects managed between Service Providers and Agencies.
Access and Authorisation	Enrolment of certificate holders (i.e. provision of access and authorisation entitlements) is the responsibility of Agencies and businesses. Guidelines on access and authorisation are available from the AGAF Access and Authorisation Guide.
Digital Certificates	• Will be based on the X.509 V3 standard. • Will provide authentication, confidentiality, integrity and non-repudiation (as required by the PKI domain). • Will accommodate the inclusion of certain attributes in non-critical extensions.

TABLE 1 – INDIVIDUAL CERTIFICATES			
	SPECIAL CATEGORY	**GENERAL CATEGORY**	**HIGH ASSURANCE CATEGORY**
NeAF Assurance Level	Level 1- 4 (with restrictions)	Level 1-3	Level 1- 4
Assurance	• Provides authentication of identity within a COI. o May also provide assurance of access or authority attributes within the COI • Minimal to high level of assurance[2] concerning the identity of the Individual within the COI.	• Minimal to moderate level of assurance concerning the identity of the Individual relevant to environments where risk and consequences of data compromise are moderate. • Provides authentication of identity in open PKI deployments.	• Moderate to high level of assurance concerning the identity of the Individual appropriate for use where the threats to data are high, or the consequences of the failure of security services are high. • Provides authentication of identity in open PKI deployments.
Non-repudiation; data integrity and confidentiality	Within the defined COI	Yes	Yes
Evidence of Identity (EOI)	Established by means of Relationship model plus any additional EOI registration /enrolment measures as required by Relationship Organisation.	Established by means of • Known Customer model • Threat / Risk Assessment model • Formal Identity Verification model.	Established by means of Formal Identity Verification model.
EOI Refresh	As defined by the COI.	Refresh required every 4-6 years.	Refresh required every two years.
Transaction Types	• Defined by COI • Defined by certificate features. • Defined by Agency/business as part of a risk assessment.	• Defined by Certificate Policy. • Defined by Agency/business as part of a risk assessment.	• Defined by Certificate Policy. • Defined by Agency/business as part of a risk assessment.

[2] The terms minimal and moderate in relation to assurance are derived from the National e-Authentication Framework (NeAF) – see http://www.finance.gov.au/e-government/security-and-authentication/authentication-framework.html.

TABLE 1 – INDIVIDUAL CERTIFICATES

	SPECIAL CATEGORY		GENERAL CATEGORY		HIGH ASSURANCE CATEGORY	
Government Information Security Levels[3]	Defined by Agency consistent with the Protective Security Manual (PSM) up to X-in-Confidence (but not Cabinet-In-Confidence).		Defined by Agency consistent with the PSM up to X-in-Confidence (excluding Cabinet-In-Confidence as this is marked with a higher classification).		Defined by Agency consistent with the PSM up to X-in-Confidence (including Cabinet-In-Confidence unless it has been marked with a higher classification).	
Certificate Characteristics	• Certificate life – based on ISM minimum standards and structure of PKI deployment (currently neither greater nor equal to 10 years). • Certificate medium[4] – at Agency/business discretion.		• Certificate life – generally maximum two years. • Certificate renewal using unexpired certificate to request renewal. • Certificate medium – at Agency/ business discretion.		• Certificate life – maximum two years. • Renewal using unexpired certificate to request renewal. • Certificate medium – at Agency/business discretion.	
Technical Specification	In accordance with ISM Security-in-Confidence (SIC) edition.		In accordance with ISM SIC edition.		In accordance with ISM SIC edition.	
Certification and Registration Authority (including RA Extended Services) Accreditation requirements	CA/RAES Gatekeeper Accreditation to meet the requirements for the HP security level. RA Gatekeeper Accreditation will not normally feature in the Special Category. But if required, it will meet the requirements for the X-in-Confidence security level.		CA/RAES Gatekeeper Accreditation to meet the requirements for the HP security level. RA Gatekeeper Accreditation to meet the requirements for the X-in-Confidence security level.		CA/RAES Gatekeeper Accreditation to meet the requirements for the Secret level. RA Gatekeeper Accreditation to meet the requirements for the X-in-Confidence security level.	
Operational security requirements – CA/RAES	IT product	Evaluation Assurance Level 4 (EAL4)[5]	IT product	EAL4	IT product	EAL4

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

[4] In this context certificate medium refers to certificates issued either electronically (i.e. soft) or on a "hard token".

TABLE 1 – INDIVIDUAL CERTIFICATES

	SPECIAL CATEGORY		GENERAL CATEGORY		HIGH ASSURANCE CATEGORY	
	Personnel	HP	Personnel	HP	Personnel	Secret
	Physical	Secure Room (SR) 1[6]	Physical	SR1	Physical	SR1
Operational Security requirements - RA	IT Product (if necessary)	EAL4	IT Product (if necessary)	EAL4	IT Product (if necessary)	EAL4
	Personnel	X-in-Confidence	Personnel	X-in-Confidence	Personnel	X-in-Confidence
	Physical	Intruder resistant	Physical	Intruder resistant	Physical	Intruder resistant
Operational Security requirements – Relationship Organisation	**IT PRODUCT NOT APPLICABLE[7]**		**NOT APPLICABLE**		**NOT APPLICABLE**	
	Personnel	Not Specified				
	Physical	Not Specified				
Operational Security requirements – Known Customer Organisation	**IT PRODUCT NOT APPLICABLE**		IT Product (if necessary)	EAL4	**NOT APPLICABLE**	
	Personnel	Protected	Personnel	Protected		
	Physical	Intruder resistant	Physical	Intruder resistant	**NOT APPLICABLE**	
Operational Security requirements – Threat/Risk Organisation	**IT PRODUCT NOT APPLICABLE**		IT Product (if necessary)	EAL4		
	Personnel	Protected	Personnel	Protected		
	Physical	Intruder resistant	Physical	Intruder resistant		

5 For further detail see ISM at http://www.dsd.gov.au/library/infosec/ism.html and the Evaluated Products List at http://www.dsd.gov.au/infosec/evaluation_services/epl/AboutEPL.html

6 For further detail see Gatekeeper Security Guidebook and ISM (http://www.dsd.gov.au/library/infosec/ism.html)

7 Where a Relationship Organisation, Known Customer Organisation or Threat and Risk Organisation utilises IT Hardware and Software that is of the same type (e.g. UniCert) as the issuing CA for the purpose of interacting with the CA for certificate issuance, then the Organisation will be required to comply with the same Accreditation requirements as a RAES.

