YOUR ONLINE PROPERTY EXCHANGE

PEXA Public Key Infrastructure (PKI)

PEXA Digital Signing Certificate Policy

Version: 2.6 Issued: January 2015 Status: Final

PEXA
Property Exchange Australia

VERSION CONTROL

Version No.	Version Details	Date
2.5	Initial accredited document	August 2014
2.6	Document amended to: • Change the certificate ordering process so that multiple certificates can be ordered when the Subscriber Organisation executes the PEXA DSC Subscriber Agreement. • 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. • Add the option for the Subscriber Organisation to sign additional certificate requests and requests to un-suspend certificates (i.e. in addition to the digital signing option).	January 2015

	PEXA Digital Signing Certificate Policy
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. The PEXA Public Key Infrastructure (PKI) supports the operation of the PEXA Platform by providing for the issuing and management of identity credentials for all users that need to sign documents in PEXA. The credentials are X.509 certificates issued to individuals within PEXA Subscriber Organisations. Each certificate contains a "public key" that can be shared. Each public key has a corresponding "private key", which must be protected by the Certificate Holder. The keypair and certificate are stored in a token, which may be a "hard" token, e.g. a secured USB key or smartcard, or a "soft" token, e.g. an encrypted file. The private key is exercised when a user signs a PEXA Document. The signature can then be verified with the user's public key, contained in the certificate. This document, the PEXA Digital Signing Certificate Policy, describes how the Digital Signing 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") with minor adaptions as recommended by the Australian Government Gatekeeper framework specifically for "Relationship Certificate" CPs. 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

	PEXA Digital Signing Certificate Policy
	• 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 CP: i. PEXA documents: • PEXA PKI Certification Practice Statement (CPS) https://www.pexa.com.au/ca/publish/pexa/documents/ • PEXA PKI Certification Authority Certificate Policy (CA CP) • PEXA PKI Administrator Certificate Policy (PA CP) • PEXA Privacy Policy http://www.pexa.com.au/privacypolicy • PEXA Participation Agreement (PA) (customised for Subscribers) available on request • PEXA Digital Signing Certificate (DSC) Subscriber Agreement available at https://www.pexa.com.au/ca/publish/pexa/documents/ • PEXA Personnel Security Policy • PEXA Asset and Media Management Policy • PEXA Vol Onboarding Process Manual ii. 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 iii. CA documentation (not available to the public): • Gatekeeper CA documentation suite – see Gatekeeper website for latest document set. iv. 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/ v. Gatekeeper documents: http://www.finance.gov.au/policy-guides-procurement/gatekeeper-public-key-infrastructure/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 vi. 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 • 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 Digital Signing Certificate Policy”.

	PEXA Digital Signing Certificate Policy
	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. The PEXA CPS and CPs can be accessed at: https://www.pexa.com.au/ca/publish/pexa/documents/ The PEXA PKI Digital Signing Certificate Policy has the following OID: **1.2.36.40677792.1.1.2** iso (1) iso-member (2) australia (36) PEXA (40677792) PKI (1) Certificate Policy (1) Digital Signing Certificate (2) This OID is present in all certificates issued under this policy.
1.3. PKI participants	Refer to CPS.
1.4. Certificate usage	
1.4.1. Appropriate certificate uses	Certificates issued under this CP and their corresponding private keys may be used to sign PEXA Documents via the PEXA Platform. Certificates are for authentication and non-repudiation only, and do not imply any authority other than the right to sign PEXA Documents on behalf of the PEXA Subscriber. In addition, Subscriber Managers and Subscriber Administrators may also sign requests for a new certificate, renewal of a certificate or requests for un-suspension on behalf of other Subscriber Managers, Subscriber Administrators or Subscriber Signers. All Certificate Holders may use their certificates to authenticate to the token management application interfaces, allowing them to manage their tokens, e.g. change the PIN. N.B. Rules governing the signing of PEXA Documents used in property transactions are outside the scope of this document.
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. For details about the amendment process in respect of this document, refer to CPS sections 1.5.4 and 9.12.
1.5.2. Contact person	Contact details for the PEXA PMA are: General Manager – Risk. ph: (03) 9912 6500 or email: 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 and CP approval procedures	Refer to CPS.

	PEXA Digital Signing Certificate Policy
1.6. Terms, Definitions and Acronyms	Some terms used in the PEXA CPS and CPs carry a different meaning to conventional PKI usage, due to their special use in the context of e-conveyancing in Australia and in the MOR and MPR. In particular, the term "Subscriber" is used as follows: • **PEXA Subscriber**: An organisation that has signed the PEXA Participation Agreement for use of the PEXA Platform; and • **PEXA Digital Signing Certificate (DSC) Subscriber**: An organisation that has signed the PEXA DSC Subscriber Agreement. Such Organisations are also PEXA Subscribers. PEXA DSC Subscribers can request and use PEXA Digital Signing Certificates (DSCs). All PEXA DSC Subscribers must be PEXA Subscribers but not all PEXA Subscribers are necessarily PEXA DSC Subscribers. PEXA Subscribers may use digital certificates issued by another Gatekeeper Accredited Service Provider to sign documents in the PEXA Platform. For other Terms and Definitions, refer to CPS Appendix B. Defined terms are capitalised.
2. Publication and Repository Responsibilities	Refer to CPS, including: 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	Requests to issue, un-suspend and renew PEXA DSCs, as described in the following subsections, must be: • Digitally Signed by a Subscriber Manager or Subscriber Administrator. Rrequests may be lodged to PEXA via signed email or via signed electronic request forms facilitated via PEXA CRM or PEXA Platforms; or • Signed by the Subscriber Organisation and submitted to PEXA in the required form. The persons signing on behalf of the Subscriber Organisation must have had their identity verified by PEXA. Requestors may use either a PEXA DSC or a digital certificate issued by another Gatekeeper Accredited Service Provider (which meets the criteria specified in the MOR, section 7.6) to Digitally Sign the aforementioned request.
3.1. Naming	
3.1.1. Types of names	Each PEXA Digital Signing Certificate (PEXA DSC) has an X.500 Distinguished Name in the Subject field which uniquely identifies the Certificate Holder within the PKI. The Distinguished Name will include: • Email (Subject's organisational email address) • Subject's name (first name, middle name, surname) • Organisation (Subscriber Organisation/Legal entity) • Country The Subject Alternative Name will also contain the Certificate Holder's organisational email address. Additionally, the Subscriber legal entity's ABN is included in a private extension in the certificate, as per requirements stated in MOR.
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.

	PEXA Digital Signing Certificate Policy
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 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 Certificate Holder in the PEXA PKI must be unique within the PKI name space. Replacement certificates for the same person may have the same Distinguished Name as previous certificates.
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	Not applicable. Keypairs are generated at the CA.
3.2.2. Subscriber organisation and Subscriber Manager identity verification	Subscriber Organisations acquire PEXA DSCs via the following process. First, the Subscriber Organisation becomes a **PEXA Subscriber**. This step entails: i. The Subscriber Organisation signs the PEXA Participation Agreement which includes provisions for nomination of a Subscriber Manager , who may or may not be the person who signed the Participation Agreement. ii. PEXA verifies the identity of the person or persons who sign the PEXA Participation Agreement in accordance with the Subscriber Identity Verification Standard. iii. PEXA conducts an organisation validation and simultaneously confirms that the person or persons signing the PEXA Participation Agreement have the authority to bind the Subscriber Organisation. Secondly, and optionally, the Subscriber Organisation may choose to becomes a **PEXA DSC Subscriber**. If the Subscriber Organisation chooses to become a PEXA DSC Subscriber, the Subscriber Organisation also signs the PEXA DSC Subscriber Agreement. As described in (i.) above, the PEXA Participation Agreement requires nomination of a Subscriber Manager. PEXA will verify the identity of the person(s) signing the PEXA Participation Agreement. The identity of all other persons receiving PEXA DSCs must be verified by the Subscriber Organisation in accordance with the Verification of Identity Standard. PEXA will issue a PEXA DSC to the Subscriber Manager and any additional Subscriber Signers nominated in the PEXA DSC Subscriber Agreement. Any Subscriber Manager or Subscriber Administrator can request additional PEXA DSCs for other Subscriber Signers (in the manner described in section 3.2.3). Further specific details associated with the process described above are provided in Appendix B.
3.2.3. Identity verification of additional PEXA DSC applicants	PEXA will create the Subscriber Manager account pertaining to the PEXA Subscriber on the PEXA Platform as an outcome of process steps i to iii, described in 3.2.2. . Additional PEXA DSC applications.may be: • lodged via either the PEXA Platform or PEXA CRM. Account creations are managed via delegation controls on the PEXA Platform as follows: Subscriber Manager >> additional Subscriber Manager >> additional Subscriber Adminnistrator >> additional Subscriber User; or

