PEXA Public Key Infrastructure (PKI)

Certification Practice Statement

Version: 2.10
Issued: January 2015
Status: Final

VERSION CONTROL

Version No.	Version Details	Date
2.9	Initial accredited document	August 2014
2.10	Document amended to: • Remove the concept of 'First Subscriber Manager' to align with the PEXA System, under which a Subscriber Organisation can appoint multiple Subscriber Managers. PEXA DSC Subscribers are still required to nominate at least one Subscriber Manager for digital certificate purposes • Corresponding changes to the definitions and acronyms in Appendix B.	January 2015

	PEXA PKI Certification Practice Statement
1. Introduction	Property Exchange Australia Limited (PEXA) operates the PEXA Platform, which is used by legal and conveyancing entities, financial institutions and government bodies to conduct property transactions electronically within the Commonwealth of Australia. This Certification Practice Statement (CPS) describes the practices of the PEXA Public Key Infrastucture (PKI) in issuing digital certificates to members of the PEXA Community of Interest. PEXA certificates facilitate property transactions by allowing participants to sign documents electronically. This CPS supports multiple Certificate Policies (CPs), refer to Appendix A for a list of supported CPs. This CPS follows the IETF standard RFC3647 ("Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework"), according to which a CPS "is a statement of the practices which a certification authority employs in issuing certificates". It is closely bound to its corresponding Certificate Policies (CPs). A CP, according to the RFC, is "*a named set of rules that indicates the applicability of a certificate to a particular community and/or class of applications with common security requirements* ". The CPS and CPs use the same headings and numbering (except where noted in a CP), and contain frequent cross-references. For explanation of Terms, Definitions and Acronyms, refer to Appendix B.
1.1 . Overview	PEXA operates the PEXA network, an IT based exchange linking the Land Registry in each Australian State and Territory with the Revenue Office in that jurisdiction, and Financial Institutions, legal practitioners and conveyancers to allow the electronic processing associated with the conveyance of property within that jurisdiction. Information about PEXA can be found at: http://www.pexa.com.au/ E-Conveyancing in Australia is regulated by the laws of the jurisdiction in which the land to be conveyed is located. The Australian Registrars' National Electronic Conveyancing Council (**ARNECC**), a body made up of representatives from Land Registries of all states and territories in Australia, oversaw the development of the E-Conveyancing National Law (ECNL), which has been applied as a law in each Australian jurisdiction. ARNECC has also

published two further documents which set out the national model requirements that apply to Electronic Lodgement Network Operators (ELNOs) and the participants in E-Conveyancing transactions. Registrars in each Australian jurisdiction are required to have regard to the desirability of maintaining consistency with national model provisions in determining the operating requirements for ELNOs and participation rules for participants in E-Conveyancing transactions in their jurisdiction. The national model documents, which are referred to throughout this document, are the Model Operating Requirements (MOR) and the Model Participation Rules (MPR).

The MORs stipulate that where a digital certificate is used to Digitally Sign a document, the ELNO must ensure that the certificates are issued by a CA operator accredited under the Australian Government's PKI governance framework, "**Gatekeeper**". The full requirements are set out in section 7.6 of the MOR.

PEXA has chosen to implement its own PKI and make that PKI available to the Community of Interest made up by participants in the PEXA Platform. The PKI provides certificates to users within the Subscriber Organisations that are required to sign documents in the PEXA Platform.

The **Community of Interest** (CoI) for the PEXA PKI comprises:

i. The Relationship Organisation and Relying Party: PEXA

ii. Organisations who have signed the PEXA Participation Agreement, including:

- Banks and other Financial Institutions including credit unions;
- Solicitors;
- Conveyancers; and
- Government bodies

iii. Other parties who rely upon signed PEXA Documents:

- Land Titles Offices and Registries; and
- State Revenue Offices.

For more information on PEXA PKI participants, refer to section 1.3.

1.1.1 Related documentation

The following documents have been referenced in this CPS:

i. PEXA documents:

- PEXA PKI Certification Authorities Certificate Policy (CA CP)
- PEXA PKI Digital Signing Certificate Policy (DS CP)
- PEXA PKI Administrator Certificate Policy (Adm CP)
- PEXA Privacy Policy http://www.pexa.com.au/privacypolicy
- PEXA Participation Agreement (PA) (customised for PEXA Subscribers) available on request
- PEXA Digital Signing Certificate (DSC) Subscriber Agreement available at https://www.pexa.com.au/ca/publish/pexa/documents/

iv. ARNECC documents:

- Model Participation Rules (MPR), ARNECC, Version 2 18 Mar 2014 http://www.arnecc.gov.au/publications
- Model Operating Requirements (MOR), ARNECC, Version 2 18 Mar 2014 http://www.arnecc.gov.au/publications

v. CA documentation (not available to the public):

- SEC1 - Security Profile for CA Operations, consisting of Security Policy, Threat and Risk Assessment, Security Plan and Key Management Plan
- SEC1 – Security Profile Supplement for PEXA
- Disaster Recovery and Business Continuity Plan (DRBCP)
- OPS1 - CA Operations Manual
- Change Management Plan
- Incident Response Plan

	• PEXA CA Key Generation Script See also Gatekeeper website for latest document set. vi. Australian Government documents: • Electronic Conveyancing National Law (ECNL) • Australian Government Information Security Manual (ISM) http://www.asd.gov.au/infosec/ism/ • Australian Government Protective Security Policy Framework (PSPF) www.protectivesecurity.gov.au/pspf/ vii.Gatekeeper documents: http://www.finance.gov.au/policy-guides-procurement/gatekeeper-public-keyinfrastructure/gatekeeper-documentation/: • Gatekeeper Accreditation Head Agreement • Gatekeeper Core Obligations Policy, Feb 2009 • Gatekeeper Relationship Certificate CP Template, Feb 2009 • Gatekeeper Compliance Audit Program, Nov 2011 viii. Standards: • RFC3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework • RFC5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile • RFC2560 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP
1.2. Document name and identification	This document is known as the "PEXA PKI Certification Practice Statement". ASN.1 Object Identifiers (OIDs) are used in PKI to uniquely identify objects such as documents, algorithms or parameters of digital certificates. The PEXA PKI Certificate Practice Statement does not require an OID. Each certificate issued under this CPS includes a pointer (URL) to the location of this CPS. PEXA PKI certificates are identified with an OID, in order to allow a participant to locate the CP under which the certificate was issued. Refer to applicable CPs for their respectiveOIDs. The PEXA CPS and CPs can be accessed at: https://www.pexa.com.au/ca/publish/pexa/documents/
1.3. PKI participants	Refer also to relevant CP.
1.3.1. Certification authorities	The PEXA PKI hierarchy consists of two levels of CAs: The Root CA (RCA) which only issues certificates to subordinate CAs. Initially, one Operational CA (OCA) has been created and issued with a certificate. The OCA in turn issues certificates to end users. The PEXA CAs are hosted in secure facilities in Canberra, ACT. **PEXA Root Certification Authority (RCA)** The PEXA RCA is the highest point in the trust hierarchy, and therefore has the highest security requirements. The RCA's certificate is self-signed, and created at a key signing ceremony attended by PEXA and Gatekeeper representatives. Its keys are stored in a Hardware Security Module (HSM), a specialised piece of equipment which generates the keypair and stores the private keys encrypted and non-exportable. The RCA is kept off-line. **PEXA Operational Certification Authority (OCA)** The PEXA Operational CA issues certificates to PEXA users and administrators. The PEXA OCA also has very high security requirements, and uses an HSM to generate, store and use its keys. PEXA OCAs' keys and certificates are created at a formal key signing ceremony.