TABLE 2 – ORGANISATIONAL CERTIFICATES			
	SPECIAL CATEGORY	**GENERAL CATEGORY**	**HIGH ASSURANCE CATEGORY**
NeAF Assurance Level	Level 1- 4 (with restrictions)	Level 1- 3	Level 1- 4
Assurance	• Provides authentication of identity within a COI. o May also provide assurance of access or authority attributes within the COI • Minimal to high level of assurance concerning the identity of the Individual within the COI.	• Minimal to moderate level of assurance concerning the identity of the Individual relevant to environments where risks and consequences of data compromise are moderate. • Provides authentication of identity in open PKI deployments.	• Moderate level of assurance concerning the identity of the Individual appropriate for use where the threats to data are high, or the consequences of the failure of security services are high. • Provides authentication of identity in open PKI deployments.
Non-repudiation; data integrity and confidentiality	Within the defined COI	Yes	Yes
Evidence of Identity (EOI)	Established by means of Relationship model plus any additional EOI registration /enrolment measures as required by Relationship Organisation.	Established by means of • Known Customer model • Threat and Risk Assessment model • Formal Identity Verification model.	Established by means of Formal Identity Verification model.
EOI Refresh	As defined by the COI.	Refresh required every 4-6 years.	Refresh required every two years.
Transaction Types	• Defined by COI. • Defined by certificate features. • Defined by Agency/business as part of a risk assessment.	• Defined by Certificate Policy. • Defined by Agency/business as part of a risk assessment.	• Defined by Certificate Policy. • Defined by Agency/business as part of a risk assessment.

TABLE 2 – ORGANISATIONAL CERTIFICATES

	SPECIAL CATEGORY		GENERAL CATEGORY		HIGH ASSURANCE CATEGORY	
Government Information Security Levels[8]	Defined by Agency consistent with the Protective Security Manual (PSM) up to X-in-Confidence (but not Cabinet-In-Confidence).		Defined by Agency consistent with the PSM up to X-in-Confidence (excluding Cabinet-In-Confidence as this is marked with a higher classification).		Defined by Agency consistent with the PSM up to X-in-Confidence (including Cabinet-In-Confidence unless it has been marked with a higher classification).	
Certificate Characteristics	• Certificate life – based on ISM minimum standards and structure of PKI deployment (currently neither greater nor equal to 10 years). • Certificate medium[9] – at Agency/business discretion.		• Certificate life – generally maximum two years. • Certificate renewal using unexpired certificate to request renewal. • Certificate medium – at Agency/business discretion.		• Certificate life – maximum two years. • Renewal using unexpired certificate to request renewal. • Certificate medium – at Agency/business discretion.	
Technical Specification	In accordance with ISM Security-in-Confidence (SIC) edition.		In accordance with ISM SIC edition.		In accordance with ISM SIC edition.	
Certification and Registration Authority (including Extended Services RA) Accreditation requirements	CA Gatekeeper Accreditation to meet the requirements for the HP security level. RA Gatekeeper Accreditation to meet the requirements for the X-in-Confidence security level.		CA Gatekeeper Accreditation to meet the requirements for the HP security level. RA Gatekeeper Accreditation to meet the requirements for the X-in-Confidence security level.		CA Gatekeeper Accreditation to meet the requirements for the Secret level. RA Gatekeeper Accreditation to meet the requirements for the X-in-Confidence security level.	
Operational security requirements – CA/RAES	IT product	Evaluation Assurance Level 4 (EAL4)	IT product	EAL4	IT product	EAL4
	Personnel	HP	Personnel	HP	Personnel	Secret
	Physical	Secure Room (SR) 1	Physical	SR1	Physical	SR1

8 Relates to information transmitted across a public network only (in accordance with the PSM).

9 In this context certificate medium refers to digital certificates issued either electronically (i.e. soft) or on a "hard token".

TABLE 2 – ORGANISATIONAL CERTIFICATES

	SPECIAL CATEGORY		GENERAL CATEGORY		HIGH ASSURANCE CATEGORY	
Operational Security requirements - RA	IT Product (if necessary)	EAL4	IT Product (if necessary)	EAL4	IT Product (if necessary)	EAL4
	Personnel	X-in-Confidence	Personnel	X-in-Confidence	Personnel	X-in-Confidence
	Physical	Intruder resistant	Physical	Intruder resistant	Physical	Intruder resistant
Operational Security requirements – Relationship Organisation	**IT PRODUCT NOT APPLICABLE**[10]		**NOT APPLICABLE**		**NOT APPLICABLE**	
	Personnel	Not Specified				
	Physical	Not Specified				
Operational Security requirements – Known Customer Organisation	**IT PRODUCT NOT APPLICABLE**		IT Product (if necessary)	EAL4	**NOT APPLICABLE**	
	Personnel	Protected	Personnel	Protected		
	Physical	Intruder resistant	Physical	Intruder resistant		
Operational Security requirements – Threat/Risk Organisation	**IT PRODUCT NOT APPLICABLE**		IT Product (if necessary)	EAL4	**NOT APPLICABLE**	
	Personnel	Protected	Personnel	Protected		
	Physical	Intruder resistant	Physical	Intruder resistant		

[10] Where a Relationship Organisation, Known Customer Organisation or Threat and Risk Organisation utilises IT Hardware and Software that is of the same type (e.g. UniCert) as the issuing CA for the purpose of interacting with the CA for certificate issuance, then the Organisation will be required to comply with the same Accreditation requirements as a RAES.

3 GATEKEEPER PKI FRAMEWORK CATEGORIES

Digital certificates issued under the Gatekeeper PKI Framework will:

- provide authentication, confidentiality, integrity and non-repudiation;
- meet X.509 Standards; and as appropriate
- be able to accommodate inclusion of the Australian Business Number (ABN).

3.1 Special

Certificates in the Special Category provide authentication, confidentiality, integrity and non-repudiation within a Community of Interest (COI).

