Australian Government
Digital Transformation Office

Gatekeeper Public Key Infrastructure Framework

V 3.1 – December 2015

Digital Transformation Office

© Commonwealth of Australia 2015

This work is copyright. Apart from any use as permitted under the *Copyright Act 1968* and the rights explicitly granted below, all rights are reserved.

Licence

With the exception of the Commonwealth Coat of Arms and where otherwise noted, all material presented in this document is provided under a Creative Commons Attribution Non-Commercial 3.0 Australia licence. To view a copy of this licence, visit: http://creativecommons.org/licenses/by-nc/3.0/au/

You are free to copy, communicate and adapt the work for non-commercial purposes, as long as you attribute the authors. Except where otherwise noted, any reference to, reuse or distribution of all or part of this work must include the following attribution:

Gatekeeper PKI Framework: © Commonwealth of Australia 2015.

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the *It's an Honour* website (http://www.itsanhonour.gov.au)

Contact us

Enquiries or comments regarding this document are welcome at:

Gatekeeper Competent Authority
C/O Director, Trusted Digital Identity Team
Digital Transformation Office
Email: authentication@dto.gov.au

Executive summary

Information and Communication Technologies (ICT) are transforming the way we work and are driving change in many industries. Governments around the world understand their decisions can assist or impede businesses to adjust to an increasingly digital economy and society. The Commonwealth Government, as a key user of ICT has an important role to play in developing and supporting the infrastructures required to support this digital transformation.

Trust is an essential element in the provision of government digital services. Agencies and their customers alike need to establish a degree of trust or confidence about the identity of parties to digital services. Where an agency may be providing online access to services and benefits it will need to ensure that these are being delivered to the correct customer. As such, authentication policies, standards and technologies are essential to ensure trust can be established and maintained between agencies and their customers.

Since 1999, the Commonwealth Government has developed and maintained the Gatekeeper Public Key Infrastructure (PKI) Framework. The Framework is an accreditation program which ensures a whole-of-government outcome that delivers integrity, interoperability, authenticity and trust between agencies and their customers.

The Gatekeeper PKI Framework includes a suite of policies, standards and procedures that govern the use of digital certificates in Government for the authentication of agencies and their customers. This document is the third edition of the Framework and outlines the requirements Service Providers need to obtain and maintain for Gatekeeper accreditation and recognition.

I recommend the Gatekeeper PKI Framework to anyone interested in providing digital services to Government.

Gatekeeper Competent Authority

November 2015

Contents

Figures

1. Framework Management

1.1 Change Log

This is the third edition of the Gatekeeper PKI Framework (The Framework). This release includes a number of changes from the 2009 edition, including:

- A reduction in red tape through the consolidation of the previous suite of 33 Gatekeeper policies and guides into 5 documents.
  - Removed Certification Authority (CA) and Validation Authority (VA) Operations Manuals as Approved Documents.
  - Consolidated the National eAuthentication Framework (NeAF), Assurance Framework and previous Gatekeeper glossaries into one document.
- All relevant requirements of the Australian Government Information Security Manual (ISM) and Australian Government Protective Security Policy Framework (PSPF) into the Gatekeeper PKI Framework.
- Alignment with the Privacy Act 1988 and Australian Privacy Principles (APPs).
- Defining LOA requirements for Registration Authorities (RA), CAs and VAs which map to the *National Identity Proofing Guidelines* (NIPG)[1] and NeAF.[2]
- Removed digital certificate classes and registration models.
  - The former accreditation and listing arrangements have been replaced with Levels of Assurance (LOAs) – 1 through 4.
  - The 'Special' and 'General' categories and Gatekeeper Listings have been mapped to LOAs.
  - Relationship Organisations have been replaced with Registration Authority requirements which map to LOAs.

1.2 Review Date

This document will be reviewed regularly and updated in line with changes to relevant government policies.

1.3 Conventions

The Gatekeeper Framework adopts the following conventions:

- **MUST** indicates a mandatory requirement that a Service Provider is required to satisfy in order to obtain or maintain Gatekeeper Accreditation.
- **MUST NOT** indicates something that if practiced, exercised or implemented will breach a Gatekeeper Accreditation requirement.
- **SHOULD** indicates something that is not mandatory but is recommended which either supports a mandatory obligation or is considered best practice.
- **COMPLIANCE** is an assessment outcome which indicates a Service Provider satisfies a mandatory requirement of Gatekeeper Accreditation.

[1] For further information see [NIPG] at section 13 of the Gatekeeper PKI Framework

[2] For further information see [NeAF] at section 13 of the Gatekeeper PKI Framework

- **NON COMPLIANCE** is an assessment outcome which indicates a Service Provider does not meet a mandatory requirement of Gatekeeper Accreditation.
  - Service Providers seeking Gatekeeper Accreditation are to meet all mandatory requirements listed in the Framework unless they obtain a waiver for a NON COMPLIANCE from their Accreditation Authority.
  - Service Providers may seek a waiver for a NON COMPLIANCE with any mandatory requirement listed in the Framework from their Accreditation Authority. The Accreditation Authority for Agencies is their Agency Head or their delegated representative. For commercial organisations the Accreditation Authority is a person or committee with the necessary authority to grant such a waiver.
  - Service Providers seeking a waiver for a NON COMPLIANCE with any mandatory requirement listed in the Framework MUST document the justification for NON COMPLIANCE, alternative mitigation measures to be implemented (if any) and an assessment of the residual security risk.
  - Service Providers MUST retain a copy of all decisions to grant a waiver for a NON COMPLIANCE with any mandatory requirement listed in the Framework.

1.4 Terms and Definitions

The terms and definitions used in this document are defined in the Identity and Access Management Glossary [IAMG][3].

1.5 Transition Arrangements

Existing accredited Service Providers will have two years from the date the Framework is published to align their Approved Documents with the new mandatory requirements. Service Provider's computing capabilities will be required to meet the new mandatory requirements as part of the next appropriate technical refresh. Throughout the transition period Service Provider's will need to ensure their Approved Documents adequately reflect the computing capabilities their Gatekeeper accredited service.

Gatekeeper Applicants not accredited as of the Framework's publication date are required to meet all mandatory requirements listed in the Framework.

1.6 Advice on this Framework

Advice on the Framework or suggestions for amendment is welcome at:

Gatekeeper Competent Authority
C/O Director, Trusted Digital Identity Team
Digital Transformation Office
Email: authentication@dto.gov.au

1.7 Document Structure

This document is structured in the following manner:

- Section 2 describes the Framework's aims and purpose;
- Section 3 introduces the concepts of e-authentication and assurance levels;

[3] For further information see [IAMG] at section 13 of the Gatekeeper PKI Framework

- Section 4 describes Public Key Infrastructure, the elements of a PKI and the security services provided by a PKI;
- Section 5 describes the Gatekeeper Framework, its structure, the accreditation process and accreditation requirements;
- Section 6 lists the Core Obligations;
- Section 7 lists the Gatekeeper Mandatory Security Requirements;
- Section 8 defines operational evaluations to be carried out by Service Providers;
- Section 9 describes the mandatory Gatekeeper documentation to be developed and maintained;
- Sections 10 through 12 describe the additional requirements specific for Registration Authorities, Certification Authorities and Validation Authorities respectively;
- Section 13 lists the sources referenced in the Framework;
- Annex A provides indicative guidance on appropriate cryptographic algorithms and key lengths;
- Annex B lists the Root CA, Subordinate CA and Subscriber Certificate Profiles.

2. Aims and Purpose

The Gatekeeper PKI Framework is a whole-of-government suite of policies, standards and procedures that governs the use of PKI in Government for the authentication of individuals, organisations and non-person entities (NPE) – such as devices, applications or computing components.

Gatekeeper operates within a broader policy environment (Figure 1) which supports the Government's agenda for the digital economy.

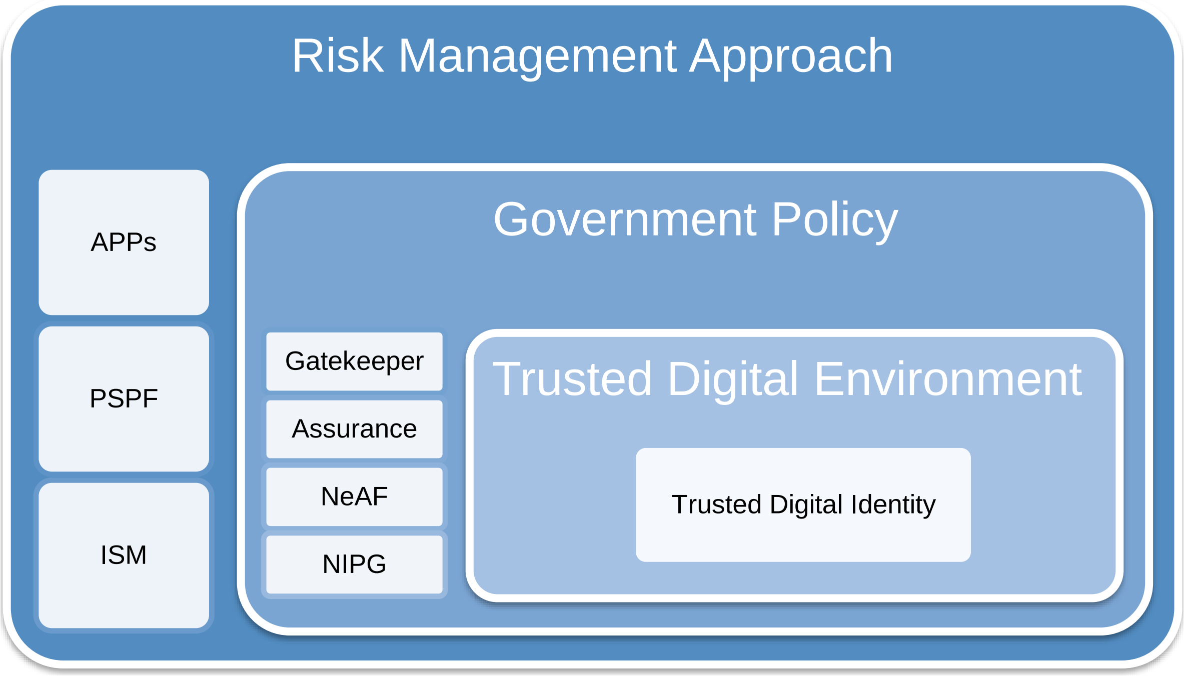
The Digital Transformation Office is responsible for conducting the Gatekeeper Accreditation Process and making recommendations to the Gatekeeper Competent Authority. The Gatekeeper Competent Authority is responsible for decisions in relation to the accreditation of Service Providers.

The Framework is mandatory for agencies using PKI to authenticate their clients through the use of digital keys and certificates issued by Gatekeeper accredited Service Providers. Gatekeeper ensures a whole-of-government outcome that delivers integrity, interoperability, authenticity and trust for Service Providers and their Subscribers. Gatekeeper aligns the application of PKI to the way government agencies interact with their customers.

Organisations operating independently of government can also become Gatekeeper accredited Service Providers. The requirements outlined in this document apply equally to government agencies and to organisations that choose to obtain and maintain Gatekeeper accreditation.

The Framework aligns with international standards such as the Canada Institute of Chartered Accountant's *WebTrust Program for Certification Authorities* and the European Telecommunications Standards Institute's *Electronic Signature and Infrastructure Policy requirements for Certification Authorities issuing public key certificates*.

Figure 1 Policy Environment



The *Australian Government Protective Security Policy Framework* and *Australian Government Information Security Manual* provide the overarching security policy context for Gatekeeper. Within the risk-based approach set out in these policy frameworks, Service Providers **MUST** satisfy Gatekeeper-specific standards and benchmarks. Additionally, Gatekeeper benchmarks enable the accreditation process to be undertaken against agreed criteria ensuring that all Service Providers operate to the same standards.

Privacy of personal information is a fundamental consideration under the Gatekeeper PKI Framework. All Service Providers are required to comply with the *Privacy Act 1988 (Cth)* and the *Australian Privacy Principles*.

The *National Identity Proofing Guidelines*, *National e-Authentication Framework* and *Third Party Identity Services Assurance Framework* (Assurance Framework) support the Gatekeeper PKI Framework. Standardised and transparent approches to identity proofing, electronic authentication and identity service provisioning are achieved through the use of these frameworks and guidelines which, together with Gatekeeper assist with establishing trusted online identities.

3. Electronic Authentication

3.1 Electronic Authentication

Electronic authentication (e-authentication) is the process of establishing confidence in a claimed digital identity presented to an online resource.

High-risk systems, applications and transactions require stronger forms of authentication that more accurately confirm the entity's digital identity as being who they claim to be, as opposed to low-risk applications where the confirmation of the digital identity is not as important from a risk perspective.

Determining the appropriate authentication approach requires a balance between the level of risk that is acceptable and the desired user experience.

Authentication is not the same as authorisation, which addresses the permissions or privileges granted to a Subscriber when accessing systems, or online services. The issue of authorisation is not addressed in the Framework.

3.2 The e-Authentication Process

Before an individual can authenticate to an online service, they must first be enrolled and issued a digital credential.

The first step of e-authentication requires an Applicant to undergo an evidence of identity check. This identity verification process is typically called 'identity proofing'. The usual sequence of events for registration is as follows:

- An Applicant applies to a Registration Authority to become a Subscriber of a Credential Service Provider[4] (CSP);
- The RA verifies the identity of the Applicant; and
- The RA associates the Applicant with the identity record created. This association may occur within or on behalf of an organisation. (On successful identity proofing the Applicant will be considered a Subscriber of the CSP.)

Once the individual's identity has been verified to a defined level of confidence or assurance, the RA will request a credential from the CSP on behalf of the Subscriber. This process is called 'credentialing'. A typical sequence of events for credentialing is as follows:

- The RA will send the CSP a registration confirmation message.
- The CSP will generate and register the credential and associate it with the Subscriber.
- The CSP will issue the credential to the Subscriber.
- The CSP will manage the credential throughout its lifecycle.

The Subscriber will then be able to use the credential to subsequently authenticate to online services.

[4] In the context of the Gatekeeper PKI Framework a CSP is a Certification Authority.

3.3 Levels of Assurance

Assurance levels are used to describe the level of importance of getting e-authentication right and the resultant level of robustness of the required solution. An identity-focused risk assessment is undertaken at the initial design or redesign stage of an information system to determine the required LOA. The degree of rigour required in the registration process and type of credential needed to deliver the required LOA are outputs of this assessment. For further information see [NeAF] at section 13 of this document.

Each assurance level also describes the degree of confidence that a Relying Party has that a Subscriber has presented a claim to an online resource that represents their identity (for example, these claims may be contained within a credential such as a digital certificate).

To determine the appropriate LOA in the entity's claimed or asserted identity, NeAF provides guidance for e-authentication stakeholders on assessing the potential risks and identifies measures to minimise their impact. In this context, the strength, or assurance level of an e-authentication solution is dependent on:

1. The strength of the registration process;
2. The strength of the underlying security characteristics of the credential, and
3. The degree of confidence the relying party has that the entity using the credential is the same entity to whom the credential was issued.

The five NeAF assurance levels are:

- Level 0: No confidence in the claimed or asserted identity.
- Level 1: Little confidence in the claimed or asserted identity.
- Level 2: Some confidence in the claimed or asserted identity.
- Level 3: High confidence in the claimed or asserted identity.
- Level 4: Very high confidence in the claimed or asserted identity.

In the context of Gatekeeper LOA 0 and LOA 1 are merged to provide a 4 tier approach to e-authentication. Further information on Gatekeeper LOAs is located in Section 5.

4. Public Key Infrastructure

4.1 Public Key Infrastructure

Public Key Infrastructure is the combination of policies, practices and technologies that enables users of an insecure online service, such as the Internet, to authenticate their identity and to securely and privately exchange information with a third party through the use of Public Key Cryptography.

Public Key Cryptography or asymmetric cryptography is a class of cryptographic algorithms which require two separate keys – one which is public and one which is private. Although different, the keys are mathematically linked in a manner which enables actions performed by one key to be verified with the other. For example, a public key can be used to encrypt information or to verify a digital signature, whereas a private key can be used to decrypt information or to create a digital signature.

The central function of a PKI is the provision of digital keys and certificates that can authenticate the identity of an individual, organisation or NPE. It also provides the management, distribution and revocation of those digital certificates.

4.2 Security Services provided by a PKI

Depending on the operating model, the use of PKI may provide authentication, integrity, non-repudiation and confidentiality security services for online transactions, with assurance of:

- Confidentiality of the information or information channel (where required),
- Validity of the information conveyed and received (data integrity),
- Identity of the parties involved in the transactions (authentication),and
- Accountability of commitments or actions (non-repudiation).

These features are provided with some or all of the following systems:

- A digital certificate (or public key certificate) is an electronic data structure signed by a CA which identifies the Subscriber and business entity (if appropriate) the Subscriber represents. It binds the Subscriber to a key pair by specifying the public key of the key pair. It also contains any other information required by the Certificate Profile for that digital certificate. The key pair can be generated in either software or hardware. Software-based digital certificates are typically stored on Subscriber's computer hard drives or group drives whereas hardware-based digital certificates are typically stored in hardware form (e.g. USB and smartcards) which connect to Subscriber's computers and networks.
- A digital signature is a cryptographic technique that applies a mathematical algorithm to a document based on a certificate holder's private key. This creates a unique seal which is inherently difficult[5] to forge and that can be checked by a Relying Party to confirm that the document or file has not been altered or interfered with.
- A digital signing certificate is a combination of the above two systems.
- An encryption scheme is a cryptographic technique that applies a mathematical algorithm to messages and information in such a way that only authorised parties can read it. Using an encryption scheme turns a message or information into an unreadable mix of characters known as ciphertext. This is done with the use of an encryption key, which specifies how the message or information is to be encoded. Unauthorised parties will be able to view the unreadable data but will be unable to determine anything about the message contents. The intended recipient of the

[5] It is computationally infeasible to forge a digital signature which uses a Government approved cryptographic algorithm.

information is able to decode the ciphertext using a decryption algorithm and a secret or private decryption key, which only they have access to.

- A digital encryption certificate is a combination of a digital certificate and an encryption scheme.
- Service (or device) certificate authentication is where only one party involved with an online service is required to manage the authenticated session. This means only one party needs a digital certificate but both parties must be able to execute PKI cryptography. Most web servers and browsers have this functionality built in. Service authentication is typically used where many remote parties need to connect securely to a web server. General uses of service authentication include Internet banking, logging into social media sites and accessing online government services.
- Client certificate authentication is necessary when transacting parties require mutual authentication. This typically occurs when higher levels of confidence are required in the identity of the transacting parties and requires both parties to verify their identity with a digital certificate. Client authentication is generally used when accessing or transacting highly sensitive information (e.g. corporate banking data, medical records or information relating to national security).