	PEXA Digital Signing Certificate Policy
	• signed by the Subscriber Organisation and submitted to PEXA in the required form. . For non-repudiation purposes, PEXA will store signed request forms. PEXA Operations staff will check to confirm that the request originates from an authorised requester (i.e. Subscriber Manager or Subscriber Administrator) and that the signature is valid. Prior to requesting a PEXA DSC, the Subscriber Organisation must ensure that the identity of the Certificate Recipient has been verified in accordance with the Verification of Identity Standard. Alternatively the Subscriber Organisation may engage either a VOI Agent or VOI Officer to perform the Verification of Identity of the Certificate Recipient. The Subscriber Organisation must also comply with its Verification of Identity obligations in clause 9 of the PEXA DSC Subscriber Agreement.
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 (re-key) requests	
3.3.1. Identification and authentication for routine renewal (re-key)	PEXA DSC Subscribers are responsible for identifying their own users and approving certificate renewals. A Subscriber Organisation will request a new certificate for another Certificate Holder within their Organisation. All certificate requests are signed by the Subscriber Organisation. Subscriber Managers and Subscriber Administrators can renew their own certificates; an email signed with the Subscriber Manager or Subscriber Administrator's current and valid certificate constitutes sufficient Verification of Identity. If the Subscriber Manager or Subscriber Administrator's old certificate has expired, they will have to complete a new VOI check and contact the PEXA Support desk to request a new certificate. For more information about the renewal process, refer to section 4.7.
3.3.2. Identification and authentication for re-key after revocation	As per renewal, section 3.3.1 *except* renewal request cannot be signed with a revoked certificate – a Subscriber Manager or Subscriber Administrator requesting a replacement certificate from a PEXA Administrator must complete a new VOI check prior to the PEXA Administrator processing the request.
3.4. Identification and authentication for revocation request	Prior to acting upon a request from a party to revoke *another party's* certificate aSubscriber Manager, Subscriber Administrator or a PEXA Administrator (where the request is made directly to a PEXA Administrator) must verify the requestor's identity to ensure they are entitled to request revocation for the certificate in question (refer to section 4.9.2 Who can request revocation). If the requestor is not known to the Subscriber Manager, Subscriber Admnistrator or PEXA Administrator, the Subscriber Manager, Subscriber Admnistrator or PEXA Administrator may ask that the requestor presents: • Proof of Identity (e.g. photo ID such as driver's license); and • Proof of position/relationship to certificate to be revoked (e.g. providing a phone contact who can verify the person's position). Refer to section 4.9 for more information on the Revocation process.

	PEXA Digital Signing Certificate Policy
3.5. Identification and Authentication for Key Recovery Request	Not applicable.

4. Certificate Life-cycle Operational Requirements	Requests to issue, un-suspend and renew PEXA DSCs, as described in the following subsections, must be: • Digitally Signed by a Subscriber Manager or Subscriber Adminnistrator. Requests may be lodged to PEXA via signed email or via signed electronic request forms facilitated via PEXA CRM or PEXA Platforms; or • signed by the Subscriber Organisation and submitted to PEXA in the required form. Requestors may use either a PEXA DSC or a digital certificate issued by another Gatekeeper Accredited Service Provider (which meets the criteria specified in the MOR, section 7.6) to Digitally Sign the aforementioned request.
4.1. Certificate application	
4.1.1. Who can submit a certificate application	PEXA Administrators: • will request a certificate for a Subscriber Manager of each PEXA DSC Subscriber (upon successful completion of the PEXA On-boarding process); and • may also request a certificate for additional Subscriber Managers in exception conditions (e.g. a Subscriber Manager leaves the Subscriber Organisation without appointing a replacment Subscriber Manager). The Subscriber Organisation can sign and submit applications for digital Certificates. Any Subscriber Manager or Subscriber Administrator can request a certificate for a individual in a subordinate or equivalent role. Roles follow the following heirarchy (from highest to lowest status): Subscriber Manager >> Subscriber Administrator >>Subscriber User. No individual in any role can request a certificate on their own behalf.
4.1.2. Enrolment process and responsibilities	Throughout the validity period of a PEXA Subscriber account, Subscriber Manager or Subscriber Administrator or the Subscriber Organisation can request PEXA DSCs for other PEXA users (in accordance with restrictions outlined in 4.1.1). The options available for requesting PEXA DSCs are described in section 3.2.3. Requests for additional PEXA DSCs will contain the Certificate Recipient's first name, middle name/s, surname and email address, corresponding to same parameters on the user's PEXA account. In the case of requests generated within the PEXA Platform, the same aforementioned parameters are submitted across the secure interface between PEXA Platform and PEXA CA.
4.2. Certificate application processing	Following on from enrolment of a new PEXA Subscriber Organisation or a PEXA User, where a certificate request has been sent to the PEXA PKI, CA Operations will generate keys and certificates as follows: i. For applicants who will be supplied with a USB Token (the default form-factor), CA Operations use a Card Management System to generate keys and certificates on a smartcard chip, which is then inserted into a USB key. The token is sent in a tamper-evident envelope via Australia Post to the Subscriber, addressed to the Certificate Recipient, together with instructions and drivers and/or software (if required). The token is protected by a randomly generated PIN, which is sent one day later in a separate secure PIN mailer via Australia Post. ii. For applicants who have been approved to use a soft token, this will be delivered as a PKCS#12 file on a CD. The PKCS#12 file is sent in a tamper-evident envelope via Australia Post to the Subscriber, addressed to the Certificate Recipient, together with instructions and drivers and/or software (if required). The token is protected by a randomly generated PIN, which is sent one day later in a separate secure PIN mailer via Australia Post. In order to qualify for use of soft tokens, the PEXA DSC Subscriber must demonstrate that they have implemented an ISO/IEC 27001:2005 security framework. iii. Both hard and soft token recipients will be provided with installation instructions as follows: • For USB Token – recipients are required to reset (personalise) their PIN.

	• For soft tokens – recipients are required to set PIN protection during the soft token importation process.
4.2.1. Performing identification and authentication functions	Refer to section 3.2 for detail.
4.2.2. Approval or rejection of certificate applications	Approval of a PEXA DSC request will occur after successful enrolment of a Subscriber Organisation has been completed. Provided the certificate request is correctly formed and correctly executed , the CA will issue a certificate to the applicant. Any rejections due to a badly formatted certificate request will be communicated to PEXA Support Desk at the end of each day.
4.2.3 Time to process certificate applications	Certificate requests will in most cases be processed within 1-2 business days of receipt of the request. The token is sent one business day after the PIN mailer has been sent.
4.3 Certificate issuance	
4.3.1. CA actions during certificate issuance	The PEXA CMS and OCA perform the following checks after receiving a certificate request: i. authenticate the certificate request to ensure that it has come from an approved source; ii. verify that the request is correctly formed; iii. generate the key pair (on a USB Token or in a soft token according to the request); iv. generate a PIN which protects the token from unauthorised access; v. compose and sign the certificate (OCA); vi. load the certificate into the hard or soft token; vii. provide the token to the applicant as per applicable CP; and viii. publish the certificate in accordance with this CP and the CPS.
4.3.2. Notification to subscriber by the CA of issuance of certificate	The Certificate Recipient is notified of the issuance of the certificate in the letter containing the token.
4.4. Certificate acceptance	
4.4.1. Conduct constituting certificate acceptance	Certificate Recipients are deemed to have accepted certificates upon having exercised their private key. Signing a document in PEXA is considered exercising their private keys.
4.4.2. Publication of the certificate by the CA	Certificates are published in the internal CA repository upon issuance.
4.4.3. Notification of certificate issuance by the CA to other entities	CA Operations will contact the PEXA Support Desk if a certificate request has been rejected. The managed CA service provider sends a monthly report to PEXA detailing: • issued certificates • revoked certificates • suspended certificates • unsuspended certificates • expired certificates
4.5. Key pair and certificate usage	

