YOUR ONLINE PROPERTY EXCHANGE

PEXA Public Key Infrastructure (PKI)

Certification Authority Certificate Policy

Version: 1.0 Issued: August 2014 Status: Final

PEXA
Property Exchange Australia

	PEXA Certification Authority Certificate Profile
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. The PEXA Public Key Infrastructure (PKI) supports the operation of PEXA by issuing and managing identity credentials for all users that need to sign instruments in PEXA. The credentials are X.509 certificates issued to individuals within Subscriber Organisations. This document, the *PEXA PKI Certification Authority Certificate Policy*, describes how the PEXA CA keys and certificates are managed, and the roles and responsibilities of the PKI participants in relation to the use and management of keys and certificates. It should be read in conjuction with the *PEXA PKI Certification Practice Statement* (CPS). The CP and CPS use almost identical format, headings and numbering, and contain frequent cross-references. The format of this CP is based on the IETF standard RFC3647 ("Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework. For explanation of Terms, Definitions and Acronyms, refer to CPS 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.

	PEXA Certification Authority Certificate Profile
	1.1.1 Related documentation The following documents have been referenced in this CP: i. PEXA Documents: • PEXA PKI Certification Practice Statement (CPS) • 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 1 April 2013 http://www.arnecc.gov.au/publications • Model Operating Requirements (MOR), ARNECC, Version 1 April 2013 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 • OPS1 - CA Operations Manual • PEXA Managed CA design documents • Incident Response Plan • Disaster Recovery and Business Continuity Plan (DRBCP) • 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-key-infrastructure/gatekeeper-documentation/: • 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 • RFC8250 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile • [RFC6960] 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 Authority Certificate Policy" (PEXA CA CP). ASN.1 Object Identifiers (OIDs) are used in PKI to uniquely identify objects such as documents, algorithms or parameters of digital certificates. PEXA PKI certificates contain an OID identifying the CP under which the certificate was issued. Both CPS and CPs can be accessed at: https://www.pexa.com.au/ca/publish/pexa/documents/

	PEXA Certification Authority Certificate Profile
	The PEXA PKI Certification Authority Certificate Policy covers certificates for the PEXA CAs as well as PEXA OCSP certificates, and can be identified by the following two OIDs: **1.2.1 CA certificate OID** **1.2.36.40677792.1.1.1** iso (1) iso-member (2) australia (36) PEXA (40677792) PKI (1) Certificate Policy (1) CAs (1) This OID is present in all CA certificates issued under this policy. **1.2.2 OCSP certificate OID** **1.2.36.40677792.1.1.4** iso (1) iso-member (2) australia (36) PEXA (40677792) PKI (1) Certificate Policy (1) OCSP (4) This OID is present in all OCSP certificates issued under this policy.
1.3. PKI participants	Refer to CPS for PKI Participants relating to end user certificates.
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 entities. 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 tamper proof. The RCA is kept off-line. **PEXA Operational Certification Authority (OCA)** The PEXA Operational CA issues certificates to users and administrators of the PEXA system. The PEXA OCA also has very high security requirements, and uses an HSM to generate, store and use its keys. The OCA's certificate is created at a key signing ceremony attended by PEXA and Gatekeeper representatives.
1.3.2. Registration authorities (Relationship Organisation)	For the purposes of this CA CP, Registration Authority functions such as: • Verification of Identity of certificate applicants and Key Custodians; • registration in the PEXA PKI; • creation of a certificate request; and • further certificate lifecycle management; are carried out by CA Operations staff. Refer to CPS and the PEXA Digital Signing CP for information about registration of Subscribers and Subscriber Signers.