Closed PKI deployments, such as a COI within the Special Category, restrict the use of digital certificates to a known set of Relying Parties where these parties are usually contractually bound to the issuing CA.

Within the Special Category are Relationship Certificates, Hosted Certificates and as appropriate other Supplementary Certificates.

Any Gatekeeper Accredited/Recognised CA[11] can issue digital certificates in the Special Category.

3.2 General

Digital certificates under the General Category are issued to Individuals, Organisations and Devices.

Certificates in the General Category provide authentication, confidentiality, integrity and non-repudiation.

The Certificate Policy under which the certificate is issued must specify Key Usage in the Certificate Profile.

PKI deployments in the General Category are regarded as "open" – i.e. digital certificates are able to be relied upon by multiple Agencies without the necessity for contractual arrangements between them and the issuing CA.

Certificates in the General Category will be issued under a range of EOI models and will be distinguished on the basis of the EOI Model and level of EOI assurance underpinning issue of a digital certificate.

Within the General Category are identity Certificates (both Individual and Organisation) and as appropriate Supplementary Certificates.

Any Gatekeeper Accredited/Recognised CA can issue digital certificates in the General Category.

[11] Reference to a CA can also refer to a Gatekeeper Accredited Registration Authority Extended Services.

3.3 High Assurance

A High Assurance Certificate provides authentication, confidentiality, integrity and non-repudiation. PKI deployments in the High Assurance Category are regarded as "open" – i.e. digital certificates are able to be relied on by multiple Agencies without the necessity of contractual arrangements between them and the issuing CA.

High Assurance Certificates will only be issued on the basis of the Formal Identity Verification model.

Within the High Assurance Category are Individual and Organisation Certificates and as appropriate Supplementary Certificates.

Only CAs that have been Gatekeeper Accredited/Recognised as meeting the "Secret" security classification requirements are able to issue digital certificates in the High Assurance Category.

4 CERTIFICATION AUTHORITY

The emphasis in the Framework is on providing assurance to End-Entities of the overall security (physical, logical and personnel) of Service Providers involved in the generation and issuance of digital certificates.

This is achieved through Gatekeeper Accreditation of Service providers which includes evaluation of their operational policies and procedures and secure facilities against Gatekeeper Policy and Criteria (which in turn link to Australian Government security standards in the Commonwealth Protective Security Manual (PSM) and Australian Government Information and Communications Technology Security Manual (ISM)). Service Providers comprise Certification Authorities (CAs) and Registration Authorities (RAs).[12]

Gatekeeper Recognition of other PKI domains is addressed in more detail in the Gatekeeper Cross-Recognition Policy.

4.1 Security

Gatekeeper accreditation of a CA will focus on the security elements of its operations rather than those aspects that are more commercial in nature, the rationale being that commercial issues are more appropriately addressed by individual Agencies as part of their service agreement negotiations. The core security requirements for Gatekeeper Accreditation are established in the PSM and ISM.

The requirement for Service Providers to comply with rigorous government security standards in relation to physical, logical and personnel will ensure that both Agencies and their clients can have confidence and trust in the PKI services that are

[12] A CA that issues X.509 v3 Public Key Certificates which bind Subscribers to their Public Keys, vouches for their contents, is trusted by Relying Parties to do so, and may provide warranties to that effect. A RA is an entity that performs services in relation to registration and verification of the identity of applicants for Public Key Certificates.

deployed by protecting against counterfeiting and subversion of backend processes. In particular, the requirement for Common Criteria EAL4 rated CA and RA products is retained to help prevent fraudulent ordering of digital certificates.

4.2 Certificates

Under the Framework, CAs will be able to operate as "service bureaus", responsive to Agencies (either directly or via Gatekeeper Accredited RAs) and issue digital certificates on request via standard Public Key Cryptography Standards (PKCS) protocols. Each Agency will enrol Subscribers for defined PKI-enabled applications according to scheme or programme-specific business rules.

Gatekeeper Accredited CAs can simplify their business models and delivery of certification services. The CA's business model can be constant over a range of different PKI applications. Certificate supply arrangements can be more readily novated from one backend CA to another, as Agencies from time to time negotiate better deals for themselves. A change of backend digital certificate supplier would only require that the new service provider is Gatekeeper Accredited.

While the format for digital certificates remains the X.509 standard, Supplementary Certificates will allow Agencies to define particular digital certificate requirements based on identified business needs rather than accepting standard digital certificates issued by Gatekeeper Accredited CAs. Consistent with international practice and dependent on Agency requirements, Organisations (represented by individual Key Holders) and Individuals may hold multiple digital certificates each tailored to specific Agency Transactions.

The CA need have no interest at all in the semantic contents of the digital certificates it issues other than to ensure compliance with the X.509 standard. So long as there are safeguards in place to mitigate false digital certificate requests, the CA need not be concerned about the intended application of the digital certificates.

4.3 Gatekeeper Accreditation

Under the Framework CAs will no longer be required to undergo re-accreditation each time the semantics of a given Certificate Profile is changed. New digital certificate applications could be set up quickly with no impact on the CA's Accreditation.

Annual compliance audits would remain as a condition of Gatekeeper accreditation.

4.4 Legal

Within defined Communities of Interest in the Special Category there is no requirement for a contract or other legal arrangement between end users of digital certificates and the CA. The Services Agreement between the CA and Agency will define obligations and responsibilities and establish liability and performance arrangements.

The obligations and responsibilities of Subscribers will be specified through their business relationship with the Agency. The Gatekeeper Core Obligations Policy will establish the baseline for such arrangements.

In the General and High Assurance Categories (i.e. open PKI deployments) it is expected that Subscriber Agreements will remain an integral part of the Framework.

5 EVIDENCE OF IDENTITY MODELS

5.1 Gatekeeper Bindings

Digital certificates issued by Gatekeeper Accredited/Recognised CAs require verification of the identity of the Key Holder to meet the Gatekeeper Binding requirements.

With the introduction of different EOI Models in the Framework there are a variety of ways in which the Gatekeeper Bindings[13] can be demonstrated.

5.1.1 Individual

EOI Step	Example
Bind the physical person to the name of the Key Holder.	Face-to-face EOI check with trusted third party.