4.5.1. Subscriber Private Key and Certificate Usage	Refer to section 1.4.1 for appropriate certificate uses. Subscriber Signers use certificates issued under this CP for signing PEXA Documents used in property exchange transactions such as mortgage discharges, property transfers, settlement and disbursements. When signing a document, the user must enter the PIN which protects the private key. In addition to signing PEXA Documents, for digitally signed requests made by a Subscriber M[anager or Subscriber Administrator, the Subscriber Manager or Subscriber Administrator will use their certificate to sign certificate management requests on behalf of other users within the Subscriber Organisation. This may be done from within the PEXA Platform, or via signed email to the PEXA Support desk. Usage of PEXA PKI certificates outside of the PEXA system is not permitted. Without limiting other obligations of PEXA DSC Subscribers set out in this CP or in the PEXA DSC Subscriber Agreement, a PEXA DSC Subscriber must: • take reasonable steps, and ensure each Certificate Holder takes reasonable steps to prevent the Compromise, loss, disclosure, modification, or unauthorised use of their certificate or corresponding Private Key; • provide measures to Certificate Holders to avoid Compromise of the Private Key associated with their certificates; • ensure that all information provided to PEXA in relation to issue and use of certificates is true and complete; • immediately notify PEXA if: - it becomes aware that a certificate or corresponding Private Key has been Compromised, or there is a substantial risk of compromise; - any Certificate Holder ceases to be an employee or agent of the PEXA DSC Subscriber; - any Certificate Holder ceases to be authorised to hold certificates on behalf of the PEXA DSC Subscriber; - the PEXA DSC Subscriber ceases to belong to the PEXA Community of Interest; or - there is any other change to the information provided to PEXA in relation to the issue and use of certificates; and • ensure that certificates are only used for the purposes for which they were issued and only for purposes for which Certificate Holders have the actual authority of the PEXA DSC Subscriber; and • if requested by PEXA, provide complete and accurate information or anything else relating to issue or use of certificates under this CP and the PEXA DSC Subscriber Agreement. Each Subscriber Manager and Subscriber Administrator must take reasonable steps to ensure that the PEXA DSC Subscriber for whom they manage and administer Subscriber Signers complies with the obligations set out above. Each Certificate Holder must: • take reasonable steps to prevent the Compromise, loss, disclosure, modification, or unauthorised use of their certificate or corresponding Private Key; • immediately notify the PEXA DSC Subscriber at whose request they were issued with a certificate under this CP, if they become aware that a certificate or corresponding Private Key has been Compromised, or there is a substantial risk of compromise; • not delegate responsibility for the creation or renewal of a certificate unless authorised to do so by the PEXA DSC Subscriber at whose request they were issued with a certificate under this CP ; • ensure that all information provided to PEXA in relation to issue and use of their certificatesis true and complete; • use certifcates only for the purposes for which they were issued and only for purposes for which they have the actual authority of the PEXA DSC Subscriber at whose request they were issued with a certificate under this CP; • on receipt of a certificate, check the details and promptly notify PEXA if any details are not correct; and

	• if requested by PEXA, provide complete and accurate information in relation to the issue or use of their certificates.
4.5.2. Relying Party (PEXA) Public key and Certificate Usage	As part of the digital signature creation process, PEXA will validate the certificate (used to sign) and verify the certificate status by sending a certificate status request to a dedicated server using Online Certificate Status Protocol. The signed certificate status response will be stored together with the digital signature and the signed document indefinitely on the PEXA Platform. The document, signature and signature metadata is also sent to the relevant Land Titles Office. The LTO acknowledges the receipt of the lodgement, and after verifying that the transaction is valid, sends another message accepting the lodgement. Should LTOs need to verify a signature at a later date, they will use XML standards based signature verification tools/applications to do so. All the information required to validate the signature and the integrity of the document signed is included in the data provided in the transaction by PEXA in standard XML DigSig[1] format. Without limiting the above, each time a PEXA Document is Digitally Signed in a PEXA Workspace using a certificate, PEXA will verify that the certificate used to create the Digital Signature: • was created with the Private Key corresponding to the Public Key defined in the certificate of the Subscriber Signer who Digitally Signed the PEXA Document; and • is current, and is not revoked or suspended.
4.6. Certificate renewal	Refer to section 4.7 Certificate re-key
4.7. Certificate re-key (renewal)	Certificates issued under this CP are always issued with a new keypair, i.e. "renewal" means a user will get a new certificate and keys when the old certificate expires.
4.7.1. Circumstance for certificate re-key	Renewal of certificates can be requested within 6 weeks prior to the certificate expiry date. A new certificate may also be issued following revocation.
4.7.2. Who may request re-key	Cerificate renewals can be performed by the following: • the Subscriber Organisation; • Subsdriber Managers and Subscriber Administrators (subject to heirarchical controls[2]) for any other Certificate Recipient; and • Subscriber Managers and Subscriber Administrators can renew their own certificate.
4.7.3. Processing certificate re-key requests	The Subscriber Organisation will be notified of the need to renew a Certificate Holder's expiring certificate. Notifications will be issued weekly when the expiring certificate enters the renewal window (which is 6 weeks prior to the expiry date). The Subscriber Manager, Subscriber Administrator, or the Subscriber Organisation will then request a new certificate from the PEXA CA. Certificate renewals can be requested via the relevant request form, executed by the Subscriber Organisation or visa the relevant function on the PEXA Platform, via PEXA CRM or by sending a digitally signed request to PEXA Service Desk. Refer to section 3.3.1 for identification and authentication requirements for certificate re-key requests. The processing of a certificate renewal requests is the same as for a new certificate – refer to sections 4.2, 4.3 and 4.4.

[1] XML Signature Syntax and processing standard, http://www.w3.org/TR/xmldsig-core/

4.7.4. Notification of new certificate issuance to subscriber	No notification is sent to Certificate Recipients prior to the letter containing the token itself.
4.7.5. Conduct constituting acceptance of a re-keyed certificate	Certificate Recipients are deemed to have accepted their new certificate upon having having signed their first document in PEXA or sent their first signed email to PEXA Support Desk.
4.7.6. Publication of the re-keyed certificate by the CA	Certificates are published in the internal CA repository upon issuance.
4.7.7. Notification of certificate issuance by the CA to other entities	Refer to section 4.4.3.
4.8. Certificate modification	Not applicable. If certificate details require modification, a new certificate must be requested.
4.9. Certificate revocation and suspension	
4.9.1. Circumstances for revocation	A PEXA DSC Subscriber must cause its Subscriber Managers or Subscriber Administrators, as applicable, to revoke a certificate issued to a Certificate Holder nominated by it, if the PEXA DSC Subscriber or any of its employees, agents or contractors becomes aware that: • the Certificate Holder's token is lost; • the Certificate Holder's token is stolen;or • the Certificate Holder's Private Key is Compromised. If a PEXA DSC Subscriber suspects but cannot confirm any of the above, it must cause the relevant certificate to be suspended until the suspected loss, theft or Compromise has been confirmed or disproven. Refer to section 4.9.13. A PEXA DSC Subscriber must also revoke a certificate issued to a Certificate Holder nominated by it if: • the Certificate Holder leaves the Subscriber Organisation, or no longer requires signing privileges; or • details in the certificate are incorrect and a new certificate is being issued. PEXA may revoke any certificate issued under this CP if it is satisfied on reasonable grounds that the certificate has been Compromised or the use of the certificate has Jeopardised a Conveyancing Transaction. In addition, under certain circumstances as described in the Participation Agreement and the MPR (refer MPR Schedule 7), a Registrar may direct PEXA to "restrict, suspend or terminate" a PEXA Subscriber. Examples of where such a direction may be given by a Registrar to PEXA are where the Registrar knows or has reasonable grounds to believe that the PEXA Subscriber is in material breach of its obligations, or has or may act negligently in a way which may impact on a Conveyancing Transaction or fails to remedy any failure to pay land registry fees within a reasonable time. Where PEXA is directed by a Registrar to terminate a PEXA Subscriber, PEXA will correspondingly revoke any certificates issued to a PEXA DSC Subscriber's Users. In accordance with the Participation Agreement between it and a PEXA Subscriber, PEXA may also terminate a User under certain circumstances (and if the PEXA Subscriber is a PEXA DSC Subscriber, PEXA may revoke certificates issued to that Susbscriber's users under this CP). These circumstances include where PEXA considers it reasonably necessary to terminate a User in order to ensure compliance by the Subscriber with the ECNL, the MOR and/or the MPR.
4.9.2. Who can request revocation	Certificate revocations can be requested by: • A Certificate Holder (for their own certificate only);

