Australian Government

Department of Defence

Public Key Infrastructure

Defence Public Key Infrastructure Levels of Assurance Requirements Certificate Policy Object Identifiers (OIDs)

Version 2.0

May 2016

Owner

Defence PKI Policy Board
c/ CDMC (DKN-S1-078)
Department of Defence
PO Box 7920
CANBERRA BC ACT 2610

Authorisation

Peter Lavender
PKI Operations Manager

Signature: _____ *(Date)*

Document acceptance

FUNCTION	DATE	NAME	POSITION	SIGNATURE
Prepared:	**Apr 2011**	Verizon Business		
Reviewed:		R. Brown	PKI Engineer	
Reviewed:	**Nov 2014**	G. Fittler	PM PKI Certificate Project	
Released:	**Nov 2014**	P. Lavender	Ops Man PKI	

Change History[1]

VERSION	ISSUE DATE	DESCRIPTION/ AMENDMENT	CHANGED BY
0.1 Draft	Apr 2011	Initial draft	Verizon Business
1.0	Nov 2014	Updated and released.	G. Fittler, P. Lavender
2.0	May 2016	Released	PKI Operations Manager

[1]

Reference Documents

CODE	DOCUMENT NAME
[XCA-Options]	Cross Certification Options Paper v0.3 – April 2010
[Pub1010]	CCEB Publication 1010 – PKI Cross-Certification between CCEB Nations v1.3.4.2 – September 2010
[RFC5280]	Internet X.509 PKI Certificate and CRL Profile – May 2008
[PIV-I]	X.509 Certificate and CRL Profile for Personal Identity Verification Interoperable Cards
[GK2015]	Gatekeeper PKI Framework - v3.1 December 2015
[MS-Agree]	Microsoft Windows – Government Certification Authority Agreement
[NIST800-131]	NIST Special Publication 800-131A Rev. 1 – Transitions: Recommendations for Transitioning the Use of Cryptographic Algorithms and Key Lengths – November 2015
[NIST800-78-3]	NIST Special Publication 800-78-4 – Cryptographic Algorithms and Key Sizes for Personal Identity Verification – May 2015
ISO 29115	(DRAFT) Entity Authentication Assurance
ISM	Australian Government Information and Communications Technology Security Manual
PSM	Commonwealth Protective Security Manual
NeAF	National e-Authentication Framework – January 2009
	National Identity Security Strategy's Gold Standard Enrolment Framework

CONTENTS

FIGURES

TABLES

EXECUTIVE SUMMARY

All human co-operation is based on trust, meaning that we choose co-operation partners and make commitment decisions based on how much we trust the other party. Digital certificates and public-key infrastructures represent an attempt to mimic real-world human assessment of identity and trustworthiness in an automated and mechanical fashion[2].

An accurate determination of an entities identity is needed to make sound access control and security decisions in both the logical and physical environments.

In order to conduct business in an online world, entities need to be able to identify themselves remotely and reliably. However, different Public Key Infrastructures (PKI) / Identity Providers (IdP) follow different policies and procedures for issuing electronic identity credentials.

Identity assurance, in an online context, is the ability of a Relying Party to determine, with some level of certainty, that a claim to a particular identity made by some entity can be trusted to actually be the claimant's "true" identity. Identity claims are made by presenting an identity credential to the Relying Party. In the case of Defence where the entity is a person or resource involved in information assurance, this credential is an X.509 digital certificate.

In order to promote trust, improve interoperability and facilitate identity federation across organisations and borders the Defence PKI is required to express a Level of Assurance (LoA) Object Identifier (OID) within its certificate profile that can be used by Relying Parties who must trust the electronic identity provided by the Defence PKI.

The level of assurance provided is measured by the strength and rigor of the identity proofing process, the credential's strength, and the management processes the service provider applies to it.

Defence has defined four levels of assurance (LoA) that can be assigned to individuals and three levels for resources. These are:

Table 1 – Defence Assurance Levels

ASSURANCE LEVEL		INDIVIDUAL	RESOURCE	DESCRIPTION
1	**Low Assurance**	X	X	Little or no confidence in the asserted identity
2	**Medium Assurance**	X	X	Some confidence in the asserted identity
3	**High Assurance**	X	X	High confidence in the asserted identity
4	**Very High Assurance** (High Assurance with Biometrics)	X		Very High confidence in the asserted identity

Defence has determined, based on the National e-Authentication Framework risk consequences matrix, the Level of Assurance required:

a. for Defence individuals is LoA4 (Very High Assurance); and

b. the minimum level of assurance for Defence Resources is LoA2 (Medium Assurance).

[2] Audun Jøsang, Ingar Glenn Pedersen, and Dean Povey (2000) *PKI Seeks a Trusting Relationship*, ACISP '00 Proceedings of the 5th Australasian Conference on Information Security and Privacy

1 INTRODUCTION

The Australian Defence Organisation (ADO) is expanding the capability of the Defence Public Key Infrastructure (PKI) through initiatives like cross certification with other member nations of the Combined Communications-Electronics Board (CCEB) and the publication of the Defence PKI Root Certification Authority (RCA) certification into the Microsoft Root Certificate Store.

This expansion has led to a reassessment of the certificates that the Defence PKI issues and the ability of a Relying Party to gain a level of trust in a certificate.