	PEXA PKI Certification Practice Statement
1.3.2. Registration authorities (Relationship Organisation)	PEXA, as the Relationship Organisation, establishes its relationship with Subscriber Organisations through the enrolment process defined in the Model Operating Requirements (MOR). The process includes validation of the Subscriber Organisation, identification of the individuals who have binding authority, verification of the identity of the aforementioned individual and entering into an agreement (the PEXA Participation Agreement). PEXA leverages this process to enter into an additional agreement to supply PEXA Digital Signing Certificates (DSC), whereby the Subscriber Organisation can chose to become a PEXA DSC Subscriber. During this process, a Subscriber Manager is nominatedby the Subscriber Organisation. Following the Verification of Identity of the Subscriber Manager (conducted by either VOI Agent, VOI Officer or by the PEXA DSC Subscriber), PEXA will issue a PEXA DSC to the Subscriber Manager and any other Certificate Recipient so named in the PEXA DSC Subscriber Agreement. The Subscriber Organisation or any Subscriber Manager is able to submit certificate requests for further PEXA Users within their organisation. Hence, registration and certificate management functions in the PEXA PKI are carried out by: • PEXA in its function as the "Relationship Organisation", managing enrolment of Subscriber Organisations, requesting certificates for the Subscriber Manager, passing on certificate and certificate status change requests to the CA; • PEXA VOI Officers or VOI Agents performing Verification of Identity (VOI) checks of Certificate Recipients; • PEXA DSC Subscribers, performing VOI checks of their Certificate Recipients. N.B Under the Gatekeeper "Community of Interest" model in the "Special" category, there is no Registration Authority accreditation required. PEXA is listed as a "Relationship Organisation" (PEXA) on the Gatekeeper website.
1.3.3. Subscribers	The term 'Subscriber' is used in both the MOR context and in the PKI context. In order to avoid any potential ambiguity, a distinction will be made between the two subscriber contexts in the PEXA PKI documentation set as follows: • **PEXA Subscriber** – a 'Subscriber' in the MOR context A PEXA Subscriber is an organisation that signs the PEXA Participation Agreement in order to transact on the PEXA Platform. • **PEXA Digital Signing Certificate (DSC) Subscriber** – 'Subscriber' in the PKI context. A PEXA DSC Subscriber is an organisation that signs the PEXA DSC Subscriber Agreement in order to attain PEXA DSCs from PEXA. Where used in this CP, the term 'Subscriber' may refer to PEXA Subscribers, or to PEXA DSC Subscribers, or both, as the context requires.
1.3.4. Relying parties	Full validation of digital signatures (as defined in RFC 3647) applied to PEXA Documents by Subscriber Signers is performed by the PEXA Platform. Within this context, digital signature verification includes validating the status of the PEXA digital certificate that was used to generate said digital signature at the time of signing. PEXA is therefore the only Relying Party within the PEXA PKI. It should be noted that there are other participants that will rely on the outcome of a signed PEXA Document. As all the relevant information and meta-data is included in the output from the PEXA Platform (including the online certificate status response at the time of signing) , these participants do not require access to other revocation information. These participants are defined under section 1.3.5.

1.3.5. Other participants	**1.3.5.1. PEXA Policy Management Authority** The governing body for the PEXA PKI is the PEXA Policy Management Authority (PMA). PEXA's PMA is the Governance, Risk and Compliance (GRC) Committee, which is comprised of PEXA's CEO, COO, CFO, CIO, GM Risk, GM Corporate Governance, Compliance & Privacy and General Counsel and a senior representative of the incumbent CA Services Provider. **1.3.5.2. Managed CA service provider** PEXA have contracted the day-to-day operation of the CA and token provisioning system to a third party managed service provider. **1.3.5.3. PEXA VOI Agent** An organisation that has entered into a formal agreement with PEXA to conduct VOI on behalf of PEXA. **1.3.5.4. ARNECC** ARNECC is the regulatory body established to facilitate the implementation and ongoing management of the regulatory framework for National E-Conveyancing. ARNECC membership comprises the Land Titles Registrars from each Australian state and territory or their nominee. **1.3.5.5. Registrars/Land Titles Offices** The Land Titles Registrars ("The Registrar") are responsible for overseeing the operation of Electronic Lodgement Networks (ELN) within their jurisdiction. The Registrar's responsibilities and powers include giving the initial approval to operate, to audit and to revoke an ELNO should it not meet its obligations under the MOR. The Registrars' role is outlined in the MOR and MPR. These entities are ones that rely upon Digitally Signed PEXA Documents. As part of the lodgement verification process (and for each lodgement instance), the destination entity will perform an independent Digital Signature verification check (excluding certificate status checking). **1.3.5.6. State Revenue Offices** State Revenue Offices are responsible for providing Duty Assessment data to the ELN. Some of these entities are ones that rely upon Digitally Signed PEXA Documents. As part of the assessment process, the destination entity will perform an independent Digital Signature verification (excluding certificate status checking) of the Digitally Signed PEXA Document.' **1.3.5.7. Australian Government PKI governance - Gatekeeper** As a Gatekeeper accredited organisation, PEXA is under obligation to conform with Gatekeeper policies applicable to the "Special" category, issuing "Relationship Certificates". Gatekeeper policies are published by the Department of Finance, and can be found at: http://www.finance.gov.au/policy-guides-procurement/gatekeeper-public-keyinfrastructure/ Upon accreditation, the Gatekeeper Competent Authority will list the PEXA CA and Relationship Organisation/Community of Interest on its website. It will also monitor compliance with the accreditation requirements through the Gatekeeper Compliance Audit Program (GCAP). Any changes to Approved Documents (including this CPS) is subject to review by the Gatekeeper Competent Authority.
1.4. Certificate usage	Certificates issued under CPs related to this CPS must only be used within the PEXA system. For more detail, refer to applicable CP.
1.5. Policy administration	

	PEXA PKI Certification Practice Statement
1.5.1. Organisation administering the document	The PEXA PKI Policy Management Authority (PMA) is responsible for administering this document and related Certificate Policies. Refer also to section 9.12 – Amendments.
1.5.2. Contact person	Contact details for the PEXA PKI PMA are: General Manager – Risk ph: (03) 9912 6500; or e: grc@pexa.com.au
1.5.3. Authority determining CPS suitability for the policy	The PEXA PMA is responsible for determining the suitability of this CPS to support a particular CP.
1.5.4. CPS and CP approval procedures	This CPS and any changes to it or related CPs are approved by the PEXA PMA. Any changes other than minor ones which do not materially affect the acceptability of a certificate type, must also be approved by the Gatekeeper Competent Authority, as the CPS and CPs are Approved Documents. The following process will be used to approve amendments to this CPS and correlating CPs: i. Proposed changes are to be integrated into a draft document and submitted to the PEXA PMA. ii. The proposed changes are reviewed by the PEXA PMA. iii. Once the proposed changes are acceptable to all stakeholders, the PEXA PMA will endorse the changes and forward the endorsed changes to the Gatekeeper Competent Authority. iv. Upon acceptance by the Gatekeeper Competent Authority, the PEXA PMA will approve; -the document for publication; and -implementation of the proposed changes. v. Upon finalisation of the document, the Gatekeeper Competent Authority amends Schedule 2 of the Gatekeeper Accreditation Head Agreement (list of Approved documents).
1.6. Terms, Definitions and Acronyms	For Terms, Definitions and Acronyms, refer to Appendix B. Defined terms are capitalised.
2. Publication and Repository Responsibilities	
2.1. Repositories	The following repositories support the PEXA PKI: • **CA database**. Stores certificates and Certificate Revocation Lists (CRLs). • **Card Management System**. (CMS) internal database. Contains information about Certificate Holders and tokens. • **PEXA CRM**. Stores information pertaining to PEXA Subscribers and PEXA Members. • **PEXA Platform database**. Stores a subset of Subscriber information and PEXA transactions. • **PEXA CA certificate repository**. Publishes the PEXA RCA and OCA certificates. • **PEXA PKI document repository**. Publishes documents, including this CPS and correlating CPs. These are available to members of the PEXA Community of Interest on the PEXA website at: https://www.pexa.com.au/ca/publish/pexa/documents/

2.2. Publication of certification information	The PEXA PKI is a closed PKI; **certificates** are not published outside the PEXA PKI. **Certificate status information** (via OCSP) is only available to the PEXA Platform. This **CPS** and the related **CPs** are available to members of the Community of Interest on the PEXA website.
2.3. Time or frequency of publication	**Certificates** are placed in the CA database directly upon creation. A new **CRL** is generated and published upon status change of a certificate, or minimum daily. This **CPS** and corresponding **CPs** will be published once changes have been approved in accordance with Section 1.5.4.
2.4. Access controls on repositories	**Certificates & CRLs** - CA and CMS repositories are protected by logical and physical access controls and are not accessible to external parties. **PEXA repositories** are protected by logical and physical access controls in accordance with PEXA internal policies, and are not accessible to external parties. **CPS** and **CPs** repositories – These repositories are available for read-only access to members of the Community of Interest on the PEXA website. A login account is required. NB. Certificates and CRLs are Digitally Signed and cannot be modified without detection.
3. Identification and Authentication	
3.1. Naming	
3.1.1. Types of names	Each certificate has an X.500 Distinguished Name which uniquely identifies the Subject within the PKI. Refer to applicable CP for details.
3.1.2. Need for names to be meaningful	Distinguished names used within a certificate indicate a binding between a public key and a real-world identity. The name should be meaningful within the PEXA PKI context. Refer to applicable CP for details.
3.1.3. Anonymity or pseudonymity of Subscribers	Anonymous or pseudonymous names are not allowed unless an exception is made in the applicable CP.
3.1.4. Rules for interpreting various name forms	Certificates use X.500 Distinguished Names that are readily distinguishable and do not require special interpretive rules. Refer to applicable CP for details.
3.1.5. Uniqueness of names	Refer to applicable CP for details.
3.1.6. Recognition, authentication, and role of trademarks	Not applicable.