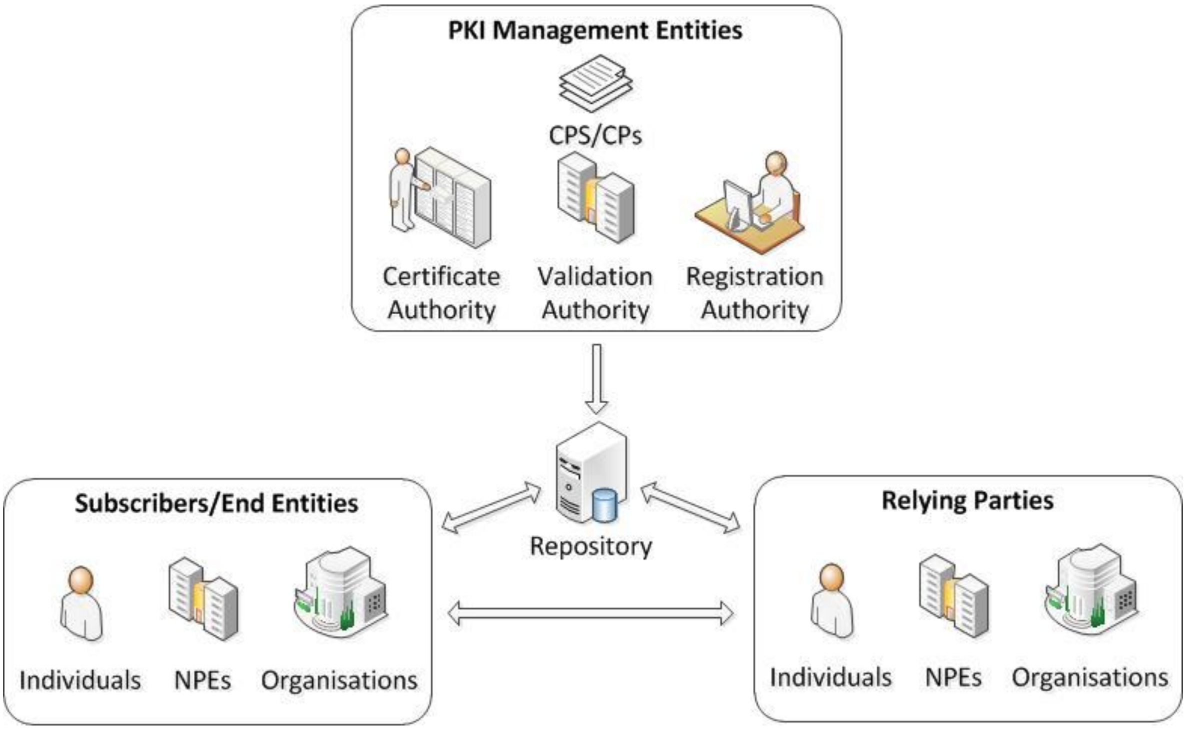
4.3 Elements of Public Key Infrastructure

A PKI may consist of the following components including:

- Registration Authority undertakes functions such as identity proofing and processes requests for new digital certificates, requests for renewal of digital certificates and requests for revocation of digital certificates.
- Certification Authority creates and issues digital certificates and Certificate Revocation Lists (CRLs). Digital certificates issued by the CA are digitally signed which binds the subject name (i.e. Subscriber identity) to the public key.
- Repository is a generic term used to describe any capability which may store or make available certificates, CRLs or Online Certificate Status Protocol (OCSP) services to Subscribers. CRLs and OCSP services are maintained by CAs or VAs which contain the validity and currency status of certificates.
- Validation Authority is a PKI management entity which can be used to check the validity and currency of digital certificates. A VA is typically used when certificate generation and certificate status services are managed by separate Service Providers. For example, the Australian Taxation Office issues *AUSKey* digital certificates to Subscribers and the Department of Industry *VANGuard* trust broker provides the service to validate the status of *AUSKey* digital certificates.
- Subscriber also referred to as an End-Entity, Certificate Holder, or Key Holder that is issued a key pair and certificate which, depending on the rules outlined in its associated Certification Practice Statement (CPS) and Certificate Policy (CP), can be used to authenticate to online resources or digitally sign or encrypt electronic documents. Subscribers are responsible for protecting the private key and not disclosing it to others. Subscribers can be individuals, organisations or NPEs.
- Relying Party receives, verifies and accepts digital certificates.
- Certificate Policy consists of a set of rules that indicate the applicability of the certificate to a particular community and/or class of applications with common security requirements.
- Certification Practices Statement (CPS) describes the rules and operating practices which the CA will follow when providing digital certificate services. It may include a description of service offerings, detailed procedures for certificate life-cycle management, operational information, legal obligations and financial liabilities.
- Subscriber (and Relying Party) Agreement is a document that explains the rights and obligations of a Subscriber (and Relying Party) in accepting, using and protecting a digital certificate and key pair. The person responsible for the certificate and key pair issued to devices or NPEs will typically sign the Subscriber Agreement.

The following diagram (Figure 2) shows the relationships between these components. The arrows indicate the flow of digital certificates and certificate status information.

Figure 2 Elements of a PKI



5. Gatekeeper PKI Framework

5.1 Purpose

The Gatekeeper PKI Framework is a whole-of-government suite of policies, standards and procedures that governs the use of PKI in Government for the authentication of individuals, organisations and NPEs – such as devices, applications or computing components.

Gatekeeper Accreditation supports PKI hierarchies that:

- issue digital keys and certificates to Subscribers interacting in open environments (e.g. the Internet),
- issue digital keys and certificates to Subscribers participating in closed environments (e.g. communities of interest), or
- issue digital keys and certificates to Subscribers that interact in both open and closed environments (e.g. hybrid communities).

Digital keys and certificates issued by Gatekeeper accredited Service Providers are suitable for use with the following types of transaction:

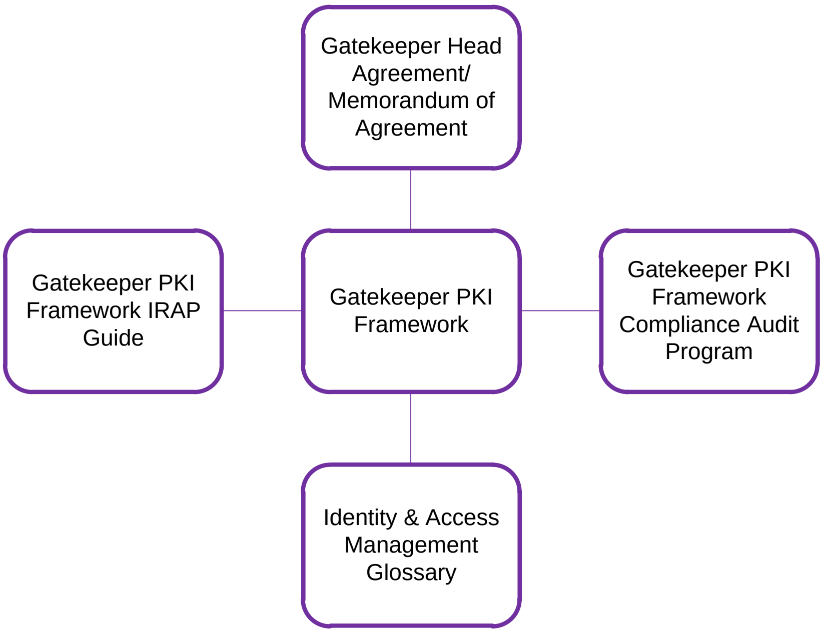
- business-to-individual (B2I),
- business-to-business (B2B),
- business-to-government (B2G),
- government-to-government (G2G),
- individual-to-government (I2G) and
- Individual-to-individual (I2I).

Registration Authorities, Certification Authorities and Validation Authorities are the Service Providers accredited under the Gatekeeper PKI Framework.

5.2 Framework Structure

The Framework is built around five core documents as shown in Figure 3 below.

Figure 3 Framework Structure


Gatekeeper Head Agreement/ Memorandum of Agreement
Gatekeeper PKI Framework IRAP Guide
Gatekeeper PKI Framework
Gatekeeper PKI Framework Compliance Audit Program
Identity & Access Management Glossary

- The *Gatekeeper PKI Framework* (this document) defines the minimum requirements for Service Providers to obtain and maintain Gatekeeper accreditation.
- The *Gatekeeper PKI Framework IRAP Guide* provides Information Security Registered Assessors Program (IRAP) Assessors with a guide to assess the implementation of security controls and practices by Service Providers.
- The *Gatekeeper Head Agreement/Memorandum of Agreement* is the formal agreement between the Digital Transformation Office (DTO) (on behalf of the Commonwealth) and the Service Provider. This agreement establishes the conditions under which the Service Provider is accredited and outlines what is required in order for the Service Provider to maintain its Gatekeeper Accreditation.
- The *Gatekeeper PKI Framework Compliance Audit Program* provides guidance to auditors and Service Providers on the scope and conduct of the compliance assessment required under the Framework.
- The *Identity and Access Management Glossary* contains a list of acronyms and associated terms related to the Framework. The Glossary also contains all related terms associated with the NeAF and Assurance Framework.

5.3 Levels of Assurance

Similar to the NeAF and NIPGs, the Gatekeeper Framework is designed around the concept of assurance levels. The four Gatekeeper assurance levels are:

Level	Description	RA	CA	VA
1	No or little confidence	In the registration processes used to identify the claimant.	In the credentialing processes used to manage digital certificates throughout their lifecycle.	In the certificate validation services provided.
2	Some confidence			
3	High confidence			
4	Very high confidence			

5.4 Commonwealth Government Requirements

Commonwealth Government policy does not mandate the use of PKI for authenticating online transactions. Use of PKI for authentication purposes is purely a business decision for Commonwealth agencies. However, Commonwealth agencies wishing to use digital certificates to authenticate their clients are required to use Gatekeeper accredited Service Providers. This has been Commonwealth Government policy since July 1999.

5.5 Risk Management

Gatekeeper operates within a risk management context and aligns with the Australian Government's Protective Security Policy Framework and the Australian Government Information Security Manual.

- The PSPF defines a series of core policies and mandatory requirements to which applicable Commonwealth agencies and bodies must demonstrate their compliance. These requirements cover protective security governance, personnel security, information security and physical security.
- The ISM is designed to assist Australian government agencies in applying a risk-based approach to protecting their information and systems. The ISM includes a set of information security controls that, when implemented, will help agencies meet their compliance requirements for mitigating security risks to their information and systems.

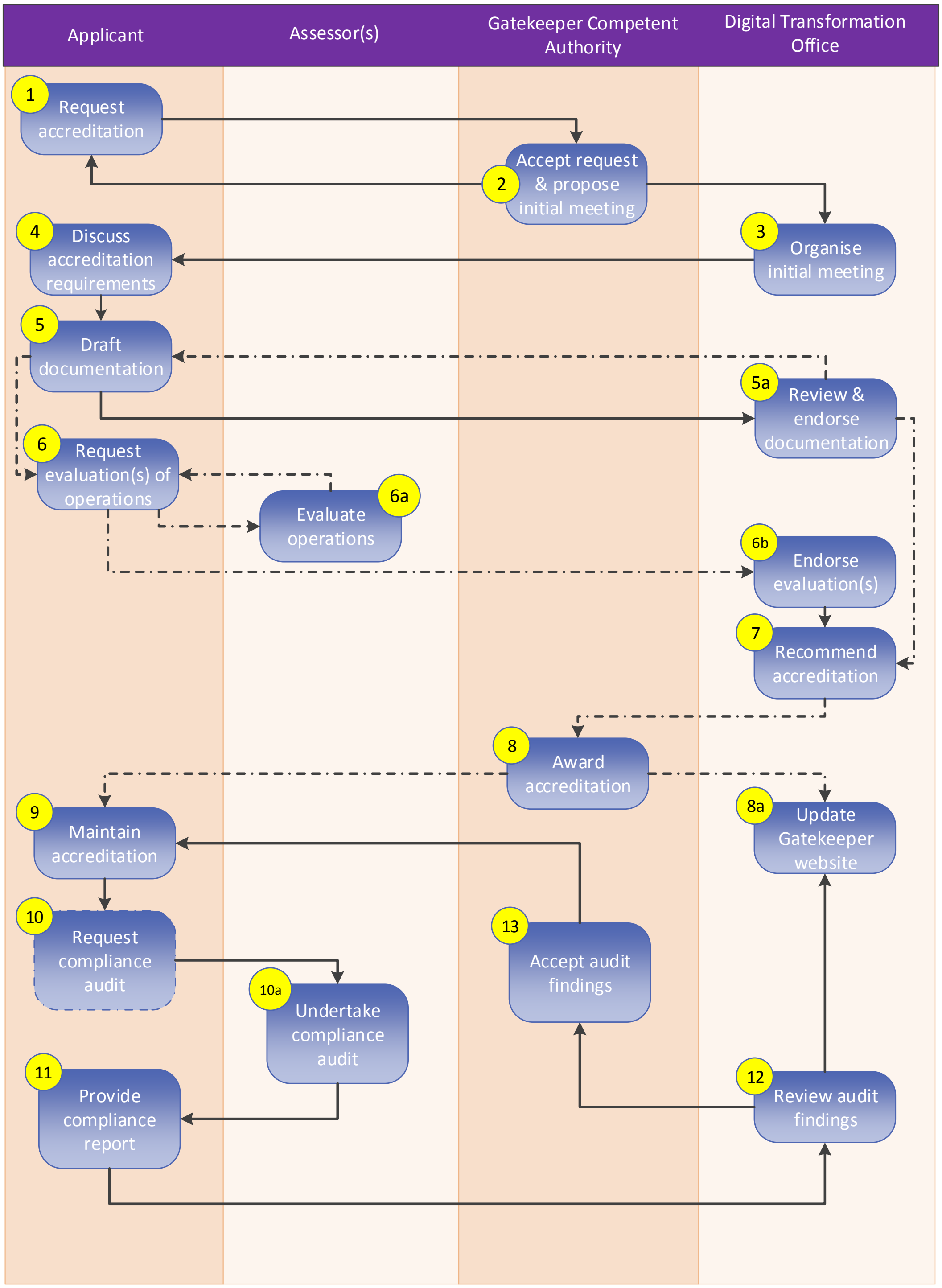
Service Providers who apply for Gatekeeper Accreditation undergo rigorous evaluation of all aspects of their PKI operations, including compliance with Australian Government protective security requirements outlined in the PSPF and ISM.

5.6 Accreditation Process

5.6.1 Obtain and maintain accreditation

The Accreditation Process is outlined in Figure 4 below:

Figure 4 Accreditation Process


Applicant
Assessor(s)
Gatekeeper Competent Authority
Digital Transformation Office
1 Request accreditation
2 Accept request & propose initial meeting
3 Organise initial meeting
4 Discuss accreditation requirements
5 Draft documentation
5a Review & endorse documentation
6 Request evaluation(s) of operations
6a Evaluate operations
6b Endorse evaluation(s)
7 Recommend accreditation
8 Award accreditation
8a Update Gatekeeper website
9 Maintain accreditation
10 Request compliance audit
10a Undertake compliance audit
11 Provide compliance report
12 Review audit findings
13 Accept audit findings

- The Applicant submits a formal request in writing to the Gatekeeper Competent Authority (authentication@dto.gov.au) seeking Gatekeeper accreditation to a defined LOA as a RA, CA, VA or a combination of these.
- The Gatekeeper Competent Authority formally responds to the request and an initial meeting with the Applicant is convened to discuss the accreditation process.
- The Applicant drafts its documentation and organises independent evaluations of its operations for compliance with Gatekeeper Policies and Criteria. For Service Providers this includes an IRAP evaluation and a Privacy Impact Assessment (PIA).
- The Digital Transformation Office commences its evaluation of the Applicant's documents for compliance with Gatekeeper Policies and Criteria. Once the DTO is satisfied the documents meet the requirement for Gatekeeper Accreditation they are considered Approved Documents for the purposes of accreditation.
- Following successful completion of the evaluation process, the DTO recommends accreditation to the Gatekeeper Competent Authority and a Head Agreement or Memorandum of Agreement between the DTO and the Service Provider is negotiated and signed and a Certificate of Accreditation is presented to the Service Provider. The Agreement will include the list of Approved Documents.
- The Service Provider's details are listed on the DTO website.
- The Service Provider maintains accreditation by providing its services in accordance with its Approved Documents.
- The Service Provider submits itself to an annual compliance audit on the anniversary of their accreditation date in accordance with the Gatekeeper Compliance Audit Program. The audit findings are provided to the Digital Transformation Office. The Gatekeeper Competent Authority will accept the audit findings (and work with the Service Provider to resolve any identified issues) and the DTO website will be updated to reflect the Service Provider's accreditation status.

5.6.2 Gatekeeper Accreditation Disclaimer

GATEKEEPER ACCREDITATION DISCLAIMER

The Gatekeeper Competent Authority is responsible for ensuring that the accreditation process is conducted with due care and in accordance with published Gatekeeper Criteria and Policies.

The Gatekeeper Competent Authority is not liable for any errors and/or omissions in the final Approved Documents, which remain the responsibility of the accredited Service Provider.