In order to conduct business in an online world, entities need to be able to identify themselves remotely and reliably. In most cases, however, it is not sufficient for the typical electronic credential (usually a basic userID/password pair or a digital certificate) to simply make the assertion that "I am who I say I am - believe me." A Relying Party needs to be able to know to some degree of certainty that the presented electronic identity credential truly represents the entity presenting the credential. In the case of self-issued credentials, this isn't possible. However, within Defence electronic identity credentials are issued by the Defence PKI.

Four separate audiences are affected by a transaction---and the inherent trust therein:

1. Users of electronic identity credentials,
2. Entities that rely upon the credentials issued by the Defence PKI,
3. Providers of electronic identity provider (IdP) services and auditors or assessors who review the business processes of IdPs (within the ADO this is the Defence PKI), and
4. Relying Parties who must trust electronic identity credentials provided by the Defence PKI.

Different PKIs/IdPs follow different policies and procedures for issuing electronic identity credentials. In the business world, and especially in government, the more trustworthy the credential, the more stringent the rules governing identity proofing, credential management and the kind of credentials issued. But while different IdPs follow their own rules, more and more end users (also called subscribers) and online services (often called relying parties) wish to trust existing credentials and not issue yet another set of userID/passwords or other credentials for use to access one service. This is where the concept of assurance levels within the federated identity environment becomes important. Assurance levels provides PKIs/IdPs and relying parties with a common set of identity trust conventions that transcend individual PKI/IdPs, users, or networks, so that a relying party will know it can trust a credential issued by PKI/IdP 'A' at a level of assurance comparable to a common standard, which will also be agreed upon by PKI/IdPs 'B,' 'C,' and 'D.'

The ADO, through the Defence PKI issues certificates to end entities. In order to promote trust, improve interoperability and facilitate identity federation across organisations and borders the Defence PKI is required to express an Assurance Level Object Identifier (OID) within its certificate profile that can be used by Relying Parties who must trust the electronic identity provided by the Defence PKI.[3]

The overall goal is to achieve appropriate security assurance for multiple applications by efficiently verifying the claimed identity of entities seeking electronic access to, or purporting to be from, the Defence Information Environment (DIE).

[3] The PKI is validating the linkage between the provided identity and the digital certificate so that the Level of Assurance expressed in the certificate is correct.

1.1 Scope

This document details the Levels of Assurance (LoA) that will be applied to Defence entities issued certificates by the Defence PKI and their associated OIDs.

This document will be used by Relying Parties to map Assurance Levels in order to determine trust in the representative electronic entity. As such, it documents the levels of assurance and the underlying methodology and controls that the Defence PKI undertakes to issue a certificate that pertains to a certain level of assurance.

1.2 Qualifications

The LoA expressed in Defence certificates does not include assurance with respect to the application using the certificate (eg. email or web page systems, etc) as the PKI does not control their implementation or configuration. It has been assumed that they correctly apply the tenets of X.509.

It is the implementer's responsibility to ensure that the components, interfaces, communications, storage media, managerial processes and services used within the identity verification process are designed and built in a secure manner.

Whilst authentication of an entities identity is a fundamental component of physical and logical access control processes, this document does not specify assurance levels in relation to physical access[4].

1.3 Deviations

Certificates issued by the Defence PKI will be aligned with this document, however, the ADO reserves the right to risk manage implementation shortfalls from the LoA being expressed. Where applicable the outcome of the risk assessment will be documented in the relevant Certificate Policy where it deviates from a LoA being expressed.

When a deviation is granted, the PKI Policy Board shall post the deviation on a web site accessible by Relying Parties, and shall either initiate a permanent change to the policy, or shall place a specific time limit on the deviation.

[4] Humans can use the card 'token' for visual comparison, whereas automated systems can use the electronically stored data to conduct automated identity verification.

2 ASSURANCE LEVELS

2.1 Background

Identity assurance, in an online context, is the ability of a Relying Party to determine, with some level of certainty, that a claim to a particular identity made by some entity can be trusted to actually be the claimant's "true" identity. Identity claims are made by presenting an identity credential to the Relying Party. In the case where the entity is a person, this credential may take several forms, including:

a. personally identifiable information such as name, address, birth date, etc;

b. an identity proxy such a username, loginID, or email address; and

c. an X.509 digital certificate.

Identity assurance specifically refers to the degree of certainty that an identity assertion made by a PKI, or IdP, to a Relying Party about some entity, actually refers to the entity who made a claim of identity by presenting an identity credential to the Relying Party. In order to issue this assertion, the PKI must first determine whether or not the claimant possesses and controls an appropriate token, using a predefined authentication protocol. Depending on the outcome of this authentication procedure, the assertion returned to the Relying Party by the PKI allows the Relying Party to decide whether or not to trust that the identity associated with the credential actually "belongs" to the person presenting the credential.

The degree of certainty that a Relying Party can have about the true identity of the entity presenting an identity credential, after receiving an identity assertion from a PKI, is what is referred to as the "Assurance Level". Assurance Levels are the levels of trust associated with a credential as measured by the associated technology, processes, and policy and practice statements controlling the operational environment associated with the credentials, tokens, and authentication procedures. (Within a PKI this is typically documented in accordance with RFC 3647 within the Certificate Policy.)

The level of assurance provided is measured by the strength and rigor of the identity proofing process, the credential's strength, and the management processes the service provider applies to it.

Figure 1 identifies the high level components that are used in determining the levels of assurance within Defence.