5.1.2 Organisation

EOI Step	Examples
Bind the Organisation to a business name and if appropriate to an ABN.	Australian Business Register (ABR) search; Australian Securities and Investments Commission (ASIC) search.
Bind the physical person to the name of the Key Holder.	Face-to-face EOI check with trusted third party.
Bind the Key Holder to the Organisation	Letter of Authority signed by Authoriser sighted by trusted third party.
Bind the Authoriser to the Organisation	ASIC check, ABR search, phone verification.

5.2 Relationship Model

Under this model, a Relationship Certificate is issued where one Organisation (known as the Relationship Organisation) has an ongoing relationship with a client (whether Individual or representative of an Organisation) and as a result is prepared to:

- rely on its knowledge of, and history of its dealings with that Individual or Organisation to authorise the issuance of a digital certificate to that Individual or Organisation; and

13 Binding means the process of linking a credential to an identity in an assured manner. With respect to EOI it is the process of establishing a linkage between an Individual or entity and their claimed or documented identity in an assured manner.

- accept (to an internally defined risk level and for internally determined purposes) a digital signature verified by that Relationship Certificate, as having been applied by the known Individual or Organisation for future online dealings.

This enables Relationship Certificates to provide authentication, confidentiality, integrity and non-repudiation within a defined COI.

A Community of Interest (COI) is a set of Individuals and/or Organisations which agree to transact according to a defined set of rules. A COI may range from a single Relying Party (Relationship Organisation) with multiple Subscribers to multiple Relying Parties and Subscribers.

The details of the relationships will vary from one COI to another and confidence in Relationship Certificates is determined by what the relationship is, how the relationship is attained and maintained and what applications the digital certificate is intended to support across the COI.

In effect, each Relying Party participating in the COI, is relying on the Relationship Organisation's representation to the issuing CA (and perhaps directly to the Relying Party) that it has assured itself of the identity of the subject named in the digital certificate.

In order to achieve a level of trust across Agencies in the identity represented by a Relationship Certificate, a high degree of disclosure (basis of Certificate issuance, Certificate usage, life-cycle management etc) between the Relationship Organisation and Relying Parties will be required.

Under this model, applicants (whether individuals or as representatives of an Organisation) for Relationship Certificates may not be required to undergo an additional identity verification process.

Further details on the Relationship Model can be found in the Relationship Certificate Guidebook.

5.3 Known Customer Model

This model allows for digital certificates in the General Category to be issued on the basis that a client (whether Individual or representative of an Organisation) of an Organisation (known as a Known Customer Organisation) is a Known Customer of that Organisation in accordance with the Gatekeeper Known Customer Listing Requirements.

A Known Customer is where a Known Customer Organisation has an ongoing relationship with either a known Individual or known Organisation; and

- that Individual or representative of an Organisation has at some time in the past undergone a face-to-face EOI process which complies with Gatekeeper EOI Policy; and

- the Known Customer Organisation is prepared to authorise the issuance of a digital certificate, and to rely on that Digital Certificate.

The Australian Standard - AS4860-2007 - *Knowledge-based identity authentication - Recognizing Known Customers* - facilitates the deployment of a range of authentication credentials appropriate to the needs of government agencies and their clients.

Finance has developed the Known Customer Organisation Listing Requirements as summarised below:

Gatekeeper Known Customer Organisation requirement	Details
Requirement 1 Performed a prior EOI check in accordance with Gatekeeper EOI policy.	The certificate applicant must have (within the preceding five years): - undergone a Gatekeeper Formal Identity Verification check consistent with Gatekeeper EOI policy.
Requirement 2 Evaluated the adequacy of its EOI information holdings as a basis for requesting issuance of a digital certificate.	A Known Customer Organisation will be required to provide the Gatekeeper Competent Authority with documentation on its policies and procedures for managing data integrity for review and sign off.
Requirement 3 Evaluated whether Individuals have maintained their relationship with the Organisation in accordance with the Known Customer Organisation Listing Requirements.	The Known Customer Organisation must provide an assurance to the Gatekeeper Competent Authority that the Digital Certificate applicants have, and continue to interact on a regular basis with the Known Customer Organisation in accordance with any applicable regulatory or compliance requirements.
Requirement 4 Established policies and procedures to ensure the on-going security and integrity of its data holdings	The Known Customer Organisation will be required to demonstrate to the Gatekeeper Competent Authority its compliance with similar security standards as apply to Gatekeeper Accredited Registration Authorities.
Requirement 5 Committed to the Gatekeeper Core Obligations Policy.	The Known Customer Organisation must submit the following documents to Finance for review as a precondition to listing. 1. Privacy Management Strategy; 2. Liability Policy in relation to the accuracy of client information provided to the issuing CA; and 3. Risk Management Strategy.
Requirement 6 Performed EOI check on new customers in accordance with the Gatekeeper EOI policy.	Policies and procedures for enrolling / registering "new customers" including policies relating to retention of EOI records.

Other Organisations can choose to accept the digital certificate as verifying the identity of the Key Holder, to a risk level considered acceptable for certain applications, on the basis that the Known Customer concept has been applied by a Gatekeeper Listed Known Customer Organisation (without necessarily knowing which Agency authorised the issue of that digital certificate). This approach is similar to that used by the banking sector in issuing credit cards.

Under this model, applicants (whether Individuals or as representatives of an Organisation) for digital certificates in the General Category will not be required to undergo a formal face-to-face EOI check at the time of certificate request (the identity check will already have been undertaken). Under this model, digital certificates may be "pushed" out to end users rather than requiring the Individual or Organisation to go through traditional application processes.

Further details on the Known Customer Model can be found in the General Category Guidebook and the Known Customer Organisation Listing Requirements.

5.4 Threat and Risk Assessment Model

Under this model, digital certificates in the General Category are issued on the basis that a Client (whether Individual or representative of an Organisation) of an Organisation (known as a Threat and Risk Organisation) can be identified through the Organisation's internal identity management processes. These processes will undergo an independent Threat and Risk Assessment (TRA) to meet Gatekeeper Listing Requirements.