	PEXA Certification Authority Certificate Profile
1.3.3. Subscribers	The term "Subscribers" is not used in this CP in order to avoid confusion with the use of the term in related PEXA PKI documents (refer to CPS). For the purpose of this CP, there are "Certificate Holders" (operators) and "Key Custodians" (persons responsible for CA and Core Component keys and certificates).
1.3.4. Relying parties	Relying parties for certificates issued under this CP are: • the PEXA Platform; • the PEXA PKI Core Components (which validate the certificates of CA Operators and other Core Components).
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 current 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 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-key-infrastructure/ 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 CP) is subject to review by the Gatekeeper Competent Authority.
1.4. Certificate usage	The Certification Authorities (CAs) in the PEXA PKI consist of a Root CA (RCA) and an Operational CA (OCA). Certificates governed by this CP include: i. the self-signed certificate of the PEXA Root CA ii. certificates issued by the PEXA Root CA to Operational CAs iii. certificates issued to the PEXA OCSP responder iv. certificates issued to other Core Components, i.e: • Registration Authority (RA) component • Registration Authority Auditor (RAA) component • RA Exchange (RAX) component • Certificate Status Server (CSS) component • UniCERT Programmatic Interface (UPI) v. certificates issued to operators of the PEXA CAs. i. to iv. are device certificates, i.e. issued to a machine, whereas v. are issued to individuals (operators). Key custodians are nominated for i-iv.
1.4.1. Appropriate certificate uses	Certificates issued under this CP and their associated private keys, allow the **RCA** to: i. sign its own certificate (self-signing); ii. sign a OCA certificate; iii. sign the operational certificates required by the PKI infrastructure; and iv. sign its own internal log files. Certificates issued under this CP and their associated private keys, allow a **OCA** to:

	PEXA Certification Authority Certificate Profile
	i. sign Subscriber certificates; ii. sign the operational certificates required by the PKI; and iii. sign its own internal log files. **OCSP responder** certificates are used for authenticating the OCSP responder device and signing responses. **Core Component** and **CA operator** certificates are used for authentication and/or confidentiality within the system.
1.4.2. Prohibited certificate uses	Certificates issued under this CP must not be used for other purposes than those described in Section 1.4.1.
1.5. Policy administration	
1.5.1. Organisation administering the document	The PEXA PKI Policy Management Authority (PMA) is responsible for administering this document and the CPS. Refer to CPS.
1.5.2. Contact person	Contact details for the PEXA 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 the PEXA CPS to support a particular CP.
1.5.4. CPS approval procedures	Refer to CPS sections 1.5.4 and 9.12.
1.6. Terms, Definitions and Acronyms	For Terms & Definitions, refer to CPS Appendix B. Defined terms are capitalised.
2. Publication and Repository Responsibilities	Refer to CPS, sections: 2.1. Repositories 2.2. Publication of certification information 2.3. Time or frequency of publication 2.4. Access controls on repositories
3. Identification and Authentication	
3.1. Naming	
3.1.1. Types of names	Each certificate must have an X.500 Distinguished Name which uniquely identifies the Subject within the PKI. For CA certificates, the Distinguished Name will include: • Common Name (eg. “PEXA PKI Root CA”) • Organisational Unit (“CAs”) • Organisation (“PEXA”) • Country (“AU”) For OCSP certificates, the Distinguished name will include: • Common Name (eg. “PEXA OCSP”) • Organisational Unit (“OCSP”) • Organisation (PEXA) • Country (“AU”) For CA Operators, the Distinguished Name will include: • Component+Group number (e.g. “OCAO1” or “OCAO2”)

	PEXA Certification Authority Certificate Profile
	• Organisational Unit (e.g. CA Operations) • Organisation (e.g. "<managed CA service provider>") • Country ("AU") Refer to Appendix A.for certificate profiles.
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.
3.1.3. Anonymity or pseudonymity of Subscribers	Anonymous or pseudonymous names are not allowed.
3.1.4. Rules for interpreting various name forms	Certificates will use X.500 Distinguished Names that are readily distinguishable and do not require special interpretive rules.
3.1.5. Uniqueness of names	Each Distinguished Name assigned to a device or person in the PEXA PKI must be unique within the PKI name space. Renewal certificates for the same device or person may have the same Subject Name as the replaced certificate.
3.1.6. Recognition, authentication, and role of trademarks	Refer to clause 14 of the PEXA DSC Subscriber Agreement.
3.2. Initial identity validation	
3.2.1. Method to prove possession of private key	All keys are generated at the managed CA service provider's data centres. Private Key generation of critical PKI Core Components (incl. CAs and OCSP responders) is performed using Hardware Security Modules (HSMs). These private keys are generated internally which ensures that the private key is never exposed or accidentally released. To initiate the key generation process the CA operator must activate the HSM in the presence of the witnesses as dictated by the Key generation ceremony script. CA operators use hard token technology for their authentication private keys, with passphrase access controls. The key generation process requires the operator to enter their token's passphrase thereby proving the operator has possession of the token with the generated private key. Where soft tokens are used, certificate requests are submitted to the CA via PKCS#10 requests, where proof of possession of the private key is ensured as the key pair is generated at the time the certificate request is created and has been used to sign the request.
3.2.2. Authentication of organisation identity	Written requests from PEXA for **CA** key generation must be backed up with out-of-bands contact with a PEXA PMA representative for confirmation. Authentication of the Organisation and validation of authority is achieved through the combination of: • the written request for key generation from the PEXA PMA; and • the written nomination of PEXA witnesses from the PEXA PMA; and • verifying the identity of PEXA witnesses prior to the key generation. **CA Operators** must be employees at the relevant CA data centre.
3.2.3. Authentication of individual identity	**CA keys** Prior to the key generation taking place, PEXA witnesses will be required to go through a VOI check performed by CA Operations staff. **CA Operator and Core Component keys** CA Operators that are to be issued PEXA CA operator certificates or are nominated as key custodians for Core Component keys (incl. OCSP keys) must be under the direct supervision of (and thus known to) the CA Operations Team Lead.