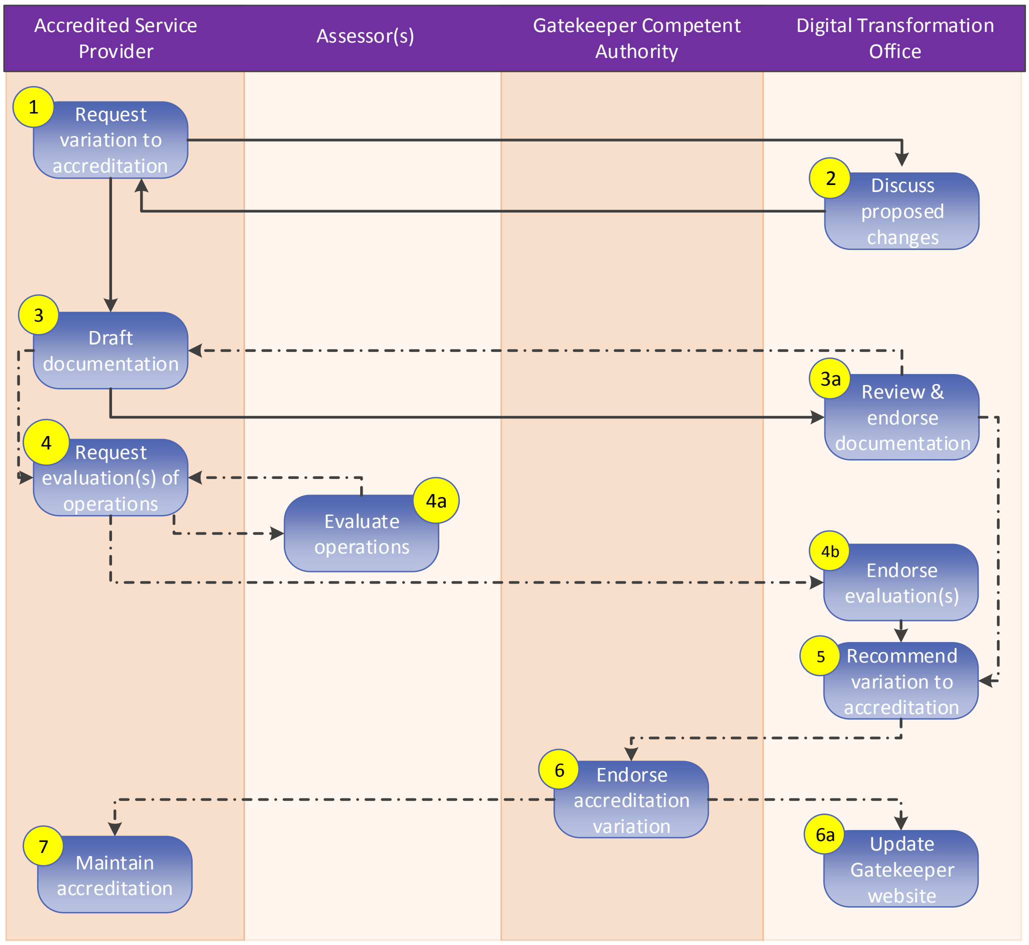
The Digital Transformation Office is not responsible and cannot be held liable for any loss of any kind in relation to the use of digital keys and certificates issued by a Gatekeeper accredited Service Provider. By granting a Service Provider Gatekeeper Accreditation the Digital Transformation Office makes no representation and gives no warranty as to the:

- Accuracy of any statements or representations made in, or suitability of, the Approved Documents of a Gatekeeper accredited Service Provider;
- Accuracy of any statement or representation made in, or suitability of, the documentation of a Service Provider in a Gatekeeper recognised PKI domain; or
- Standard or suitability of any services thereby provided by any Subscriber or Relying Party or application.

5.6.3 Variation to accreditation

The accreditation variation process is outlined in Figure 5 below:

Figure 5 Accreditation Variation Process


Accredited Service Provider
Assessor(s)
Gatekeeper Competent Authority
Digital Transformation Office
1
Request variation to accreditation
2
Discuss proposed changes
3
Draft documentation
3a
Review & endorse documentation
4
Request evaluation(s) of operations
4a
Evaluate operations
4b
Endorse evaluation(s)
5
Recommend variation to accreditation
6
Endorse accreditation variation
6a
Update Gatekeeper website
7
Maintain accreditation

- The accredited Service Provider advises the Digital Transformation Office of a need to vary the terms of its accreditation. A typical variation is a change to an Approved Document as a result of an adverse audit finding.
- The Digital Transformation Office will discuss the proposed changes with the Service Provider.
- Depending on the nature of the proposed change, Approved Documents may need to be revised and submitted to the Digital Transformation Office for review and endorsement. Similarly, for proposed changes with possible significant impacts, the Digital Transformation Office may direct the Service Provider to organise independent evaluations (i.e. IRAP, PIA) of its operations.
- Following successful completion of the documentation review and possible operational evaluations, the Digital Transformation Office will recommend to the Gatekeeper Competent Authority that a variation to the accredited Service Provider's Head Agreement or Memorandum of Agreement be granted.
- Once granted, the details of the variation will be reflected on the Digital Transformation Office website.
- The accredited Service Provider will maintain its accreditation by providing its services in accordance with its Approved Documents and undertake annual compliance audits as shown in step 10 of Figure 4.

5.7 Accreditation Requirements

Gatekeeper Accreditation provides participants in Gatekeeper PKI deployments with assurance as to the operational competence and protective security of the organisations responsible for the registration, generation, issuance, storage and management of digital keys and certificates.

Ongoing compliance with Gatekeeper Policies, Criteria and Approved Documents is mandatory for Service Providers to achieve and maintain Gatekeeper Accreditation. The following table lists compliance obligations and to whom they apply.

Requirement	RA	CA	VA	Section
Gatekeeper Policies				
Core Obligations Policy	X	X	X	6
Gatekeeper Mandatory Security Requirements	X	X	X	7
Identity Proofing	X			10.6 & 10.7
Gatekeeper Criteria				
Privacy Impact Assessment	X	X	X	8.2
Information Security Registered Assessors Program	X	X	X	8.1 See [IRAP]
Annual Compliance Audits	X	X	X	See [GCAP]
Gatekeeper Approved Documents				
Information Security Policy	X	X	X	9.2
Protective Security Risk Review	X	X	X	9.3
Security Risk Management Plan	X	X	X	9.4
System Security Plan	X	X	X	9.5
Physical and Environmental Security Plan	X	X	X	9.6
Personnel Security Plan	X	X	X	9.7
Incident Response Plan	X	X	X	9.8
Cryptographic Key Management Plan	X	X	X	9.9
Disaster Recovery and Business Continuity Plan	X	X	X	9.10
Certification Practice Statement		X		11.1
Certificate Policy		X		11.1
Operations Manual	X			11.3

5.8 Mandatory Requirements

The Framework requires compliance with the following regimes:

Regulatory Regime	Reference
Protective Security Policy Framework	[PSPF]
Agency personnel security management guidelines	[APSG]
Australian Government personnel security management protocol	[AGPSP]
Information security management guidelines – Australian Government classification system	[ISMG1]
Information security management guidelines – Management of aggregated information	[ISMG2]
Physical security management guidelines – Physical security of ICT equipment, systems and facilities	[PSMG1]
Physical security management guidelines – Security zones and risk mitigation control measures	[PSMG2]
Protective security governance guidelines – Business impact levels	[BIL]
Securing government business – Protective security guidance for executives	[SGB]
Australian Government Information Security Manual	[ISM]
Archives Act 1983	[AA1983]
National Archives of Australia – Administrative Functions Disposal Authority	[AFDA]
Gatekeeper PKI Framework Information Security Registered Assessors Program Guide	[IRAP]
Gatekeeper PKI Framework Compliance Audit Program	[GCAP]
ITU-T X.500 (10/12) Information technology – Open Systems Interconnect – The Directory: Overview of concepts, models and services	[X.500]
National e-Authentication Framework	[NeAF]
National Identity Proofing Guidelines	[NIPG]
Privacy Act 1988	[PA1988]
Privacy Amendment (Enhancing Privacy Protection) Act 2012	[PA2012]
RFC3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework	[RFC3647]
RFC 5280 Internet X.509 Public Key Infrastructure and Certificate Revocation List (CRL) Profile	[RFC5280]
Telecommunications Cabling Provider Rules 2000	[TCPR]

5.9 Recommended Standards and Guides

To assist with meeting the compliance obligations of the Framework Applicants **SHOULD** consider the following standards and guides:

Recommended Standards and Guides	Reference
Australian National Audit Office Business Continuity Management – Building resilience in public sector entities	[ANAO]
AS/NZS 5050:2010 Business Continuity – Managing disruption-related risk.	[ANZ5050]
AS/NZS ISO 31000:2009 Risk Management Principles and Guidelines	[ANZ2009]
Australian Standard HB 167:2006 Security Risk Management	[HB167]
CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates	[CABF]
Canada Institute of Chartered Accountants, 2011, Trust Service Principles and Criteria for Certification Authorities, Version 2.0, Canada Institute of Chartered Accountants, Canada	[WebTrust]
European Telecommunications Standards Institute, Electronic Signature and Infrastructure (ESI); Policy requirements for certification authorities issuing public key certificates, (ETSI TS 102 O42)	[ETSI]
Federal Information Processing Standard (FIPS) 140–2 Security Requirements for Cryptographic Modules	[FIPS]
ISO/IEC 27005:2011 Information Technology – Security Techniques – Information Security Risk Management	[27005]
National Institutes of Standards and Technology Special Publication 800–57 Part 1 Recommendation for Key Management Part 1: General (Revision 3)	[800–57]
Office of the Australian Information Commissioner Data Breach Notification	[DBN]
Office of the Australian Information Commissioner Guide to Undertake Privacy Impact Assessments	[PIA]
RFC 6960 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP	[RFC6960]
RFC 5019 The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments	[RFC5019]
Third Party Identity Services Assurance Framework	[TPISAF]

6. Core Obligations

6.1 Core Obligations Policy

This policy sets out the Core Obligations as determined by the Gatekeeper Competent Authority in relation to the application, generation, issuance and on-going management of digital keys and certificates issued by a Service Provider in Gatekeeper PKI deployments.

The Gatekeeper Competent Authority will not grant Gatekeeper Accreditation to a Service Provider that seeks through its documentation to avoid or exclude liability for breaches of its Gatekeeper Core Obligations as specified in the following sections.

6.2 Liability

Liability is the legal obligation to compensate another party when an obligation has been breached.

The source of the obligation can be a contract, a common law obligation, a statutory obligation or an equitable obligation. Liability will follow when an obligation of the kind that is spelt out in the following sections of this policy is breached.

6.3 Service Providers

Service Providers **MUST**:

- Be registered with the Australian Business Register (ABR) and maintain a current Australian Business Number (ABN);
  - Loss of ABR registration will result in termination of the Service Provider's Gatekeeper Accreditation.
- Meet all relevant third party evaluation requirements as set out in the Framework including:
  - Undertake an assessment of all PKI-related systems using a registered IRAP Assessor listed on the Australian Signals Directorate (ASD) IRAP website. Unless otherwise directed by the Gatekeeper Competent Authority this is a one-off evaluation as per step 6a in the accreditation process listed at Figure 4;
- Undertake a PIA for all PKI-related systems that collect, process, store or disclose personal information. Unless otherwise directed by the Gatekeeper Competent Authority this is a one-off evaluation as Section 5.6.1 in the accreditation process;
- Be physically located within Australia and provide services from within Australia[6];
- Develop, maintain and provide PKI services in accordance with their Approved Documents;
- Undergo an annual Gatekeeper Compliance Audit;
- Document their compliance with Gatekeeper Core Obligations in their legal documentation such as CPS, CP, Subscriber and Relying Party Agreements (where relevant) or into other Approved Documents submitted for approval by the Gatekeeper Competent Authority; and
- Implement the mandatory *Top 4 Strategies to Mitigate Targeted Cyber Intrusions* as detailed in the ISM, comprising:
  - Application Whitelisting,

[6] Any remote connections to the PKI environment must also occur from within Australia.

  - Patch Applications,
  - Patch Operating Systems, and
  - Restrict Administrative Privileges
- Adopt a risk-management approach and implement alternative security controls for:
  - Technologies which lack available software to enforce the mandatory controls, and
  - Scenarios or circumstances which prevent enforcement of the mandatory controls.
- Develop and maintain a change management process which at a minimum defines the actions to be undertaken before and after standard, urgent and emergency changes are implemented.

Service Providers **SHOULD** implement the recommended ISM controls that relate to the Top 4 Strategies. Although not considered mandatory these controls are best practice and complement the Top 4 Strategies. Service Providers may take a risk-based approach to implementing these controls, as is the norm for a risk based approach to protective security.

6.4 Certification Authority

6.4.1 Standards

A CA **MUST** ensure all:

- Digital certificates conform to the Request for Comment (RFC) 5280 format;
  - Annex B lists the Root CA, Subordinate CA and Subscriber Certificate Profiles to be used; and,
  - Any digital certificate extensions that do not conform to RFC 5280 **MUST** be marked non-critical).
- CRLs conform to the X.509 v2 profiles as described in RFC5280;
- OCSP responses conform to RFC5019 (if OCSP is supported); and
- CPS and CPs conform to the document framework as described in RFC3647.

A CA **SHOULD** ensure all OCSP responses conform to RFC6960.

6.4.2 Certification Practice Statement / Certificate Profile

A CA **MUST**:

- Perform digital certificate lifecycle operations in a manner which is compliant with its CPS;
- Display the Gatekeeper Accreditation Disclaimer (Section 5.6.2) in their CPS and CPs;
- Ensure the security objectives identified in the Information Security Documentation are reflected in the CPS and CPs;
- Ensure the CP under which each digital certificate is issued clearly specifies the Key Usage within the Certificate Profile;
- Ensure all CPS and CPs undergo a legal evaluation by an authorised legal assessor from the *Gatekeeper Legal Evaluation Panel*[7] and,
- Make available as much of its published CPS and CPs as necessary to allow a relying party to make an informed decision on trust.

[7] For further information see [GLEP] at section 13 of the Gatekeeper PKI Framework

A CA **MUST NOT**:

- Escrow or backup Subscriber private keys used for non-repudiation; and
- Mark the Key Usage Extension in Subscriber digital certificates as both Critical and Mandatory.

6.4.3 Staff Training

A CA **MUST**:

- Provide all personnel performing information verification duties with skills-training that covers basic PKI knowledge, authentication and vetting policies and procedures, including the CPS and CA CP; and,
- Maintain records of such training and ensure that personnel maintain a skill level that enables them to perform such duties satisfactorily.

6.4.4 Certificate Generation

A CA **MUST,** when generating a digital certificate, ensure that:

- The certificate information provided to it by an RA has been accurately transcribed into the digital certificate;
- All other certificate information it generates itself is accurate; and,
- The digital certificate contains all the elements required by the certificate profile contained in the CP.

6.4.5 Key Generation

A CA **MUST** ensure that each key pair to be used with a certificate can work.

6.4.6 Possession of Private Key

A CA **MUST** take all reasonable actions to ensure that the Subscriber is in control of the activation data and private key(s) corresponding to the public key identified in the digital certificate before the private key can be used.

6.4.7 Private Key Use

A CA **MUST** ensure the Root CA Private Keys are not used to sign certificates except in the following cases:

- Self-signed certificates to represent the Root CA itself;
- Certificates for Subordinate CAs (and Cross Certificates);
- Certificates for infrastructure purposes (e.g. administrative role certificates, internal CA NPE certificates, and OCSP certificates); and
- Certificates issued solely for the purpose of testing products with certificates issued by the Root CA.

6.4.8 Certificate Repository

A CA **MUST**:

- In accordance with the ITU-T Recommendation [X.500] and [RFC3647], generate, maintain and make available a list of revoked digital certificates in a manner accessible by all potential Relying Parties using standard protocols and technologies to enable them to verify, in a timely manner, the currency of a particular digital certificate;

- Operate and maintain its CRL and, if supported, OCSP capabilities with resources sufficient to provide a response time of ten seconds or less under normal operating conditions; and
- Ensure the location where certificates and CRLs are published has restricted write access so that only valid certificates and CRLs issued by approved PKI entities can be published by an authorised person or process.

6.4.9 Certificate Revocation

A CA **MUST**:

- Provide a process for Subscribers to request revocation of their own certificates. The process **MUST** be described in the CPS and relevant CP;
- Provide Subscribers and Relying Parties with clear instructions for reporting suspected Private Key compromise, certificate misuse, or other types of fraud or inappropriate conduct relating to certificates. The CA **MUST** publically disclose the instructions through a readily accessible online means accessible by Subscribers and Relying Parties;
- Ensure the prompt revocation of a digital certificate in accordance with the requirements of the CP under which it was issued and in accordance with the requirements outlined in the *CA Requirements* section for the specific LOA of the accreditation; and,
- Revoke a certificate if one or more of the following occurs:
  - The Subscriber notifies the CA that the original certificate request was not authorised and does not retrospectively grant authorisation;
  - The CA obtains evidence that the Subscriber's private key corresponding to the public key in the certificate suffered a key compromise or no longer complies with the requirements outline in the CP;
  - The CA obtains credible evidence any certificate it has issued has been misused;
  - The CA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or other contractual or terms of use agreements that apply;
  - The CA is made aware that the certificate was not issued in accordance with its CP or CPS;
  - The CA determines that any of the information appearing in the certificate is inaccurate or misleading;
  - The CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the certificate; and
  - The CA obtains credible evidence of a possible compromise of a Subordinate CA's private key.

6.4.10 Key Archive and Recover

The protection of a Key Archive **MUST** be commensurate with the protection afforded to the CA and **MUST** implement network filtering, identity segmentation and security controls corresponding to the CAs LOA.

Private keys **MUST** be encrypted within the Key Archive Store to mitigate attacks where the store is stolen and accessed offline.

Any instance of key recovery **MUST** be logged, audited and alerted so they can be reviewed by the appropriate authority.

THE CA **MUST** only archive encryption keys to enable recovery of encrypted data. Keys used for digital signature or authentication **MUST NOT** be archived.

6.4.11 CA Termination

In the event that a Gatekeeper accredited CA terminates its operations whether voluntary or involuntary it **MUST NOT**:

- Enter into any new contracts with customers, or renew existing contracts; or,
- Enter into any new Subscriber Agreements, or renew existing Subscriber Agreements.

In the event that a Gatekeeper accredited CA terminates its operations whether voluntary or involuntary it **MUST**:

- Make arrangements to novate to another Gatekeeper accredited CA or terminate all Subscriber agreements that were entered into in accordance with the relevant CP;
- Give notice to the Gatekeeper Competent Authority and all associated parties (e.g. Subscribers, Relying Parties) advising them of its intention to terminate its contracts with them, the termination to be effective in accordance with the terms of the relevant contract;
- Continue to provide the services, in particular the maintenance of a CRL or other listing of revoked digital certificates in accordance with the contractual arrangements it has with agencies, and any relevant Approved Documents which include arrangements to accommodate significant interruptions in the provision of the service; and
- Co-operate with the Digital Transformation Office and other Service Providers, to achieve a seamless and secure migration of the agencies and Subscribers to a new Gatekeeper accredited CA.

6.4.12 Logging

The CA **MUST** record at least the following events:

- CA key lifecycle management events, including:
  - Key generation, backup, storage, recovery, archival and destruction; and,
  - Cryptographic device lifecycle management events.
- CA and Subscriber lifecycle management events, including:
  - Certificate requests, renewal requests, re-key requests, revocation requests and revocation actions;
  - Acceptance and rejection of certificate requests; and,
  - Issuance of certificates.
- Generation of CRLs and if supported, OCSP entries
- Security events, including:
  - Successful and unsuccessful PKI system access attempts;
  - Changes to rights assigned to privileged accounts;
  - System outages, hardware failures and other anomalies;
  - Firewall and router activities; and,
  - Entries to and exits from the CA facility.

Logs **MUST** be retained for a minimum of seven years after action is completed in accordance with the [AA1983] and [AFDA].