As part of the independent TRA, the following factors must be assessed:

- strength of the Organisation's EOI processes in delivering the Bindings required by Gatekeeper, namely verifying the:
  - identity of Organisation/Individual;
  - documentation binding either the owner, chief executive, or other officer or employee (being a person who has a clear capacity to commit the Organisation) to the Organisation;
  - documentation binding the Individual Certificate Holder to the Organisation; and
  - documentation binding the physical person of the Individual Key Holder to the name provided by either the owner, chief executive or other officer or employee of either the owner, chief executive or other officer or employee with clear capacity to commit the Organisation;
- privacy/legislative implications for the use of Organisation data holdings as an identifier;
- documented processes and procedures audited against actual practices;
- identification of threats and risks and risk mitigation procedures implemented by the Organisation;
- full disclosure of the documents and processes employed by the Organisation; and
- evaluation of the implementation of Organisation EOI processes and procedures against implemented EOI procedures for other digital certificates in the General Category.

Under this model:

- applicants (whether Individuals or representatives of an Organisation) for digital certificates in the General Category will not be required to undergo a formal face-to-face EOI check at the time of certificate request; and
- digital certificates may be "pushed" out to end users rather than requiring the Individual or Organisation to go through traditional application processes.

Further details on the Threat and Risk Assessment Model can be found in the General Certificate Guidebook and the Threat and Risk Organisation Listing Requirements.

5.5 Delegated RA Process

The essence of the Delegated RA process is that the verification of the identity of a specific Key Holder within an Organisation is not performed by a Gatekeeper Accredited RA but by the Organisation itself (through the Certificate Manager). Further details on the responsibilities of a Certificate Manager are contained in the General Business Certificate Policy Specification.

A representative of the Organisation (the Certificate Manager) is issued a digital certificate by a Gatekeeper Accredited/Recognised CA after:

- undergoing a face-to-face identity verification process under the Formal Identity Verification EOI Model at a Gatekeeper Accredited Registration Authority (RA); or
- being a Client of a Known Customer Organisation or Threat and Risk Organisation.

Any additional digital certificates requested by the Certificate Manager for the Organisation will require the identity of additional Key Holders to be vouched for by the Organisation (via the Certificate Manager). The Delegated RA process results in certain obligations in relation to digital certificate lifecycle management being taken by the business. These obligations are found in the appropriate Policy Specification. For example, the General Business Certificate Policy Specification states that the Certificate Manager must:

1. on behalf of the Organisation, vouch for the identity of all representatives for whom additional General Business Certificates are requested; and
2. undertake on behalf of the Organisation that it will accept responsibility for the use of all General Business Certificates.

To utilise this process, Organisations will need to consider:

- face-to-face EOI registration requirements; and
- Certificate Manager requirements in the relevant Policy Specification.

Where an Agency's risk profile requires assurance as to the identity of the Key Holder, they will be able to distinguish between digital certificates issued to a Certificate Manager and those issued to additional Key Holders within an Organisation on the basis of information contained in the digital certificate itself and the associated Certificate Policy.

5.6 Formal Identity Verification Model

Under this model:

- all applicants (whether Individuals or representatives of an Organisation) for High Assurance Certificates; and
- all applicants (whether Individuals or representatives of an Organisation) that do not qualify as Clients of Known Customer Organisations or Threat and Risk Organisations under the General Category

will be required to undergo a Formal Identity Verification process at a Gatekeeper Accredited Registration Authority.

5.6.1 Individuals

An Individual is required to submit EOI documentation to meet the necessary Gatekeeper Binding requirements.

The submitted EOI documents **must** meet the following requirements:

- the applicant's name is on every document. Where the EOI documents bear a different name, the linkage between that EOI document, the name to be enrolled and the applicant must be clearly established;
- the applicant's address is on at least one of the documents;
- the applicant's signature is on at least one of the documents;
- the applicant's date of birth is on at least one of the documents; and
- a recognisable photograph of the applicant is on at least one of the documents.

5.6.1.1 General

The EOI documentation[14] presented **must** consist of:

- one Category A document establishing evidence of commencement of identity in Australia; AND
- one Category B document establishing a linkage between Identity and Person (photo and signature); OR
- two Category B documents establishing a linkage between Identity and Person (photo and signature); AND

[14] For a list of the documentation, refer to the Gatekeeper EOI Policy.

- one Category C document establishing the operation of that identity in the community.

5.6.1.2 High Assurance

The EOI documentation presented **must** consist of:

- one Category A document establishing evidence of commencement of identity in Australia; AND
- one Category B document establishing a linkage between Identity and Person (photo and signature); AND
- one Category C document establishing the operation of that identity in the community; OR
- one Category A document establishing evidence of commencement of identity in Australia; AND
- Two Category B documents establishing a linkage between Identity and Person (photo and signature)

In addition to presenting EOI documentation at the time of the EOI check, the Individual or employee is also required to undergo a signature verification check and a photograph comparison.

5.6.2 Organisations

An Organisation through its employees is required to submit documentation to identify the Organisation to meet the necessary Gatekeeper binding requirements.

The Organisation identity documentation **must** comprise:

- an original or certified copy of the notice issued by the Registrar of the Australian Business Register (ABR) bearing the Organisation's name and the Australian Business Number (if either the owner, chief executive or other officer or employee with clear capacity to commit the Organisation is named as the Public Officer on the document issued by the Registrar of the ABR, then this document only will suffice);
  - a secondary check involving online verification with the ABR to link the Organisation's ABN to its business name is recommended;

OR

- if the notice issued by the Registrar of the ABR cannot be provided then a legal or regulatory document binding either the Individual or the Authoriser to the Organisation;
  - in this case online verification with the ABR to link the Organisation's ABN to its business name must be achieved.

The employee representing an Organisation is also required to submit EOI documentation and the documentation must comply with certain requirements.

The submitted EOI documents **must** meet the following requirements:

- the applicant's name is on every document. Where the EOI documents bear a different name then the linkage between that EOI document, the name to be enrolled and the applicant must be clearly established;
- the applicant's address is on at least one of the documents;
- the applicant's signature is on at least one of the documents;
- the applicant's date of birth is on at least one of the documents; and
- a recognisable photograph of the applicant is on at least one of the documents.

5.6.2.1 General

The EOI documentation[15] presented **must** consist of:

- one Category A document establishing evidence of commencement of identity in Australia; AND
- one Category B document establishing a linkage between Identity and Person (photo and signature) OR
- two Category B documents establishing a linkage between Identity and Person (photo and signature); AND
- one Category C document establishing the operation of that identity in the community.