	• Subscriber Managers and Subscriber Administrators (subject to heirarchical controls[3]) for any Certificate Holder within their organisation; • PEXA Support Desk; and • The Registrar (through PEXA, refer to section 4.9.1). Any Certificate Holder may contact either their Subscriber Manager, Subscriber Administrator or PEXA Support Desk. Subscriber Managers or Subscriber Administrators may also contact PEXA Support Desk for certificate revocation In certain circumstances, the CA Operator is able to revoke a new certificate that has been issued with errors, provided it has not yet left the premises of the CA Operations. In this case they will revoke the certificate from within the PEXA CMS software.
4.9.3. Procedure for revocation request	Certificate revocations can be actioned as follows: • via email request or phone call to PEXA Support Desk (who, in turn perform the relevant function on PEXA CMS); or • via the relevant function on the PEXA Platform. Before actioning the request, the Subscriber Manager, Subscriber Administrator or PEXA Administrator (where the request is made directly to a PEXA Administrator) must establish: • the identity of the person requesting the revocation (the Certificate Holder); and • the reason for revocation; and • if there are any transactions pending that the Certificate Holder has signed with the certificate to be revoked. If there are transactions pending, it is the responsibility of the PEXA Subscriber to determine whether these should be unsigned (refer MPR section 7.9). The next action depends on who is processing the revocation request: a) If a Subscriber Manager or Subscriber Administrator is carrying out the revocation request, they will trigger the revocation by: • deleting the PEXA login account of the Certificate Holder; or • sending an email to the PEXA Support Desk with the revocation request details. A PEXA Administrator will then request the revocation from CA Operations. b) If a **PEXA Administrator** is carrying out the revocation request, they will trigger the revocation by: • deleting the PEXA login account of the Certificate Holder; or • sending an email to CA Operations with the revocation request details. When a revocation request is made to the CA, it will add the certificate serial number to the Certificate Revocation List (CRL). The certificate status server is then updated with the new CRL. If the Certificate Holder requires a new certificate, the Subscriber Manager or Subscriber Administrator (or PEXA Administrator) can request one for them. Subscriber Managers must act on a request for revocation within one business hour of receiving the request from a Certificate Holder within their organisation. If a Subscriber Manager or Subscriber Administrator needs to revoke the certificate of a Certificate Holder within their organisation due to any of the circumstances as described in 4.9.1, they can do so. If the Registrar requires a Subscriber or Subscriber User to be restricted, suspended or terminated, they must contact the PEXA Support desk in writing. A PEXA Administrator will establish the identity and authority of the requestor, as well as the reason for the request before actioning it. They may then suspend or terminate the Subscriber Organisation's or

[3] Subscriber Managers can perform said task to another Subscriber Manager, Subscriber Administrator or Subscriber Signer; Subscriber Administrators can only perform said task to another Subscriber Administrator or Subscriber Signer.

	Signer's right to sign documents, or to use PEXA. Requests must be investigated and actioned (if necessary) as soon as possible. If another party is aware of the loss of a token or compromise of a private key, they should contact the Subscriber Organisation or the PEXA Support desk – refer to section 4.9.15.
4.9.4. Revocation request grace period	There is no "grace period" within which the Certificate Holder must revoke the certificate. If a Certificate Holder suspects any of the conditions in section 4.9.1 to be true, they must request the suspension of the certificate as soon as practical to allow for investigation. The suspension of a certificate provides a temporary revocation state which can be reversed.
4.9.5. Time within which CA must process the revocation request	Revocation requests submitted via the PEXA Platform or PEXA CMS have immediate effect in the CA. In the event that revocation requests submitted return an error condition, PEXA will immediately liase with CA Operations to remedy the situation and PEXA Subscribers affected.
4.9.6. Revocation checking requirement for relying parties	Before relying on a PEXA DSC, potential relying parties should ensure their requirements for revocation checking are met by the operation of the PEXA PKI as described in this CP and the CPS.
4.9.7. CRL issuance frequency (if applicable)	CRLs are updated when the status of a certificate has changed, or daily when there are no status changes.
4.9.8. Maximum latency for CRLs (if applicable)	Refer to the CA CP.
4.9.9. On-line revocation/status checking availability	The PEXA PKI runs its own dedicated Online Certificate Status Protocol (OCSP) service. This service is only available to PEXA. The service is available 24/7.
4.9.10. On-line revocation checking requirements	PEXA will check the certificate status of a certificate used in a signing transaction immediately before the transaction occurs. The OCSP response is included in the transaction record.
4.9.11. Other forms of revocation advertisements available	Not applicable.
4.9.12. Special requirements - key compromise	No special requirements.
4.9.13. Circumstances for suspension	A PEXA DSC Subscriber must suspend a PEXA DSC in the following circumstances: • it suspects that the Certificate Holder's token is lost or stolen; or • it suspects that the Certificate Holder's Private Key is Compromised; or • the Certificate Holder is on extended leave; or • the Certificate Holder no longer requires *signing privileges* in the PEXA Platform (but still needs access to their PEXA account); or • the Certificate Holder is under investigation. PEXA may suspend any certificate issued under this CP if it is satisfied on reasonable grounds that the certificate has been Compromised or the use of the certificate has Jeopardised a Conveyancing Transaction. In addition, under certain circumstances as described in the Participation Agreement and the MPR (Schedule 7), the Registrar or PEXA may request the suspension of a PEXA Subscriber's ability to use the PEXA Platform. Examples of where such a direction may be given by a Registrar to PEXA are where the Registrar knows or has reasonable grounds to suspect that the PEXA Subscriber is in material breach of its obligations, or has or may act negligently in a way which may impact on a Conveyancing Transaction or fails to remedy promptly any failure to pay land registry fees. Where PEXA is directed by a Registrar to terminate a PEXA Subscriber, PEXA will correspondingly revoke any certificates issued to a PEXA DSC Subscriber's Users. In such circumstances, the Subscriber's PEXA account would be suspended, with the effect that none of the Subscribers' PEXA users would be able to access PEXA. In accordance with the Participation Agreement between it and a PEXA Subscriber, PEXA may also suspend a User under certain circumstances (and if the PEXA Subscriber is a PEXA DSC Subscriber, PEXA may also suspend certificates issued to that

	Susbscriber's users under this CP). These circumstances include where PEXA considers it reasonably necessary to suspend a User in order to ensure compliance by the Subscriber with the ECNL, the MOR and/or the MPR.
4.9.14. Who can request suspension	Certificate suspensions can be requested by: • a Certificate Holder (for their own certificate only); • SMs and SAs (subject to hierarchical controls[4]) for any Certificate Holder within their organisation; and • PEXA Support Desk. Any individual may contact either an Subscriber Manager, Subscriber Administrator or PEXA Support Desk. In addition, any person who is aware of the actual or potential misuse or compromise of a PEXA token or private key should contact the Subscriber Organisation or the PEXA Support desk.
4.9.15. Procedure for suspension request	Certificate suspensions can be actioned as follows: • via email request or phone call to PEXA Support Desk (who, in turn perform the relevant function on PEXA CMS); or • via the relevant function on the PEXA Platform. When a suspension request is made to the CA, it will add the certificate serial number to the Certificate Revocation List (CRL) with the reason code "CertificateHold". The certificate status server is updated with the new CRL. If aSubscriber Manager or Subscriber Administrator needs to suspend the certificate of a Certificate Holder within their organisation due to any of the circumstances as described in 4.9.13, they can do so. Subscriber Managers must act on a request for suspension within one business hour of receiving the request from a Certificate Holder within their organisation. Other requests must be investigated and actioned (if necessary) as soon as possible. Any person who is aware of the actual or potential misuse or compromise of a PEXA token or private key should contact the Subscriber Organisation or the PEXA Support desk. Before actioning such a suspension request, the authorised administrator must: • verify the identify of the requestor; and • establish that the reason for the suspension request is legitimate.
4.9.16. Limits on suspension period	There is no limit on the suspension period. (A suspended certificate can remain suspended until it expires, at which time it will no longer be listed as suspended.)
4.9.17. Un-suspension	Certificate un-suspensions can be performed by the following: • Subscriber Managers and Subscriber Administrators (subject to heirarchical controls[5]) for any other Certificate Holder; and • PEXA Support Desk – can un-suspend certificates issued to Subscriber Managers. No individual can un-suspend their own certificate. A Certificate Holder must contact a Subscriber Manager or Subscriber Administrator to un-suspend their certificate. Subscriber Managers must contact the PEXA Support Desk. Certificate un-suspensions can be actioned as follows:

[4] Subscriber Managers can perform said task to another Subscriber Manager, Subscriber Administrator or Subscriber Signer; Subscriber Administrators can only perform said task to another Subscriber Administrator or Subscriber Signer.