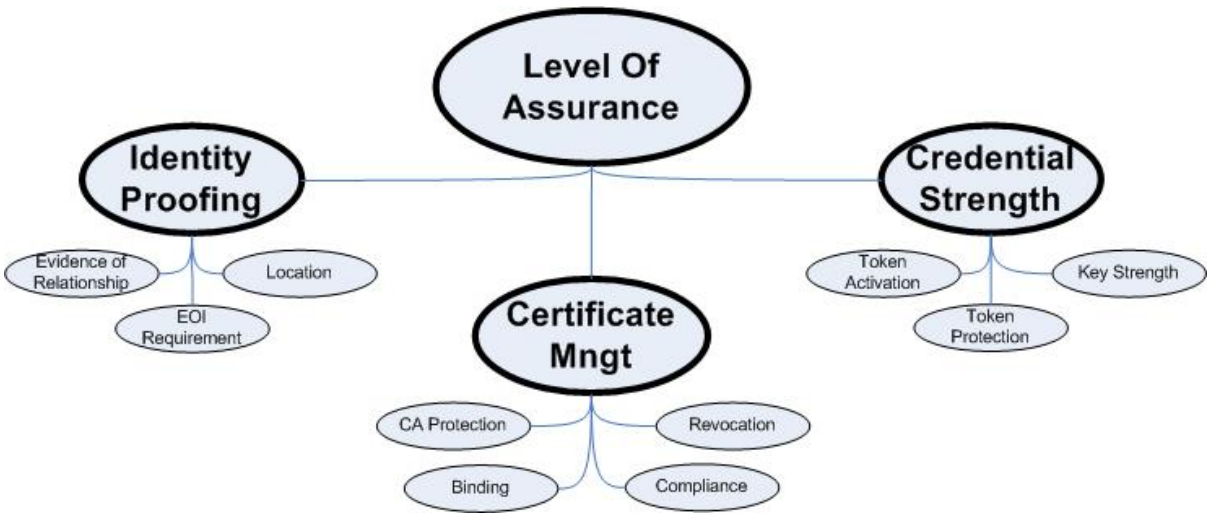

Figure 1 – Components used to measure Levels of Assurance

2.2 Assurance Level Definition

The Draft ISO 29115 (Entity Authentication Assurance) defines four LoA. Each LoA describes the degree of confidence in the processes leading up to and including the authentication process itself, thus providing the assurance that the entity asserting a particular identity (i.e. the claimant) is in fact the entity to which that identity was assigned. The claimant can be a human or non-person entity (NPE).

The ISO associates LoA1 as the lowest level of assurance and LoA4 as the highest level of assurance.

Each assurance level has a set of minimum requirements that must be met in the areas of identity proofing, certificate management and the strength of the credential. In addition, these requirements may be different for an individual compared to a resource. For example, an individual will need to prove who they are and their association with the ADO within the EOI measurement requirement, whereas a resource may require validation that the resource is providing an ADO business need, and validation of the resource owner's identity.

The LoA associated with a public key certificate is an assertion of the Certificate Authority (CA) of the degree of confidence the Relying Party may reasonably place in the binding of the Subscriber's public key to the identity and the privileges asserted in the certificate. LoA depends on the proper registration of Subscribers and proper generation and management of the certificate and associated private keys. Personnel, physical, procedural and technical security controls contribute to the assurance level issued by a PKI.

As such, the Defence PKI will assign assurance levels to both individuals and resources based on the four levels of assurance detailed in Table 2, although all four levels may not be issued to resources.

Table 2 – Defence Levels of Assurance

ASSURANCE LEVEL		DESCRIPTION
1	**Low Assurance**	Little or no confidence in the asserted identity
2	**Medium Assurance**	Some confidence in the asserted identity
3	**High Assurance**	High confidence in the asserted identity
4	**Very High Assurance** (High Assurance with Biometrics)	Very High confidence in the asserted identity

2.3 Assurance Level Selection

Determining which LoA is appropriate in a given situation depends on a variety of factors based on a risk assessment of the transactions or services for which the entities will be authenticated. It is mainly based on the consequences of an authentication error and or misuse of credentials, the resultant harm or impact and their likelihood of occurrence. The higher the perceived risk, the higher the LoA should be and therefore the more stringent the requirements for assurance. Lower authentication requests can use either suitable low assurance certificates or correspondingly a higher assured certificate.

By mapping impact levels to LoA, parties to an authentication transaction can determine what LoA they require and then identify if the identity being asserted meets that LoA prior to placing relance on the assured identify accordingly.

The following table provides an indicative description of possible consequences and their respective severities based on the Australian National e-Authentication Framework (NeAF).

Table 3 – NeAF LoA consequence and severity

CONSEQUENCE	SEVERITY				
Consequence rating	**Insignificant**	**Minor**	**Moderate**	**Major**	**Severe**
Inconvenience to any party	No inconvenience	Minimal inconvenience	Minor inconvenience	Significant inconvenience	Substantial inconvenience
Risk to any party's personal safety	No risk	No risk	No risk	Any risk to personal safety	Threaten life directly
Release of personally or commercially sensitive data to third parties without consent	No impact	Would have little impact	Measurable impact, breach of regulations or commitment to confidentiality	Release of information would have a significant impact	Would have severe consequences to a person, agency or business
Financial loss to any client of the service provider[5] or other third party	No loss	Minimal	Minor	Significant	Substantial
Financial loss to Agency / service provider	No loss	Minimal < 2% of monthly agency budget	Minor 2% to < 5% of monthly agency budget	Significant 5% to < 10% of monthly agency budget	Substantial ≥ 10% of monthly agency budget
Impact on government finances or economic and commercial interests	No impact	No impact	Cause financial loss or loss of earning potential	Work significantly against	Substantial Damage
Damage to any party's standing or reputation	No damage	No damage	Minor: short-term damage	Limited long-term damage	Substantial long-term damage
Distress caused to any party	No distress	No distress	Minor: short-term distress	Limited long-term distress	Substantial long-term distress
Threat to government agencies' systems or capacity to conduct their business	No threat	No threat	No threat	Agency business or service delivery impaired in any way	Agency business halted or significantly impaired for a sustained period[6]
Assistance to serious crime or hindrance of its detection	Would not assist in or hinder detection of unlawful activity	Would not assist in or hinder detection of unlawful activity	Prejudice investigation or facilitate commission of violations that will be subject to enforcement efforts	Impede investigation or facilitate commission of serious crime	Prevent investigation or directly allow commission of serious crime