	PEXA PKI Certification Practice Statement
3.2. Initial identity validation	**Verification of Identity requirements** There are no specific VOI processes or requirements stipulated for the identity verification of Certificate Holders in the Gatekeeper "Special" category. The VOI process in this category is determined by the Relationship Organisation and the Community of Interest. The VOI requirements of the PEXA PKI Community of Interest are based on those documented in ARNECC's Model Operating Requiremens (MOR) and the Model Participation Rules (MPR). PEXA DSC Subscribers are able to leverage off existing processes (e.g. the employee hiring process) when determining compliance with the MPR. Refer to applicable CP for detail.
3.3. Identification and authentication for re-key (renewal)	Refer to applicable CP.
3.4. Identification and authentication for revocation request	Refer to applicable CP.
3.5. Identification and Authentication for Key Recovery Request	Not applicable.
4. Certificate Life-cycle Operational Requirements	Refer to applicable CP, sections: 4.1. Certificate application 4.2. Certificate application processing 4.3. Certificate issuance 4.4. Certificate acceptance 4.5. Key pair and certificate usage 4.6. Certificate renewal 4.7. Certificate re-key (renewal) 4.8. Certificate modification 4.9. Certificate revocation and suspension 4.10. Certificate status services 4.11. End of subscription 4.12. Key escrow and recovery
5. Facility, Management, and Operational Controls	***This section covers Facility, Management and Operational Controls of the PEXA CA in the facility where it is hosted.*** ***For information on the equivalent subjects as they relate to the facilities used for registration activities, refer to applicable CP.*** ***N.B. Headings in this section do not correspond to headings in the PEXA Digital Signing CP (DS CP), as the DS CP is following the document structure recommended in the Gatekeeper Relationship Certificate Policy template.***

	PEXA PKI Certification Practice Statement
5.1. Physical controls	Controls in this section apply to both the primary and secondary data centres.
5.1.1. Site location and construction	The PEXA CAs are housed in Australian capital city-based secure data centres, comprising a primary site and a secondary site (for disaster recovery purposes). Certification received from the ASIO T4 Protective Security section and an Authorised Physical Security Evaluator certifies that the physical security inspection of the facilities meet the requirements set by the Protective Security Policy Framework (PSPF) as specified by the Gatekeeper PKI Framework.
5.1.2. Physical access	Physical access is restricted to authorised personnel in the normal course of their duties. Unauthorised personnel will be permitted on a strict needs basis only and with prior authorisation of the CA hosting facility management. Such persons must be under supervision of an authorised person. Security Construction and Equipment Committee (SCEC) endorsed access control protocols are strictly observed. The PEXA CAs are housed in a 'Logical No-Lone Zone', meaning that two people must always be present for any actions to be carried out on the CAs.
5.1.3. Power and air conditioning	The CA Operations infrastructure equipment is connected to a standard power supply. All critical components are connected to uninterruptible power supply (UPS) units to prevent abnormal shutdown in the event of a power failure. The CA Operations infrastructure equipment has an air conditioning system which controls temperature and humidity. Backup air conditioning units are provided for the secure servers within the CA room.
5.1.4. Water exposures	The CA Operations infrastructure equipment is protected against water exposure by: • being located on top of built in raised floors; and • the data centre not being in a flood zone.
5.1.5. Fire prevention and protection	The CA Operations infrastructure equipment is subject to fire prevention and protection procedures. Early detection of smoke in the CA Operations computer rooms is assured through the use of an extremely sensitive "very early smoke detection apparatus" (VESDA) system which continuously samples air from under the computer room floor and from the computer room itself. On detection of an unacceptably high level of smoke in the sampled air, the VESDA unit triggers a discharge from the fire suppression system. In addition to this automatic fire suppression system, suitable fire extinguishers are maintained in the secure operating area. The proximity swipe-card system supports emergency evacuation procedures to cater for environmental hazards such as fire and natural disasters.
5.1.6. Media storage	All magnetic media containing sensitive information, including backup media, is stored in containers, cabinets or safes with fire protection capabilities which are located either within the secure operating area or in a secure off-site storage area. No classified or sensitive information may be removed from the applicable premises without approval from the CA Operations ITSO. All removals must be recorded in the appropriate register, for example the CA Operations classified media register.

5.1.7. Waste disposal	Paper documents and magnetic media containing any private keys or commercially sensitive or confidential information are securely disposed of: • in the case of magnetic media; - physical damage to, or complete destruction of the asset; or - the use of an approved utility to wipe or overwrite magnetic media that is compliant with the ISM. • in the case of printed material; - cross-cut shredding in accordance with Australian Government requirements. Two persons must be present when destroying classified media.
5.1.8. Off-site backup	An approved secure facility that is certified by ASIO T4 is used for the storage and retention of off-site backup software and data. The off-site facility: • has appropriate levels of physical security in place; and • may be accessed by authorised personnel for the purposes of retrieving software and data 24/7.
5.2. Procedural controls	
5.2.1. Trusted roles	CA Operations contains a number of designated 'positions of trust'. These positions underpin the secure and reliable operation of the infrastructure, and as such must be filled by competent and trustworthy people (although several positions of trust may be filled by the same person) who are holders of an Australian Government Security Clearance. The general principle is that any role providing an opportunity to compromise private key material or impact on the Certificate life cycle must be a trusted role.
5.2.2. Number of persons required per task	Multi-person control is used where feasible in order to provide enhanced security and checks and balances over CA Operations. In particular: • logical access controls for CA Operations staff have been implemented to ensure that no one person can access alone a CA machine and therefore the sensitive information contained on those machines; • the CA Engineers are broken into the following two groups: - Group 1 - has access to the passwords for crypto elements; and - Group 2 - has access to the logon passwords for the server operating system and database applications; • any task requiring the creation, backup or import into a database of a CA Operations component private key (Trusted Element) takes place in a logical no-lone zone environment and therefore involves two trusted persons, one performing the function and the second fulfilling a security monitoring role.
5.2.3. Identification and authentication for each role	Each CA Operations staff member has a separate log on account to each secure server so all operations can be traced to an individual staff member. Each CA Operations staff member maintains a complex password to confirm their individual log on credentials to their administrator account in accordance with ISM requirements. These passwords are changed at regular intervals. Privileged access in the CA System (CA Operator accounts - CAOs) requires multifactor authentication. All computer accounts used by CA Operations staff on CA Operations networks shall be owned by the CA Operations ITSA and shall only be used for the activities for which they have been provided. These accounts shall not be used for non-CA Operations related activities without the prior authorisation of the CA Operations ITSA.