[5] Subscriber Managers can perform said task to another Subscriber Manager, Subscriber Administrator or Subscriber Signer; Subscriber Administrators can only perform said task to another Subscriber Administrator or Subscriber Signer.

	• via email request or phone call to PEXA Support Desk (who, in turn perform the relevant function on PEXA CMS); or • via the relevant function on the PEXA Platform. In all cases, prior to un-suspending the certificates, Subscriber Managers, Subscriber Administrators or the PEXA Support Desk must: • verify the identity of the requestor; and • verify their authority to request un-suspension of the certificate in question; and • establish that the reason for the un-suspension request is legitimate.
4.10. Certificate status services	
4.10.1. Operational characteristics	Certificate Status services are provided through an OCSP service exclusively accessible to the PEXA system, as it is the only party which requires real time certificate status information.
4.10.2. Service availability	OCSP responders are deployed in a high availability configuration, with a target of 99.9% availability.
4.11. End of subscription	When a PEXA Participation Agreement or PEXA DSC Subscriber Agreement is terminated by either party, all the PEXA DSC Subscriber's PEXA certificates will be revoked.
4.12. Key escrow and recovery	Not applicable.
5. RO Operational Controls	***NB. Section 5 of this short form CP does not match Section 5 headings in the PEXA CPS. They are replaced by "RO Operational Controls" sections below as recommended by the Gatekeeper Framework in the certificate policy template for Relationship Certificates.*** ***5.1 Personnel controls*** ***5.2 Logical and Technological controls*** ***5.3 Physical controls*** ***5.4 Business continuity of the RO*** ***5.5 RO termination*** ***5.6 Management of Client Information*** ***5.7 Verification of Identity Controls*** ***Refer to CPS for the Facility, Management, and Operational Controls of the CA.***
5.1. Personnel controls	
5.1.1. Qualifications, experience, and vetting requirements	PEXA personnel are vetted at the time of hiring. All staff, whether permanent, consultancy organisations, contractors through agencies or direct contractors, must undergo a police check, a 10 year background check, as well as bankruptcy and probity checks before being allowed to commence duties related to PEXA Operations. Consultancy organisations providing staff working on PEXA systems or premises are required to either perform their own police and background checks on their staff or in certain cases, provide a certificate of compliance on an annual basis to confirm compliance. The requirements are detailed in PEXA Personnel Security policy, an internal document.
5.1.2. Training	Personnel that are involved in PEXA operations undergo training in: i. Operational procedures ii. Privacy principles iii. Document verification (if involved in VOI checks) iv. System Security v. Disaster Recovery and Business Continuity Procedures

	vi. PKI concepts and technology. Items ii. and iv. are addressed under the "compliance" section of the PEXA employee induction program. VOI Officers undergo training as outlined in section 5.7.
5.1.3. Re-training 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.
5.1.4. Job rotation frequency and sequence	PEXA staff will be added to or removed from the relevant PKI-associated roles according to the workloads required.
5.1.5. Roles requiring separation of duties	A staff member with daily operations duties in PEXA will not act in the role of General Manager – Technology (responsible for security) or perform official audits on the PEXA Operations.
5.1.6. Sanctions for unauthorised actions	Staff members or contractors who have been found to misuse resources or otherwise carry out unauthorised actions will be managed in accordance with the PEXA Incident Reporting Process and subject to sanctions in accordance with the PEXA Code of Conduct Policy. Depending on the nature of the actions and the motivation, sanctions may range from counselling, suspension of access rights, through to dismissal and legal action.
5.1.7. Independent contractor requirements	Contractors and Consulting firms may be required to hold positions of trust on an as needed basis. All Contractors must sign a 'Contracting Agreement' which incorporates confidentiality provisions. All Consulting firms must sign a 'Non-Disclosure Agreement' which also incorporates confidentiality provisions.
5.2. Logical and Technological controls	***For information regarding CA logical security, refer to CPS documentation sections 5 and 6.*** ***The following sections describe logical security controls for PEXA and Subscriber environments.***
5.2.1. Network controls	**PEXA system** The PEXA system uses a multi-tier architecture, with firewalls separating security domains. A dedicated crypto server provides cryptographic services within the PEXA system. PEXA transactions are signed. Transport level encryption (SSL/TLS) is employed when data is transferred to PEXA and out of PEXA (to Land Title Offices). Databases are encrypted as follows: • PEXA Platform Database - encrypted using AES256 algorithm; and • PEXA CRM – encrypted using a combination of 3DES and AES. PEXA records date/time of a transaction signing in the database. The OCSP response includes a time stamp which is signed by the OCSP responder. PEXA can reference that time stamp as a point in time the certificate was validated. Systems are synchronised with an external time source. Audit logs are collected from all servers and aggregated, allowing real-time monitoring and analysis. Servers are protected with firewalls, anti-virus software and Intrusion Detection System (IDS), with external facing infrastructure also having Intrusion Prevention System (IPS) services, "Distributed Denial Of Service" (DDOS) filtering and regular vulnerability scans. **Subscriber systems**

<table>
<tr><td></td><td>Signing is achieved on the Subscriber Signer’s desktop using an applet downloaded from the PEXA system.

All PEXA transactions use SSL/TLS server authentication and encryption (https).

Subscriber Organisations are required to protect access to the PEXA system to meet requirements of the MPR, section 7 “Obligations Regarding System Security and Integrity”, including but not limited to:

• comply with PEXA Security policy forming part of the Participation Agreement;
• install and keep updated virus protection software on the Subscriber Organisation’s computers;
• protect security items (e.g. tokens and passwords); and
• train and monitor its users in relation to the Subscriber Organisation’s security obligations.</td></tr>
<tr><td>5.2.2. Access Control</td><td>PEXA system

Administrative access to PEXA CRM is controlled by PEXA using individual accounts stored on LDAP servers, providing an audit record which identifies the individual carrying out an activity. Production systems are fully separated from non-production infrastructure.

Break Fix or Application accounts have their passwords stored in a secure password vault (as software based cryptographic container for storing passwords). These passwords are changed after usage.

Data centre operators (refer to section 5.3.1) have access to the system servers in order to provide low level services such as operating system patching and security services. Data centre operators do not have access to applications.

Subscriber systems

Subscriber Organisations are required to protect access to the PEXA system to meet the requirements of the MPR, section 7 “Obligations Regarding System Security and Integrity”.

The security controls that secure signing of documents in PEXA comprise:

• PEXA logon security control (to protect the PEXA User's logon account); combined with;
• PEXA DSC private-key usage security controls.

The PEXA User's logon account is protected by a password (minimum seven alpha-numeric characters) with regular refresh enforcement.

The PEXA DSC hard and soft tokens are protected by a PIN comprising six numeric characters. USB Tokens will lock after ten failed entries.</td></tr>
<tr><td>5.2.3. Remote access</td><td>The PEXA Platform is accessible remotely by PEXA Users who logon via username/password authentication over an https session. The following text pertains to the use of VPN technology for access to other PEXA System components.

PEXA supports VOI interviews in remote locations, and the associated VOI documents are captured electronically and transferred to PEXA CRM in a secure manner.

The options provided by PEXA for conducting a VOI and the various combinations are listed in the table below. For each alternative, the VOI documents are digitised at the source and transferred securely onto a secure web host. For each alternative, upon completion of the VOI session (and any associated processing), an email will be sent to PEXA Operations. A PEXA On-boarding Officer will then log into the secure web host (with the reference link provided in the email notification) using secure authentication, download the VOI documents, and upload same to the associated Subscriber User’s relevant CRM account. In summary, VOI documents are attained by PEXA using a “pull” approach.