The information security classification level associated with the information that will be "exchanged" during the transaction is also a consideration in assessing the consequences of a particular threat being realised.

Information with a protective marking of "Sensitive" and / or classified at "PROTECTED" and above can only be transmitted across an unclassified network such as the internet under certain circumstances. While the adoption of higher-assurance may represent one solution to mitigate threats in relation to classified information the application of alternative risk mitigation approaches will need to be considered (eg. 'bearer' or 'in-line' network encryption).

5 The amounts to be considered are suggested as: Minimal <$50; Minor $50 to <$200; Significant $200-<$2000; and Substantial ≥ $2,000. These figures are guidelines only based on impact on an "average" individual. Where the client is known to be a corporation of other similar entity, these figures would need to be adjusted upward. If multiple clients will suffer the loss, the impact level should be adjusted accordingly to reflect the total losses to clients.

6 The period here may vary from agency to agency – some agencies may be able to endure a halt in business for a number of days without serious impact on the government or society. Others more directly involved in public safety and similar services would be less tolerant of outages.

Based on identifying that eight out of ten areas of the impact matrix have a Severe rating, Defence has determined that the LoA required:

a. for Defence individuals is LoA4 (Very High Assurance); and

b. the minimum level of assurance for Resources[7] or non-person entities (NPE) is LoA2 (Medium Assurance).

2.3.1 Level of Environmental Protection

The Defence data networks on which the certificates will be used will have various levels of protection. Examples of mechanisms that provide network protection include network encryption, physical isolation, accredited gateways or data diodes, and firewalls. These mechanisms are used to create a collection of system high networks and enclaves. The probability of attack on protected networks is reduced because:

a. access is limited to people individually identifiable and authorised to use the network and its interconnection points with other networks (i.e., the gateways or firewalls);

b. even for those with access, risk tolerance must be high, due for example to the lack of anonymity on the network and its access points; and,

c. the capabilities of an attacker inside the network are hampered by the lack of availability of hacker tools, and the difficulty of bringing them from the outside.

The true amount of risk reduction associated with using these mitigation mechanisms can only be determined by a system security evaluation. Examples of differing levels of environmental protection are:

2.3.1.1 Highly Secured Environment:

Networks that are protected either with encryption devices approved by the Defence Signals Directorate (DSD) for protection of classified data, DSD approved gateways or data diodes, or via physical isolation, and that are certified for processing system-high classified data, where exposure of unencrypted data is limited to individuals holding appropriate security clearances.

2.3.1.2 Moderately Secured Environment:

Physically isolated networks or networks connected to the internet via DSD approved gateways/firewalls or data diodes in which access is restricted based on legitimate need. Additionally, the networks are protected by DSD approved Type 1 encryption and may be accessible by foreign nationals.

2.3.1.3 Minimally Secured Environment:

Unencrypted networks connected to the Internet, either directly or via a firewall.

2.4 General Usage

The guidance in this section is based on the previous discussion of consequence rating and information value. Emphasis is placed on two types of activity: integrity and access control to information considered sensitive by Defence and information related to electronic transactions or e-commerce (financial and/or authoritative).

The authority responsible for approving the specific LoA required for a particular implementation will vary from organisation to organisation but within Defence is the

[7] Internationally the term NPE is gaining favour over the terms Resources or Devices (in the PKI environment they were associated with Type 3 or Device certificates). In the context of Defence the term Resource implies NPE.

applicable Business Owner (who will have to consider the Relying Parties needs) and is normally the system accreditation agency acting in accordance with the applicability guidance detailed below.

2.4.1 LoA1 – Low Assurance

This level is intended for applications handling unclassified information of low value transmitted across an unclassified network (eg. internet). Generally Defence CAs should not issue Low Assurance certificates; in preference the Defence PKI should issue Medium and above assurance certificates exclusively. Access to Defence information resources shall never be allowed on the basis of Low Assurance certificates. Low assurance certificates, (or non-Defence equivalent certificates) may be accepted by Defence relying parties for the purpose of authenticating or encrypting communication that does not access or process Defence information (e.g., meeting coordination, accessing web site information that has been cleared for unlimited distribution). These certificates may, for example, be issued by non-Defence commercial providers.

2.4.2 LoA2 – Medium Assurance

This level is intended for applications handling unclassified medium value information in Moderately Secured Environments, unclassified high value information in Highly Secured Environments, and discretionary access control of classified information in Highly Secured Environments.