	PEXA Certification Authority Certificate Profile
3.2.4. Non-verified subscriber information	Not applicable.
3.2.5. Validation of authority	Refer to section 3.2.2.
3.2.6. Criteria for interoperation	Not applicable.
3.3. Identification and authentication for renewal	
3.3.1. Identification and authentication for renewal	As per section 3.2.
3.3.2. Identification and authentication for renewal after revocation	**CA and OCSP keys** Renewal is not allowed after revocation for CA and OCSP responder certificates, i.e. a new entity must have a new Distinguished Name. **CA Operator keys** For operators, renewal after revocation shall occur in the same manner as for initial Verification of Identity.
3.4. Identification and authentication for revocation request	Revocation of an OCA's certificate must be requested in writing, signed by a representative of the PEXA PMA. The requestor's identity must be verified by CA Operations prior to carrying out the revocation.
3.5. Identification and Authentication for Key Recovery Request	Not applicable.
4. Certificate Life-cycle Operational Requirements	
4.1. Certificate application	
4.1.1. Who can submit a certificate application	A request to create new Root CA or OCA with associated components must be in writing, signed by a representative from the PEXA PMA.
4.1.2. Enrolment process and responsibilities	The process for the application and generation of Root CA and OCA keys and certificates is detailed in the PEXA Key Generation Script.
4.2. Certificate application processing	Following on from a request for key generation, CA operations will prepare for a key generation ceremony which involves the witnessed creation of a self-signed Root CA, followed by the key generation and signing of an OCA certificate. Keys are generated within a Hardware Security Module (HSM). The process is documented in the PEXA PKI Key Generation Script.
4.2.1. Performing identification and authentication functions	Refer to 3.2
4.2.2. Approval or rejection of certificate applications	The PEXA PMA must approve any new CA certificate applications. Incomplete or incorrect certificate applications received by CA operations will be rejected.

	PEXA Certification Authority Certificate Profile
4.2.3. Time to process certificate applications	As agreed between PEXA and the managed CA service provider.
4.3. Certificate issuance	**Root CA**, **OCA**, **OCSP and Core Component** certificates are created from the information entered by CA operators. Key custodians (for CAs, OCSP and Core Component certificates) and Certificate Holders (for CA operator certificates) are present at the CA bootstrap process, and will be required to enter passphrases at times during the process. The key generation is also witnessed by a representative from PEXA and from the Gatekeeper Competent Authority. The process is documented in detail in the PEXA PKI Key Generation Script.
4.3.1. CA actions during certificate issuance	The PEXA RCA or OCA software application (as applicable) performs the following checks after receiving a certificate request: i. authenticate the certificate request message to ensure that it has come from an approved source; ii. verify that the request is correctly formed; iii. compose and sign the certificate; iv. return the certificate to the source; and v. publish the certificate in accordance with this CP and the CPS.
4.3.2. Notification to subscriber by the CA of issuance of certificate	No stipulation.
4.4. Certificate acceptance	
4.4.1. Conduct constituting certificate acceptance	Certificate Holders and Key Custodians must carefully check the issued certificate for correctness before using the keys and certificates. PEXA are deemed to have accepted the **RCA** and **OCA** certificates when PEXA witnesses sign the Key Generation Script after the completed Key generation ceremony. PEXA PKI component key custodians and CA Operators are deemed to have accepted a certificate when they exercise the private key.
4.4.2. Publication of the certificate by the CA	The RCA and OCA certificates are published in the internal CA repository and on PEXA's website upon issuance. https://www.pexa.com.au/ca/publish/pexa/CAcerts/ Refer to section 2 of the CPS.
4.4.3. Notification of certificate issuance by the CA to other entities	No stipulation.
4.5. Key pair and certificate usage	
4.5.1. Subscriber Private Key and Certificate Usage	Key and certificate usage is defined in section 1.4.
4.5.2. Relying Party Public key and Certificate Usage	RCA and OCA certificates form part of the certificate chain of trust of subordinate certificates. It is in this function that Relying Parties must perform checks on validity, certificate status, usage in accordance with stipulated key usage before relying on the subordinate certificate.
4.6. Certificate renewal	Refer to 4.7 Certificate Re-key.
4.7. Certificate re-key	Creation of a new RCA or OCA will occur as per initial Certificate application – refer to sections 4.1 – 4.4.