6.5 Registration Authority

6.5.1 Identity Proofing

A RA **MUST:**

- Take all reasonable actions to verify[8] the accuracy and sufficiency[9] of identity documentation, including any client application forms and supporting documentation received;
- Ensure the accurate recording and secure transmission of all relevant certificate information to the relevant CA;
- Ensure the secure storage of all retained Applicant and Subscriber information in accordance with the requirements of its Approved Documents; and
- In the event that an error is identified in the identity proofing process that gives rise to uncertainty as to the identity of a particular Subscriber, promptly notify the CA that generates the digital certificate of the error and request the revocation of the digital certificate.

6.5.2 Staff Training

- A RA **MUST** provide all personnel performing identity verification duties with skills-training that covers basic PKI knowledge, authentication and vetting policies and procedures, including CPS and CA CP.

6.5.3 RA Termination

In the event that a Gatekeeper accredited RA terminates its services, whether voluntary or involuntary it **MUST NOT** conduct any new registration activities for Applicants or Subscribers.

In the event that a Gatekeeper accredited RA terminates its services, whether voluntary or involuntary it **MUST** give notice to the Gatekeeper Competent Authority and all CAs with whom it has a relationship in accordance with the terms of the relevant contract.

6.6 Validation Authority

6.6.1 Standards

A VA **MUST** be able to process:

- Digital certificates which conform to the X.509 v3 format and CRLs which conform to the X.509 v2 profiles as described in RFC5280; and,
- OCSP responses which conform to RFC5019

A VA **SHOULD** be able to process OCSP responses which confirm to RFC6960.

[8] Verify means to determine or test the accuracy of identity documentation submitted by an Applicant (including photographic evidence) and including signature verification in accordance with:

- The procedures set out in the RA's Approved Documents;
- The relevant CP and CPS; and
- The service agreement between the RA and CA.

[9] Sufficiency means that the documents submitted by an Applicant in relation to the particular certificate being requested satisfy the Gatekeeper Identity Proofing Policy

6.6.2 Staff Training

A VA **MUST**:

- Provide all personnel performing information verification duties with skills-training that covers basic PKI knowledge, authentication and vetting policies and procedures, including the CPS and CA CP; and,
- Maintain records of such training and ensure that personnel maintain a skill level that enables them to perform their duties satisfactorily.

6.6.3 Certificate Repository

A VA **MUST**:

- In accordance with [X.500] and [RFC3647], maintain and make available a list of revoked digital certificates in a manner accessible by all potential Relying Parties using standard protocols and technologies to enable them to verify, in a timely manner, the currency of a particular digital certificate; and,
- Operate and maintain its repository capabilities which house CRL (and optionally OCSP) services with resources sufficient to provide a response time of ten seconds or less under normal operating conditions.

6.6.4 VA Termination

In the event that a Gatekeeper accredited VA terminates its operations, whether voluntary or involuntary it **MUST NOT** conduct any certificate validation activities for Relying Parties

In the event that a Gatekeeper accredited VA terminates its operations, whether voluntary or involuntary it **MUST** give notice to the Gatekeeper Competent Authority and all associated parties (e.g. CAs) advising them of its intention to terminate its contracts with them, the termination to be effective in accordance with the terms of the relevant contract.

6.7 Subscriber

A Subscriber **MUST**:

- Ensure that all information provided, and any representations made to a Gatekeeper accredited RA are complete and accurate;
- Perform any additional requirements as specified in the CP under which the digital certificate was issued;
- Take all reasonable measures to protect their private key and activation data from compromise and take all necessary precautions to prevent loss, disclosure, modification or unauthorised use of their private key;
- Promptly notify the relevant CA in the event that they consider or suspect there has been a compromise of their private key; and
- Promptly notify the relevant RA in the event that they consider the identity information provided by them is or may be incorrect.

6.8 Relying Party

A Relying Party **SHOULD**:

- Verify that the digital certificate is current and has not been revoked or suspended, in a manner specified in the CPS and CP under which the digital certificate was issued;
- Verify that the digital certificate is being used within the limits specified in the CPS and CP under which the digital certificate was issued; and
- Promptly notify the relevant CA in the event that they consider or suspect there has been a compromise of a Subscriber's private key.

7. Gatekeeper Mandatory Security Requirements

Service Providers' are required to comply with the Gatekeeper Mandatory Security Requirements, which have been derived from the PSPF mandatory obligations described in the Securing Government Business – Protective Security Guidance for Executives10 The following table describe the Gatekeeper Mandatory Security Requirements and their mapping to the PSPF mandatory obligations.

	Gatekeeper Mandatory Security Requirements	**PSPF Reference Mandatory Obligations**
Gatekeeper 1: **Training**	Service Providers **MUST** provide all staff (ongoing and non-ongoing), including contractors:	
	• With sufficient information and security awareness training to ensure they are aware of, and meet their protective security requirements.	GOV–1
	• Guidance on Sections 70 and 79 of the Crimes Act 1914, section 91.1 of the Criminal Code 1995, the Freedom of Information Act 1982 and the Australian Privacy Principles contained in the Privacy Amendment (Enhancing Privacy Protection) Act 2012 including how this legislation relates to their role.	GOV–9
Gatekeeper 2: **Appointment of security officials**	To fulfil their security obligations, Service Providers **MUST** appoint:	
	• An Information Technology Security Adviser (ITSA) or equivalent position or title to advise senior management on the ICT security of the Service Provider's PKI and related systems.	GOV–2
	• An Information Technology Security Manager (ITSM) or equivalent position or title responsible for the Service Provider's day-to-day performance of protective security functions.	GOV–2
	• Service Providers MUST ensure that the ITSA and ITSM have detailed knowledge of organisation specific protective security policy, protocols and protective security requirements in order to fulfil their protective security responsibilities.	GOV–3
Gatekeeper 3: **Security Policies**	Service Providers **MUST**:	
	• Prepare a Security Risk Management Plan (SRMP) as part of their Information Security Documentation to manage their security risks. This plan MUST be regularly reviewed and updated or revised when changes in risks and the Service Provider's operating environment dictate;	GOV–4

[10] For further information see [SGB] at section 13 of the Gatekeeper PKI Framework

	Gatekeeper Mandatory Security Requirements	**PSPF Reference Mandatory Obligations**
	• Develop their own protective security policies and procedures to meet their specific business needs;	GOV–5
	• Develop policies and procedures to assess and manage the ongoing suitability for employment of their personnel;	PERSEC–2
	• Ensure that security vetting is only applied where necessary and the level required as determined by the outcomes of their Protective Security Risk Review (PSRR);	PERSEC–2
	• Identify designated Positions of Trust within their Organisation that require access to security classified assets or information;	PERSEC–3
	• As part of their Information Security Documentation develop and implement an Information Security Policy (ISP).	INFOSEC–1
Gatekeeper 4: **Security Risk Management Plan**	Service Providers **MUST:**	
	• Adopt a risk management approach to cover all areas of protective security activity across their Organisation. This approach **SHOULD** be in accordance with the Australian Standard for Risk Management AS/NZS ISO 31000:2009 *Risk management – Principles and guidelines* and the *Australian Standard HB 167:2006 Security Risk Management*.	GOV–6
	• Prepare a SRMP to manage their security risks.	INFOSEC–2
	The SRMP **MUST** be reviewed or revised annually or sooner when changes occur in threats, risks or the Service Provider's PKI operating environment	GOV–4
Gatekeeper 5: **Audit**	Service Providers **MUST**:	
	• Undertake an annual Gatekeeper PKI Framework Compliance Audit against their approved documentation, and	
	• Report the outcomes of the Gatekeeper PKI Framework Compliance Audit to the Gatekeeper Competent Authority. The report MUST state any areas of non-compliance, including details on measures taken to address such non-compliances.	GOV–7
Gatekeeper 6: **International obligations**	Service Providers **MUST**, where required by a Commonwealth Agency, adhere to any provisions concerning the security of people, information and assets contained in multilateral or bilateral agreements and arrangements to which they agency is a party	GOV–10

	Gatekeeper Mandatory Security Requirements	PSPF Reference Mandatory Obligations
Gatekeeper 7: **Disaster Recovery and Business Continuity Plan**	Service Providers **MUST** establish a Disaster Recovery and Business Continuity Plan (DRBCP) to provide for the continued availability of critical services and assets, and of other services and assets when warranted by a threat and risk assessment. The Plan **SHOULD** be consistent with the *Australian National Audit Office Better Practice Guide on Business Continuity Management*.	GOV–11
Gatekeeper 8: **Security vetting**	Service Providers **MUST** ensure that employees, contractors and temporary staff who require access to PKI resources and Subscriber/Relying Party information:	PERSEC–1
	• Are authorised to have access, have had their identities established, have undertaken appropriate security training; and hold a Security Clearance appropriate to their job requirements.	PERSEC–5
	• Security clearances **MUST** be sponsored by an Australian Government agency and undertaken by the Australian Government Security Vetting Agency (AGSVA).	PERSEC–6
Gatekeeper 9: **Personnel security**	Service Providers **MUST** have in place personnel security aftercare arrangements. Individuals holding security clearances should advise the AGSVA of any significant change in personal circumstance that may impact on their continuing suitability to access security classified resources.	
	Service Providers **MUST** have separation policies and procedures for departing clearance holders, which include a requirement to:	PERSEC 9
	• Inform AGSVA when a clearance holder leaves their ongoing employment or contract engagement with the Service Provider; and	
	• Advise AGSVA of any security concerns.	
Gatekeeper 10: **Information classification**	Service Providers **MUST**:	
	• Implement policies and procedures for the security classification and protective control of information assets (in electronic and paper-based formats) which match their value, importance and sensitivity;	INFOSEC–3
	• Document and implement operational procedures and measures to ensure information, ICT systems and network tasks are managed securely and consistently, in accordance with the level of required security. This includes implementing the mandatory Top 4 Strategies to Mitigate Targeted Cyber Intrusions as detailed in the ISM.	INFOSEC–4

	Gatekeeper Mandatory Security Requirements	PSPF Reference Mandatory Obligations
	• Have in place control measures based on business requirements and assessed/accepted risks for controlling access to all information, ICT systems, networks (including remote access), infrastructures and applications. Access control rules must be consistent with business requirements and information classification as well as legal obligations;	INFOSEC–5
	• Have in place security measures during all stages of ICT system development, as well as when new ICT systems are implemented into the operational environment. Such measures must match the assessed security risk of the information holdings contained within, or passing across, ICT networks infrastructures and applications;	INFOSEC–6
	• Ensure that information security measures for all information processes, ICT systems and infrastructure comply with any legislative or regulatory obligations under which they operate.	INFOSEC–7
Gatekeeper 11: **Physical Security**	Service Providers **MUST**:	
	• Provide clear direction on and address, physical security through the development and implementation of a Physical and Environmental Security Plan;	PHYSEC–1
	• Ensure they fully integrate protective security early in the process of planning, selecting, designing and modifying their facility(s);	PHYSEC–3
	• Ensure that any proposed physical security measure or activity does not breach relevant employer occupational health and safety obligations; and	PHYSEC–4
	• Implement a level of physical security measures that minimises or removes the risk of ICT equipment and information being made inoperable or inaccessible, or being accessed, used or removed without appropriate authorisation.	PHYSEC–6
	Service Providers **SHOULD** have in place policies and procedures to:	PHYSEC–2
	• Identify, protect and support employees under threat of violence, based on a threat and risk assessment of specific situations. In certain cases, Service Providers may have to extend protection and support to family members and others;	
	• Report incidents to management, human resources, security and law enforcement authorities, as appropriate;	
	• Provide information, training and counselling to employees; and	
	• Maintain thorough records and statements on reported incidents.	

	Gatekeeper Mandatory Security Requirements	PSPF Reference Mandatory Obligations
Gatekeeper 12: **Security responsiveness**	Service Providers **MUST** develop plans and procedures to move up to heightened security levels in case of emergency and increased threat. The Australian Government may direct its Service Providers to implement heightened security levels.	PHYSEC–7

8. Operational Evaluations

8.1 Information Security Registered Assessors Program

The ASD is the Commonwealth authority on information and cyber security with a mandate to provide technical advice and assistance to secure Australian government information. Cyber and information security is a top national security priority for government. Cyber intrusions on government, critical infrastructure and other information networks are a real threat to Australia's national security and national interests.

The Information Security Registered Assessors Program is an ASD initiative to provide high quality ICT assessment services aimed at maximising the security of Australian government information and associated ICT systems.

IRAP Assessors must demonstrate a strong understanding of Australian government information security policies through a combination of recognised ICT and audit qualifications, experience, tailored training and the successful completion of an IRAP entrance examination. Successful applicants who become registered IRAP Assessors are able to provide ICT assessment services to government.

IRAP Assessors are endorsed by ASD to conduct independent assessment of any system, network or gateway, for compliance with the ISM, PSPF and other Australian government guidance.

The IRAP Assessor will conduct an assessment through the following activities:

- System documentation review,
- Onsite evidence gathering,
- Interviews with key staff, and
- Evidence gathering against ISM and PSPF requirements.

> Service Providers **MUST** undertake an assessment of all PKI-related systems using a registered IRAP Assessor listed on the ASD IRAP website.

8.2 Privacy Impact Assessment

The *Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Privacy Amendment Act)* made many significant changes to the *Privacy Act 1988*. These changes commenced on 12 March 2014. *The Privacy Regulations 2013*, made under the Privacy Act, also commenced on 12 March 2014.

The *Privacy Act* now includes a set of 13 new harmonised privacy principles[11] that regulate the handling of personal information by Australian and Norfolk Island Government agencies and some private sector organisations. These principles are called the *Australian Privacy Principles*. They replace both the *Information Privacy Principles* (IPPs) that applied to Australian Government agencies and the *National Privacy Principles* (NPPs) that applied to some private sector organisations.

The APPs set out standards, rights and obligations for the handling, holding, accessing and correction of personal information (including sensitive information).

[11] For further information see [PA2012] at section 13 of the Gatekeeper PKI Framework

APP1 requires APP entities to take reasonable steps to implement practices, procedures and systems that will ensure compliance with the APPs and enable them to deal with enquiries or complaints about privacy compliance. Conducting a PIA will assist entities to ensure privacy compliance. A PIA identifies how a Service Provider can have an impact on an individual's privacy, and makes recommendations for managing, minimising or eliminating privacy impacts.

The *Guide to undertake privacy impact assessments (PIA guide)*[12] has been prepared by the OAIC to describe the process for undertaking a PIA. The PIA Guide is intended to provide guidance to all APP entities.

Service Providers **MUST** undertake a PIA for all PKI-related systems that collect, process, store or disclose personal information.

Privacy and security are inherently linked insofar as good security practices will contribute to the protection of a Subscriber's personal and sensitive information. Similarly an analysis of data flows will identify potential privacy issues that will require mitigation as part of the Service Provider's overall security risk management practices.

The outcomes of a PIA will provide a valuable input to the Service Provider's risk management strategy and ensure that the Service Provider's security policies and practices are adequate to ensure the protection of personal information.

[12] For further information see [PIA] at section 13 of the Gatekeeper PKI Framework

9. Gatekeeper Approved Documents

9.1 Information Security Documentation

In support of the PSPF and ISM compliance obligations, Gatekeeper contains mandatory security requirements to which accredited Service Providers **MUST** comply.

Implementation of the relevant PSPF and ISM requirements will be fully documented in the Service Providers Information Security Documentation. Where appropriate, the Framework will provide guidance on compliance requirements and the source of the requirement.

It is a mandatory Gatekeeper requirement that Service Providers adopt a risk management approach to cover all areas of protective security activities across their PKI operating environment. The following documents form the mandatory Information Security Documentation suite that accredited Service Providers are required to develop and maintain:

- Information Security Policy (ISP);
- Protective Security Risk Review;
- Security Risk Management Plan (SRMP);
- System Security Plan (SSP), comprising;
  - Standard Operating Procedures;
- Physical and Environmental Security Plan;
- Personnel Security Plan;
- Incident Response Plan (IRP);
- Cryptographic Key Management Plan; and,
- Disaster Recovery and Business Continuity Plan (DRBCP).

> Information Security Documentation is a core document suite that **MUST** be maintained by all Service Providers.

These documents address all elements of the Service Provider’s protective security arrangements and are used to support the accurate and consistent application of policy and procedure within a Service Provider’s PKI environment.

Service Providers should ensure that Information Security Documentation is developed by personnel with a degree of competency in Public Key Infrastructure and general knowledge of Gatekeeper Policies and Criteria.

As the SRMP, SSP, SOPs, IRP and DRBCP form the underpinning documentation suite for an information system, it is essential that they are logically connected and consistent. Furthermore, each document developed for an information system will need to be consistent with the ISP.

The suite of Gatekeeper Approved Documents to be developed is dependent on the type of accreditation being sought by the Service Provider. Below is a summary of the Approved Documents to be developed for Gatekeeper Accreditation. Any changes to these documents will require a Service Provider to vary their accreditation in accordance with Section 5.6.3.

Accreditation Category	Gatekeeper Approved Documents
Registration Authority	Information Security Documentation AND Registration Authority Operations Manual
Certification Authority	Information Security Documentation AND Certification Practices Statement AND Certificate Policy(s).
Validation Authority	Information Security Documentation.

Note

An important component of a Service Provider's risk management approach relates to information handling and applying protective markings to assets. Appropriate marking and/or classification of information applies not only to the collection of personal and other information as part of the registration process (relevant to Registration Authorities) but also information such as passwords and passphrases that enable CA employees and contractors access to PKI hardware and software.

In relation to information collected as part of the registration process Service Providers **MUST** also consider issues of data aggregation and its impacts on handling requirements, security markings and/or classification.

The *Information Security Management Guideline – Management of aggregated information*[13] provides guidance on good management practices to address the security risks associated with the aggregation of large volumes of information. The guidelines assist in identifying the value of aggregated information and provide guidance on the appropriate protections for aggregated information.

9.1.1 Documentation maintenance

The threat environment and Service Providers' businesses are dynamic. If a Service Provider fails to maintain their current Information Security Documentation, their security measures and processes may cease to be effective.

Service Providers **MUST** review their Gatekeeper Approved Documents at least annually or sooner when changes occur in threats, risks or the Service Provider's PKI operating environment.

9.2 Information Security Policy

The ISP describes a Service Provider's commitment to information security, its approach to information security management and defines information security management responsibilities. It addresses the intended security objectives relating to personnel, access controls, business continuity and protection of services, assets and business processes. These objectives are linked to the Service Provider's PSRR and SRMP.

[13] For further information see [ISMG2] at section 13 of the Gatekeeper PKI Framework

Service Providers **MUST** have an ISP.