Guidance:

a. All applications appropriate for Low Assurance certificates;

b. Digital signature services for systems handling information that is determined to be vital to the operational readiness or mission effectiveness of deployed forces in terms of both content and timeliness and national security information on an encrypted network;

c. Privacy and authentication in support of access control security services (e.g., separation of communities of interests) for access to classified Special Compartmented or Special Access information on networks protected using DSD approved Type 1 cryptography appropriate to the data being protected, or on networks that are physically isolated and approved to process the classified data; and,

d. Acceptable non-repudiation for routine orders, administrative processes and minor value financial transactions other than transactions involving issuance or acceptance of contracts and contract modifications. This would include acceptance and payment for small and medium value financial transactions, travel claims, payroll, etc.

2.4.3 LoA3 – High Assurance

This level is intended for applications handling unclassified medium value information in Minimally Secured Environments, unclassified high value information in Moderately Secured Environments, and discretionary access control of classified information in Highly Secured Environments. This level is also intended for all applications operating in environments appropriate for Medium Assurance but which require a higher degree of assurance and technical non-repudiation.

Guidance:

a. All applications appropriate for Low or Medium Assurance certificates;

b. Authentication of individuals to services operating within the Defence domains; and

c. Acceptable non-repudiation for operational orders, medium value financial transactions and performing contracting and contract modifications.

2.4.4 LoA4 – Very High Assurance

This level is intended for applications handling high value unclassified information in Minimally Secured environments.

Guidance:

a. All applications appropriate for Medium and High Assurance certificates;

b. Digital signature services for unclassified or national security information in an unencrypted network;

c. Protection (authentication and confidentiality) for information crossing classification boundaries when such a crossing is already permitted under a system security policy (e.g., sending unclassified information through a data diode from RESTRICTED to SECRET); and,

d. Technical non-repudiation for major value financial or electronic commerce applications.

3 ASSURANCE COMPONENTS

As identified in Figure 1 above, the ADO has a number of components that is used to provide the foundation for the determining the appropriate assurance level provided for an individual or resource.

In order to increase Relying Party acceptance Defence has expressed, where possible, the metric used for the respective components upon internationally available references.

The guidelines used to determine the measurement of the respective components include: (Draft) ISO 29115; the publications released by the US National Institute of Science and Technology (NIST); NeAF; the Australian Government Gatekeeper Framework; the Australian Government Information and Communications Technology Security Manual and the Commonwealth Protective Security Manual (see the Reference Documents for full list of references).

The following table documents the concepts behind the significant LoA components within the ADO. Other factors, or constraints, are amplified in the relevant Certificate Policy and Relying Parties should refer to these.

Table 4 – Significant LoA Component definitions

IDENTITY PROOFING	
	• Evidence of Identity (EOI) EOI is the validation of the process that confirms that the individual or resource has uniquely validated their identity to the PKI. The EOI validation for an individual is simply ensuring that an appropriate process is followed, and that the individual provides enough documentation to uniquely confirm their identity. The EOI validation for a resource is a little more complex, which is why the level of assurance measurement is separated for resources and individuals. In simple terms, the EOI of a resource is validation that the resource is ADO owned and controlled. In addition, how often an entity has to revalidate (refresh) their identity over the life of their association with the PKI assists in providing confidence to Relying Parties. Measurement of EOI assurance within the ADO is aligned with the Gatekeeper PKI Evidence of Identity Policy and the National Identity Security Strategy's Gold Standard Enrolment Framework (with modifications for Defence application in accordance with ISO 29115, as appropriate). NB. For all certificates issued the Defence PKI shall ensure that names are unique within the ADO and be capable of providing records of identity proofing to Relying Parties as necessary.
	• Evidence of Relationship The general principle is: the closer the relationship between entities the higher the confidence in the identity. As such, the Subscriber can either be completely divorced from the 'registration authority' or 'known' to the organisation (more assurance if known and using certificates within the registration authorities' environment). In relation to RFC 3647 this is associated with 'Who can submit an application'. *For a commercial CA this can somewhat be equated to aligning increases in confidence levels to increases in the guarantees offered*. For all Defence certificates there must be evidence of a relationship ('Known Customer') before a certificate can be issued[8].

[8] Requires the entity to establish they have an existing relationship with Defence (this can be achieved via sponsorship from the chain-of-command; posting order, recruitment letter or inclusion in a Defence authoritative source/database).

	• Location EOI registration can either be conducted remotely (eg. over a network) or locally (eg. face-to-face) with a 'registration authority'. Where evidence is passed from remote locations there is less confidence in its authenticity, the presence of the applicant and protection from attack (eg. man-in-the-middle, replay, etc). Defence will use (Draft) ISO 29115 and NIST Electronic Authentication Guideline (NIST SP 800-63-1) to assess the location component.
CREDENTIAL STRENGTH (IN RELATION TO THE END ENTITY)	
	• Token[9] Protection The protection afforded to the token within which the certificate is stored contributes to the assurance that only the Subscriber is using the associated private keys. The medium in which the certificate can be stored can either be in the software form or a hard token (smartcard or similar token, or hardware security module). In addition, the token can be accredited (against either the Common Criteria or PIV standards) with respects to how 'vulnerable' the certificate (or private key) is to attack. The measurement of this component of determining the LoA of a certificate can be separated through the assessment of whether the certificate needs to be stored on a soft or hard token and that tokens accreditation level. Defence will use the Common Criteria framework Protection Profile, FIPS, DSD Cryptography Evaluation and NIST PIV accreditation to associate the tokens LoA.
	• Token Activation (use) Every token contains a 'secret' (typically a key or password) used to authenticate the Subscribers identity. In order to validate that the entity authorised the transaction, the Relying Party needs to be confident in the security controls around accessing that certificate, this includes a number of controls such as: • proof of possession via one or more of the three factors of authentication – something you know (eg. password, etc), something you have (eg. PIN-protected smartcard, etc) and something you are (eg. biometric, etc). • Credential storage uses control mechanisms to protect against unauthorised disclosure or tampering. Defence will use the (Draft) ISO 29115 and NIST Electronic Authentication Guideline (NIST SP 800-63-1) to assess the token activation method.
	• Life (Time) of Key Strength The strength of a key (authentication and confidentiality key within a PKI) can be measured by its entropy[10], which is computed by its key length and the type of algorithm used. Noting that as the key size of certain algorithms is increased, then so to is the time to process/use the algorithm increased which could become impractical within the environment. However, the strength of a key is only valid at a point in time (the longer the time period the more likely it is that the algorithm has been broken) therefore, the key strength for assurance purposes will be associated with the life time strength of the key. (Academic research, that includes factoring techniques and expected increases in computing speed, anticipates when an algorithm may be compromised or in serious danger of being broken.) At this stage Australia does not publish life time strength of keys (or algorithm road maps) as such life of the key strength will be determined based on NIST SP 800-57-1.