	PEXA Certification Authority Certificate Profile
	A new RCA should be created 10 years prior to the current one expiring, to allow for the expiry of subordinate (OCA) certificates within the validity time of the issuer. A new OCA should be created 3 years prior to the current one expiring, to allow for the expiry of subordinate end user certificates within the validity time of the issuer.
4.8. Certificate modification	Not applicable.
4.9 Certificate revocation and suspension	
4.9.1 Circumstances for revocation	Circumstances for revocation of a certificate issued under this CP include, but are not limited to, the following: • a private key, or a token holding a private key, is lost, damaged or compromised; • a change occurs to certificate details (e.g. change of name); • details in the issued certificate are found to be inaccurate; • to protect the security or integrity of the PEXA PKI; or • the certificate is no longer required. If the PEXA RCA is compromised, it will not be revoked, however all subordinate certificates must be revoked and a new hierarchy created.
4.9.2 Who can request revocation	A request to revoke a **OCA** or OCSP responder certificate must be made by a representative of the PEXA PMA. **CA Operator** certificates can be revoked by: • the Certificate Holder • the CA Operations Team Lead or Information Technology Security Officer (ITSO).
4.9.3 Procedure for revocation request	A request for the revocation of an **OCA** must be provided in writing, signed by a representative of the PEXA PMA. The CA Operations Team Lead will check the authenticity of the request by an out-of-bands method (i.e. phone call to a PEXA registered contact). Refer to Incident Response Plan for emergency procedures.
4.9.4. Revocation request grace period	No stipulation.
4.9.5. Time within which CA must process the revocation request	The CA Operations Team Lead must action a revocation request within one business day of having verified the authenticity of the request.
4.9.6. Revocation checking requirement for relying parties	Relying parties (refer to section 1.3.4) must validate a certificate including checking the certificate status prior to relying on a signature created with the certificate.
4.9.7. CRL issuance frequency (if applicable)	RCA CRLs will be issued upon revocation of an issued certificate or at least quarterly OCA CRLs are issued upon revocation of an issued certificate or at least daily.
4.9.8. Maximum latency for CRLs (if applicable)	Maximum latency between the generation and publication of a CRL is 24 hours. The maximum latency must account for the time to: • generate the CRL; • transfer the CRL from the CA to the OCSP responder; and • scheduled periods of system unavailability. N.B. When PEXA revokes or suspends a user's certificate, their PEXA account would be deleted (revocation) or the user's signing privileges disabled (suspension) and they would be unable to transact.