The Service Provider **SHOULD** consider the following when developing their ISP:

ISP Considerations	
The policy objectives	How the policy objective will be achieved
The guidelines and legal framework under which the policy will operate	The stakeholders
What resourcing will be available to support the implementation of the policy	What performance measures will be established to ensure that the policy is implemented effectively

The key components in a Service Provider's ISP **SHOULD** include at a minimum:

ISP Key Components	
Configuration control	Personnel responsibilities
Networking and connections with other systems	Access control
Emergency procedures and cyber security incident management	Personnel security, physical security and media control
Information security awareness and training	Change management

9.3 Protective Security Risk Review

Security risks cannot be managed if they are unknown. Even if they are known, failing to deal with them is a failure of security risk management. For this reason a PSRR and a SRMP are required to identify and manage security risks.

Service Providers **MUST** ensure that every PKI-related system is covered by a PSRR and a SRMP.

Risk Management Standards

Service Providers **SHOULD** develop the PSRR and SRMP in accordance with Australian or international standards for risk management.

Security risk management is of greater value to a Service Provider when it is based on an industry-recognised approach to risk management, such as those produced by Standards Australia and the International Organisation for Standardization (ISO) / International Electro-technical Commission (IEC).

Standards Australia publishes AS/NSZ ISO 31000:2009 Risk Management Principles and Guidelines and HB 167:2006 Security Risk Management. The ISO/IEC has developed the risk management standard ISO/IEC 27005:2011 Information Technology – Security Techniques – Information Security Risk Management, as part of the ISO/IEC 27000 family of information security management system standards.

The PSRR addresses all aspects of a Service Provider's operations (physical, logical and personnel) and addresses both internal and external threats. The PSRR should also consider the threat and risks to the provider not only from its own perspective but also from the perspective of Subscribers and Relying Parties.

Protection of business-critical assets involves the identification and classification of threats and risks to the Service Provider's PKI services, assets and business processes; and the development and implementation of appropriate risk management strategies.

> Service Providers **MUST** document their risk tolerance threshold. Security risks deemed acceptable **MUST** be formally accepted by the responsible authority and continually monitored

The PSRR contributes to the development of the SRMP. This element of the Service Provider's Information Security Documentation sets out effective threat mitigation plans that reduce residual risk to a level that is acceptable to the Service Provider.

Service Providers **SHOULD** consider the following non-exhaustive list[14] of typical information security threats when developing their PSRR:

Type	**Threat Source**	
Physical Damage	Fire, water	Destruction of equipment
	Dust, corrosion, freezing	Pollution
	Facility security breach	
Natural events	Climatic or Seismic phenomenon	Flood
	Volcanic or Meteorological phenomenon	Bush fire
Loss of essential service	Failure of air conditioning or water supply system	Loss of power supply
	Failure of telecommunications equipment	
Compromise of information	Data from untrustworthy sources	Interception of compromised interference signals
	Remote spying	Tampering with hardware
	Eavesdropping	Tampering with software
	Theft of media or documents	Theft of equipment
	Retrieval of recycled or discarded media	Unauthorised disclosure

[14] The table is derived from [27005] & [IRAP]

Type	Threat Source	
Technical failures	Equipment failure or malfunction	System overloads due to business traffic
	Breach of information system maintainability	Configuration errors
Unauthorised actions	Fraudulent copying of information	Unauthorised use of equipment, services or user privileges
	Corruption of data	Illegal processing of data
	Malicious use (internal – privileged user)	Data spill
Compromise of functions	Error in use	Abuse or forging of rights
	Denial of actions	Breach of personal availability
	Operator negligence	Hacking
	Criminal use – identity fraud	Malicious code injections
	Social engineering of administrative staff	

9.4 Security Risk Management Plan

The key components in a Service Provider's SRPM **SHOULD** include at a minimum:

Insert header text for accessibility	Insert header text for accessibility
Goals and objectives of the risk management process	Scope of the risk assessment, including risk tolerance, specific inclusions and exclusions.
Staff responsibilities within the risk management process	Relationship between the system under review and objectives of the wider organisation
Risk assessment methodologies	System description
Data descriptions and flows	Risk treatment options and plans

Assets to be protected **MUST** be identified as part of the risk management process.

Assets to be protected in a PKI include but are not limited to:

Assets to be protected in a PKI include but are not limited to:	
Subscriber certificates	Subscriber private keys and activation data
Private keys of Certificate Authorities	Private keys of CA and RA operators
Hardware Security Module (HSM) passphrases	Database passphrases
PKI equipment (CA servers, HSMs, RA workstations)	Essential service equipment (network infrastructure, communications systems, perimeter security devices, backup systems and power supplies)
Copies taken of identity and other registration information	Operational information (audit logs, transaction histories, CA lifecycle, archives, CRLs and OCSP responses)
Security classified information	System users
Staff and Contractors	Backup procedures
Logical access controls	Data transfer procedures

Key risks that the Service Provider **SHOULD** consider (but not limited to):

Key risks that the Service Provider SHOULD consider (but not limited to):	
Building location, type and construction	Shared tenancy requirements (physical and logical)
Local crime activity	Location and security of environments used for the creation and issuance of digital certificates
Availability and redundancy of entry points for communications services	Availability and redundancy of entry pints for other essential services
Building setbacks relative to street frontage	Inadequate PSRR and SRMP undertaken
Pedestrian traffic	Vehicular traffic
Lack of regular security reviews	Inadequate vetting of staff or contractors
Intermittent electricity outages	Internet connectivity outages
Fire	Long term electricity outages
Inappropriate storage of keys, certificates and passphrases	Poor disaster recovery and business continuity planning

Key risks that the Service Provider SHOULD consider (but not limited to):	
Cryptographic product failure	Failures in the registration process when enrolling applicants for digital certificates
Relying Party software application error	System integration failures
Inadequate treatment to physical security requirements	Failure to comply with standards
Malicious code infection	Unauthorised access to systems
Information leakage (data spill risks)	Reputation damage resulting from system or information compromise
Exploitation through security vulnerabilities	Abuse of privilege by administrators
Denial of service	Use of non-evaluated products

9.5 System Security Plan

The SSP is part of the SRMP and describes the implementation and operation of security controls for a system.

Service Providers **MUST** ensure that every PKI-related system is covered by an SSP.

The key components in a Service Provider's SSP **MUST** include at a minimum:

Key components in a Service Provider's SSP MUST include at a minimum:	
Security philosophy	Security roles and responsibilities
Management of staff	Management of visitors (e.g. escorting)
Management of contractors	Response details in the event of an incident (e.g. CA compromise)
Staff training requirements	System monitoring and maintenance regimes
Staff authorisation, clearance and briefing requirements	Physical access controls
Standard Operating Procedures for system-specific roles	Network and logical access controls
Key management	Personnel access controls
Intruder alarm systems	Role and access privileges of guards

Key components in a Service Provider's SSP MUST include at a minimum:	
Staff requirements to hold Positions of Trust.	Intrusion detection and prevention strategies
Application and operating system patching strategies	Event logging

9.5.1 Standard Operating Procedures

Standard Operating Procedures provide a step-by-step guide to undertaking security related tasks. They provide assurance that tasks can be undertaken in a repeatable manner, even by users without strong knowledge of the system.

Service Providers **MUST** ensure that SOPs are developed for all PKI-related systems.

Information relating to the system-specific roles and responsibilities of IT security advisors, system managers, system administrators and system operators (i.e. employees with defined access rights to the CA operating system and peripheral systems to perform certificate lifecycle management functions) **SHOULD** be included in the SSP documentation.

Service Providers **SHOULD** develop SOPs for:

- Information Technology Security Manager ITSM,
- Information Technology Security Officer (ITSO),
- System Administrators, and,
- System Users.

Service Providers **MUST** include in standard procedures for all personnel with access to systems, a requirement that they notify an ITSM of any cyber security incident and access to any data which they are not authorised to access.

The ITSM SOPs cover the management and leadership activities related to system operations. Service Provider's **SHOULD** document the following procedures in the ITSM's:

TOPIC	**PROCEDURE TO BE INCLUDED**
Cyber Security Incidents	Reporting and managing cyber security incidents

The ITSO SOPs cover the operationally focused activities related to system operations. Service Providers **SHOULD** document the following procedures in the ITSO's SOPs:

TOPIC	**PROCEDURE TO BE INCLUDED**
Access control	Authorising access rights to applications and data
Asset musters	Labelling, registering and mustering assets, including media
Audit logs	Reviewing system audit trails and manual logs, particularly for privileged users and retention schedule for logs

TOPIC	PROCEDURE TO BE INCLUDED
Configuration control	Approving and releasing changes to the system software and configurations
Cyber security incidents	Detecting potential cyber security incidents
	Establishing the cause of any cyber security incident, whether accidental or deliberate
	Actions to be taken to recover and minimise the exposure from a cyber-security incident
Data transfers	Managing the review of media containing information that is to be transferred off-site (including sites used for backup operations, archival and storage)
	Managing the review of incoming media for viruses or unapproved software
ICT equipment	Managing the sanitation, destruction and disposal of unserviceable ICT equipment and media
System integrity audit	Reviewing system user accounts, system parameters and access controls to ensure that the system is secure
	Checking the integrity of system software
	Testing access controls
	Inspecting ICT equipment and cabling
System maintenance	Maintaining the ongoing security and functionality of system software, including: maintaining awareness of current software vulnerabilities, testing and applying software patches, updates and antivirus signatures, and applying appropriate hardening techniques
User account management	Authorising new system users, removing or disabling unused accounts, replacing default passwords, account sharing and account lockouts

Whilst the system administrator SOPs primarily focus on the administrative activities related to system operations they also support the ITSO SOPs. Service Providers **SHOULD** document the following procedures in the ITSO's SOPs:

TOPIC	PROCEDURE TO BE INCLUDED
Access control	Implementing access rights to applications and data
Configuration control	Implementing changes to the system software and configurations

TOPIC	PROCEDURE TO BE INCLUDED
System backup and recovery	Backing up data, including audit logs
	Securing backup tapes
	Recovering from system failures
User account management	Adding and removing system users
	Setting user privileges
	Cleaning up directories and files when a user departs or changes roles

The user SOPs focus on day-to-day activities that users need to be aware of, and comply with, when using systems. Service Provider's **SHOULD** document the following procedures in the System User's SOPs:

TOPIC	PROCEDURE TO BE INCLUDED
Cyber security incidents	What to do in the case of a suspected or actual cyber security incident
End of day	How to secure systems at the end of the day
Media control	Procedures for handling and using media
Passphrases	Protecting passphrases, authentication tokens and activation data
Temporary absence	How to secure systems when temporarily absent

Service Providers **SHOULD** require ITSMs, ITSOs, system administrators and system users to sign a statement confirming they have read and agree to bind by their respective SOPs.

9.6 Physical and Environmental Security Plan

A Physical and Environmental Security Plan documents measures to counter identified risks to a Service Provider's functions, information, logical assets, people and physical assets operating within their PKI environment. This includes PKI environments which are fixed, mobile and operate from the cloud.

Every operating environment that contains a PKI-related system **MUST** be covered by a Physical and Environmental Security Plan.

Service Providers are required to evaluate the different risks owned or leased facilities and cloud environments, people, information, logical assets, functions and physical assets during business hours and out-of-hours. Controls needed during operating hours should take into account the increased risks from public and customer contact as well as insider threats. While these risks still exist out of hours, there may be a higher risk from external sources such as break and enters.

Service Providers are required to assess the impact of compromise, loss of integrity or unavailability of their Physical and Environmental Security Plans to their security and operations.

A Physical and Environmental Security Plan **SHOULD** address:

- measures that are scalable to meet increases in threat levels;
- the location and nature of the operating environment;
- whether the Service Provider has sole or shared ownership or tenancy of the operating environment;
- whether the public or other non-agency personnel have a right of entry to the operating environment;
- the potential sensitivity or possible security classification of information to be stored, handled, processed or otherwise used in each part of the operating environment;
- ICT assets, including, but not limited to, data, software, hardware and portable equipment such as laptops, tablets, smart phones and personal electronic devices;
- ICT-related equipment (for example, file servers, workstations, terminals, main distribution frames and cabling[15]) and utilities;
- any other resources that will be within the operating environment;
- specifications as to the security ratings of the various areas and zones within the operating environment;
- any requirements for *No Lone Zones;*
- protective measures required for:
  - the entire operating environment; and
  - designated areas within the operating environment, such as a room intended hold information of a higher classification than the rest of the operating environment.
- what differing measures will be required for:
  - storage, handling and processing of classified or sensitive information; and
  - classified or sensitive discussions and meetings.

9.7 Personnel Security Plan

Personnel Security is the management of staff to assist in the protection of a Service Providers people, information and assets. In a security aware culture personnel security includes three major components:

- identification of suitable staff to access Service Provider information, resources and assets;
- education and training of staff about their security roles and responsibilities; and
- monitoring and evaluation of staff’s continued suitability.

Service Providers **MUST** implement a PSP.

A Service Provider’s PSP **SHOULD** cover the following elements:

- Pre-employment checks:
  - Identity verification,

[15] For further information see [TCPR] at section 13 of the Gatekeeper PKI Framework

  - Eligibility checks (e.g. citizenship or visa working conditions),
  - Qualification checks,
  - Previous employment checks (e.g. referee checks), and,
  - Criminal record check.
- Employee screening and where necessary, security clearance requirements for positions,
- Security awareness, training and education
- Monitoring and evaluation of:
  - Access controls,
  - Physical and logical access privileges,
  - Physical access and IT systems monitoring, and
  - Maintenance and repair of IT systems by uncleared technicians.

9.8 Incident Response Plan

An IRP outlines actions to take in response to a Cyber Security Incident. In most situations, the aim of the response will be to:

1. Preserve any evidence relating to the Cyber Security Incident, and
2. To prevent the incident from escalating.

(Returning to normal operations is an objective of the DRBCP)

Service Providers **MUST** develop and maintain an IRP and supporting procedures.

Service Providers **MUST** include, as a minimum the following in the IRP:

- Broad guidelines on what constitutes a Cyber Security Incident,
- The expected response (and timeframe) to each cyber security incident type,
- The minimum level of Cyber Security Incident response and investigation training for users and system administrators,
- The authority responsible for initiating investigations of a cyber-security incident,
- The steps required to ensure the integrity of evidence supporting a cyber-security incident,
- The steps necessary to ensure that critical systems remain operational,
- Security incident responsibilities and procedures for each PKI-related system in relevant SSP, SOPs and IRP,
- How to formally report cyber security incidents, and
- Procedures for dealing with data spills which Service Providers **MUST** treat as a security incident.
  - Data spills **MUST** be reported to ASD, the Gatekeeper Competent Authority and the information owner.
  - Data spills **SHOULD** be reported to the Office of the Australian Information Commissioner (OAIC). Guidance is available in [DBN].

Service Providers **SHOULD** include the following contents in the IRP:

- Clear definitions of the types of Cyber Security Incidents that are likely to be encountered,
- The authority responsible for responding to Cyber Security Incidents,

- The criteria by which the responsible authority would initiate or request formal, police or Australian Security Intelligence Organisation (ASIO) investigations of a cyber-security incident,
- Other authorities or parties (e.g. clients and agencies) impacted by the incident which need to be informed in the event of an investigation being required, and
- The details of the system contingency measures or a reference to these details if they are located in a separate document.

Service Providers **MUST** ensure that all security incidents are recorded in a register.

The recorded information **MUST** include, at a minimum:

- The date the cyber security incident was discovered,
- The date the cyber security incident occurred,
- A description of the cyber security incident, including people and locations involved,
- The actions taken in response to the incident, and
- The person to whom the cyber security incident was reported.

Service Providers **SHOULD** use the register as a reference for future security risk assessments.

9.9 Cryptographic Key Management Plan

The security of information protected by PKI directly depends on the strength of the keys, the effectiveness of mechanisms and protocols associated with the keys and the protection afforded the keys. All keys need to be protected against modification, and private keys need to be protected against unauthorised disclosure. Key management provides the foundation for the secure generation, storage, distribution, use and destruction of keys.

9.9.1 Cryptographic Key Management Plan

The CKMP identifies the implementation, standards, procedures and methods for key management in PKI service providers and provides a good starting point for the protection of cryptographic systems, keys and digital certificates.

The level of detail included in the CKMP **MUST** be commensurate with the criticality, sensitivity and classification of the information to be protected.

The Service Provider’s CKMP **SHOULD** include, at a minimum:

The Service Provider’s CKMP SHOULD include at a minimum:	
Objectives	Objectives of the cryptographic system and CKMP, including Service Provider aims
Accounting	How accounting will be undertaken for the cryptographic system
	What records will be maintained
	How records will be audited

The Service Provider's CKMP SHOULD include at a minimum:	
Cyber Security Incidents	A description of the conditions under which compromise of keys should be declared
	References to procedures to be followed when reporting and dealing with compromised keys
Key Management	How are keys generated
	How are keys delivered to intended users
	How keys are received, installed and activated
	Key distribution, including local, remote and central
	How keys are transferred, stored, backed up and archived
	How keys are recovered as part of disaster recovery of business continuity management
	How keys are revoked, suspended, deactivated and destroyed
	How keys are changed or updated
	Logging and auditing of key management related activities
Maintenance	Maintaining the cryptographic system software and hardware
	Destroying cryptographic equipment and media
References	Vendor documentation
	Relevant policies
Sensitivity or classification	Sensitivity or classification of the cryptographic system hardware, software and documentation
System description	Sensitivity or classification of information protected
	The use of keys
	The environment
	Administrative responsibilities
	Key algorithms
	Key lengths
	Key lifetime

The Service Provider's CKMP SHOULD include at a minimum:	
Topology	Diagrams and descriptions of the cryptographic system topology including data flows

9.9.2 Compromise of keys and digital certificates

Keys or digital certificates used for digitally signing or encrypting messages that are suspected of being compromised (that is, lost, stolen, copied, or uncontrolled), are incapable of offering any assurance in the integrity of the subsequent messages digitally signed or encrypted by that key. Likewise, no assurance can be placed in the confidentiality of a message encrypted using the public key, since third parties could intercept the message and decrypt it using the private key.

> Service Providers **MUST** immediately revoke digital certificates suspected of being compromised.

9.9.3 ASD Approved Cryptographic Algorithms

Whilst there is no guarantee or proof of security of an algorithm against presently unknown intrusion methods, the algorithms listed in this section have been extensively scrutinised by industry and academic communities in a practical and theoretical setting and have not been found to be susceptible to any feasible intrusion. There have been some cases where theoretically impressive vulnerabilities have been found, however these results are not of practical application.

> Service Providers **MUST** use encryption products that implement ASD Approved Cryptographic Algorithms (AACAs).

The AACAs fall into three categories: asymmetric or public key algorithms, hashing algorithms and symmetric encryption algorithms.

The approved asymmetric/ public key algorithms are:

- Diffie-Hellman (DH) for agreeing on encryption session keys,
- Elliptic Curve Diffie-Hellman (ECDH) for agreeing on encryption session keys,
- Digital Signature Algorithm (DSA) for digital signatures,
- Elliptic Curve Digital Signature Algorithm (ECDSA) for digital signatures, and
- Rivest-Shamir-Adleman (RSA) for both digital signatures and passing encryption session keys.