5.6.2.2 High Assurance

The EOI documentation presented **must** consist of:

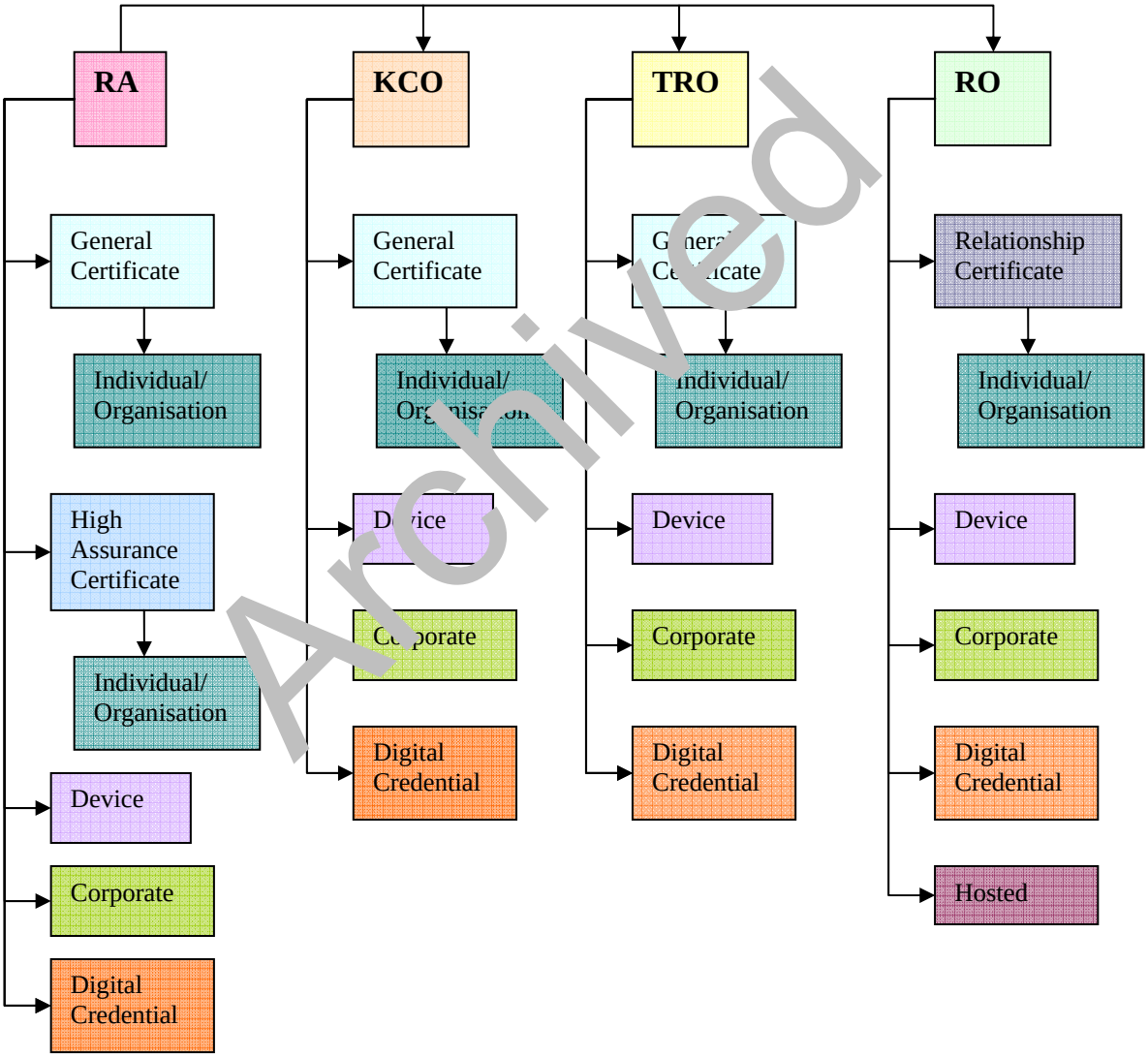
- one Category A document establishing evidence of commencement of identity in Australia, AND
- one Category B document establishing a linkage between Identity and Person (photo and signature); AND
- one Category C document establishing the operation of that identity in the community; OR
- one Category A document establishing evidence of commencement of identity in Australia; AND
- two Category B documents establishing a linkage between Identity and Person (photo and signature).

Further details on the Formal Identity Verification Model can be found in the General Category Guidebook.

[15] For a list of the documentation refer to the Gatekeeper EOI Policy.

6 ORGANISATIONS THAT PERFORM IDENTITY VERIFICATION

The following Organisations perform the verification of the identity of Subscribers using different Gatekeeper EOI Models:



6.1 Relationship Organisation

A Relationship Organisation is an Organisation that has an established relationship with its Clients which it and the COI considers adequate as the basis for requesting or authorising the issuance of digital certificates.

At its simplest form the Relationship Organisation will request/authorise the issuance of a Relationship Certificate to its Clients who will use their Relationship Certificates to conduct Transactions with the Relationship Organisation (i.e. the COI comprises the Relationship Organisation and its Clients).

While in principle the relationship concept could be expected to lose its meaning outside the context of a specific Organisation-customer relationship, it is possible to extend that relationship within a wider COI (i.e. multiple Organisations and Relying Parties).

A COI may be established where:

- there is a pre-existing working relationship between the members of the COI;
- members of the COI can demonstrate a shared benefit to all parties;
- members of the COI can ensure that there are no adverse privacy or security implications arising from the relationship;
- members of the COI have assessed whether the relationship established between the Relationship Organisation and the client is acceptable for it to trust; and
- members of the COI have the ability to negotiate the terms and conditions under which the broader community will operate.

6.2 Known Customer Organisations

A Known Customer Organisation is an Organisation which has been Listed under Gatekeeper as having complied with the Gatekeeper Known Customer Organisation Listing Requirements.

A Known Customer Organisation is able to request/authorise the issuance of digital certificates in the General Category to Individuals and Organisations.

6.3 Threat and Risk Organisation

A Threat and Risk Organisation is an Organisation which has been Listed under Gatekeeper as having undergone an independent Threat and Risk Assessment of its internal EOI processes.