	All CA Operations staff must undergo a formal vetting process conducted by an accredited vetting service (refer to section 5.3.1).
5.2.4. Roles requiring separation of duties	To enhance security of the infrastructure the following roles are fulfilled by different individuals: • the CA Operations ITSA will normally remain separate from the CA Operations staff in order to provide an independent review of audit logs unless in exceptional circumstances (i.e. staffing issues whereby integrity of the CA service being operated could be breached); and • the ITSO (Information Technology Security Officer) always remains separate from the CA Operations system staff in order to provide an independent third party when reviewing and auditing CA Operations.
5.3. Personnel controls	
5.3.1. Qualifications, experience, and clearance requirements	All CA Operations staff must have the requisite qualifications, experience and clearance requirements to perform their duties. Security clearances must be by a recognised authority (Australian Government Security Vetting Agency – AGSVA). Clearance levels are determined by the classification of the data and areas accessed. Minimum clearance levels are defined in the SEC1 - Security Profile.
5.3.2. Background check procedures	The CA Operations security clearance process includes formal vetting procedures including a comprehensive background check.
5.3.3. Training requirements	A formal training program, founded on competency-based training principles is in place. The CA Operations ITSA is responsible for ensuring that new and inexperienced PKI staff are appropriately trained and supervised. All CA Operations staff are trained in: • basic PKI concepts; • the use and operation of the infrastructure software, including the RCA, OCAs and CMS as applicable; • documented procedures; • computer security awareness and procedures; and • the meaning and effect of this CPS and related CPs.
5.3.4. Retraining frequency and requirements	The introduction of any new security procedure or major software release will be accompanied by a corresponding education program for affected staff, to ensure that they are aware of their new responsibilities. Remedial training is completed when recommended by audit findings/recommendations.
5.3.5. Job rotation frequency and sequence	CA Operations implements either formal job rotation practices or cross-training in order to ensure operations continuity.

5.3.6. Sanctions for unauthorised actions	Where a staff member has been found to have misused the resources to which they have been granted access, these actions shall be documented and passed to the CA Operations ITSA or senior personnel, who will report the incident to the ITSO. Sanctions against contract employees shall be in accordance with the terms and conditions of their contract. Depending on the nature of the actions sanctions may range from counselling and/or suspension of access rights, through to dismissal and/or legal action. Criminal sanctions apply for contravention of relevant legislation, for example the *Crimes Act 1914* (Commonwealth).
	Prohibited actions include: • connecting private computers and peripherals to the CA Operations network; • installing unauthorised software (including copyright infringed items). All software installations must be in accordance with the requirements of CA Operations policies and the documented change management procedures; • using CA Operations systems for unauthorised purposes; • having diagnostic tools (capable of testing or breaking security resident in any system) on their machines; and • changing the configuration of any CA Operations hardware or software without approval of the ITSA or the CA Operations configuration and change control board.
5.3.7. Independent contractor requirements	Refer to sections 5.3.1, 5.3.2 and 5.3.6
5.3.8. Documentation supplied to personnel	All CA Operations operational personnel have access to the following documentation: • all relevant hardware and software documentation; • application manuals where appropriate; • policy documents, including CPs; and • infrastructure policy, operations and procedure documents, including this CPS as appropriate. Note that the infrastructure is largely composed of commercial-off-the-shelf products. Software documentation is available to CA Operations. General documents relating to the operation of the infrastructure will be made freely available to CA Operations, for example through publication on the CA Operations network. Access to more sensitive documents such as the SEC1 - Security Profile is limited to appropriately cleared personnel and only provided on a need-to-know basis.
5.4. Audit logging procedures	All CA operations are monitored, recorded and audited.
5.4.1. Types of events recorded	Audit records to be kept include: • Certificate action statements; • Key generation records; • Certificate generation requests; • Certificate issuance records, including CRLs; • Audit records including security related events; • Revocation records; • Reinstatement records; • Token details (stock control/issued/failed); • Other token related events; • Documentation – version control; • Registration records; and • Formal correspondence, including emails.

5.4.2. Frequency of processing log	Audit logs are processed on a daily, weekly, monthly, quarterly and annual basis. Electronic logs are reviewed by CA Operations staff as part of the Daily System Operational Tasks (DSOTs). DSOT sheets are reviewed and archived by the CA Operations ITSO.
5.4.3. Retention period for audit log	Audit logs are maintained on-site for a maximum period of three months, and then transferred to the off-site secure facility (see section 5.1.8). Archived logs are retained for a period of seven years, or such longer period as required by the Archives Act 1983 (Commonwealth) and any Records Disposal Authorities published by the National Archives of Australia. (Refer to applicable CP for retention of PEXA transaction data and logs.)
5.4.4. Protection of audit log	Active audit logs are protected by access control and No Lone Zones (where applicable). The CA software signs logs to prevent modifications not being detected. CA Operations audit logs on removable media are stored in B-class containers located in the CA Operations secure operations room prior to archiving. Archived CA Operations audit logs are stored in the off-site secure facility (see section 5.1.8).
5.4.5. Audit log backup procedures	CA Operations has established and maintains a detailed backup procedure for audit logs which is documented in the SEC1 - Security Profile and OPS1 - CA Operations Manual. These documents are not publicly available.
5.4.6. Audit collection system (internal vs. external)	The CA Operations audit collection system is a combination of automated and manual processes performed by the operating system running the UniCERT software, the UniCERT software itself, and by operational personnel. The audit mechanisms and procedures used are documented in the SEC1 Security Profile.
5.4.7. Notification to event-causing subject	CA Operations staff will notify the CA Operations ITSA when a process or action causes a critical security event or discrepancy. Unless required to do so by law, it is at the ITSA's discretion whether to notify the event-causing person or organisation.
5.4.8. Vulnerability assessments	Processes for monitoring the security risk level and to detect any actual security incidents are maintained and include: • vulnerability detection and analysis processes; and • malicious software prevention and detection processes.
5.5. Records archival	

5.5.1. Types of records archived	Sufficient archives of information relating to the operation of that entity will be retained to enable a proper audit and disaster recovery. CA Operations uses a framework of documents and records that it requires for running a CA. Listed below are documents which will be archived. • Certificate Policies • Certification Practice Statement (this document) • SEC1 Security Profile • SEC1 Security Profile Supplement • CA Operations Manual • Disaster Recovery and Business Continuity Plan (DRBCP) • PEXA CA Design Document • PEXA CA Installation Manual. • PEXA CA Key Generation Script • PEXA CA certificate requests • PEXA CA certificate Action Statement • PEXA CA certificate Revocation Request • Subscriber certificate Reinstatement Requests • Subscriber certificate Suspension/Revocation Action Statement • Configurable Items list • Independent Witness Statements • Hardware Support Agreements • Software Licensing Agreements • Classified Media Register • System Operational Tasks Sheets (Daily, Weekly, Monthly, Quarterly, Annual) • PEXA CA Change Orders and Pre-Approved Changes • CMS Records
5.5.2. Retention period for archive	In general, records and tape back-up archives are retained for a period of at least seven years from date of the action to which the record relates is completed in accordance
	with the *Archives Act 1983* (Commonwealth). The records and archives will be retained by such longer period as required by the Archives Act 1983 (Cth) and the Australian National Archive Policy, Administrative Functions Disposal Authority (2000). Disposal will be conducted in accordance with acceptable professional standards existing at that time to securely and permanently destroy the records. Prior to the disposal the CA Operations Manager shall on each occasion check: • current legislation to verify there is no statutory requirement to hold archived records for more than 7 years; and • whether there is a requirement to archive records for a longer period, in which case the records will not be disposed of.
5.5.3. Protection of archive	All archives are stored at the secure off-site facility (see section 5.1.8). They are couriered to the secure data repository in lockable containers purchased specifically for these records and stored for seven years. Archives moved off-site will utilise a system of delivery tickets and registers. Where archives are classified, two person integrity in accordance with the PSPF Safe-Hand procedures applies.
5.5.4. Archive backup procedures	Archive backup procedures have been established to ensure complete restoration of current service or verification, e.g. of CA databases, software library archives, keys and certificates. Details are specified in the following CA Operations documents: • SEC1 - Security Profile; and • OPS1 - CA Operations Manual. These documents are not publicly available.