The approved hashing algorithm is:

- Secure Hashing Algorithm 2 (SHA–224, SHA–256, SHA–384 and SHA–512).

The approved symmetric encryption algorithms are:

- Advanced Encryption Standard (AES) using key lengths of 128, 192 and 256 bits, and
- Triple Data Encryption Standard (3DES).

9.10 Disaster Recovery and Business Continuity Plan

The DRBCP helps minimise the disruption to the availability of information and systems after a security incident or disaster by documenting the response procedures.

Service Providers **MUST** develop and maintain a DRBCP.

As availability requirements will vary based on the business requirements they cannot be stipulated within the Framework. Specific availability requirements will be a matter for negotiation with the Relying Party. As such, Service Providers will need to determine availability requirements and implement appropriate security measures to achieve them.

Developing a Disaster Recovery Plan will reduce the time between a disaster occurring and critical functions of systems being restored. Developing a Business Continuity Plan can help ensure that critical functions of systems continue to operate when the system is in a degraded state.

9.10.1 Business Continuity Standards

Service Providers **SHOULD** develop business continuity plans in accordance with either of the following Australian standards for business continuity plans:

- Standards Australia produces AS/NZS 5050:2010 Business Continuity – Managing disruption-related risk*16*, which sets out a definition and process for business continuity management and provides a workbook that may be used by organisations to assist in implementation.
- The Australian National Audit Office has released a Business Continuity Management Better Practice Guide*17* to assist organisations to plan for, and build resilience into, critical business processes.

9.10.2 Testing and validation of the DRBCP

Regular testing and validation of the DRBCP is crucial to effective disaster recovery and business continuity planning with the results of these tests being recorded and incorporated into the review and updates of the DRBCP.

Testing and validation of the DRBCP **SHOULD** be carried out at regular intervals throughout the year and **SHOULD** be implemented in the following steps:

1. identify area(s) to be tested and evaluated,
2. prepare the plans,
3. undertake testing and validation,
4. review and assess the results, and
5. update plans accordingly.

[16] For further information see [ANZ5050] at section 13 of the Gatekeeper PKI Framework

[17] For further information see [ANAO] at section 13 of the Gatekeeper PKI Framework

10. Registration Authority

10.1 Registration Authority

Registration Authorities undertake identity proofing of an Applicant requesting a digital certificate and may, depending on their business model and commercial relationship with the issuing CA, also play a role in relation to requests for certificate renewals and revocations.

Identity proofing activities conducted by a RA for digital certificates will be performed in accordance with the Gatekeeper Identity Proofing Policy. This policy is consistent with the *National Identity Proofing Guidelines* and defines the minimum identity verification activities to defined LOAs performed by the RA. Identity proofing activities conducted by a RA for certificate renewal or certificate rekey will be performed in accordance with the appropriate CPS and/or CP.

The intent of these activities is to address the five identity proofing objectives:

1. Confirm uniqueness of identity in the intended context,
2. Confirm the claimed identity is legitimate,
3. Confirm the operation of the identity in the community over time,
4. Confirm the linkage between the identity and the person claiming the identity, and
5. Confirm the identity is not known to be used fraudulently.

Depending on the identity proofing objective and the LOA being met, biometric comparisons, interviews (in-person or remote) and verification of identity information or documents from authoritative sources[18] are supported. Gatekeeper Accreditation requires there be confidence that the functions performed by the CA and RA interlock satisfactorily to form a consistent and reliable Chain of Trust. The RA acts as an intermediately between Applicants and a CA and provides the essential function of identity proofing. It must be trusted to undertake identity proofing on Applicants, pass accurate certificate requests and (as appropriate) certificate revocation requests to a CA. The RA does not sign, issue or manage Subscriber digital certificates.

RAs may perform the registration function for more than one CA. The assurance of performing this function must be consistent with the obligations of the CA and is to be undertaken in accordance with the CPS and/or CP of each of the Gatekeeper accredited CAs to which the RA provides a service.
If, for example a CA provides a service that meets LOA 3 requirements, it shall, at a minimum use a RA that performs identity verification services at LOA 3. A RA operating at LOA 4 may also provide registration services to CAs that meet LOA 1, LOA 2 or LOA 3 requirements.

The use of a non-accredited entity to undertake identity proofing is recognised under Gatekeeper.
If the entity undertaking the identity proofing is mandated in regulations or legislation to do so for the Subscriber or for the COI in which the Subscriber participates. In either case the provisions detailed in the regulations or legislation take precedence over the Gatekeeper requirements for identity proofing.

[18] This includes authoritative sources accessible to accredited Verification Service Providers under the Third Party Identity Services Assurance Framework.

10.2 Evidence of Identity Rigour and Storage

Gatekeeper considers personal information to be a sensitive asset and requires accredited Registration Authorities to assign at a minimum, a DLM of *Sensitive: Personal*[19] to all personal information held, processed, stored or disclosed.

In relation to information collected as part of the registration process Service Providers **MUST** also consider issues of data aggregation and its impacts on security classification and handling requirements.

The *Information Security Management Guideline – Management of aggregated information*[20] provides guidance on good management practices to address the security risks associated with the aggregation of large volumes of information. The guidelines assist in identifying the value of aggregated information and provide guidance on the appropriate protections for aggregated information.

The RA may also choose to implement a greater degree of security than is required by Gatekeeper because of a greater perceived threat to its operations. This should be highlighted in the PSRR and SRMP, which should also describe the security arrangements in place for the protection of personal information collected during the identity proofing process.

10.3 RA Operations Manual

A RA Operations Manual **SHOULD** contain, at a minimum, the following information:

- Roles and responsibilities of the RA and associated staff (i.e. RA Operators);
- The process and procedures in place to support identity proofing;
- The procedures used to register, verify, authenticate and validate an Applicant (and Subscriber) requesting a digital certificate;
- Operational procedures describing the manner in which all nominated personnel employed within the RA perform any task undertaken with the RA;
- Overview of emergency security incident response plans (including data spills), vulnerability assessment and change management processes;
- The degree of system logging used and the types of events captured.
- Detailed descriptions of the procedures followed for:
  - Access control measures and procedures for RA facilities,
  - Backup and archive procedures, and,
  - Publication of information for staff regarding operational practices.
- Details of all interactions between the RA and CA;
- Details of all operations consistent with those described in the Information Security Documentation;
- Processes and procedures in place for:
  - Storing identity information collected, and,
  - Digital certificate renewals, revocations and suspension requests.

[19] For further information see [ISMG1] at section 13 of the Gatekeeper PKI Framework

[20] For further information see [ISMG2] at section 13 of the Gatekeeper PKI Framework

- Graphics and functional flow diagrams to enhance the presentation of information in the document;
- Auditing requirements (internal and external);
- A complete glossary of terms used in the document; and,
- Relevant standards referenced in the document.

10.4 Registration Authority Levels of Assurance

This section (and the subsequent table) details the assurance requirements to be met by RAs. Each level defines characteristics and minimum criteria that **MUST** be met in order to gain and maintain accreditation at a particular level.

LOA 1

At this level identity is unique within the intended context. There is little confidence in the accuracy or legitimacy of the claimed identity. Self-claimed or self-asserted identity (including pseudonymity) is possible but not anonymity.

Identity assertions at this level are appropriate for transactions with minimal consequences to Relying Parties from the registration of a fraudulent identity.

LOA 2

At this level identity is unique within the intended context, identity has been asserted by authoritative sources and identity may be used in other contexts. There is some confidence in the claimed identity.

Identity assertions at this level are appropriate for transactions with some minor consequences associated with the registration of fraudulent identity.

LOA 3

At this level identity is unique within the intended context, the identity is recognised by authoritative sources, identity information is verified with authoritative sources, identity can be used in other contexts and the Subscriber is linked to the identity. There is high confidence in the claimed identity.

Identity assertions at this level are appropriate for transactions with serious consequences associated with registration of fraudulent identity.

LOA 4

At this level identity is unique within the intended context, the identity is recognised by authoritative sources, identity information is verified with authoritative sources, identity can be used in other contexts and the Subscriber is linked to the identity. There is very high confidence in the claimed identity.

If the Subscriber is an individual then a local, face to face interview is required. This provides greater opportunities for examining the integrity of original identity documents provided as evidence of identity and establishing a link between a Subscriber and a claimed identity.

Identity assertions at this level are appropriate for transactions with very serious consequences associated with the registration of fraudulent identity.

Requirement	LOA 1	LOA 2	LOA 3	LOA 4
Identity Verification				
Objective 1: Unique in context	Check that the Subscriber is the sole claimant of the identity being claimed.			
Objective 2: Claimed identity is legitimate (commencement of identity deceased identity check)	No stipulation	No stipulation	Verify one of the following: • Australian Birth Certificate • Australian Passport • Immigration Record • Australian Citizenship Certificate • Australian Visa (supported by a foreign passport) • ImmiCard Check the identity is not that of a deceased person by either: • verifying birth certificate with issuing authority, or • check the Fact of Death file	At an in-person interview verify one of the following: • Australian Birth Certificate • Immigration Record • Australian Citizenship Certificate • Australian Visa (supported by a foreign passport) • ImmiCard Check the identity is not that of a deceased person by either: • verifying birth certificate with issuing authority, or • check the Fact of Death file
Objective 3: Operation of the identity in the community over time	No stipulation	Verify one PRIMARY and one SECONDARY piece of evidence	Verify one PRIMARY and one SECONDARY piece of evidence with an authoritative source (e.g. issuing authority)	As per LOA 3 requirements AND provide evidence at an in-person interview

Requirement	LOA 1	LOA 2	LOA 3	LOA 4
Objective 4: Link between the identity and the person claiming the identity	No stipulation	No stipulation – evidence provided to meet Objective 3 is sufficient to meet Objective 4	Verify link between claimed identity and claimant via one of the following: • Manual/visual comparison of a person's face against a photo on a PRIMARY document • Verification of a biometric previously collected • Knowledge based authentication	As per LOA 3 requirements, except that a visual comparison of a person's face or verification of a biometric to occur as part of an in-person face to face interview
Objective 5: Identity is not known to be fraudulent	No stipulation	No stipulation	Check information/records held within the organisation of known fraudulent identities (if such information exists). Once technology permits these checks **SHOULD** also include checks against information on known fraudulent identities held with authoritative sources such as law enforcement and government agencies.	

10.5 Individual Identity Proofing

The table below lists the types of evidence of identity documents that are acceptable as either PRIMARY or SECONDARY documents.

- PRIMARY evidence is generally government issued evidence types with robust identity proofing processes, issuance and management processes. Where it is a physical document, it will generally contain a photograph and security features.
- SECONDARY evidence includes evidence types from government or non-government sources that are supported by moderate identity proofing processes, issuance and management processes.

Type of evidence	Weighting
Australian passport (including Ordinary, Frequent traveller, Diplomatic, Official and Emergency)	Primary
Foreign passport	Primary
Australian driver licence	Primary
Australian government issued proof of age card/photo card	Primary
Australian secondary student identity document (issued by a government agency or Australian school only)	Primary
ImmiCard	Primary
DFAT issued Certificate or Document of Identity	Secondary
DFAT issued United Nations Convention Travel Document	Secondary
Foreign government issued documents (e.g. driver licences)	Secondary
Medicare Card	Secondary
Enrolment with the Australian Electoral Commission	Secondary
Security Guard/Crowd Control photo licence	Secondary
Evidence of right to a government benefit (DVA or Centrelink)	Secondary
Consular photo identity card issued by DFAT	Secondary
Police Force Officer photo identity card	Secondary
Australian Defence Force photo identity card	Secondary
Commonwealth or state/territory government photo ID card	Secondary
Aviation Security Identification Card	Secondary

Type of evidence	Weighting
Maritime Security Identification Card	Secondary
Firearms licence	Secondary
Credit reference check	Secondary
Australian tertiary student photo identity document	Secondary
Australian secondary student photo identity document	Secondary
Certified academic transcript from an Australian university	Secondary
Trusted referees report	Secondary
Bank or credit card	Secondary
Other authoritative online sources of evidence verified by a Third Party Identity Provider	Secondary

10.6 Organisation Identity Proofing

This section describes the organisation identity proofing requirements to be met by RAs when undertaking identity proofing activities on Subscribers (organisations, individuals and NPEs) who are subsequently issued digital certificates to act on behalf of an organisation. Organisation certificates can be used at all LOAs under Gatekeeper:

- At LOA 1 and LOA 2 the organisation **MUST** be identified in the digital certificate. The Subscriber (if different from the organisation) **SHOULD** also be identified.
- At LOA 3 and 4 the organisation and the Subscriber (if different from the organisation) **MUST** be identified in the digital certificate.

10.6.1 Key Organisation Roles

Within the organisation two classes of individuals are important, the Authoriser and the Certificate Manager.

Authoriser

An Authoriser is a member of a class of persons with a clear capacity to commit an organisation and to appoint a Certificate Manager. Persons who are members of this class may include but are not limited to a Chief Executive Officer, Company Director, Trustee, Sole Trader, Partner or Company Owner.

The Authoriser's association with the organisation **MUST** be evidence by reference to:

- An authoritative public register (such as the ABR or the Australian Securities and Investments Commission); and
- Appropriate legal, regulatory documents issued by a government Agency; or
- Appropriate legal, regulatory documents issued by a non-government Agency.

Certificate Manager

A Certificate Manager is an employee or representative of an organisation duly authorised by the Authoriser to perform the Certificate Management duties appropriate to the LOA commensurate for certificates being requested.

For example, if an organisation requires certificates which provide a high level of assurance (i.e. LOA 3) the CM must undergo an LOA 3 identity proofing process.

The duties of a Certificate Manager may include:

- Submit an application to hold an organisational certificate;
- Complete, sign and lodge the necessary documentation that provide evidence of the binding between the organisation and the Certificate Manager;
- Request digital certificates as required for use by Subscribers of the organisation; and,
- On behalf of the organisation:
  - Verify the identity of Subscribers for whom digital certificates are requested to an LOA commensurate for the certificate being requested. For certificates being issued to NPEs (such as a device or web server), the custodian or person responsible for the NPE is required to have their identity verified by the Certificate Manager to the LOA commensurate for the certificate being requested; and,
  - Ensure Subscribers and NPE custodians read, understand, sign and comply with any certificate terms of use.

An organisation may have one or more Certificate Managers. A small organisation may have only one Certificate Manager while a large or decentralised organisation may choose to appoint a number of Certificate Managers for practical or operational purposes.

Given the critical role played by the Certificate Manager the allocation of such positions **MUST** be strictly managed by the organisation. The organisation **MUST** ensure the privileges grated to a Certificate Manager are removed when no longer required.

The Certificate Manager as described above and the person providing the Certificate Manager with the authority (the Authoriser) may be one and the same person, for example, in a small organisation. A person appointed by the organisation as a Certificate Manager cannot appoint other Certificate Managers unless the person is also an Authoriser.

10.6.2 Organisation Identity Proofing Requirements

Organisation identity proofing requires Applicants to provide legal or regulatory documents as evidence of the organisation's existence. The organisational documents presented for establishing the organisation identity **MUST** identify the organisation and confirm that the Authoriser is a member of the organisation.

The RA is responsible for verifying the identity of the organisation, the identity of the Authoriser of the business entity and the identity and authorisations of the Certificate Manager to request certificates on behalf of the organisation.

Organisational identity proofing is satisfied for all LOAs if either Option 1 or Option 2 is completed:

Option	Organisation Identity Proofing Requirement
Option 1	• An original or certified copy of the notice issued by the Registrar of the ABR bearing the business entity's name and ABN. If either the owner, chief capacity or other officer or employee with clear capability to commit the business entity is named as the Public Officer on the document issued by the Registrar of the ABR, then this document only will suffice; and • Online verification with the ABR to link the Organisation's ABN to its business name.
Option 2	• 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 business entity; and • Online verification with the ABR to link the Organisation's ABN to its business name.

11. Certification Authority

11.1 Certification Authority

The CA is the core component of a PKI which issues digital certificates. The digital certificates bind a Subscriber's identity (i.e. subject name) to the public key in the certificate. The CA is also responsible for digital certificate lifecycle operations, including the revocation of certificates. This is generally achieved through the use of CRLs, OCSP, or a combination of both. The CA can maintain its own certificate status services or delegate this to a separate entity, such as a VA.

In order to implement a CA effectively, a series of policies are used to govern its operations, including the CPS and CP.

- The CPS is a public document which describes the practices that the CA service will employ in managing the certificates it issues. These statements describe the PKI certificate framework, mechanism supporting the application, issuance, acceptance, usage, suspension/revocation and expiration of certificates signed by the CA, and the CA's legal obligations, limitations and miscellaneous provisions. This document is evaluated against [AA1983], [PA1988], [PA2012], [RFC3647] and for compliance with the Gatekeeper Core Obligations Policy.
- The CP is a document which defines a named set of rules regarding the applicability of a certificate to a particular community and/or class of applications with common security requirements. A CP may be used by a Relying Party to help in deciding whether a certificate and the binding therein are sufficiently trustworthy and otherwise appropriate for a particular application. Similar to the CPS, this document is evaluated against [AA1983], [PA1988], [PA2012], [RFC3647] and for compliance with the Gatekeeper Core Obligations Policy.

Other documents **SHOULD** also be used, such as service contracts (and associated terms and conditions) or a Subscriber Agreement, which defines the undertakings that Subscriber's will make in order to obtain and use certificates confirming their identity. It is expected that this will be part of the terms and conditions used to encourage user participation in digital service delivery. It is also expected that the Subscriber Agreement will include references to Relying Parties and their responsibilities, or references to Relying Party Agreements, which may also require evaluation.

11.2 Use of accredited identity proofing Service Providers

CAs **MUST** use either a Gatekeeper accredited RA or a Verification Service Provider accredited under the Third Party Identity Services Assurance Framework[21] for identity proofing[22].

Gatekeeper Accreditation requires confidence that the functions performed by the CA and the RA interlock satisfactorily to form a consistent and reliable Chain of Trust. The RA acts as an intermediary between Applicants and a CA and provides the essential function of identity proofing. The RA must be trusted to undertake identity proofing on Applicants (and Subscribers), pass accurate certificate requests and (as appropriate) certificate revocation requests to a CA.

[21] For further information see [TPISAF] at section 13 of the Gatekeeper PKI Framework

[22] The use of a non-accredited entity to undertake identity proofing is recognised under Gatekeeper. If the entity undertaking the identity proofing is mandated in regulations or legislation to do so for the Subscriber or for the COI in which the Subscriber participates. In either case the provisions detailed in the regulations or legislation take precedence over the Gatekeeper requirements for identity proofing.

