ECHOWORX™

IT PAYS TO BE SECURE

Root CA2

Certificate Policy and Certification Practices Statement

Version: 1.15
Document Release: CPS-CA2-001
Effective Date: Mar. 12, 2024
Public document
(unclassified)

Echoworx Corporation
4101 Yonge Street, Suite 708,
Toronto, Ontario M2P 1N6 Canada

Root CA2

Certificate Policy and Certification Practices Statement

Revision History

Version	Date	Amendment Details	Author	Approver
0.1	30 Sep, 2005	• Initial Draft	M.J. B	
0.2	2 Oct, 2005	• Added sections for Key Life Cycle Management and CA • Environmental Controls.	M.J. B	
0.3	5 Oct, 2005	• Minor changes only.	M.J. B	
1.0	6 Oct, 2005	• Marked final.	M.J. B	
1.1	26 Oct, 2005	• Slight changes to certificate profiles for CDP and CPS URLs • and correct ordering of DN attributes. Added References • section. Added appendix with root certificate in PEM and text • formats with fingerprints. Removed appendix with extraneous • OIDs.	M.J. B	
1.2	10 Aug, 2008	• Added version control and Correction of various URL	Alex L	Greg A
1.3	16 Jun, 2009	• Update section 2.17 “Acceptable uses and limits on reliance” • Update section 3.2.3 Subordinate CA key archival • Update section 3.2.4 Subordinate CA key destruction • Update section 4.11 Certificate status • Updated section 5.7 Event logging	Echoworx	Greg A
1.4	26 Aug, 2009	• Added section 5.5 Security management • Added section 5.6 Asset classification and management • Added section 5.7 Personnel security • Updated section 5.9 with approximate distance between CA • primary and recovery site and actual and suspected CA private • key compromise	Echoworx	Greg A
1.5	1 Feb, 2012	• Update section 3.2.1 1024 to 2048	Alex L	Greg A
1.6	7 Aug, 2013	• Update section 3.1.3, 3.1.4 for CA Key Archive and CA • Key destruction.	Alex L	Greg A
1.7	30 Mar, 2015	• Update doc to reflect subca to support sha2 section • 4.12.2	Alex L	Greg A
1.8	31 Aug, 2018	• Update version number as per WebTrust yearly • requirement. Nothing has changed	Alex L	Greg A
1.9	21 Feb, 2019	• Added Definition of Terms section • Updated version number as per WebTrust yearly requirement; nothing has changed	Brian C	Alex L

Version	Date	Amendment Details	Author	Approver
		• Updated the document as per latest standard template		
1.10	11 Feb, 2020	• Updated version number as per WebTrust yearly requirement; nothing has changed • Updated contact numbers on the back cover	Brian C	Alex L
1.11	15 Mar, 2021	• Updated version number as per WebTrust yearly requirement; nothing has changed • Updated the document template	Vibhuti N	Alex L
1.12	24 Jan, 2022	• Updated version number as per WebTrust yearly requirement. • Replace token with HSM. • Updated the document template	Randy Y	Alex L
1.13	17 May, 2022	• Modified instances of “level” in section 3.1 Root CA Management for capitalization. • Updated section 3.1.2, 3.2.2 FIPS to 140-2 Level 3 from FIPS 140-1 level 3 • Updated version number and effective date.	Josh T	Alex L
1.14	14 Sep, 2022	• Document reviewed, no changes necessary.	Josh T	Alex L
1.15	12 Mar, 2024	• Completed 2023 documentation review. No changes necessary.	Victoria E, Kevin F	Alex L

Contents

Index of Tables

1. Introduction

This document constitutes the Certificate Policy (CP) and Certification Practices Statement (CPS) for the Echoworx Root CA2 certification authority. The purpose of this document is to publicly disclose to subscribers and relying parties the policies and practices under which this certification authority is operated.

This document has been prepared in accordance with recommended best practices defined by the American Institute of Certified Public Accountants, Inc. and Canadian Institute of Chartered Accountants in the document entitled AICPA/CICA WebTrust$^{SM/TM}$ Program for Certification Authorities, version 1.0, dated 2000/08/25 [WebTrust].

2. General Practices

This section addresses general practices with respect to the operation of this root CA, including the identification of relevant policies; the target community of interest and applicability of certificates; contact information; limits of liability; financial responsibilities; legal considerations; fees; requirements and obligations of relevant parties and acceptable usage of certificates and limitations of reliance thereupon.

2.1. Policy Authority

The governing body of this PKI (Public Key Infrastructure) is the Echoworx Policy Authority (PA), who is responsible for the selection/definition of the certificate policy (CP) for the organization, development and management of the certification practices statement (CPS) and the correct day-to-day operation of the PKI.

2.2. Policy Identification

The Echoworx Root CA2 certification authority operates as a **Type 1** root CA (see table below) that may issue X.509 certificates to subordinate CA entities for issuing end-entity certificates.

Certificate Class	Network Protection	System Protection	Private Key Protection
Type '1' Root CA	**Dedicated system** • Always off-line	**High security controls** • Two-factor user authentication • Intrusion detection • Audit logging	**HSM** • Stored in vault when not used • Multi-party access controls • Audited key ceremonies
Type '2' Root CA	**Multi-purpose workstation** • Disconnected as needed for CA operations	**High security controls** • LiveCD OS used as needed w/ temporary storage (securely wiped)	**Removable Media** • Stored in vault when not used • Multi-party access controls • Audited key ceremonies

Table 1: Root CA Certificate Classes

Subordinate (or Intermediate) issuing CA(s) shall be denoted as Class A, B, or C depending upon the environmental controls for the operational security regime (as described in the table below) and operated in accordance with policies and practices commensurate therewith.