[9] A token is something the Subscriber possesses and controls used to authenticate the Subscribers identity. It incorporates one or more of the three factors of authentication – something you know, something you have and something you are.
[10] Entropy can be defined as a measure of the key strength.

CERTIFICATE MANAGEMENT	
	• Certificate Authority (CA) Protection (physical and logical) The CA and supporting infrastructure, such as Hardware Security Modules (HSMs) for key storage, provide the foundation for the technical components within the certificate management process. The protection component is an assessment of the controls (both physical and logical) that the organisation puts around the protection of the CA and supporting infrastructure from network separation to physical and procedural security controls. A measure of the protection associated with the CA (and/or supporting infrastructure) can be provided via a combination of the Evaluation Assurance Level (EAL) of the respective products under the Common Criteria process, its protective rating in accordance with the Australia Information Security Manual (ISM) and its status under the Australian Government Gatekeeper Framework accreditation process. ADO CAs (and supporting infrastructure) are protected 'as if SECRET', which is validated by Defence's Information Assurance agency and accredited against the Gatekeeper Framework to the High Assurance Level.
	• Binding (Certificate Issuance) A CA issues a certificate binding a public key to a particular distinguished name in the X.500 tradition, or to an alternative name such as an e-mail address or a DNS-entry. The technical controls and processes associated with this binding provide confidence that the public key has been bound to the correct Subscriber. This confidence can be associated with the method of delivery of the public and private keys, whether the process is contiguous or not, and actions performed by the CA during the issuance, or renewal, of the certificate and notification mechanisms, if any, used by the CA to notify the Subscriber of the issuance of the certificate.
	• Revocation A certificate is revoked by the CA when the binding between the end entity and its public key is no longer considered valid. Relying Parties, as part of the process to confirm the validity of certificates, check that they have not been revoked by either using the Certificate Revocation List (CRL) or a speedier validation method that involves the use of the Online Certificate Status Protocol (OCSP). The length of time between CRL/OCSP updates determines the amount of risk the Relying Party is exposed to in that a revoked certificate may not be valid. As such, this component is measured by the issuance frequency of the CRL.
	• Compliance (Audit and Other Assessments) A CA can be assessed against the certificate policies or Certificate Practice Statement that it is recognised as implementing. This assessment confirms that the technical controls and processes are being followed which in turn provides a level of trust to both Relying Parties and Subscribers. The rigour and independence of the auditing processes of the CA (and supporting infrastructure) will be used as the basis for the measurement of this component. The Defence PKI is independently audited annually against the Gatekeeper PKI Framework which confers a trusted status to CA services within the Commonwealth.

NB. Adherence to relevant privacy principles and privacy regimes are not included in the LoA as they are not applicable. The Defence PKI will comply with the requirements of the Australia Privacy Act.

4 ASSURANCE LEVEL MAPS

The following section of this document tables the varying levels of assurance, and specifies the minimum and/or mandatory requirements around the fore-mentioned measurement components to meet a Level of Assurance.

NB. Application accreditations may require higher levels of assurance than specified in this document for the stated application.

The mapping of assurance levels for individuals and resources is documented separately.

4.1 Individual – Low Assurance

The following table assesses each of the measurement components for ADO to issue an individual a certificate with LOW Assurance:

Table 5 – Individual Low Assurance

MEASUREMENT COMPONENT	REQUIREMENT	COMMENTS
IDENTITY PROOFING		
EOI Requirement	• May be self-assured identity • EOI Refresh – No Stipulation	The name associated with the Subscriber is provided by the Applicant **without** verification.
Evidence of Relationship	• Affiliated with Defence	
Location	• No Stipulation	Identity proofing may be Local or Remote.
CREDENTIAL STRENGTH		
Token Protection	• Accreditation - No Stipulation • Medium - No Stipulation	May be Soft or Hard Token.
Token Activation	• Possession proof – No Stipulation • Credential storage – protected by discretionary access controls	Activation can be undertaken by the application without deliberate Subscriber action. Access controls limit access to the individual, administrators and those applications that require access.
Life (Time) of Key Strength	< 3 years is acceptable	Based on NIST SP 800-57-1.