<table>
<tr><th>Location options for conducing VOI</th><th>Who can perform a VOI</th><th>VOI tool employed</th></tr>
<tr><td rowspan="2">Subscriber premises</td><td>VOI Agent</td><td>VOI secure transmission Tool</td></tr>
<tr><td>VOI Officer</td><td>VOI secure transmission Tool</td></tr>
</table>
</td></tr>
</table>

	<table><tr><td>Gatekeeper-accredited RA premises</td><td>Authorised Gatekeeper-accredited RA employee</td><td>As supplied by the Gatekeeper-accredited entity</td></tr><tr><td>PEXA premises</td><td>VOI Officer</td><td>VOI secure transmission Tool</td></tr><tr><td>Conference facility</td><td>VOI Officer</td><td>VOI secure transmission Tool</td></tr></table> Administrator access to the PEXA CRM is via VPN technology, with rigorous authentication and authorisation processes applied in order to restrict access to PEXA technical support officers only, and solely for technical support purposes.
5.2.4. Change control	System change controls in place for the PEXA system include: • Change management policy and procedures; • maintenance of a configuration baseline; and • access and user actions logged and sent through to a centralised audit log server. Events and/or errors that meet specific criteria generate alerts that are sent to operators. Changes to the PEXA PKI proposed after the initial bootstrap must be approved by the following PEXA approval boards and associated processes: • Change Approval Board; • Change Control Board; and • Architecture Review Board. N.B. Any changes that alter the contents of the Gatekeeper Approved Documents (other than minor ones which do not materially affect the acceptability of a certificate type) must also be approved by the Gatekeeper Competent Authority. See CPS section 1.5.4.
5.2.5. Off-site backup	In addition to the real-time replication of the encrypted PEXA CRM (databases, file systems and logs) between primary and secondary sites over SSL-secured links, both daily and weekly backups of the data are generated and retained at the secondary site for up to 7 days. Weekly backups will also be transferred over SSL-secured links to a third physical secure storage facility where data will be retained for up to seven years.
5.3. Physical controls	
5.3.1. Site location and access	The PEXA CA infrastructure is located at the managed CA service provider's data centres. These premises are certified using ASIO-T4 physical security specifications to a level required by Gatekeeper. For more information regarding CA physical security, refer to the CPS and CA documentation. N.B. Some CA documentation is classified and not made public. The PEXA CRM is hosted at a commercial data centre with a primary and DR site. The data centre infrastructure and security processes are certified to ISO 27001 Security Management Standard. Data centres are monitored 24/7 and use backup power supply, environmental controls and physical access controls. PEXA premises, from which PEXA CRMs are managed, are located in Melbourne and Sydney, and are protected by building access cards. Security zones divide the area into an outer area with controlled access to the public, and staff-only areas for PEXA administration. VOI checks may take place at PEXA's offices, or a VOI Agent's location around the country. In some instances, 'roaming' VOI Officers may enrol new Subscribers at roadshows or conventions. Sponsors may perform VOI checks at applying Subscriber premises.
5.3.2. Ad hoc sites	Ad-hoc sites may be used to conduct face-to-face VOI checks of the Subscriber Binding Authority. Ad-hoc sites will typically include Subscribers' business premises or PEXA conferencing venues. Face-to-face VOI checks will involve:

	• checking of the applicant's identity documents; and • making electronic copies of the applicant's documents. VOI checks will occur in an area that precludes access by parties that are not privy to the check. The VOI documents will be scanned and transmitted using a purpose-built, secured smartphone application that will transfer said documents to a secured PEXA destination.
5.3.3. Media storage	Any organisation or Individual Documents collected by PEXA and stored on CRM will be retained indefinitely. This requirement is defined in the MOR, section 19.1. Other than digital records in PEXA databases, PEXA does not store media. Refer to 5.3.4.
5.3.4. Media disposal	All PEXA data must be protected throughout its life cycle inclusive of disposal. Requirements are detailed in the PEXA Asset and Media Management Policy, an internal document. Any forms submitted by Subscribers in paper form via post will be scanned into electronic form upon receipt and transferred to the relevant Subscriber CRM location. These paper forms will then be destroyed in accordance with PEXA security policies.
5.4. Business continuity of the RO	The ROs Business Continuity Capabilities form an integrated component of the PEXA Governance, Risk Management and Compliance (GRC) framework. The capabilities have been developed based on leading industry practice and standards including AS NZS 5050:2010. The objective of these capabilities is to ensure continuity of critical processes in the event of a disruption to the availability of system, people and facilities. The ROs Business capability are subject to annual independent review, in order to fulfil ELNO compliance obligations as defined in the ARNECC MOR. PEXA PKI and digital certificate regime is a process and set of infrastructure which falls with the scope of this business continuity capabilities. The PEXA RO consists of the following systems: • PEXA CMS • PEXA Platform - Digital Certificate Management subcomponents • PEXA CRM PEXA has a primary and secondary site for all systems located on different power and telco grids. The secondary site is to be used for disaster recovery situations should the primary site be unavailable or inoperable.
5.5. RO Termination	In the event that PEXA terminates its certificate management operations (whether voluntarily or involuntarily) it must: • give notice to all PEXA DSC Subscribers, terminating its contracts relating to certificate management with them (the termination to be effective in accordance with the terms of the relevant contract); • continue to provide the services (in particular the maintenance Certificate status checking Services) in accordance with any contractual arrangements it has with its PEXA DSC Subscribers and any relying parties; • co-operate with Dept. of Finance, the managed CA service provider and other PKI participants to achieve a seamless and secure migration of Subscribers to a new Gatekeeper accredited Service Provider; • provide notice to all affected parties; • if transferring personal information from one to other PKI; ensure it is protected as required under the Privacy plan. Circumstances for PEXA's termination in its role as the Relationship Organisation for the PEXA PKI, include the loss of approval to operate as an ELN in accordance with the MOR or the loss of Gatekeeper accreditation. Refer also to CPS section 5.8 (CA termination).
5.6. Management of client information	

5.6.1. Information collection and verification	The process associated with on-boarding organisations and the information exchanged at each stage of the process is as outlined in section 3.2.2. As is described, the information collected and verified includes: • Organisation Documents – these pertain to the Subscriber Organisation and are used to validate the identity of a PEXA Member; and • Individual Documents – these pertain to an individual and are used to validate the identity of the PEXA DSC Subscriber Binding Authority. The information Handled includes both publically available information and Personal Information. The information that may be collected for the purposes of conducting an organisation validation is listed in Appendix B.2. The information that may be collected for the purposes of conducting an Individual VOI is listed in Appendix B.3. Organisation information is Handled by either PEXA On-boarding Officers or Sponsors. Individual Documents are only Handled by VOI Agents or VOI Officers. Further information on how PEXA Handles Personal Information is available at http://www.pexa.com.au/privacypolicy .
5.6.2. Maintenance of client information	The subset of information collected (as described in section 5.6.1) that needs to be maintained on the PEXA Platform or PEXA CRM comprises: i. Contact details associated with the PEXA Subscriber; ii. Financial operational information (bank details); and iii. Supporting documents that prove a PEXA Subscriber's on-going eligibility to be a PEXA Subscriber. Items i. and ii. above are maintained by PEXA Operations based on updates provided by PEXA Subscribers. Item iii. documents either expire, or their currency is subject to change as a result of action by the credential authority (such as suspension or restriction). Documents that expire will be identified by regularly-generated 'document expiry reports' generated by the PEXA CRM. Changes to the currency of documents will occur either by receipt of change advice sent by the relevant credentiality authority, or are supplied by the PEXA Subscriber to PEXA Operations. For any documents listed above, any change notification: • may be advised by phone, fax, email or post; and • will have the source of the change notification verified by PEXA Operations prior to changing the status on PEXA CRM. **For digital certificate-related information**, PEXA DSCs include minimal Certificate Holder information which is susceptible to change over time. The fields are (Name field) and Email address in the Certificate Holder's Distinguished name field. Changes to these field parameters are initiated by PEXA DSC Subscribers and PEXA will act upon certificate change requests according to instructions provided by the PEXA DSC Subscriber or facilitate via the PEXA Platform.
5.6.3. Physical and logical security of repositories	All PEXA Member or PEXA Subscriber information (i.e. subsets of tables in Appendix B.1 and B.2) is stored in the PEXA CRM. A subset of the aforementioned information is duplicated to the PEXA Platform. Organisation Documents are transferred to the PEXA CRM using one of the following three methods: i. Uploaded to PEXA CRM by PEXA Member Using this method, the PEXA Member will log onto to the PEXA CRM (web-facing portion) using the account supplied during sales phase, via a secure https session. ii. Using electronic forms in combination with email Using this method, the PEXA Member fill the requisite form and then selects <send> on the form, which launches the email application (on member's computer) which will send the form data to the PEXA On-boarding email address. Upon receipt of the information, a