	PEXA Certification Authority Certificate Profile
4.9.9. On-line revocation/status checking availability	Online revocation status server is available to relying parties 24/7.
4.9.10. On-line revocation checking requirements	PEXA use of CA certificates is checked using the PEXA OCSP responder (refer to DS CP). (CA Operator and Core Component certificate status checks are internal to the CA system, using CRLs.)
4.9.11. Other forms of revocation advertisements available	No stipulation.
4.9.12. Special requirements - key compromise	Refer to the Disaster Recover and Business Continuity Plan (DRBCP) (not available to the public).
4.9.13. Circumstances for suspension	Not applicable.
4.9.14. Who can request suspension	Not applicable.
4.9.15. Procedure for suspension request	Not applicable.
4.9.16. Limits on suspension period	Not applicable.
4.9.17. Un-suspension	Not applicable.
4.10. Certificate status services	
4.10.1. Operational characteristics	Certificate Status services are provided for certificates issued by the OCA and RCA through an OCSP service.
4.10.2. Service availability	OCSP responders for certificates issued by the OCA and RCA are deployed in a high availability configuration, with a target of 99.9% availability.
4.11. End of subscription	Not applicable.
4.12. Key escrow and recovery	Not applicable.
5. Facility, Management, and Operational Controls	Refer to CPS for details of CA controls, sections: 5.1. Physical controls 5.2. Procedural controls 5.3. Personnel controls 5.4. Audit logging procedures 5.5. Records archival 5.6. Key changeover 5.7. Compromise and disaster recovery 5.8. CA termination Refer to Digital Signing CP for details of RO controls.
6. Technical Security Controls	Refer to CPS for details relating to the CA, sections: 6.1. Key pair generation and installation 6.2. Private key protection and cryptographic module engineering controls 6.3. Other aspects of key pair management 6.4. Activation data 6.5. Computer security controls 6.6. Life cycle technical controls

	PEXA Certification Authority Certificate Profile
	6.7. Network security controls 6.8. Time-stamping Refer to Digital Signing CP section 5.2 for details of PEXA & Subscriber environments.
7. Certificate, CRL, and OCSP Profiles	
7.1. Certificate profile	Refer to Appendix A.
7.1.1. Version number(s)	All certificates are X.509 Version 3 certificates.
7.1.2. Certificate extensions	Refer to Appendix A.
7.1.3. Algorithm object identifiers	Certificates issued under this CP will use the following algorithm for signatures: sha256WithRSAEncryption {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}
7.1.4. Name forms	Refer to Appendix A.
7.1.5. Name constraints	Name constraints are not present.
7.1.6. Certificate policy object identifier	Refer to section 1.2 and Appendix A.
7.1.7. Usage of policy constraints extension	Policy constraints are not present.
7.1.8. Policy qualifiers syntax and semantics	The CPS Pointer qualifier may be used in certificates issued under this CP. The CPS Pointer, if used, shall contain a URI link to the Certification Practice Statement (CPS) supporting this CP, or to a webpage from which the CPS can be downloaded.
7.1.9. Processing semantics for the critical certificate policies extension	This policy does not require the certificate policies extension to be critical.
7.2. CRL profile	Refer to Appendix A.
7.3. OCSP profile	Refer to Appendix A.
8. Compliance Audit and Other Assessments	Refer to CPS for compliance audits, sections: 8.1. Frequency or circumstances of assessment 8.2. Identity/qualifications of assessor 8.3. Assessor's relationship to assessed entity 8.4. Topics covered by assessment 8.5. Actions taken as a result of deficiency 8.6. Communication of results
9. Other Business and Legal Matters	
9.1. Fees	Not applicable.
9.2. Financial responsibility	Not applicable.
9.3. Confidentiality of business information	Treatment of confidential information exchanged in relation to CA creation and maintenance is governed by contractual agreements between PEXA and the managed CA service provider.
9.4. Privacy of personal information	

	PEXA Certification Authority Certificate Profile
9.4.1. Privacy plan	Refer to PEXA Privacy Policy (http://www.pexa.com.au/privacypolicy) for PEXA Operations.
9.4.2. Information treated as private	Information collected as part of a Verification of Identity check is considered personal (private) information and is subject to protections as per the Privacy Act 1988 (Cth).
9.4.3. Information not deemed private	Any information collected by PEXA that does not fall within the definition of Personal Information as defined in the Privacy Act 1988 is not considered by PEXA to be Private Information.
9.4.4. Responsibility to protect private information	All parties comply with their obligations under the Privacy Act 1988 (Cth), including the Australian Privacy Principles. Personnel are trained accordingly.
9.4.5. Notice and consent to use private information	The managed CA service provider complies with its obligations under the Privacy Act 1988 (Cth), including the Australian Privacy Principles.
9.4.6. Disclosure pursuant to judicial or administrative process	The managed CA service provider complies with its obligations under the Privacy Act 1988 (Cth), including the Australian Privacy Principles.
9.4.7. Other information disclosure circumstances	The managed CA service provider complies with its obligations under the Privacy Act 1988 (Cth), including the Australian Privacy Principles.
9.5. Intellectual property rights	Governed by contractual agreements between PEXA and the managed CA service provider.
9.6. Representations and warranties	Governed by contractual agreements between PEXA and the managed CA service provider.
9.7. Disclaimers of warranties	Governed by contractual agreements between PEXA and the managed CA service provider.
9.8. Limitations of liability	Governed by contractual agreements between PEXA and the managed CA service provider.
9.9. Indemnities	Governed by contractual agreements between PEXA and the managed CA service provider.
9.10. Term and termination	Refer to CPS.
9.11. Individual notices and communications with participants	Refer to CPS.
9.12. Amendments	Refer to CPS.
9.13. Dispute resolution provisions	Governed by contractual agreements between PEXA and the managed CA service provider.
9.14. Governing law	This CP is governed by the laws from time to time in force in Victoria, Australia.
9.15. Compliance with applicable law	All parties comply with all applicable laws.
9.16. Miscellaneous provisions	Not applicable.
9.17. Other provisions	Not applicable.