Maintaining this trust requires CAs to use the identity proofing function provided by an accredited RA. Alternatively, CAs may choose to use a Verification Service Provider accredited under the *Third Party Identity Services Assurance Framework* for identity proofing. Such an arrangement will require the CA to choose a Verification Service Provider accredited to a commensurate LOA.

11.3 Certification Authority security assurance

Service Providers need confidence that software products and hardware technologies perform as claimed and provide the security necessary to mitigate likely threats. This confidence is best achieved through a formal and impartial security evaluation of the products by an independent entity.

The ASD recognises a number of evaluation programs including:

- The Common Criteria scheme through the Australasian Information Security Evaluation Program (AISEP) using licensed commercial facilities to perform evaluation of products.
- Security evaluations conducted through the National Information Assurance Partnership (NIAP), a Common Criteria Evaluation and Validation Scheme.
- Cryptographic product evaluations called an ASD Cryptographic Evaluation (ACE) for products which contain cryptographic functions.

These programs have been established to manage the different characteristics of families of security enforcing technologies. Certification Authorities and digital certificate related technologies are evaluated as part of these programs.

11.3.1 The Evaluated Products List

The ASD maintain a list of products that have been formally and independently evaluated on the Evaluated Products List (EPL). The product listings on the EPL also include important evaluation documentation that provides specific requirements and guidance on the secure use of the product. The EPL is available from the ASD website.

The ASD is in the process of transitioning away from the EPL to Protection Profiles (PP).

11.3.2 Protection Profiles

To assist Service Providers in selecting appropriate security products, ASD has introduced approved PPs. A PP is a document that stipulates the security functionality that must be included in a Common Criteria evaluation to meet a range of defined threats. Protection Profiles also define the activities to be undertaken to assess the security functionality of a product. ASD approved PPs are published on the ASD website.

Cryptographic security functionality is included in the scope of products evaluated against an ASD approved Protection Profile. ASD is currently establishing cryptographic testing as part of the AISEP and NIAP Common Criteria evaluations. When this is established, evaluations against an ASD approved PP may undergo a simplified ACE process. This will assist in reducing the completion time taken to perform the evaluation.

To facilitate the transition to ASD approved PPs, a cap of Evaluation Assurance Level (EAL) 2 applies for all traditional EAL based assessments performed in the AISEP, including those technologies with no existing ASD approved Protection Profile. Evaluations conducted in other nations' Common Criteria schemes will still be recognised by ASD.

Service Providers **MUST** use accredited software and hardware products that have undergone a security evaluation through an ASD recognised evaluation program.

Service Providers wishing to use an evaluated product in an unevaluated configuration **MUST** undertake a security risk assessment including:

- The necessity of the unevaluated configuration,
- Testing of the unevaluated configuration in the Service Provider's environment, and
- New vulnerabilities introduced due to the product being used outside of its evaluated configuration.

11.4 Certification Authority Levels of Assurance

This section (and the subsequent table) details the assurance requirements to be met by CAs including the requirements to be when issuing certificates to PKI management entities and Subscribers. Each level defines the minimum criteria that **MUST** be met in order to gain and maintain accreditation at a particular assurance level.

LOA 1

This level is intended for Subscribers handling information of little or no value within minimally secured environments. Digital certificates at this level require no or low assurance of the binding between the identity of the entity named in the certificate and the Subscriber. The keys and certificates can only be generated in a software security module and be stored in a software form factor. Given the limited assurance provided, a Key Usage of non-repudiation is not permitted, nor are Extended Key Usages of smartcard logon or code signing.

LOA 2

This level is intended for Subscribers handling information of some value within moderately secured environments. Digital certificates at this level require some assurance of the binding between the identity of the entity named in the certificate and the Subscriber. The keys and certificates can be generated in either a software or hardware security module and can be stored in either a software or hardware form factor. There are no limits on the permissible Key Usages or Extended Key Usages.

LOA 3

This level is intended for Subscribers handling information of high value within highly secure environments. Digital certificates at this level require high assurance of the binding between the identity of the entity named in the certificate and the certificate holder. The keys and certificates can be generated in either a software or hardware security module and can be stored in either a software or hardware form factor. PIN unlocks are required each time the private key is activated.

LOA 4

This level is intended for Subscribers handling information of very high value within very highly secure environments. Digital certificates at this level require very high assurance of the binding between the identity of the entity named in the certificate and the certificate holder. The keys and certificates can only be generated in a hardware security module and can only be stored in a hardware form factor. PIN unlocks are required each time the private key is activated. No Lone Zones are required for all environments that house a CA.

The following table details the requirements to be met at each LOA

		LOA 1	**LOA 2**	**LOA 3**	**LOA 4**
CA Protections					
Minimum Physical Security[23] No Lone Zones		ZONE 1 No Stipulation	ZONE 2 As per LOA 1	ZONE 3 As per LOA 1	As per LOA 3 Required
Security Assurance of CA products (including infrastructure and HSMs)		EAL 2 or PP	As per LOA 1	As per LOA 1	As per LOA 1
Minimum Personnel Security (Clearance)[24]		Baseline	As per LOA 1	As per LOA 1	As per LOA 1
Certificate Validity Periods[25]	Root CA	112-bit entropy =20 yr max 128-bit+ entropy = 30 yr max	As per LOA 1	As per LOA 1	As per LOA 1
	Subordinate CA	112-bit entropy =10 yr max 128-bit+ entropy = 15 yr max	As per LOA 1	As per LOA 1	As per LOA 1
	Subscriber	112-bit entropy =2 yr max 128-bit+ entropy = 3 yr max	As per LOA 1	As per LOA 1	As per LOA 1
Credential Management					
Form Factor Credential activation		Software only No Stipulation	Soft or hard As per LOA 1	As per LOA 2 PIN unlock for each use	Hard only As per LOA 3

[23] For further information see [PSMG2] at section 13 of the Gatekeeper PKI Framework

[24] For further information see [APSG] & [AGPSP] at section 13 of the Gatekeeper PKI Framework

[25] Annex A provides indicative guidance on cryptographic algorithms and key lengths.

		LOA 1	LOA 2	LOA 3	LOA 4
Security assurance of credentials		EAL 2 or PP	AS per LOA 1	AS per LOA 1	AS per LOA 1
Key Usage	Digital Signature	Yes	Yes	Yes	Yes
	Non-Repudiation (content commitment)	No	Yes	Yes	Yes
	Key Encipherment	Yes	Yes	Yes	Yes
	Data Encipherment	Yes	Yes	Yes	Yes
	Key Agreement	Yes	Yes	Yes	Yes
	Encipher Only	Yes	Yes	Yes	Yes
	Decipher Only	Yes	Yes	Yes	Yes
Extended Key Usage	Server Authentication	Yes	Yes	Yes	Yes
	Client Authentication	Yes	Yes	Yes	Yes
	Code Signing	No	Yes	Yes	Yes
	Email Protection	Yes	Yes	Yes	Yes
	Smartcard Logon	No	Yes	Yes	Yes
Credential Revocation		Within 96 hrs	Within 72 hrs	Within 48 hrs	Within 24 hrs

	LOA 1	LOA 2	LOA 3	LOA 4
CRL Validity Period (for Subordinate CAs)	60 day max	30 day max	20 day max	10 day max

11.5 Object Identifiers

11.5.1 Gatekeeper Object Identifiers

Subscriber digital certificates issued by CAs **SHOULD** indicate, by means of a certificate extension (mandatory, non-critical) the level of assurance provided by the certificate. This information will be included in the certificate as follows:

Object	Identifier
gatekeeperLOA	{iso(1) member-body(2) australia(36) government(1) gatekeeper(333).loa(5).(n)} where n = the LOA of the certificate 1 = No or little assurance in the binding 2 = Some confidence in the binding 3 = High confidence in the binding 4 = Very high confidence in the binding

11.5.2 Algorithm Object Identifiers

Service Providers **MUST** only certify public keys associated with cryptographic algorithms identified below and **MUST** only use the signature algorithms identified below to sign certificates, CRLs and other PKI products.

11.5.3 Signature Algorithm Object Identifiers

Certificates issued by Service Providers shall identify the signature algorithm using the following object identifiers:

Object	Identifier
sha224WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs–1(1) 14}
sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs–1(1) 11}
sha384WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs–1(1) 12}
sha512WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs–1(1) 13}
ecdsa-with-SHA1	{iso(1) member-body(2) us(840) ansi-x9–62 (10045) signatures (4) 1}
ecdsa-with-SHA256	{iso(1) member-body(2) us(840) ansi-X9–62(10045) signatures(4) ecdsa-with-SHA2 (3) 2}

11.5.4 Subject Public Key Algorithm Object Identifiers

Certificates issued by Service Providers shall identify the cryptographic algorithm associated with the subject public key using the following object identifiers:

Object	Identifier
RsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) PKI certificates(1) PKI certificates–1(1) 1 }
Id-ecPublicKey	{iso(1) member-body(2) us(840) ansi-x9–62(10045) public key-type (2) 1}
id-ecDH	{iso(1) identified-organization(3) certicom(132) schemes(1) ecdh(12)}
Dhpublicnumber	{iso(1) member-body(2) us(840) ansi-x942(10046) number-type(2) 1}

11.5.5 Elliptic Curve Public Key Curve Object Identifiers

Where certificates contain an elliptic curve public key, the parameters shall be specified as one of the following named curves:

Object	Identifier
ansip256r1	{iso(1) member-body(2) us(840) 10045 curves(3) prime(1) 7}
ansip384r1	{iso(1) identified-organization(3) certicom(132) curve(0) 34}
ansip521r1	{iso(1) identified-organization(3) certicom(132) curve(0) 35}

12. Validation Authority

12.1 Validation Authority

A Validation Authority’s primary responsibility is to confirm the currency of a Subscriber’s digital certificate by checking the revocation status of the certificate and advising the Relying Party. This function may involve the VA either checking the revocation status directly with the issuing CA or by the VA itself hosting a copy of the CRL generated by the CA.

A VA will not confirm or otherwise assert whether the certificate is being used within other limits imposed by the issuing CA and published in the relevant CP – this responsibility remains with the Relying Party.

Gatekeeper Accreditation requires there be confidence that the functions performed by the CA and VA interlock satisfactorily to form a consistent and reliable chain of trust. The CA creates and issues digital certificates to Subscribers.

The VA acts as an intermediary between Subscribers and Relying Parties by verifying the currency of digital certificates. It must be trusted by all parties to perform this role to the required LOA. For example, if a CA accredited at LOA 3 utilises a VA then the VA must also obtain LOA 3 accreditation. The protective security requirements to be met by the VA are the same as for CAs (see section 11.4 for further information).

VAs may perform the certificate validation for more than one CA. The assurance of performing this function must be consistent with the obligations of the CA and is to be undertaken in accordance with the CPS of each of the Gatekeeper accredited CA to which the VA provides a service.

13. References

The following sources have been referenced in the Framework.

Term	Definition
[800–57]	National Institute of Standards and Technology, 2012, *Recommendation for Key Management Part 1: General (Revision 3)*, (NIST SP 800–57), National Institute of Standards and Technology, Maryland, USA.
[27005]	International Organization for Standardization, 2011, *Information technology – Security techniques – information security risk management,* (ISO/IEC 27005:2008), International Organization for Standardization, Switzerland.
[AA1983]	Archives Act 1983
[ACP185]	Public Key Infrastructure Tiger Team, 2011, *Public Key Infrastructure (PKI) Cross-Certification Between Combined Communications-Electronic Board (CCEB) Nations*, (ACP185), CCEB, Washington, USA.
[AFDA]	National Archives of Australia, 2010, *Administrative Functions Disposal Authority (AFDA)*, National Archives of Australia, Canberra.
[AGPSP]	Attorney General's Department, 2014, *Australian Government Personnel Security Management Protocol*, Attorney General's Department, Canberra.
[ANAO]	Australian National Audit Office, 2009, *Business Continuity Management: Building resilience in public sector entities*, Australian National Audit Office, Canberra.
[ANZ2009]	Standards Australia/Standards New Zealand, 2009, *Risk management – Principles and guidelines,* (AS/NZS ISO 31000:2009), Standards Australia & New Zealand, Sydney & Wellington.
[ANZ5050]	Standards Australia/Standards New Zealand, 2010, *Business Continuity – Managing disruption-related risk,* (AS/NZS 5050:2010), Standards Australia & New Zealand, Sydney & Wellington.
[APSG]	Attorney General's Department, 2014, *Agency Personnel Security Guidelines*, Attorney General's Department, Canberra.
[BIL]	Attorney General's Department, 2014, *Protective Security Governance Guidelines – Business Impact Levels*, Attorney General's Department, Canberra.
[CABF]	The CA/Browser Forum, 2014, *Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.1.8*, The CA/Browser Forum
[DBN]	Office of the Australian Information Commissioner, 2012, *Data breach notification*, Office of the Australian Information Commissioner, Canberra.

Term	Definition
[ETSI]	European Telecommunications Standards Institute, 2013, *Electronic Signature and Infrastructure (ESI); Policy requirements for certification authorities issuing public key certificates,* (ETSI TS 102 O42), European Telecommunications Standards Institute, Sophia Antipolis Cedex, France.
[FIPS]	National Institute of Standards and Technology, 2001, *Security Requirements for Cryptographic Module*s, (FIPS 140–2), National Institute of Standards and Technology, Maryland, USA.
[GCAP]	Digital Transformation Office 2015, *Gatekeeper PKI Framework Compliance Audit Program (GCAP)*, Digital Transformation Office
[GLEP]	Digital Transformation Office 2015, *Gatekeeper Legal Evaluation Panel,* Digital Transformation Office
[HB167]	C. Gibson, G. Love, N. Fergus, D. Parsons, M. Tarrant, M. Anderson & J. Kilgour, 2006, *Security risk management*, (HB 167:2006), Standards Australia & New Zealand, Sydney & Wellington.
[IAMG]	Digital Transformation Office 2015, *Identity and Access Management Glossary*, Digital Transformation Office
[IRAP]	Digital Transformation Office, 2015, *Gatekeeper PKI Framework Information Security Registered Assessors Program (IRAP) Guide*, Digital Transformation Office
[ISM]	Australian Signals Directorate, 2015, 201*4 Australian Government Information Security Manual: Controls*, Australian Signals Directorate, Canberra.
[ISMG1]	Attorney General's Department, 2014, *Information Security Management Guidelines – Australian Government Security Classification System,* Attorney General's Department, Canberra.
[ISMG2]	Attorney General's Department, 2012, *Information Security Management Guidelines – Management of aggregated information,* Attorney General's Department, Canberra.
[NeAF]	Department of Finance and Deregulation, 2009, *National e-Authentication Framework*, Department of Finance, Canberra.
[NIPG]	Attorney General's Department, 2014, *National Identity Proofing Guidelines,* Attorney General's Department, Canberra.
[PA1988]	Privacy Act 1988
[PA2012]	Privacy Amendment (Enhancing Privacy Protection) Act 2012
[PIA]	Office of the Australian Information Commissioner, 2014, *Guide to undertaking privacy impact assessments*, Office of the Australian Information Commissioner, Canberra.

Term	Definition
[PSMG1]	Attorney General's Department, 2011, *Physical Security Management Guidelines: Physical Security of ICT equipment, systems and facilities*, Attorney General's Department, Canberra.
[PSMG2]	Attorney General's Department, 2012, *Physical Security Management Guidelines – Security Zones and Risk Mitigation Control Measures*, Attorney General's Department, Canberra.
[PSPF]	Attorney General's Department, 2014, *Protective Security Policy Framework*, Attorney General's Department, Canberra.
[RFC3647]	S. Chokhani, W. Ford, R. Sabett, C. Merrill & S. Wu, 2003, *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*, (RFC 3647), The Internet Society, Switzerland.
[RFC5019]	A. Deacon & R. Hurst, 2007, *The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments,* (RFC5019), The Internet Society, Switzerland.
[RFC5280]	D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley & W. Polk, 2008, *Internet X.509 Public Key Infrastructure and Certificate Revocation List (CRL) Profile*, (RFC 5280), The Internet Society, Switzerland.
[RFC6960]	S. Santesson, M. Myers, R. Ankney, A. Malpani, S.Galperin & C.Adams, 2013, *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP*, (RFC6960), The Internet Society, Switzerland.
[SGB]	Attorney General's Department, 2014, *Securing Government Business – Protective Security Guidance for Executives*, Attorney General's Department, Canberra.
[TCPR]	Australian Communications Media Authority 2012, *Telecommunications Cabling Provider Rules 2000 (as amended)*, Australian Communications Media Authority.
[TPISAF]	Department of Finance, 2013, *Third Party Identity Services Assurance Framework,* Department of Finance, Canberra.
[X.500]	International Telecommunications Union, 2012, *X.500: Information Technology – Open Systems Interconnect – The Directory: Overview of concepts, models and services*, (X.500), International Telecommunications Union, Switzerland.
[WebTrust]	Canada Institute of Chartered Accountants, 2011, *Trust Service Principles and Criteria for Certification Authorities, Version 2.0*, Canada Institute of Chartered Accountants, Canada

ANNEX A – Algorithms & Key Lengths

This section has been derived from cryptographic best practice from the National Institute of Standards and Technology (NIST) as described in [800–57].

This section emphasises the importance of acquiring cryptographic systems with appropriate algorithm and key sizes to provide adequate protection for the expected lifetime of the system, and any information to be protected by that system during the lifetime of that information

Comparable Algorithm Strengths

Cryptographic algorithms provide different ‘strengths’ of security, depending on the algorithm and key size used. Two algorithms are considered to be of comparable strength for a given key size if the effort required to ‘break the algorithm’ or determine the key is approximately the same using a given resource. The security strength of an algorithm for a given key size is traditionally described in terms of the amount of work it takes to try all the keys for an algorithm with a key size of "X" that has no short cut attacks (i.e., the most efficient attack is to try all possible keys).

The recommended, comparable key-size classes below are based on assessments made by the cryptographic community. Advances in factoring algorithms, general discrete-logarithm attacks, elliptic-curve discrete-logarithm attacks and quantum computing may affect these equivalences in the future.

New or improved attacks or technologies may be developed that leave some of the current algorithms completely insecure. If quantum attacks become practical, the asymmetric techniques may no longer be secure. Periodic reviews are performed to determine whether the stated equivalences need to be revised. (e.g. the key size needs to be increased) or whether the algorithms are no longer secure.

The table below[26] provides comparable security strengths for AACAs.