A Threat and Risk Organisation is able to request/authorise the issuance of digital certificates in the General Category to Individuals and Organisations.

6.4 Registration Authority

A Registration Authority (RA) is a Gatekeeper Accredited Service Provider that performs independent third party Formal Identity Verification (i.e. face-to-face EOI check) in relation to the Registration of applicants for digital certificates. A RA only conducts formal face-to-face EOI checks and submits the application and EOI documentation to the CA for certificate production and issuance.

A RA will usually operate under a Services Agreement with the issuing CA and its practices and procedures will be set out in its Operations Manual and will be consistent with the issuing CA's Certification Practices Statement. Under the Framework, services from Gatekeeper Accredited RAs will be required only under the General and High Assurance Categories.

Where a RA performs some of the functions of a CA (e.g. Key Generation), it must seek Gatekeeper accreditation as a Registration Authority Extended Services (RAES).

7 SUPPLEMENTARY CERTIFICATES

The Framework will enable Agencies and Service Providers to develop and implement X.509 v3 compliant Supplementary Certificates. This will enable an Agency to specify elements of a digital certificate that will meet its particular requirements including the use of extensions within the Certificate Profile.

Supplementary Certificates are able to be deployed across all categories of the Framework but are likely to be more commonly applied within the Special Category where a digital certificate is needed to meet the specific requirements of an Agency or a COI. Requests for deployment of Supplementary Certificates in all Gatekeeper digital certificate categories will be considered by the Gatekeeper Competent Authority on a case-by-case basis through the approval of the relevant Certificate Policy.

The following sections of the Framework outline four possible types of Supplementary Certificates.

7.1 Device Certificate

Device Certificates are used to identify and authenticate applications or devices (including a process or service) that are owned and/or operated by an Organisation.

An individual within the Organisation (usually the Certificate Manager) will still be required to take responsibility for the digital certificate; however, he/she will not be named in the digital certificate.

Further information on the Device Certificate can be found in the Device Certificate Policy Specification.

7.2 Digital Credential Certificate

A Digital Credential Certificate combines a digital certificate with verified credentials of an Individual or Organisation.

A Digital Credential Certificate could contain:

- attributes that are lifelong characteristics of the Key Holder, for example, professional qualifications required for lawyers and engineers;
- applications in regulatory fields where qualifications/occupation/authority are paramount rather than identity, for example, e-conveyancing; and
- authority and access elements.

Further details on the Digital Credential Certificate will be available when the Digital Credential Certificate Policy Specification is developed[16].

7.3 Corporate Certificate

A Corporate Certificate enables an Organisation to be identified in the digital certificate without requiring an individual's name or the specific name of the device on which the digital certificate is installed to be included in the Subject Distinguished Name field of the Certificate.

This distinguishes the Corporate Certificate from the Gatekeeper Device Certificate which requires the device to be accurately identified. This has the effect of providing greater flexibility for an Organisation to determine the manner in which the digital certificate is being deployed and allows the Organisation to determine which of its employees will have access to the digital certificate.

A Corporate Certificate could be issued to an Organisation and the same digital certificate used by a number of employees within that Organisation. It would be applicable where an Agency needs to know only that a Transaction was initiated by a specific Organisation and where the identity of the individual undertaking the Transaction is not critical.

It will also be possible for the Corporate Certificate to contain additional user specified information so that Corporate Certificates can be issued to Organisations for use by its officers/employees holding particular positions (e.g. General Manager) or performing particular roles (e.g. Occupational Health and Safety Representative).

Such additional information provides further assurance to Relying Parties. Since the Corporate Certificate is not bound to a person, it does not require the Corporate Certificate to be revoked when an individual moves on from a position or ceases to perform a particular function.

[16] This Policy Specification is under development.

Further details on the Corporate Certificate can be found in the Corporate Certificate Policy Specification.

7.4 Hosted Certificate

Hosted Certificates are digital certificates introduced to facilitate take-up of PKI by small businesses.

Hosted Certificate deployment typically occurs when a Subscriber contracts with an external Organisation (the Host) specifically for the purpose of the storage, management and use of digital certificates and associated signing and encryption Keys on its behalf.

The Hosted Certificate will have the same functionality as other digital certificates issued by Gatekeeper Accredited/Recognised CAs, but in addition it will also authenticate the identity of the Host and the device or application on which the digital certificates and Keys are installed in accordance with the relevant Hosted Certificate Policy (CP). As with all PKI deployments it is an Agency's responsibility to conduct a business risk assessment prior to implementing Hosted Certificate.

The Hosted Certificate will provide a Relying Party with the necessary evidentiary trail back to the Subscriber that originated a specific transaction.

Further details on the Hosted Certificate can be found in the Hosted Certificate Policy Specification.

8 CERTIFICATE LIFE AND KEY PAIRS

Certificate life under Gatekeeper (as it will be in any PKI implementation internationally) is derived from the strength of the cryptographic algorithm that is used to generate the Certificate's Keys. In Australia, the Defence Signals Directorate is responsible for determining the maximum life of a digital certificate (derived from estimates of the length of time it would take to "break" the Key).

DSD has advised that, in Australia as is generally the case around the world, the maximum life of a 2048 bit Key is defined to 10 years. Most digital certificates currently issued to end-users under Gatekeeper employ 1024 bit Keys and have a maximum two year life. The Framework offers the scope to increase the life of end-user digital certificates provided that it can be accommodated within the maximum 10 year lifespan.

As an alternative to varying Certificate life (and noting the upper limit imposed by the length of the Root CA Key) consideration may also be given to increasing Key lengths. The rationale is that a longer key will require a longer period of time to "break" thus effectively increasing the life of the digital certificate.

8.1 Key Pairs

Under the Framework, digital certificates can be issued with either single or dual Key Pairs. Dual Key Pair digital certificates are issued with two Private and Public Key Pairs - one Key Pair for authentication/signing and the other Key Pair for confidentiality/ encryption respectively. Single Key Pair digital certificates are issued with one Public and Private Key Pair that may be used for either authentication or confidentiality.

While dual Key Pairs remain the preferred method of Certificate issuance under the Framework, CAs can issue digital certificates that operate with a single Key Pair.