APPENDIX A. CERTIFICATE AND CRL PROFILES

A.1 PEXA Root CA certificate

Field	Critical	Certificate Value	Notes
Version		V3 (2)	Version 3 of X.509
Serial		Unique Serial Number	Unique value generated by the issuing CA
Issuer Signature Algorithm		SHA-2WithRSAEncryption	SHA-256
Issuer Distinguished Name		CN= PEXA Root CA OU= CAs O= PEXA C= AU	Encoded as printable string.
Validity Period		Not before <UTCtime> Not after <UTCtime>	30 years from issuance
Subject Distinguished Name		CN= PEXA Root CA OU= CAs O= PEXA C= AU	Encoded as printable string where possible, and otherwise using UTF-8
Subject Public Key Information		4096 bit RSA key modulus, rsaEncryption	
X.509 V3 extensions:			
Authority Key Identifier	No	<octet string>	The value of this field is the 20 byte SHA-1 hash of the binary DER encoding of the signing CA's public key information.

Field	Critical	Certificate Value	Notes
Subject Key Identifier	No	<octet string>	The value of this field is the 20 byte SHA-1 hash of the binary DER encoding of the subject's public key information.
Key Usage	Yes	certificate signing CRL signing digital signature non-repudiation	Digital signature is for the purpose of signing of transaction log entries only.
Extended key usage			Not Present
Certificate policies	No	[1] Policy OID: {1.2.36.40677792.1.1.1} [2] Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: URL= https://www.pexa.com.au/ca/publish/pexa/documents/	The OID of the CA CP. Location of CPS.
Basic Constraints	Yes	CA=True Path length constraint=none	

A.2 PEXA Operational CA certificate

Field	Critical	Certificate Value	Notes
Version		V3 (2)	Version 3 of X.509
Serial		Unique Serial Number	Unique value generated by the issuing CA
Issuer Signature Algorithm		SHA-2WithRSAEncryption	SHA-256
Issuer Distinguished Name		CN= PEXA Root CA OU= CAs O= PEXA C= AU	Encoded as printable string.
Validity Period		Not before <UTCtime> Not after <UTCtime>	10 years from issuance
Subject Distinguished Name		CN= PEXA Operational CA <nnn> OU= CAs O= PEXA C= AU	Encoded as printable string where possible, and otherwise using UTF-8
Subject Public Key Information		2048 bit RSA key modulus, rsaEncryption	
X.509 V3 extensions:			
Authority Key Identifier	No	<octet string>	The value of this field is the 20 byte SHA-1 hash of the binary DER encoding of the signing CA's public key information.
Subject Key Identifier	No	<octet string>	The value of this field is the 20 byte SHA-1 hash of the binary DER encoding of the subject's public key information.
Key Usage	Yes	certificate signing	Digital signature is for the purpose of signing of transaction log entries only.

Field	Critical	Certificate Value	Notes
		CRL signing digital signature non-repudiation	
Extended key usage		Not Present	
Certificate policies	No	[1] Policy OID: {1.2.36.40677792.1.1.1} [2] Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: URL= https://www.pexa.com.au/ca/publish/pexa/documents/	The OID identifying PEXA CA certificates in the CA CP. Location of CPS.
Basic Constraints	Yes	CA=True Path length constraint=none	
Authority Information Access	No	[1] Access method: CAIssuer{1.3.6.1.5.5.7.48.2} Access location: https://www.pexa.com.au/ca/publish/pexa/CAcerts/PEXARCA<nnn>.crt [2] Access method: OCSP {1.3.6.1.5.5.7.48.1} Access location: http://ocsp.pexa.net.au	Location of Root CA certificate. Location of OCSP responder.