1. Column 1 indicates the number of bits of security (entropy) provided by the algorithm and key sizes in a particular row.
2. Column 2 identifies the symmetric-key algorithms that provide the indicated level of security (at a minimum).
3. Column 3 indicates the minimum size of the parameters associated with the standards that use finite-field cryptography. Examples of such algorithms include Digital Signature Algorithm for digital signatures and Diffie-Hellman for key agreements.
4. Column 4 indicates the value for *k* (the size of modulus *n*) for algorithms based on integer-factorisation cryptography. Examples of such algorithms include the RSA algorithm. The value or *k* is commonly considered to be the key size.
5. Column 5 indicates the range of *f* (the size of *n*, where n is the order of the base point *G*) for algorithms based on elliptic-curve cryptography that are specified for digital signatures and for key establishment. The value of f is commonly considered to be the key size.

[26] Table derived from [800–57]

Bits of entropy	Symmetric key algorithms	FFC (e.g. DSA, D-H)	IFC (e.g. RSA)	ECC (e.g. ECDSA)

80	n/a	L = 1024
		N = 160
			K = 1024	F = 160–223

112	3TDEA	L = 2048
		N = 224
			K = 2048	F = 224–225

128	AES–128	L = 3072
		N = 256
			K = 3072	F = 256–383

192	AES–192	L = 7680
		N = 384
			K = 7680	F = 384–511

256	AES–256	L = 15360
		N = 512
			K = 15360	F = 512+

The table below[27] provides comparable security strengths for hashing functions, which, when used provide indicated security strength for the generation of digital signatures and hash message authentication code values, for deriving keys using key-derive functions and for random number generation.

Bits of entropy	Digital signature and hash algorithms	HMAC	Key Derivation Functions[28]	Random Number Generation[29]
80	SHA–1[30]	SHA–1	SHA–1	SHA–1
112	SHA–224	SHA–224	SHA–224	SHA–224
128	SHA–256	SHA–256	SHA–256	SHA–256
192	SHA–384	SHA–384	SHA–384	SHA–384
256	SHA–512	SHA–512	SHA–512	SHA–512

[27] Table derived from [800–57]

[28] The security strength for key-derivation assumes that the shared secret contains sufficient entropy to support the desired security strength

[29] The security strength assumes that the random number generator has been provided with adequate entropy to support the desired security strength

[30] SHA–1 has been demonstrated to provide less than 80 bits of security for digital signatures and may be susceptible to collision attacks. While no practical collision attacks have been published for SHA–1, they may become feasible in the near future. The use of SHA–1 is therefore not suitable for the generation of digital signatures. New systems should use one of the larger hash functions. For the present time SHA–1 is included here for digital signatures to reflect its widespread use in existing systems.

Defining appropriate algorithm suites for accredited Service Providers

Many applications require the use of several different cryptographic algorithms. When several algorithms are used to perform the same service, some algorithms are inherently more efficient because of their design (e.g. AES has been designed to be more efficient that 3DEA).

In many cases, a variety of key sizes may be available for an algorithm. For some of the algorithms (e.g. public key algorithms such as RSA), the use of larger key sizes than are required may have an adverse impact on operations. For example, larger RSA key sizes may take longer to generate or longer to process information. However, the use of key sizes that are too small may not provide adequate security.

The table below[31] provides guidance for Service Providers that may be used to select an appropriate suite of algorithms and key sizes for use with digital certificates. The aim of the table is to provide Service Providers with ‘indicative guidance’ on cryptographic entropy (or security strength) requirements in the coming years.

This guidance is intended to enable Service Providers to better prepare for, and align with algorithms and/or key sizes recommended by the international cryptographic community which are subsequently mandated in the ISM as AACAs. The table is organised as follows:

- Column 1 is divided into two sub-columns. The first sub-column indicates the security strength to be provided. The second sub-column indicates whether cryptographic protection is being applied to data (e.g. digital signing or encryption) or whether cryptographically protected data is being processed (e.g. signature verification or decryption).
- Column 2–5 indicate time frames during which the security strength is acceptable, deprecated, OK for legacy use or deprecated.
  - ‘Acceptable’ indicates that the algorithm or key length is not known to be insecure.
  - ‘Deprecated’ means that the use of an algorithm or key length that provides the indicated security strength may be used if its use has been considered as part of a risk management activity and the residual risk is acceptable to the Service Provider, Subscribers and/or Relying Parties.
  - ‘Legacy-use’ means that an algorithm or key length may be used because of its use in legacy applications; however its continued use should be considered as part of a risk management activity.
  - ‘Disallowed’ means that an algorithm or key length is not a recommended AACA and **MUST NOT** be used for applying cryptographic protection.

Bits of Security Strength		**2010 – 2013**	**2014 – 2030**	**2031+**
80	Applying	Deprecated	Disallowed	Disallowed
	Processing	Legacy Use		Disallowed
112	Applying	Acceptable		Disallowed
	Processing	Acceptable		Legacy Use
128	Applying	Acceptable		

[31] Table derived from [800–57]

<table>
<tr><th colspan="2">Bits of Security Strength</th><th>2010 – 2013</th><th>2014 – 2030</th><th>2031+</th></tr>
<tr><td></td><td>Processing</td><td colspan="3">Acceptable</td></tr>
<tr><td rowspan="2">192</td><td>Applying</td><td colspan="3">Acceptable</td></tr>
<tr><td>Processing</td><td colspan="3">Acceptable</td></tr>
<tr><td rowspan="2">256</td><td>Applying</td><td colspan="3">Acceptable</td></tr>
<tr><td>Processing</td><td colspan="3">Acceptable</td></tr>
</table>

If the security life of information extends beyond one time period specified in the table into the next time period, the algorithm and key sizes specified for the latter time period **SHOULD** be used for applying cryptographic protection. The following examples are provided to clarify the use of the table:

1. If information is cryptographically protected (e.g. digitally signed) in 2010 and the maximum-expected security life of the digitally signed information is two years, any of the approved digital-signature algorithms or keys sizes that provide at least 80 bits of security strength may be used. However if only 80 bits of protection is used, there is some residual risk that the Subscriber and/or Relying Party will need to accept given the 'legacy use' indication in the table.
2. If a similar piece of information was cryptographically protected in 2013 and the maximum-expected security life of the digitally signed information is two years, then an algorithm or key size that provides at least 112 bits of security strength is required.

Transitioning to New Algorithms and Key Sizes

The estimated time period during which data protected by a specific cryptographic algorithm (and key size) remains secure is called the 'algorithm security lifetime'. During this time, the algorithm may be used to both apply cryptographic protection (e.g. digitally sign) and to process the protected information (e.g. to verify a digital signature). The algorithm used is expected to provide adequate protection for the protected data during this time, which depending on legislative or regulatory requirements of the Service Provider, their Subscribers and/or Relying Parties may be in the order of several years or decades.

Typically, a Service Provider selects the cryptographic services that are needed for a particular application or service. Then, based on the algorithm security lifetime and the security life of the data to be protected, an algorithm and key size suite is selected that is sufficient to meet the requirements.

The organisation then establishes a key management system and supporting cryptographic key management plan, which includes validated cryptographic products that provide the services required by the application. As an algorithm and/or key size suit nears its expiration date, transitioning to a new algorithm and key size suite **SHOULD** be planned and documented in the CKMP.

When the algorithm or key size is determined to no longer provide the desired protection for information (e.g. if the algorithm may be have been 'broken'), any information 'protected' by the algorithm or key size is considered to be 'suspect' (the data may no longer be confidential, or the integrity cannot be assured). If the protected data is retained, it **SHOULD** be re-protected using an AACA and key size that will protect the information for the remainder of its security life.

ANNEX B – Certificate Profile

The tables below[32] contain specific certificate information and extensions to ensure operational integrity. The tables do not address all certificate extensions. Other use extensions **SHOULD** conform to RFC5280. Extensions that do not confirm to RFC5280 shall be marked non-critical. The table uses the following terms:

- **Required critical** – the extension shall be present and is always marked critical.
- **Required** – the extension shall be present and may be marked non-critical.
- **Optional** – the extension may be included at a Service Provider's discretion.
- **Not Used** – the extension shall never be used.

Root CA Certificate

Field/ Extension	Root CA Certificate
Version	**Required**
	V3 (2)
Serial Number	**Required**
	Must be unique to an Issuer
Issuer Signature Algorithm	**Required**
	• **sha256WithRSAEncryption {1 2 840 113549 1 1 11}** Or one of the following signature algorithms: • sha224WithRSAEncryption {1 2 840 113549 1 1 14} • sha384WithRSAEncryption {1 2 840 113549 1 1 12} • sha512WithRSAEncryption {1 2 840 113549 1 1 13} • ecdsa-with-SHA1 {1 2 840 10045 4 1} • ecdsa-with-SHA256 {1 2 840 10045 4 3 2} • ecdsa-with-SHA384 {1 2 840 10045 4 3 3} • ecdsa-with-SHA512 {1 2 840 10045 4 3 4}
Issuer Distinguished Name	**Required**
	Each RDN is a printableString and contains a single attribute type and attribute value tuple

[32] Tables have been derived from [ACP185]

Field/ Extension	Root CA Certificate
Validity Period	**Required**
	Maximum of 20 years from date of issue in UTC format if using 112-bits of security Maximum 30 years from date of issue in UTC format if using at least 128-bits of security. Note: the notBefore component will be the certificate’s issue date. The notAfter component is the day ending the validity period.
Subject Distinguished Name	**Required**
	Each RDN is a printableString and contains a single attribute type and attribute value tuple
Subject Public Key Information	**Required**
	Key size to provide at least 112 bits of security strength or greater for certificates with a maximum validity period of 20 years Key size to provide at least 128 bits of security strength or greater for certificates with a maximum validity period of 30 years The following encryption algorithms are acceptable: • RsaEncryption {1 2 840 113549 1 1 1 } • Id-ecPublicKey {1 2 840 10045 2 1}
Issuer Unique Identifier	**Not Used**
Subject Unique Identifier	**Not Used**
Issuer’s Signature	**Required**
	ASN.1 DER encoded certificate signature value corresponding to Issuer signature algorithm
Authority Key Identifier	**Optional**
	keyID, Octet String Recommended that that the octet string contain the 20 byte SHA–1 hash of the binary DER encoding of the subject CA’s public key information
	Not Used
	Issuer DN, Serial Number tuple
Subject Key Identifier	**Required**

Field/ Extension	**Root CA Certificate**
	Recommended that the octet string contain the 20 byte SHA–1 hash of the binary DER encoding of the subject CA's public key information
Key Usage	**Required** **Critical**
	keyCertSign, CRLSign
Basic Constraints	**Required** **Critical**
	cA True; path length constraint absent or value per PKI hierarchy
Extended Key Usage	**Not Used**
Private Key Usage Period	**Not Used**
Certificate Policies	**Required**
	Sequence of one or more policy information terms, each of which consists of an object identifier OID and optionally id-qt-cps | id- qt-unotice qualifiers
Field/ **Extension**	Root CA Certificate
Policy Mappings	Optional
	Sequence of one or more pairs of OIDs; each pair includes an issuerDomainPolicy and a subjectDomainPolicy
Subject Alternative Name	**Not Used**
Issuer Alternative Name	**Not Used**
Subject Directory Attributes	**Not Used**
Name Constraints	**Optional**
	If included, it shall contain permittedSubtrees or excludedSubtrees field. Recommend that if asserted it be marked critical.
Policy Constraints	**Optional**
	inhibitPolicyMapping with skipcerts=0
	Required

Field/ Extension	**Root CA Certificate**
Authority Information Access	id-ad-caIssuers Primary HTTP URI mandatory Secondary LDAP URI optional
	id-ad-ocsp Optional
CRL Distribution Points	**Optional**
	Primary HTTP URI mandatory Secondary LDAP URI optional
Subject Information Access	**Optional**
	Id-ad-carepository Primary HTTP URI mandatory if extension is present Secondary LDAP URI optional
Freshest CRL	**Not Used**
Inhibit Any Policy	**Optional** [33]
	skipcerts=0

[33] This is not conformant to RFC 5280 however is required do overcome potential application compatibility issues

Subordinate CA Certificate

Field/ Extension	Subordinate **CA certificate**
Version	**Required**
	V3 (2)
Serial Number	**Required**
	Must be unique to an Issuer
Issuer Signature Algorithm	**Required**
	• **sha256WithRSAEncryption {1 2 840 113549 1 1 11}** Or one of the following signature algorithms: • sha224WithRSAEncryption {1 2 840 113549 1 1 14} • sha384WithRSAEncryption {1 2 840 113549 1 1 12} • sha512WithRSAEncryption {1 2 840 113549 1 1 13} • ecdsa-with-SHA1 {1 2 840 10045 4 1} • ecdsa-with-SHA256 {1 2 840 10045 4 3 2} • ecdsa-with-SHA384 {1 2 840 10045 4 3 3} • ecdsa-with-SHA512 {1 2 840 10045 4 3 4}
Issuer Distinguished Name	**Required**
	Each RDN is a printableString and contains a single attribute type and attribute value tuple.
Validity Period	**Required**
	Maximum of 10 years from date of issue in UTC format if using 112-bits of security Maximum 15 years from date of issue in UTC format if using at least 128-bits of security. Note: the notBefore component will be the certificate's issue date. The notAfter component is the day ending the validity period.
Subject Distinguished Name	**Required**
	Each RDN is a printableString and contains a single attribute type and attribute value tuple.
	Required

Field/ Extension	Subordinate **CA certificate**
Subject Public Key Information	Key size to provide at least 112 bits of security strength or greater for certificates with a maximum validity period of 10 years Key size to provide at least 128 bits of security strength or greater for certificates with a maximum validity period of 15 years The following encryption algorithms are acceptable: • RSAEncryption {1 2 840 113549 1 1 1 } • id-ecPublicKey {1 2 840 10045 2 1}
Issuer Unique Identifier	**Not Used**
Subject Unique Identifier	**Not Used**
Issuer’s Signature	**Required**
	ASN.1 DER encoded certificate signature value corresponding to Issuer signature algorithm.
Authority Key Identifier	**Required**
	keyID, Octet String Recommended that that the octet string contain the 20 byte SHA–1 hash of the binary DER encoding of the subject CA’s public key information
	Not Used
	Issuer DN, Serial Number tuple
Subject Key Identifier	**Required**
	Recommended that that the octet string contain the 20 byte SHA–1 hash of the binary DER encoding of the subject CA’s public key information.
Key Usage	**Required** **Critical**
	keyCertSign, CRLSign and, optionally, others to include digitalSignature and nonRepudiation
Basic Constraints	**Required** **Critical**
	cA True; path length constraint per PKI hierarchy
Extended Key Usage	**Not Used**

Field/ Extension	Subordinate **CA certificate**
Private Key Usage Period	**Not Used**
Certificate Policies	**Required**
	Sequence of one or more policy information terms, each of which consists of an OID and optionally ID-QT-CPS and ID-QT-UNotice. Qualifiers.
Subject Alternative Name	**Not Used**
Issuer Alternative Name	**Not Used**
Subject Directory Attributes	**Not Used**
Authority Information Access	**Optional**
	id-ad-caIssuers
	Primary HTTP URI mandatory Secondary LDAP URI optional
	id-ad-ocsp **Optional**
CRL Distribution Points	**Required**
	Primary HTTP URI mandatory Secondary LDAP URI optional
Subject Information Access	**Optional**
	Id-ad-carepository Primary HTTP URI mandatory if extension is present Secondary LDAP URI optional
Freshest CRL	**Not Used**

Subscriber Certificate

Field/ Extension	Subscriber Certificate
Version	**Required**
	V3 (2)
Serial Number	**Required**
	Must be unique to an Issuer
Issuer Signature Algorithm	**Required**
	• sha256WithRSAEncryption {1 2 840 113549 1 1 11} Or one of the following signature algorithms: • sha224WithRSAEncryption {1 2 840 113549 1 1 14} • sha384WithRSAEncryption {1 2 840 113549 1 1 12} • sha512WithRSAEncryption {1 2 840 113549 1 1 13} • ecdsa-with-SHA1 {1 2 840 10045 4 1} • ecdsa-with-SHA256 {1 2 840 10045 4 3 2} • ecdsa-with-SHA384 {1 2 840 10045 4 3 3} • ecdsa-with-SHA512 {1 2 840 10045 4 3 4}
Issuer Distinguished Name	**Required**
	Each RDN is a printableString and contains a single attribute type and attribute value tuple
Validity Period	**Required**
	Maximum of 2 years from date of issue in UTC format if using 112-bits of security Maximum 3 years from date of issue in UTC format if using at latest 128-bits of security. Note: the notBefore component will be the certificate's issue date. The notAfter component is the day ending the validity period.
Subject Distinguished Name	**Required**
	Each RDN is a printableString and contains a single attribute type and attribute value tuple directoryString is encoded as printableString cn={ Host URL | Host IP Address | Host Name }
Subject Public Key	**Required**

Field/ Extension	Subscriber Certificate
Information	Key size to provide at least 112 bits of security strength or greater for certificates with a maximum validity period of 2 years Key size to provide at least 128 bits of security strength or greater for certificates with a maximum validity period of 3 years The following encryption algorithms are acceptable: • RSAEncryption {1 2 840 113549 1 1 1 } • id-ecPublicKey {1 2 840 10045 2 1} • id-ecDH {1 3 132 1 12} • dhpublicnumber {1 2 840 10046 2 1}
Issuer Unique Identifier	**Not Used**
Subject Unique Identifier	**Not Used**
Issuer's Signature	**Required**
	ASN.1 DER encoded certificate signature value corresponding to Issuer signature algorithm
Authority Key Identifier	**Required**
	keyID, Octet String Recommended that that the octet string contain the 20 byte SHA–1 hash of the binary DER encoding of the subject CA's public key information
	Not Used
	Issuer DN, Serial Number tuple
Subject Key Identifier	**Required**
	Recommended that that the octet string contain the 20 byte SHA–1 hash of the binary DER encoding of the subject CA's public key information
Key Usage	**Required**
	Critical
	One or more of: digital signature, non repudiation, key encipherment, data encipherment, key agreement
Basic Constraints	**Not Used**
Extended Key Usage	**Optional**

Field/ Extension	Subscriber Certificate
Private Key Usage Period	**Not Used**
Certificate Policies	**Required**
	Sequence of one or more policy information terms, each of which consists of an OID and optional qualifiers
Policy Mappings	**Optional**
Subject Alternative Name	**Optional;** Recommended RFC 822 Name and UPN
Issuer Alternative Name	**Not Used**
Subject Directory Attributes	**Optional**
Name Constraints	**Not Used**
Policy Constraints	**Not Used**
Authority Information Access	**Required**
	id-ad-caIssuers Primary HTTP URI mandatory Secondary LDAP URI optional
	id-ad-ocsp **Optional**
CRL Distribution Points	**Required**
	Primary HTTP URI mandatory Secondary LDAP URI optional
Subject Information Access	**Not Used**
Freshest CRL	**Not Used**
Inhibit Any Policy	**Not Used**