CERTIFICATE MANAGEMENT		
CA Protection	• Protection - as per Restricted network • Accreditation - No Stipulation	
Binding	• Issuance – No Stipulation • Renewal/re-issuance – No Stipulation	The CA should perform a check that the name is unique within the context.
Revocation (publication)	• End Entity CRL - Minimum 31 days – Issued 28 days • CA Compromise – within 18 hours of notification	
Compliance	No Stipulation	

4.2 Individual – Medium Assurance

The following table assesses each of the measurement components for ADO to issue an individual a certificate with MEDIUM Assurance:

Table 6 – Individual Medium Assurance

MEASUREMENT COMPONENT	REQUIREMENT	COMMENTS
IDENTITY PROOFING		
EOI Requirement	• Possession of valid Government Identity • EOI Refresh – 4 to 6 years	The name associated with the Subscriber **may be** pseudonymous; however the PKI shall know the actual identity of the Subscriber.
Evidence of Relationship	• Affiliated with Defence	
Location	• Local – IAW ISO 29115 LoA2 • Remote – IAW ISO 29115 LoA2	Valid 'Identification documentation' may be from a 'known' Defence System (Authoritative Source) that associates the individual's security clearance.
CREDENTIAL STRENGTH		
Token Protection	• Accreditation – Cryptographic module EAL 2+ • Medium - No Stipulation	May be Soft or Hard Token.
Token Activation	• Possession proof – single factor (password) • Credential storage – As per ISO 29115 LoA2	Password should be Complex.
Life (Time) of Key Strength	> 3 years	Based on NIST SP 800-57-1.

CERTIFICATE MANAGEMENT		
CA Protection	• Protection - as per Restricted network • Accreditation - minimum EAL Certification	Protected from unauthorised access.
Binding	• Issuance – o physically protected o process not necessarily contiguous o issuance notice sent to claimant using address provided during identity proofing • Renewal/re-issuance - must prove possession of old token	Credential and token can be issued in person, mailed in a sealed envelop or through use of communication protocol that protects the integrity of the session data. Attempts to renew/re-issue using revoked or expired tokens should fail.
Revocation (publication)	• End Entity CRL - Minimum 17 days – Issued 14 days • CA Compromise – within 18 hours of notification	PKI should have a procedure to revoke credentials within 72 hours
Compliance	Self Assessment	

4.3 Individual – High Assurance

The following table assesses each of the measurement components for ADO to issue an individual a certificate with HIGH Assurance:

Table 7 – Individual High Assurance

MEASUREMENT COMPONENT	REQUIREMENT	COMMENTS
IDENTITY PROOFING		
EOI Requirement	• IAW Gatekeeper High Assurance • EOI Refresh – every 2 years	Includes need to establish evidence of: • identity in Australia; • linkage between identity and person (photo and signature); • linkage to operating within the community; and • DOB on one document
Evidence of Relationship	• Affiliated with Defence	Foreign staff seconded to Defence also requires sponsorship by permanent Australian chain-of-command representative.
Location	• Local ONLY (No Remote) o formal face-to-face	Registration authority must be accredited with the PKI.
CREDENTIAL STRENGTH		
Token Protection	• Accreditation - Cryptographic module EAL 4+ • Hard Token only • Must not allow export of authentication keys	Card Management System activities are authenticated through the use of a card management key. Token requires tamper evident capability.
Token Activation	• Possession proof – multi-factor (hard token and PIN/password) • Credential storage – As per ISO 29115 LoA3	

Life (Time) of Key Strength	> 7 years	Based on NIST SP 800-57-1.
CERTIFICATE MANAGEMENT		
CA Protection	• Protection - as per Secret Network plus (+) o No-Lone Zone; o Logical Network Separation; o HSM used for CA/RA/Archive • Accreditation - minimum EAL4 + DCE Certification	CA and Card Management System are in their own protected enclave (with management consoles logically and physically within the enclave). Requires the presence of at least two trusted role personnel for any access to the CA.
Binding	• Issuance – as per Medium Assurance plus (+) o Process is contiguous o All interactions occur over protected channel (eg. SSL/TLS) o Verify identity prior to activation o Subscriber acknowledges participation in registration process • Renewal/re-issuance - as per Medium Assurance	The Subscriber form can be electronic, and should cover responsibilities.
Revocation (publication)	• End Entity CRL - minimum every 10 days – issued 7 days • CA Compromise – within 18 hours of notification	A CRL should be published on a daily basis. PKI should have a procedure to revoke credentials within 24 hours
Compliance	Independent annual assessment	

4.4 Individual – Very High Assurance

The following table assesses each of the measurement components for ADO to issue an individual a certificate with VERY HIGH Assurance:

Table 8 – Individual Very High Assurance

MEASUREMENT COMPONENT	REQUIREMENT	COMMENTS
IDENTITY PROOFING		
EOI Requirement	Same as High Assurance, plus (+) • Verify at least 1 government document against its source • Record two current biometrics during registration interview (facial image plus fingerprint) • Evaluate biometrics for duplicates and investigate as necessary • EOI Refresh – as per High Assurance	Verification against the relevant issuing (government) authority or other authoritative source. Biometrics provides binding between the individual, the identity record and evidence documents (chain-of-trust). This can be utilised in the future to establish chain-of-trust back to the identity record rather than re-presenting multiple evidence records.
Evidence of Relationship	• Affiliated with Defence	
Location	Same a High Assurance	
CREDENTIAL STRENGTH		
Token Protection	Same as High Assurance	
Token Activation	• Possession proof – multi factor that includes a biometric • Credential storage – As per High Assurance	
Life (Time) of Key Strength	> 10 years	Based on NIST SP 800-57-1.