A.3 OCSP responder certificate

Field	Critical	Certificate Value	Notes
Version		V3 (2)	Version 3 of X.509
Serial		Unique Serial Number	Unique value generated by the issuing CA
Issuer Signature Algorithm		SHA-2WithRSAEncryption	SHA-256
Issuer Distinguished Name		CN= PEXA Operational CA <nnn>OU= CAs O= PEXA C= AU	Encoded as printable string.
Validity Period		Not before <UTCtime> Not after <UTCtime>	10 years from issuance
Subject Distinguished Name		CN= PEXA OCSP <nnn> OU=OCSP O= PEXA C= AU	Encoded as printable string where possible, and otherwise using UTF-8
Subject Public Key Information		2048 bit RSA key modulus, rsaEncryption	
X.509 V3 extensions:			
Authority Key Identifier	No	<octet string>	The value of this field is the 20 byte SHA-1 hash of the binary DER encoding of the signing CA's public key information.
Subject Key Identifier	No	<octet string>	The value of this field is the 20 byte SHA-1 hash of the binary DER encoding of the subject's public key information.
Key Usage	Yes	digital signature	
Extended key usage	Yes	OCSPsigning	

Field	Critical	Certificate Value	Notes
Certificate policies	No	[1] Policy OID: {1.2.36.40677792.1.1.4} [2] Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: URL= https://www.pexa.com.au/ca/publish/pexa/documents/	The OID identifying OCSP certificates in the CA CP. Location of CPS.
Authority Information Access	No	[1] Access method: CAIssuer{1.3.6.1.5.5.7.48.2} Access location: https://www.pexa.com.au/ca/publish/pexa/CAcerts/PEXARCA<nnn>.crt	Location of issuing CA certificate.
OCSP No Check	No	id-pkix-ocsp-nocheck: NULL	This extension tells a client that it is not necessary to check the certificate status of this certificate.

A.4 CRL profile – PEXA Root CA

Field	Critical	Value	Notes
Version		V2 (1)	X.509 Version 2 CRL profile
Issuer Signature Algorithm		sha-2WithRSAEncryption	SHA256
Issuer Distinguished Name		CN= PEXA Root CA OU= CAs O= PEXA C= AU	
thisUpdate		<UTCTime>	Issue date of this CRL
nextUpdate		<UTCTime>	RCA CRLs will be issued on revocation or quarterly at the latest. Date by which the next CRL will be issued (at the latest – if a certificate is revoked, a CRL will be issued at that time) thisUpdate + 90 days
Revoked certificates list		0 or more pairs of certificate serial number and revocation date (in UTCTime)	
CRL V2 extensions			
CRL Number	No	<Integer>	
Authority Key Identifier	No	<Octet String>	The value of this field is the 20 byte SHA-1 hash of the binary DER encoding of the CA public key information
CRL entry extensions			
Invalidity Date	No	Optional	Date on which it is known or suspected that the private key was compromised or that the certificate otherwise became invalid.
Reason Code	No	Optional	

A.5 CRL profile – PEXA Operational CA

Field	Critical	Value	Notes
Version		V2 (1)	X.509 Version 2 CRL profile
Issuer Signature Algorithm		sha-2WithRSAEncryption	SHA256
Issuer Distinguished Name		CN= PEXA Operational CA <nnn> OU= CAs O= PEXA C= AU	
thisUpdate		<UTCTime>	Issue date of this CRL
nextUpdate		<UTCTime>	OCA CRLs are issued on revocation or daily at the latest. Date by which the next CRL will be issued (at the latest – if a certificate is revoked, a CRL will be issued at that time) thisUpdate + 10 days
Revoked certificates list		0 or more pairs of certificate serial number and revocation date (in UTCTime)	
CRL V2 extensions			
CRL Number	No	<Integer>	
Authority Key Identifier	No	<Octet String>	The value of this field is the 20 byte SHA-1 hash of the binary DER encoding of the CA public key information
CRL entry extensions			
Invalidity Date	No	Optional	Date on which it is known or suspected that the private key was compromised or that the certificate otherwise became invalid.
Reason Code	No	Optional	