The Certificate Policy must clearly specify whether the digital certificate is issued with a single Key Pair or dual Key Pairs and must specify the Key Usage in the Certificate Profile and note:

- escrowing or backing up private keys used to store data in an encrypted format - if the key is required to recover the data later – is supported;
- escrow or backup of private keys used for non repudiation is inappropriate;
- if key escrow is required then the key should not be used for nonRepudiation;
- if there is a need to store encryption keys (for data recovery), then use of a separate encryption-only key is preferred;
- where there is a need to sign data within a session to provide a binding record of a transaction, then use of a separate signing key may also be required;
- where a private key is used only to authenticate a certificate holder and negotiate a session key, then use of a key which allows both authentication and confidentiality is accepted.
- the marking of the Key Usage extension should be both Critical and Mandatory for:
  - Certificates issued with a single Key Pair
  - The signing / authentication certificate in a dual Key Pair deployment
- the marking of the Key Usage extension may be marked Mandatory and Non-Critical for
  - the confidentiality certificate in a dual Key Pair deployment

9 GATEKEEPER ADMINISTRATION

9.1 Accreditation Process

Implementation of the Framework is characterised by a streamlined administration process with the rationalisation of the Gatekeeper suite of Approved Documents and removal of the requirement for evaluation of certain aspects of a Service Provider's business and operational models.

The new processes also allow issues associated with liability limitations, caps and exclusions to be addressed by commercial negotiation between the CA and Agency (in compliance with the Gatekeeper Core Obligations Policy and consistent with the Australian Government's "A guide to limiting supplier liability in ICT contracts with Australian Government agencies" at http://www.industry.gov.au/Industry/InformationandCommunicationsTechnologiesICT/Pages/LimitingSupplierLiabilityinICTContracts.aspx.

Administration of the Framework will be characterised by:

- a reduced paperwork burden on Service Providers in terms of both the number of Approved Documents and streamlined change management processes;
- a shorter Gatekeeper Head Agreement that complements commercial Service Agreements with Agencies;
- removal of the requirement for a Service Provider's business model to be evaluated; and
- no requirement for evaluation of a Service Provider's legal documentation (i.e. CP, CPS, end user agreements) for digital certificates issued within the Special Category.

9.2 Gatekeeper Accreditation Certificate

The Gatekeeper Accreditation Certificate (GAC) is an electronic certificate issued by the Gatekeeper Competent Authority to CAs that have been granted Gatekeeper accreditation. A Relying Party will be able to decide whether to accept a digital certificate issued by a Service Provider based on whether or not the CA is Gatekeeper Accredited (evidenced by the GAC).

While the GAC CA is not regarded as a Root CA it will represent the top trust point in the Gatekeeper PKI hierarchy. The GAC CA will be Gatekeeper Accredited.

9.3 Core Obligations Policy and Liability Guideline

The Core Obligations Policy, developed under the Framework, clearly identifies the obligations of each participant within the Gatekeeper PKI domain (CA, RA, RAES, KCO, TRO, RO, Subscriber and Relying Party). Compliance with the Core Obligations Policy is mandatory across all categories of the Framework.

Within the Core Obligations Policy, guidance is provided in relation to liability limitation that is consistent with the Australian Government's "A guide to limiting supplier liability in ICT contracts with Australian Government agencies" available at http://www.industry.gov.au/Industry/InformationandCommunicationsTechnologiesICT/Pages/LimitingSupplierLiabilityinICTContracts.aspx.

9.4 Interoperability

The broad, yet well defined nature of the Framework will enhance the ability of digital certificates to be used across PKI domains, enhancing the scope for e-commerce both nationally and internationally.

From an international perspective, interoperability (cross-recognition/cross certification) will occur predominantly with respect to those digital certificates issued within the General Category under the Formal Identity Verification model.

10 SUCCESS FACTORS

The following factors are considered critical to the effective implementation and on-going administration of the Gatekeeper PKI Framework.

Interoperability	The Framework must enable digital certificates issued by Gatekeeper Accredited/Recognised CAs to be accepted (subject to appropriate internal risk assessments and enrolment processes as required) across Agencies and businesses and be recognisable by (and thus interoperable with) national and international PKI domains.
Obligations/Liability	The Framework must apportion obligations fairly placing liability on those parties within a PKI that are responsible for managing the risks associated with those obligations.
Costs	The operation of the Framework results in a reduction in ongoing operating costs to all participants. The transition to the Framework may cause additional costs for Agencies and Service Providers. The transitional arrangements should endeavour to quantify these costs and ensure that they are not such as to offset longer-term benefits.
Complexity	The Framework must offer users a straightforward means of acquiring and using digital certificates. It should also provide potential Service Providers with explicit documented requirements for Gatekeeper accreditation. To the maximum extent possible, the Framework should be based on documented national and international standards to ensure general understanding and acceptance. Where such standards are not available, Finance will facilitate their development.
Enablers (e.g. technology – signing interfaces)	The Australian Government should ensure that appropriate enablers are available to facilitate take-up of digital certificates by the broader community. These include the provision of freely available interfaces (such as the Common Signing Interface) as well as proposals for the possible development of Australian Standards for Known Customer EOI and further refinement to the protective security requirements for PKI entities.
Security	The Framework should ensure that Australian Government security standards (as reflected in ISM and the PSM) are maintained by all Gatekeeper Accredited/Recognised Service Providers. Further development of the Framework should also proceed in the knowledge that possible future government policies in relation to money laundering and identity fraud are likely to have a major impact.
Privacy	The Framework must ensure that Service Providers maintain their compliance with the *Privacy Act 1988* (Cth).
Fitness for Purpose	Digital certificates issued by Gatekeeper Accredited Service Providers should be fit for the purposes for which they are issued.
Risk Assessment	Operation of the Framework must be soundly based on accepted risk assessment parameters (i.e. AS/NZS 4360). Participants should be encouraged to assess formally the risks associated with proposed Transactions and use digital certificates that match the resultant risk profiles.
Gatekeeper	Where Agencies determine that PKI is the appropriate authentication mechanism for external purposes, digital certificates must be issued by a Gatekeeper Accredited/Recognised Service Provider and comply with Gatekeeper Policies and Criteria.