	PEXA On-boarding Officer will upload the information into the PEXA Member's PEXA CRM account. iii. Using physical forms sent by post or fax Using this method, a PEXA On-boarding Officer will digitally scan the information received and then upload it into the PEXA Member's PEXA CRM account. Some data information transfer (from form to PEXA CRM) will involve transcription. Upon completion of the aforementioned step, the physical-form documents are shredded and disposed into a secure bin that is, in turn, disposed of via a contracted secure destruction service provider. Individual Documents are transferred onto PEXA CRM using the method described in section 5.2.3. The PEXA CRM has a primary site and secondary site, located on different premises on different grids. These systems are located in dedicated server rooms. Physical access to these rooms is restricted (via building access security) to PEXA System Administrators. Logical access to the PEXA CRM by PEXA employees is restricted according to the employee's role. All activity on the PEXA CRM is logged in order to provide an audit record identifying the individual carrying out an activity. Refer also to section 5.2.
5.6.4. Contractual obligations on Subscriber Organisations	As outlined in section 3.2.3, Subscribers are required to verify the identity of a Certificate Recipient prior to requesting a PEXA DSC for Certificate Recipient from PEXA and to retain the VOI documents for potential, subsequent auditing purposes. Subscribers are also obligated to maintain client information as outlined in 5.6.2.
5.7. Verification of Identity controls	A Verification of Identity may be performed by a VOI Agent or a VOI Officer. VOI Agents (excluding Sponsors) accredit their staff to perform VOI via their respective accreditation program. VOI Officers are accredited via the 'PEXA VOI Officer Accreditation Program'. VOI Officers may be Sponsor or PEXA employees. The PEXA VOI Officer Accreditation Program comprises the following two core elements: • Assessment of the candidate - candidates must pass Security Vetting requirements (involving police, bankruptcy and insolvency check); and • Training of the candidate – involves training on the use of the VOI secure transmission Tool, and the associated procedures, including privacy principles. A Verification of Identity may also be performed by an individual employed by a PEXA DSC Subscriber to a fellow-employee in accordance with section 3.2.3.
6. Technical Security Controls	Refer to CPS for details relating to the CA. including: 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 6.7. Network security controls 6.8. Time-stamping Refer to section 5.2 for details relating to the PEXA & Subscriber environments.
7. Certificate, CRL, and OCSP Profiles	
7.1. Certificate profile	Refer to Appendix A for PEXA DSC Profile.
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	The Common Name of the Certificate Holder is as recorded in their PEXA account.
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 and the User notice qualifier may be used in certificates. 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. The User notice, if used, shall only contain the explicitText field.
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 CA CP, Appendix A.
7.3. OCSP profile	Refer to CA CP, Appendix A.
8. Compliance Audit and Other Assessments	Refer to CPS for compliance audits, including: 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 Compliance monitoring and reporting requirements for ELNOs are described in Section 15 of the MOR. Compliance examination procedure for Subscribers is described in Schedule 5 of the MPR. In addition, the obligation of the ELNO (PEXA) in monitoring the compliance of Subscribers is described in Section 14.7 of the MOR.
9. Other Business and Legal Matters	
9.1. Fees	Refer to section 13 of the PEXA DSC Subscriber Agreement for all fees and terms associated with the supply of PEXA DSCs.
9.2. Financial responsibility	
9.2.1. Insurance coverage	Insurance cover is in accordance with the MOR requirements, as follows. PEXA is covered by: • Professional Indemnity insurance ($20 million), • Fidelity Insurance ($20 million); and • Public Liability insurance policies ($10 million).
9.2.2. Other assets	Information provided upon request.

9.2.3. Insurance or warranty coverage for end-entities	PEXA provides a 12 month warranty for USB tokens – refer to section 13.3 of the PEXA DSC Subscriber Agreement.
9.3. Confidentiality of business information	
9.3.1. Scope of confidential information	Refer to clause 11 of the PEXA Participation Agreement that PEXA will enter into with each PEXA Subscriber. Subject to the scope exclusions specified in paragraph 9.3.2 of this CP, confidential information is: i. information exchanged in any form via the ELN that: • is made available by or on behalf of a party to the PEXA Participation Agreement to the other party; or • relates to the business, assets or affairs of a party to the PEXA Participation Agreement and is obtained by or on behalf of the other party, whether made available or obtained directly or indirectly, or before on or after the date of the PEXA Participation Agreement; and ii. is by its nature confidential or the receiving party knows, or ought to know, is confidential; and • includes: - information relating to the personnel, policies, business strategies, customers, products or services, contractual or commercial dealings of either party; and - information which is designated by either Party as confidential.
9.3.2. Information not within the scope of confidential information	Refer to clause 11 of the PEXA Participation Agreement. Confidential Information does not include information that: • is in or enters the public domain through no fault of the receiving party or any of its officers, employees or agents; • is or was made available to the receiving party by a person (other than the disclosing Party) who is not or was not then under an obligation of confidence to the disclosing party in relation to that information; or • is or was developed by the receiving party independently of the disclosing party and any of its officers, employees or agents; or • was known by the receiving party prior to its disclosure to that party.
9.3.3. Responsibility to protect confidential information	Refer to clause 11.2 of the PEXA Participation Agreement. A party to the PEXA Participation Agreement (Recipient) which acquires confidential information of another party to that PEXA Participation Agreement (Discloser) will not: • use any of the confidential information except to the extent necessary to exercise its rights and perform its obligations under the PEXA Participation Agreement (which, for the avoidance of doubt, may include such disclosure to third parties subject to equivalent confidentiality obligations as is necessarily incidental to a Conveyancing Transaction); and • disclose any of the confidential information except in accordance with exceptions set out in the PEXA Participation Agreement.
9.4. Privacy of personal information	
9.4.1. Privacy plan	PEXA Privacy Policy complies with the *Privacy Act* 1988, including the Australian Privacy Principles as published by the Office of the Australian Information Commissioner (OAIC). For details, refer to http://www.pexa.com.au/privacypolicy. Also refer to clause 12 of the PEXA Participation Agreement for PEXA's privacy obligations. PEXA agrees to comply with its obligations under the Australian Privacy Principles (as amended or replaced) and any other applicable privacy laws in relation to the handling of Personal Information that comes into its possession or control in the course of providing services as an ELNO.

9.4.2. Information treated as private	Individual VOI Documents 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). Associated with this certificate policy, PEXA collects and stores the Individual VOI Documents associated with processes defined in 3.2.2. Refer to PEXA Privacy Policy at http://www.pexa.com.au/privacypolicy.
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 information collected as part of an entity's or person's interaction with PEXA that is Personal Information will be protected in accordance with the requirements of the Australian Privacy Principles.
9.4.5. Notice and consent to use private information	Refer to the PEXA Privacy Policy at http://www.pexa.com.au/privacypolicy.
9.4.6. Disclosure pursuant to judicial or administrative process	Refer to the PEXA Privacy Policy at http://www.pexa.com.au/privacypolicy .
9.4.7. Other information disclosure circumstances	PEXA will only disclose Personal Information in accordance with the Australian Privacy Principles.
9.5. Intellectual property rights	Refer to clause 13 of the PEXA Participation Agreement. In summary, subject to exceptions set out in the PEXA Participation Agreement: • the PEXA Subscriber shall not have any ownership rights in any intellectual property brought into existence by PEXA in providing services as an ELNO, including services commenced or enhanced after the date of the PEXA Participation Agreement; • to the extent that the PEXA Subscriber at any time acquires any right, title or interest in any intellectual property in PEXA['s services, the PEXA Subscriber, by the PEXA Participation Agreement, assigns to PEXA all such rights, title and interest in that intellectual property; and • each party acknowledges and agrees that, unless otherwise expressly stated in the PEXA Participation Agreement, no pre-existing intellectual property rights of either party is assigned or otherwise transferred by reason of the PEXA Participation Agreement. This is not an exhaustive statement of PEXA's and a PEXA Subscriber's reciprocal rights and obligations in relation to intellectual property rights. Please refer to clause 13 of the PEXA Participation Agreement.
9.6. Representations and warranties	
9.6.1. CA representations and warranties	Refer to section 9.6.2.
9.6.2. PEXA representations and warranties	PEXA does not give any specific representations or warranties in the PEXA DSC Subscriber Agreement.
9.6.3. Subscriber representations and warranties	Upon enrolment for the use of the PEXA Platform, Subscribers agree to the terms set out in the PEXA Participation Agreement. Prior to being issued with PEXA DSCs, the Subscriber must also sign the PEXA DSC Subscriber Agreement. The obligations and warranties of the Subscriber are set out in these documents and in the MPR.
9.6.4. Relying party representations and warranties	Refer to section 9.6.2