	PEXA PKI Certification Practice Statement
5.5.5. Requirements for time-stamping of records	All automatically generated logs are time-stamped using the system clock of the computer on which they are generated. CA Operations use the Network Time Protocol (NTP) protocol to synchronise system clocks between servers, and with an external reference source. Manually generated records (e.g. CA Operations logs, or records of a manual revocation request) will record the date of occurrence, but may not record the time.
5.5.6. Archive collection system (internal or external)	Archiving is performed by CA Operations staff delegated with the responsibility for doing so. Detailed procedures for backups, archiving and storage are set out in; • SEC1 - Security Profile, and • OPS1 - CA Operations Manual. These documents are not publicly available.
5.5.7. Procedures to obtain and verify archive information	The integrity of the archives is verified in accordance with the criteria set out in the SEC1 -Security Profile: • annually at the time of the programmed security audit; • at any time when a full security audit is required; and • at the time the archive is prepared.
5.6. Key changeover	Key changeovers (also known as key renewal) of CAs that are subordinate to the RCA will be carried out in such a manner as to cause minimal disruption to participants. Subordinate CAs should obtain a new authentication key pair from the RCA a minimum of three years prior to the expiry of the certificate associated with their respective current private authentication key, and then commence signing new certificates with the new private authentication key. During this changeover period and until the expiry of the certificate associated with the current CA Operations private authentication key, both authentication public keys and associated certificates will be in use. CA Operations is committed to: • ensuring that key changeover causes minimal disruption to Subscribers; and • providing Subscribers with reasonable notice of planned key changeover.
5.7. Compromise and disaster recovery	
5.7.1. Incident and compromise handling procedures	CA Operations maintain a Disaster Recovery and Business Continuation Plan (DRBCP) and an Incident Response Plan. These documents describe incident and compromise handling procedures in detail. These documents are internal, but will be made available to those persons responsible for conducting security audits and to authorised auditors conducting external audits.
5.7.2. Computing resources, software, and/or data are corrupted	CA Operations maintain configuration baselines and have diagnostic tools and methodologies to identify software or data corruption. Software media and comprehensive backups are available to ensure rapid restoration of services.

5.7.3. Entity private key compromise procedures	If the RCA or OCA private key is compromised, the following CA Operations documents provide guidance on recovery actions: • Disaster Recovery and Business Continuity Plan; • OPS1 - CA Operations Manual; and • Incident Response Plan. These documents are not publicly available. CA Operations shall promptly advise PEXA PMA of any compromise or suspected compromise of any of the private keys belonging to any CA in the PEXA infrastructure. It is PEXA PMA's responsibility to inform the Gatekeeper Competent Authority.
5.7.4. Business continuity capabilities after a disaster	Actions are to be taken in order to restore core business operation as quickly as practicable following fire, flood or similar events. The Disaster Recovery and Business Continuity Plan provides guidance on recovery actions. This document is not publicly available.
5.8. CA termination	A termination of the PEXA RCA or OCA – planned or unplanned – would be non-trivial and requires preparation and agreed procedures. Full details of the rights and obligations of the various PKI participants are set out in the contracts between relevant parties. For the purposes of this section, keys and certificates can be taken to mean any set of keys and certificates within the RCA's chain of trust. A **programmed termination** will arise where there is termination by a CA for default or for convenience. Insofar as it is required, the CA shall affect a transfer of keys and certificates to another Gatekeeper accredited CA operator in a manner agreed with PEXA and the Gatekeeper Competent Authority. All parties will cooperate to ensure a transfer of CA services is done in a way that does not disturb the operation of the PKI or the use of its keys and certificates PEXA will: • give to the Gatekeeper Competent Authority no less than 3 months' prior written notice; • plan for the transfer of the operations to another service provider as nominated by PEXA; • implement the agreed transition plan. If a **non-programmed termination** of the PEXA CA is required, PEXA will: • provide Subscribers with as much notice as possible (where necessary); • assist Subscribers in transferring to another Gatekeeper accredited CA; and • reasonably co-operate with all stakeholders in the termination of the CA.
6. Technical Security Controls	Refer to DS CP section 5.2 for details of PEXA & Subscriber environments.
6.1. Key pair generation and installation	
6.1.1. Key pair generation	Key pairs for **CAs** are generated in Hardware Security Modules, where they remain stored under encryption. Key pairs for **Subscribers** and **PEXA Administrators** are generated in smartcards (for hard tokens) or in CMS (soft-tokens) at the CA location.

6.1.2. Private key delivery to subscriber	Tokens for **Subscribers** are delivered to the Subscriber Manager or Subscriber Administrator via Australia Post. Private keys are protected by a PIN delivered by PIN mailer sent separately to the token. Tokens for **PEXA Administrators** are delivered to the PEXA Senior Administrators via Australia Post. Private keys are protected by a PIN delivered by PIN mailer sent separately to the token.
6.1.3. Public key delivery to certificate issuer	Not applicable – key pairs are generated at the CA.
6.1.4. CA public key delivery to relying parties	The PEXA Root CA and OCA's certificates will be made available at: https://www.pexa.com.au/ca/publish/pexa/CAcerts/
6.1.5. Key sizes	RCA keys are 4096 bit RSA keys. OCA keys are 2048 bit RSA keys. End user and administrator keys are 2048 bit RSA keys. SHA keys are 256 bit.
6.1.6. Public key parameters generation and quality checking	Public key parameter generation and quality checking has been evaluated as part of the Common Criteria accreditation.
Key usage purposes (as per v3 key usage field)	CA certificates are only used for issuing certificates and CRLs, and have the following Key Usage parameters: • Certificate signing • CRL signing • Digital signing (for signing log entries) • Non-repudiation OCSP responder certificates have the following key usages defined: • Digital signing • OCSP signing (Extended key usage) All key usage extensions are marked "Critical". See certificate profiles in the relevant CP for end user certificates.
6.2. Private key protection and cryptographic module engineering controls	
6.2.1. Cryptographic module standards and controls	CA private keys are held in secure Hardware Security Modules that have been approved for use by ASD.
	Details surrounding the Common Criteria evaluation of the HSM can be found at the following URL: http://www.cybersecurity.my/mycc/mycprC037.html Smartcard chips used for hard tokens are certified to Common Criteria EAL5+ under protection profile "Javacard Minimal Configuration Protection Profile" (replaced by Javacard Closed Configuration Protection Profile), See https://www.commoncriteriaportal.org/files/ppfiles/jcsppc.pdf.

6.2.2. Private key (m out of n) multi-person control	Private keys used in the infrastructure entities managed by CA Operations are not under 'M out of N' multi-person control. Dual person control shall apply for all operations concerning the PEXA infrastructure private keys. Refer to section 5.2.2 for more detail on multi-person control.
6.2.3. Private key escrow	Private key escrow for authentication keys is not permitted.
6.2.4. Private key backup	The private keys of the RCA and OCA are stored in encrypted files on HSM smartcards. Certificate and key pairs keys are cloned during the initial Key generation ceremony of the RCA and OCA to provide for disaster recovery. Private key backup is not provided for end users.
6.2.5. Private key archival	Private keys of the RCA and OCA entities are archived at the data centres. Private keys are stored in class B containers that are located in physically secure areas. Private key archival is not provided for end users.
6.2.6. Private key transfer into or from a cryptographic module	Where an HSM is used on a CA or other Core Component, the private key is generated in the module. A second token with a cloned key pair is created during the initial key generation for transfer to a DR site. The token is protected by activation data, and the transfer is carried out in accordance with the Key Management Plan.
6.2.7. Private key storage on cryptographic module	Where an HSM is used in the infrastructure, the private key of the component is generated and retained in the HSM in an encrypted format. It will be decrypted only at the time at which it is being used.
6.2.8. Method of activating private key	The private keys of any CAs or Core Components managed or hosted by CA Operations are to be activated by cryptographic software following the successful completion of a login process that validates an authorised user. The CA Operations Key Management Plan shall specify who can activate or use private keys and how entity authentication is required to activate the private key for CAs or Core Components. Entry of activation data shall be protected from disclosure (i.e. the data should not be displayed while it is entered). The Key Management Plan can be found in SEC1 – Security Profile (not available to the public). Subscriber key activation, and protection of fhe private key, is the responsibility of the Certificate Holder. Subscriber Signer keys are protected with a PIN, which is entered prior to signing.
6.2.9. Method of deactivating private key	Private keys on HSMs are de-activated when the software application in the hardware security module is terminated by logging off or turning the power off. Private keys on smart cards for PEXA CA Core Components are de-activated when the card is removed from the card-reader, or after a set time of inactivity. Subscriber keys are deactivated when not in use (i.e. they must be activated for every signing operation). Private keys in soft tokens are de-activated when the user logs out, or the software application is shut down.
6.2.10. Method of destroying private key	The CA software destroys private keys in memory when the software shuts down.