CERTIFICATE MANAGEMENT		
CA Protection	Protection - as per High Assurance Accreditation - as per High Assurance	
Binding	• Issuance – as per High Assurance plus (+) o Process uses a biometric o PKI must receive acknowledgement of receipt of credential prior to activation o Trusted time stamp service available to date signatures • Renewal/re-issuance - as per High Assurance	Does not have to be contiguous if chain-of-trust established via biometric.
Revocation (publication)	• End Entity CRL - minimum 18 hours; OR, on Revocation • CA supports OCSP • CA Compromise – within 6 hours of notification	PKI should have a procedure to revoke credentials within 24 hours
Compliance	As per High Assurance plus (+) Government certification	

4.5 Resource – Medium Assurance

The following table assesses each of the measurement components for ADO to issue a resource a certificate with MEDIUM Assurance:

Table 9 – Resource Medium Assurance

MEASUREMENT COMPONENT	REQUIREMENT	COMMENTS
IDENTITY PROOFING		
EOI Requirement	• Record information from one authoritative source of identity • EOI Refresh – No Stipulation	Such information may include common name, description, serial number, MAC address, owner, location, manufacturer, etc.
Evidence of Relationship	• Affiliated with Defence • Resource Custodian must be appointed	Individual (the Resource Custodian) must be affiliated with Defence.
Location	• No Stipulation	Identity proofing may be Local or Remote.
CREDENTIAL STRENGTH		
Token Protection	• Accreditation – Cryptographic module EAL 2+ • Medium - No Stipulation	May be Soft or Hard Token.
Token Activation	• Possession proof – No Stipulation • Credential storage – As per ISO 29115 LoA2	If used, password should be Complex.
Life (Time) of Key Strength	> 3 years	Based on NIST SP 800-57-1.

CERTIFICATE MANAGEMENT		
CA Protection	• Protection - as per Restricted network • Accreditation - minimum EAL Certification	Be protected from unauthorised access.
Binding	• Issuance – o physically protected o process not necessarily contiguous • Renewal/re-issuance - must prove possession of old token	Credential and token can be issued in person, or through use of communication protocol that protects the integrity of the session data. Attempts to renew/re-issue using revoked or expired tokens should fail.
Revocation (publication)	• End Entity CRL - Minimum 17 days – Issued 14 days • CA Compromise – within 18 hours of notification	PKI should have a procedure to revoke credentials within 72 hours
Compliance	Self Assessment	

4.6 Resource – High Assurance

The following table assesses each of the measurement components for ADO to issue a resource a certificate with HIGH Assurance:

Table 10 – Resource High Assurance

MEASUREMENT COMPONENT	REQUIREMENT	COMMENTS
IDENTITY PROOFING		
EOI Requirement	• As per Medium Assurance • EOI Refresh – No Stipulation	
Evidence of Relationship	• As per Medium Assurance plus (+) • Must be a valid Defence resource with proof Resource linked to individual owner	Individual must be affiliated with Defence.
Location	• No Stipulation	Identity proofing may be Local or Remote.
CREDENTIAL STRENGTH		
Token Protection	• Accreditation - Cryptographic module EAL 4+ • Hard Token only • Must not allow export of authentication keys	Token requires tamper evident capability.
Token Activation	• Possession proof – No Stipulation • Credential storage – As per ISO 29115 LoA3	
Life (Time) of Key Strength	> 7 years	Based on NIST SP 800-57-1.

CERTIFICATE MANAGEMENT		
CA Protection	• Protection - as per Secret Network plus (+) o No-Lone Zone; o Logical Network Separation; o HSM used for CA/RA/Archive • Accreditation - minimum EAL4 + DCE Certification	CA and Card Management System are in their own protected enclave (with management consoles logically and physically within the enclave). Requires the presence of at least two trusted role personnel fpr any access to the CA.
Binding	• Issuance – as per Medium Assurance plus (+) o Process is contiguous o All interactions occur over protected channel (eg. SSL/TLS) • Renewal/re-issuance - as per Medium Assurance	Applicant's identity must be verified prior to certificate being activated.
Revocation (publication)	• End Entity CRL - minimum every 10 days – issued 7 days • CA Compromise – within 18 hours of notification	A CRL should be published on a daily basis. PKI should have a procedure to revoke credentials within 24 hours
Compliance	Independent annual assessment	

5 OBJECT IDENTIFIERS FOR LEVELS OF ASSURANCE

The LoA asserted by an OID will be equivalent to the lesser of the identified components (Identity Proofing, Certificate Management and Credential Strength).

In accordance with RFC 3647, the LoA OID will be identified in the certificatePolicies extension of the respective Certificate Profile.

The OIDs expressed for the respective LoA in Defence certificates will align to the Defence PKI OID arc[11]. Therefore they are:

a. 1.2.36.1.334.1.2.1.1 (Assurance Level Individual Low)
b. 1.2.36.1.334.1.2.1.2 (Assurance Level Individual Medium)
c. 1.2.36.1.334.1.2.1.3 (Assurance Level Individual High)
d. 1.2.36.1.334.1.2.1.4 (Assurance Level Individual Very High)
e. 1.2.36.1.334.1.2.2.1 (Assurance Level Resource Low)
f. 1.2.36.1.334.1.2.2.2 (Assurance Level Resource Medium)
g. 1.2.36.1.334.1.2.2.3 (Assurance Level Resource High)

[11] Note these will be replaced with Australian Government OIDs when they are ratified

This page intentionally blank