9.6.5. Representations and warranties of other participants	PEXA DSC Subscribers give the warranties contained in clause 8 of the PEXA DSC Subscriber Agreement. No representations or warranties are given by any other participants.
9.7. Disclaimers of warranties	No warranties are given or disclaimed by PEXA in its role as the CA.
9.8. Limitations of liability	Under clause 12 of the PEXA DSC Subscriber Agreement, subject to some conditions, PEXA is liable for loss arising from PEXA's fault, defect or error in relation to the issue and validation of digital certificates. Subject to the operation of the Australian Consumer Law, to the maximum extent permitted by law, PEXA excludes all liability for any loss or damage arising out of the supply or use of any hard token and associated software and instructions by or on behalf of PEXA to the Subscriber Organisation.
9.9. Indemnities	PEXA does not give any indemnities in respect of the issue and validation of digital certificates under the PEXA DSC Subscriber Agreement.
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	No specific dispute resolution provisions apply between PEXA and the PEXA DSC Subscriber.
9.14. Governing law	This CP is governed by the laws in force in Victoria, Australia.
9.15. Compliance with applicable law	PEXA complies with all applicable laws.
9.16. Miscellaneous provisions	Not applicable.
9.17. Other provisions	Not applicable.

APPENDIX A. PEXA DIGITAL SIGNING CERTIFICATE PROFILE

N.B. This certificate is used by Subscriber Managers, Subscriber Administrators and Subscriber Signers.

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>	Validity is 3 years from the <Not before> date.
Subject Distinguished Name		E=<Subject's organisational email address> CN= <First Name><Middle Name><Surname> O= <Subscriber organisation - Legal entity> C= AU	Encoded as printable string where possible, and otherwise using UTF-8 Multiple first or middle names may be entered, separated with a space, e.g. CN=<First name1> <First name2> <Middle name1> <Middle name2> <Surname>
Subject Public Key Information		2048 bit RSA key modulus, rsaEncryption	
X.509 V3 extensions:			
subject Alternative Name (Email)		<Subject's RFC822 organisational email address>	Contains the Subject's organisational email address.

Field	Critical	Certificate Value	Notes
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	digitalSignature nonRepudiation	
Extended key usage	Yes	SSL client authentication emailProtection	SSL client auth for token management emailProtection to allow SMs to sign requests by email
Certificate policies	No	Policy OID: {1.2.36.40677792.1.1.2} [1] Policy Qualifier Info: Policy Qualifier Id=CPS pointer Qualifier: URL= https://www.pexa.com.au/ca/publish/pexa/documents/	The OID of the PEXA DSC 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/PEXAOCA<nnn>.crt [2] Access method: OCSP {1.3.6.1.5.5.7.48.1} Access location: http://ocsp.pexa.net.au	Location of issuing CA certificate. Location of OCSP responder.
Private extensions:			
ABN	No	Extension OID: {1.2.36.1.333.1} Gatekeeper identification of *Australian Business Number* The ABN value is encoded as an IA5String.	Gatekeeper registered OID for the representation of an ABN.

APPENDIX B. ADDITIONAL INFORMATION

B.1 PEXA Subscriber on-boarding process (supporting section 3.2.2)

On-boarding process stage	Summary of what occurs	Resulting Organisation classification	What's collected by PEXA
Initial Contact / Sales	Organisation expresses interest in becoming a PEXA Subscriber An organisational employee provides name and email address details to PEXA PEXA sends registration web address and account logon details to organisational employee A PEXA Member account is created on PEXA CRM Organisational employee accesses web page and registration process information	PEXA Member	Organisation employee name and email address
PEXA Member Registration	All requisite forms and documents (determined by organisation type) are submitted to PEXA SBA signs the PEXA Participation Agreement SBA undertakes a VOI	PEXA Member	Registration forms submitted Supporting documentation submitted SBA VOI documents submitted Signed PEXA Participation Agreement
	Optional: PEXA Member chooses to become a PEXA DSC Subscriber, in which case the SBA signs the PEXA DSC Subscriber Agreement		Signed PEXA DSC Subscriber Agreement
'PEXA Member Registration' Assessment & Activation	PEXA conducts PEXA Member organisation validation. PEXA assesses all Registration forms and supporting documents PEXA creates the Subscriber Account on PEXA Platform PEXA Member status is changed to 'PEXA Subscriber' on PEXA CRM	PEXA Subscriber	
	If PEXA DSC Subscription option selected: PEXA generates and sends a PEXA DSC to the nominated PEXA Subscriber Manager	PEXA DSC Subscriber *(in addition to*	

On-boarding process stage	Summary of what occurs	Resulting Organisation classification	What's collected by PEXA
		PEXA Subscriber designation)	

B.2 On-boarding of Subscribers – document requirements

Documents/Requirements	Financial Institutions	Legal Practitio-ners	Conveyan-cers	Govern-ment Bodies
Registration form – signed by Binding Authority	✓	✓	✓	✓
Participation Agreement (PA) - signed by Binding Authority	✓	✓	✓	✓
Subscriber Agreement (Digital Cert preference) signed by Binding Authority	optional	optional	optional	optional
Evidence Professional Indemnity insurance (PII) – This may be a Certificate of Currency or Insurance Schedule with a paid receipt.	✓ For non ADIs	✓	✓	✓ For non crown
Evidence Fidelity insurance (FI) – This may be a Certificate of Currency or Insurance Schedule with a paid receipt.	✓ For non ADIs	-	-	✓ For non crown
Copy of Conveyancing Licence	-	-	✓	-
Copy of Practicing Certificate	-	✓	-	optional
Trust Deed- certified copy		optional	optional	optional
Partnership Deed- certified copy *only required if they are a partnership and no other evidence, such as a Power of Attorney is provided.		optional	optional	optional
Letter of Authority	optional	optional	optional	optional
Power of Attorney	optional	optional	optional	optional
Direct Debit Authority – lodgement fees	✓	✓	✓	✓
Direct Debit Authority –PEXA fees	✓	✓	✓	✓
Trust Account Authority form	-	optional	optional	-

Documents/Requirements	Financial Institutions	Legal Practitio-ners	Conveyan-cers	Govern-ment Bodies
*only required where the Applicant is using their own trust account				

B.3 Subscriber Verification of Identity documents

Extract from Subscriber Identity Verification Standard, MOR, Schedule 7.

Category 1	A passport issued by the Australian Government or a foreign passport with an Australian Visa Grant Notice evidencing an Australian resident visa ***plus*** Australian driver's licence or Proof of Age/Photo Card ***plus*** change of name or marriage certificate (if necessary).
Category 2	A passport issued by the Australian Government or a foreign passport with an Australian Visa Grant Notice evidencing an Australian resident visa ***plus*** full birth certificate, citizenship certificate or descent certificate ***plus*** Medicare, Centrelink or Department of Veterans' Affairs card ***plus*** change of name or marriage certificate (if necessary).
Category 3	Australian driver's licence or Proof of Age/Photo Card ***plus*** full birth certificate, citizenship certificate or descent certificate ***plus*** Medicare, Centrelink or Department of Veterans' Affairs card ***plus*** change of name or marriage certificate (if necessary).