	The SEC1 – Security Profile specifies who can co-ordinate the destruction of private keys and how. Media containing private keys are securely destroyed by, in the case of: • hard disks – sanitisation by overwriting in accordance with ISM; or • other media – in accordance with recommendations in ISM. Media containing a private key of a CA will be securely disposed of by sanitisation by overwriting (where feasible), then supervised physical destruction in accordance with ISM.
6.2.11. Cryptographic module rating	Refer to section 6.2.1.
6.3. Other aspects of key pair management	
6.3.1. Public key archival	The minimum archiving period is seven years in accordance with the *Archives Act 1983* and Australian National Archive Policy, Administrative Functions Disposal Authority (2000). PEXA archive will archive certificates indefinitely as part of the PEXA transaction archives
6.3.2. Certificate operational periods and key pair usage periods	RCA certificate and key pairs have the following usage period: 30 years OCA certificate and key pairs have the following usage period: 10 years
6.4. Activation data	
6.4.1. Activation data generation and installation	Activation data refers to passwords, passphrases, PINs, split keys or authentication tokens. Activation data is required to operate the **RCA** or **OCA**. Activation data together with any other access control mechanisms used by the CAs must have the level of complexity required by the classification of keys or data to be protected, as defined in the ISM. Classifications are detailed in SEC1 – Security Profile (not available to the public). All activation data is randomly generated in a secure manner and installed and utilized in a manner that prevents disclosure to unauthorized parties. Activation data for end user tokens is generated within the CMS at the CA data centre.
6.4.2. Activation data protection	Dual control access mechanisms are required to operate the RCA software, which is housed in a physically secure environment to the level defined by the Gatekeeper Framework for such activities. Data used to activate CA private keys shall be protected from disclosure by at least a combination of procedural and physical access control mechanisms. Protection of activation data is the responsibility of the Certificate Holder or key custodian. Certificate Holders are made aware of their responsibilities with regard to protection of activation data prior to receiving their token.
6.4.3. Other aspects of activation data	No activation data other than access control mechanisms is required to operate HSMs.
6.5. Computer security controls	

6.5.1. Specific computer security technical requirements	CA infrastructure hardware is controlled by: • a configuration management database (CMDB) and a configuration change control process; • performance of regular and frequent systems operability tasks to prove the correct operation of critical PKI components; • strong authentication required for core PKI system access; • No Lone Zone procedures, restrictions and controls on the use of system utilities; • the use of monitoring and alarm systems to detect and warn of unauthorised access to computer system resources; and • logging of all system access and use. All hardware items are registered in an asset tracking system.
6.5.2. Computer security rating	CA Operations uses COTS software and hardware that has been approved for use by Australian Signals Directorate and has been evaluated to Common Criteria Assurance level EAL 4+. See also section 6.2.1. for cryptographic module standards.
6.6. Life cycle technical controls	
6.6.1. System development controls	The software development controls applied in the development of the CA software used by CA Operations have been evaluated under the Australasian Information Security Evaluation Program (“AISEP”) and certified by an Australasian Information Security Evaluation Facility (“AISEF”) to meet the requirements of Common Criteria accreditation. Test and development systems are not available from the production environment and developers do not have access to production environment.
6.6.2. Security management controls	CA Operations security management controls are detailed in SEC1- Security Profile (not available to the public).
6.6.3. Life cycle security controls	PKI life cycle security controls are detailed in SEC1 – Security Profile (not available to the public).
6.7. Network security controls	CA Operations has undertaken a Threat and Risk Assessement which identifies and addresses all high or significant life cycle security threats. Details of this assessment can be found in the SEC1 – Security Profile. This document is not publicly available.
6.8. Time-stamping	Refer to section 5.5.5
7. Certificate, CRL, and OCSP Profiles	
7.1. Certificate profile	Refer to applicable CP.
7.2. CRL profile	Refer to CA CP, Appendix A.
7.3. OCSP profile	Refer to CA CP, Appendix A.

8. Compliance Audit and Other Assessments	
8.1. Frequency or circumstances of assessment	**8.1.1. Gatekeeper annual audit** PEXA CAs are subject to an annual audit by an authorised member of the Gatekeeper audit panel as per the Gatekeeper website: http://www.finance.gov.au/e-government/security-andauthentication/gatekeeper/audit-panel.html The Gatekeeper Compliance Audit Program (GCAP) consists of a self-assessment followed by the audit by the appointed panel member. It is the responsibility of PEXA to arrange for this audit. **8.1.2. ARNECC/Registrar** In relation to the CA operations, ARNECC/the Registrar requires that the CA operator is Gatekeeper accredited. The MOR states the requirements for compliance monitoring in Section 15. **8.1.3. Internal audits** The CA Operations ITSA will ensure a quarterly desktop review of all procedures and records management are carried out on the PEXA CAs.
8.2. Identity/qualifications of assessor	**8.2.1. Gatekeeper** Under the Gatekeeper compliance audit program the external audit of the CAs will be conducted by an approved authorised auditor who is a current member of the Gatekeeper Audit panel. Only individuals who are independent from CA Operations and have the necessary audit experience and training will conduct these audits. In particular, auditors must have: • a minimum of two (2) years auditing experience; • excellent understanding of IT security environments; • excellent understanding of PKI technologies and operations; and • a security clearance to at least the level of the information to be accessed. The self-assessment which forms part of the annual audit program will be conducted by CA Operations auditing staff. Where possible, qualified IRAP security auditors will perform the audit. **8.2.2. ARNECC/Registrar** In relation to the CA operations, the ARNECC/the Registrar requires that the CA operator is Gatekeeper accredited. Section 16 of MOR specifies level of qualifications held by Independent Experts used to carry out audits. **8.2.3. CA Internal Audit** No specific qualifications are required, however where possible, IRAP qualified staff will conduct audits.
8.3. Assessor's relationship to assessed entity	Where an external auditing organisation is utilised, the Auditor must be an independent third party, and must not have any actual (or potential) conflict of interest during the period of the audit.

8.4. Topics covered by assessment	When an external audit organisation is used to conduct a Gatekeeper Audit there is to be a clear Statement Of Work (SOW) produced by the auditor prior to their arrival. It is the responsibility of the PEXA PMA to ensure that the contracted auditor and the organisation they represent meets the security, compliance and privacy requirements of the managed CA service provider. **Topics covered by audit** The areas to be audited for both external and internal audits may include but are not limited to: • effective delivery of the infrastructure services; • compliance with Gatekeeper approved documents; • adherence to privacy requirements; • adherence to key management requirements;
	• physical security controls; • storage and handling requirements of information; • logical security controls; • media management requirements; • hardware/software configuration baseline management; • change management; • business continuity and disaster recovery plan; • incident management procedures; • risk management procedures; • adherence to personnel security control requirements; and • implementation of internal systems verification programmes.
8.5. Actions taken as a result of deficiency	**External Audit** The results of the annual Gatekeeper audit will be provided to the PEXA PMA and to the Gatekeeper Competent Authority. Department of Finance and PEXA will then agree timeframes for resolving identified non-compliances (refer to Head Agreement) **Internal Audit** If an adverse finding is reported during an internal audit an incident report will be submitted to the CA Operations ITSO. Where the adverse finding is of a serious nature, the CA Operations ITSA will notify the PEXA PMA and appropriate corrective action will be taken by the ITSO.
8.6. Communication of results	To provide visibility of the operations, audit reports from audits conducted on CAs will be forwarded to the managed CA service provider and PEXA PMA. In accordance with Gatekeeper accreditation requirements, final copies of the annual external audit report on the RCA and OCA must be submitted to: • the Service Provider (PEXA); and • the Gatekeeper Competent Authority; and • other parties by agreement. All audit results are considered to be sensitive commercial information and will be protected in accordance with section 9.4 of this CPS.
9. Other Business and Legal Matters	
9.1. Fees	Refer to applicable CP.
9.2. Financial responsibility	Refer to applicable CP.
9.3. Confidentiality of business information	Refer to applicable CP.

9.4. Privacy of personal information	All parties must comply with their obligations under the Privacy Act 1988 (Cth) including the Australian Privacy Principles. Refer to applicable CP and the respective Privacy Policies for more detail.
9.5. Intellectual property rights	Refer to applicable CP.
9.6. Representations and warranties	Refer to applicable CP.
9.7. Disclaimers of warranties	Refer to applicable CP.
9.8. Limitations of liability	Refer to applicable CP.
9.9. Indemnities	Refer to applicable CP.
9.10. Term and termination	
9.10.1. Term	This CPS (and related CPs) shall be effective from the date it is published on the PEXA website, until it is superseded by a new version, or its termination is declared by PEXA by email or by notice on its website or through the PEXA system.
9.10.2. Termination	This document ceases to be effective for a particular PEXA DSC Subscriber when the PEXA DSC Subscriber Agreement is no longer in force.
9.10.3. Effect of termination and survival	Provisions relating to: • Intellectual Property Rights; • Confidential Information; • the protection of Personal Information; or • an indemnity, survive the termination of this CPS.
9.11. Individual notices and communications with participants	Any Notice under this document must be in writing and must be sent to the intended recipient by: • hand delivery; • regular mail; or • email transmission Digitally Signed with a valid certificate recognised by PEXA. A Notice or other communication will be taken to have been received by the recipient: • if sent by hand delivery or registered pre-paid post – on the date it is delivered; • if sent by regular mail – 3 business days after the date of posting within Australia; or • if sent electronically – on the business day next following the day on which the notice was sent.

	PEXA PKI Certification Practice Statement
9.12. Amendments	It will occasionally be necessary to amend this CPS and/or the correlating CPs. Some of these changes will not materially reduce the assurance this CPS or its implementation provides, and will be judged by the PEXA PMA to have a non-material impact on the acceptability of certificates. If a change to the CPS or CPs will materially alter the acceptability of certificates for specific purposes, then these changes may require corresponding changes to the CPS pointer (URL) or the correlating CP's OID. (Refer to section 1.2) Minor changes such as: • those made to improve the clarity of the document; or • editorial and typographical corrections; or • changes to contact details are not considered amendments, however any change must be brought to the attention of the PEXA PMA and Gatekeeper Competent Authority to seek their agreement. Different versions of the documents must be identifiable by their version number.
9.12.1. Procedure for amendment	Refer to Section 1.5.4.
9.12.2. Notification mechanism and period	PEXA DSC Subscribers will be advised of material changes to this CPS or correlating CPs via email, post or through the PEXA system. Continued use of this CPS or correlating CPs beyond the specified date of effect will constitute acceptance of the amendments.
9.12.3. Circumstances under which OID must be changed	An OID change to a correlated CP is recommended whenever changes are made to the PKI, which materially alter the acceptability of certificates for specific purposes. This requires the consent of the PEXA PMA. Additionally all OID changes must be approved by the Gatekeeper Competent Authority prior to implementation.
9.13. Dispute resolution provisions	Refer to applicable CP.
9.14. Governing law	Refer to applicable CP.
9.15. Compliance with applicable law	Refer to applicable CP.
9.16. Miscellaneous provisions	Not applicable.
9.17. Other provisions	Not applicable.

APPENDIX A. CERTIFICATE POLICIES

PEXA Certificate Policies related to this CPS:

1) PEXA PKI Digital Signing Certificate Policy
2) PEXA PKI Certification Authority Certificate Policy
3) PEXA PKI PEXA Administrator Certificate Policy

APPENDIX B. TERMS, DEFINITIONS AND ACRONYMS

Term/Acronym	Definition/Meaning
Approved Documents	Documents that have been reviewed and approved by the Gatekeeper Competent Authority as a result of Gatekeeper accreditation.
ADI	Authorised Deposit-taking Institution (see http://www.apra.gov.au/adi/)
ARNECC	Australian Registrars' National Electronic Conveyancing Council, the regulator for electronic conveyancing in Australia. Made up of representatives of all the Land Registries.
ASD	Australian Signals Directory (previously known as DSD, Defence Signals Directory). Government agency that provides foreign signals intelligence to the Australian Defence Force and Australian Government to support military and strategic decision-making. ASDs activities include evaluation of cryptographic products for use within the Australian Government. ASD produce the Australian Government Information Security Manual (ISM).
CA	Refer to Certification Authority.
CA CP	Certification Authority Certificate Policy.
CA Operations	The team and/or location responsible for carrying out day-to-day management of the CA and credential management on behalf of PEXA.
Card Management System (CMS)	System managed by CA Operations, which personalises and prints hard tokens, creates and manages soft tokens, manages issued tokens.
Certification Authority (CA)	Certification Authority means a Gatekeeper Accredited *Service Provider* that issues Digital Certificates that have been Digitally Signed using the Certification Authority's private key and provides certificate verification and revocation services for the Digital Certificates it issues.
Certificate Holder	A person who has been issued with a digital certificate.
Certificate Recipient	Certificate Recipient means each person who is issued a Digital Certificate under a PEXA DSC Subscriber Agreement and includes the 1st Subscriber Manager, a Subscriber Manager, a Subscriber Administrator and a Subscriber Signer.
Community of Interest	A defined population of users – Subscribers and Relying Parties – that agree to use Relationship Certificates
	according to an agreed set of rules. (Source: Gatekeeper Glossary) The PEXA Community of Interest is defined in section 1.1.

Term/Acronym	Definition/Meaning
Compromised	Has the meaning given to it in the Model Participation Rules (MPR).
Core Component	Term used in the CA CP; it refers to components within the CA infrastructure which are issued with keys and certificates for authentication. Core Components for the UniCERT CA software include: -Certification Authority (CA) component -Registration Authority (RA) component -Registration Authority Auditor (RAA) component -RA Exchange (RAX) component -Certificate Status Server (CSS) component -UniCERT Programmatic Interface (UPI)
CRL	Certificate Revocation List. A list of certificates that have been revoked or suspended. (Expired certificates are not included.)
Digitally Sign	Has the meaning defined in the ECNL.
Digital Signature	Has the meaning defined in the ECNL.
DR	Disaster Recovery
DS CP	Digital Signing Certificate Policy.
ECNL	Electronic Conveyancing National Law
ELN	Electronic Lodgement Network, an electronic conveyancing platform such as PEXA.
ELNO	Electronic Lodgement Network Operator, i.e. PEXA via appointment by each Registrar.
Gatekeeper (GK)	Gatekeeper is the policy and accreditation framework developed by the Australian Government to create trust and confidence in the infrastructure underpinning the use of digital certificates with government, and as an enabler for the delivery of online government services.
Gatekeeper Competent Authority	A delegated authority from the Secretary of the Department of Finance. The First Assistant Secretary, Efficiency, Assurance and Digital Government (EADG) is the Gatekeeper Competent Authority (as at May 2014).
Government Agencies	Government Agencies involved in property transactions, such as: • Land Titles Offices • State Revenue Offices
GRC	Governance, Risk Management and Compliance

Term/Acronym	Definition/Meaning
Handle	A term that, when used in relation to 'information', means collected, exchanged, transmitted or any combination thereof.
HSM	Hardware Security Module. Hardware providing secure generation, management and operation of cryptographic keys.
Individual VOI Documents	Documents presented at a Verification of Identity check.
I-RAP	Infosec-Registered Assessor Program, see http://www.asd.gov.au/infosec/irap.htm
ISM	The Australian Government Information Security Manual, standard which governs the security of government ICT systems. Gatekeeper requires minimum requirements of ISM to be met by Service Providers. See http://www.asd.gov.au/infosec/ism/
ITSA	Information Technology Security Advisor
ITSO	Information Technology Security Officer
Jeopardise	Has the meaning given to it in the Model Participation Rules (MPR).
MOR	Model Operating Requirements, a document issued by ARNECC, which sets out the rules for Electronic Lodgement Network Operators (ELNOs).
MPR	Model Participation Rules, a document issued by ARNECC, which sets out the rules for Participants in an ELN.
No Lone Zone	Area protected by the requirement that two people are present at all times during operations. This may be enforced by technical or procedural means.
Organisation Documents	Documents that PEXA will use to establish the existence and eligibility of a PEXA Member and to verify signatories with binding authority.
PEXA	Property Exchange Australia Limited, the legal entity that operates the PEXA Platform.
PEXA Administrator	PEXA staff member of the PEXA On-boarding or PEXA Support Desk teams, who performs administration duties in the PEXA Platform and/or PEXA CRM systems.
PEXA CMS	PEXA Card Management System

Term/Acronym	Definition/Meaning
PEXA Certification Practice Statement	This document which is published by PEXA, under which it operates and manages its Certification Authority function. Refer to https://www.pexa.com.au/ca/publish/pexa/documents/
PEXA Community of Interest	See "Community of Interest". The PEXA Community of Interest is defined in section 1.1.
PEXA CRM	Is the PEXA Customer Relationship Management (CRM) host used to collect and maintain all information pertaining to PEXA Subscribers and PEXA Members for the purpose of on-boarding the Subscriber and subsequent account management and support through to PEXA Subscriber termination.
PEXA Digital Signing Certificate	Means a digital certificate issued to PEXA DSC Subscribers that may be employed to sign PEXA Documents or emails.
PEXA Document	Any registry instrument or other document in connection with a conveyancing transaction that is created on the PEXA Platform by PEXA Users, that may be Digitally Signed.
PEXA Digital Signing Certificate Subscriber Agreement	Means the agreement between PEXA and a PEXA Member or PEXA Subscriber under which the Organisation becomes a PEXA DSC Subscriber.
PEXA DSC	Has the meaning defined in PEXA Digital Signing Certificate.
PEXA DSC Subscriber	An Organisation that has signed the PEXA DSC Subscriber Agreement. Such Organisations are also PEXA Subscribers.
PEXA DSC Subscriber Agreement	Has the meaning defined in PEXA Digital Signing Certificate Subscriber Agreement.
PEXA Member	An Organisation that wishes to become a PEXA Subscriber that has lodged requisite details as part of the PEXA On-boarding process during the 'Initial Contact / Sales' stage.
PEXA On-boarding Officer	Is an employee or sub-contractor employed in the PEXA On-boarding Team. These individuals are responsible for the validation of a PEXA Member's supplied on-boarding documentation, and their consequent approval to become a PEXA Subscriber.
PEXA Operations	The group within PEXA that performs on-boarding and customer operational support functions. It includes the PEXA Support Desk and the PEXA On-boarding team.
PEXA Participation Agreement	Means the agreement between PEXA and an Organisation under which the Organisation becomes a PEXA Subscriber, enabling it to transact on the PEXA Platform.
PEXA Platform	An internet-accessible IT system that facilitates the exchange of property. This system interfaces to Land Registries' and Financial Institutions' IT systems and is accessible by PEXA Users who are part of Subscriber Organisations.
PEXA Senior Administrator	PEXA managerial staff member responsible for allocating and managing certificates for PEXA Administrators.

Term/Acronym	Definition/Meaning
PEXA Subscriber	An Organisation that has signed the PEXA Participation Agreement, enabling it to transact on the PEXA Platform.
PEXA Support Desk	Is the PEXA facility through which all support requests may be lodged and serviced. PEXA Support is accessible via email and phone.
PEXA Support Officer	Is a member of the PEXA Support Desk. Their role includes providing support to customers for life-cycle management of PEXA Digital Certificate.
PEXA User	An individual who is employed by a PEXA Subscriber who has been provisioned with a PEXA Platform account who may be a Subscriber Manager, Subscriber Administrator, Subscriber Signer or Subscriber User.
PEXA VOI Officer Accreditation Program	Accreditation program for prospective VOI Officers. See section 5.7 of the DS CP.
PKI	Public Key Infrastructure, a framework comprising of technology, people, policies and practices, which puts into place a framework for the use of private and public key technology (based on asymmetric cryptography). PKI enables the use of digital signing and encryption for integrity, confidentiality, authentication and non-repudiation.
PMA	Policy Management Authority, a body that governs the PKI operations, providing direction and accountability. The PEXA PKI PMA is described in section 1.3.5.
Practitioner	Australian Legal Practitioner or Licensed Conveyancer
Private Key	Has the meaning given to it in the Model Participation Rules (MPR).
PSPF	Australian Government's Protective Security Policy Framework, provides the appropriate controls for the Australian Government to protect its people, information and assets. The PSPF is owned by the Attorney General's Department (AGD).
Public Key	Has the meaning given to it in the Model Participation Rules (MPR).
RA	See Registration Authority

Term/Acronym	Definition/Meaning
Registrar	The state and territory official who has responsibility for each jurisdiction's Land Registry function: • New South Wales – Registrar General • Victoria – Registrar of Titles • Queensland – Registrar of Titles • Western Australia – Registrar of Titles (or other officer of the Land Registry nominated by the Chief Executive of the Western Australian Land Information Authority) • South Australia – Registrar General • Northern Territory – Registrar General • Australian Capital Territory – Registrar General • Tasmania – Recorder of Titles
Registration Authority (RA)	(Definition from Gatekeeper glossary) A Service Provider that: • is responsible for the registration of applicants for Digital Certificates by checking Evidence of Identity (EOI) documentation submitted by the applicant for its compliance with Gatekeeper EOI Policy; • is responsible for the provision of completed and authorised application form including copies of the submitted EOI documents to the relevant CA; and • may be responsible for the secure distribution of signed Digital Certificates to Subscribers. **See description of Registration Authority for the PEXA PKI in section 1.3.2.**
Relationship Certificate	A Digital Certificate issued by a Service Provider to Clients of a Relationship Organisation, according to business rules specific to the Community of Interest (COI) of which the Relationship Organisation is a part. (Source: Gatekeeper Glossary)
Relationship Organisation	The Organisation within (or comprising) a Community of Interest that has an established relationship with its Clients considered adequate for the issuance of Digital Certificates. (Source: Gatekeeper Glossary)
Service Provider	Under Gatekeeper, an accredited or recognised entity that provides CA or RA services. When indicating another type of "service provider", lower case has been used.

Term/Acronym	Definition/Meaning
Sponsor	An Organisation that has been appointed by PEXA to perform a variety of functions including on-boarding PEXA Subscribers. Sponsors include software application and service providers to the conveyancing or legal practice sectors and thereby have an existing relationship with potential PEXA Subscribers. Sponsor functions include acting as a VOI Agent, in which case they will appoint one or more VOI Officers.
Subscriber Administrator	A Subscriber User who also has: • the ability to make the changes permitted under the MPR Participation Rule 7.3.3 on behalf of the Subscriber (but excluding setting financial limits on Subscriber Signers' signing rights; and • can perform certificate management task as described in section 4; and • may be a Subscriber Signer.
Subscriber Identity Verification Standard	Means the standard for the Verification of Identity of potential PEXA Subscribers as set out in Schedule 7 of the MOR. This standard is employed to verify the identity of the person or persons who execute a PEXA Subscriber Agreement.
Subscriber Manager	A Subscriber User who also: • has the ability to make the changes permitted under the MPR Participation Rule 7.3.3 on behalf of the Subscriber; • can perform certificate management task as described in section 4; and • may be a Subscriber Signer.
Subscriber Organisation	A legal entity that is authorised under a participation agreement to use an ELN to complete conveyancing transactions on behalf of another person or on their own behalf. See also "PEXA Subscriber" and "PEXA DSC Subscriber".
Subscriber Signer	A PEXA User who has been granted signing privilege to Sign PEXA Documents.
Subscriber User	A PEXA User with entry-level privileges on the PEXA Platform.

Term/Acronym	Definition/Meaning
Verification of Identity	Verification of Identity, also defined within Gatekeeper as an Evidence of Identity (EOI) check, is the process of verifying identity documents in the presence of the person who's identity is to be verified. The two VOI standards that apply to the PEXA PKI are: • the Subscriber Identity Verification Standard; and • the Verification of Identity Standard. For consistency, only the term 'Verification of Identity' has been used in the PEXA CPS and CP documents.
Verification of Identity Standard	Means the standard of that name set out as schedule 8 in the MPR, as amended from time to time. This standard is employed to verify the identity of any Certificate Recipient.
VOI	See Verification of Identity.
VOI Agent	An Organisation that has been appointed by PEXA to conduct a face-to-face Verification Of Identity (VOI). VOI Agents include Sponsors.
VOI Officer	An individual employed by either PEXA or a Sponsor who has been accredited by PEXA to conduct VOI interviews on PEXA's behalf.
VOI secure transmission Tool	A tool that allows VOI documents to be digitized and securely transferred to the PEXA CRM.