Certificate Class	Network Protection	System Protection	Private Key Protection
Class 'A' Subordinate CA	**Secure network zone w/ layer-1 separation** • Highly restricted access controls • Intrusion monitoring	**Medium - High security controls** • Two-factor user authentication • Intrusion detection • Audit logging • Remote monitoring • Site surveillance	**HSM** • On-line signing engine
Class 'B' Subordinate CA	**Private network zone w/ layer-1 separation** • Restricted access controls • Intrusion detection	**High security controls** • Intrusion detection • Audit logging • Remote monitoring • Site surveillance	**Encrypted on Fixed Disk** • Clear key in system memory for on-line signing operations
Class 'C' Subordinate CA	**Internal network** • Firewall perimeter access controls	**Medium security controls** • Intrusion detection • Audit logging	**Encrypted on Fixed Disk** • Clear key in system memory for on-line signing operations

Table 2: Subordinate CA Certificate Classes

2.2.1. Policy Object Identifiers (OIDs)

Certificate policy identifiers for certificates issued (directly) by this CA are given in the table (below). Echoworx Corporation was assigned the OID prefix 1.3.6.1.4.1.15505 by the Internet Assigned Numbers Authority (IANA) [https://www.iana.org/], whose registry is now managed by the Internet Corporation for Assigned Names and Numbers (ICANN) [https://www.icann.org/].

OID Value	OID Name
Echoworx Object identifiers	
1.3.6.1.4.1.15505.10	(echoworx.policy)
Certificate Policy identifiers	
1.3.6.1.4.1.15505.10.1	(policy.certificatePolicy)
1.3.6.1.4.1.15505.10.1.1	(certificatePolicy.testPurposesOnly)
1.3.6.1.4.1.15505.10.1.2	(certificatePolicy.reserved)
Root CA Certificate Policy identifiers	
1.3.6.1.4.1.15505.10.1.3	(certificatePolicy.rootCA)
1.3.6.1.4.1.15505.10.1.3.1	(rootCA.type1)
1.3.6.1.4.1.15505.10.1.3.2	(rootCA.type2)
Subordinate CA Certificate Policy identifiers	
1.3.6.1.4.1.15505.10.1.4	(certificatePolicy.subordinateCA)
1.3.6.1.4.1.15505.10.1.4.1	(subordinateCA.classA)
1.3.6.1.4.1.15505.10.1.4.1.1	(classB.escrowAllowed)
1.3.6.1.4.1.15505.10.1.4.2	(subordinateCA.classC)

OID Value	OID Name
1.3.6.1.4.1.15505.10.1.4.2.1	(classA.escrowAllowed)
1.3.6.1.4.1.15505.10.1.4.3	(subordinateCA.classB)
1.3.6.1.4.1.15505.10.1.4.3.1	(classC.escrowAllowed)

Table 3: Certificate Policy Object Identifiers (OIDs)

2.3. Community and Applicability

This document defines the policies and practices under which Echoworx Corporation (hereafter 'Echoworx') operates a Certification Authority (CA) and contingent upon which it issues Public Key Certificate credentials to authorized subordinate Certification Authority (Subordinate CA) entities for the issuance thereby of end-entity certificates to users of Echoworx-enabled applications, such as its Echoworx Encrypted Mail product, operated as a subscription service offering pursuant to agreements in place between these parties and any others in whose name(s) the service may be offered.

This CA is established to provide certification services for a variety of external customers. The CA makes use of customer-designated personnel to act as Registration Authority (RA) agents to verify the identity of subscribers, in accordance with the indicated certificate policy. Subscribers include all parties who contract with the CA and/or its customers on whose behalf digital certificates are issued. All parties who may rely upon the certificates issued by the CA are considered relying parties.

This certificate policy and certification practices statement (CP/CPS) is applicable to all certificates issued by this root CA. Subordinate CA(s) and/or end-entity certificates may have specific associated CP and/or CPS documents that supplement the information provided herein. The policies and practices described in this CP/CPS apply to the issuance and use of certificates and certificate revocation lists (CRLs) for users within the community of subject certificate entities and relying parties.

2.4. Contact Information

This Certification Authority is owned and operated by Echoworx Corporation. General inquiries and customer requests may be addressed to:

Echoworx Corporation
Attn: Director of Certification Services
4101 Yonge Street, Suite 708
Toronto, Ontario, Canada
M2P 1N6

Email: ca-info@echoworx.com
Web: https://www.echoworx.com/

Tel: +1 416-226-8600
Fax: +1 416-226-8629

2.5. Limits of Liability (No Warranty)

Echoworx asserts no control over how members of the community protect their own credentials. UNDER NO CIRCUMSTANCES IS Echoworx RESPONSIBLE FOR THE CONSEQUENCES TO A RELYING PARTY OF MAKING USE OF CREDENTIALS Echoworx ISSUES. Echoworx OFFERS NO WARRANTY OF ANY KIND AND DISCLAIMS ANY WARRANTY OF MERCHANTABILITY OR OF FITNESS FOR A PARTICULAR PURPOSE. Echoworx CANNOT BE HELD LIABLE FOR ANY DAMAGES OF ANY KIND WHETHER DIRECT, INDIRECT, INCIDENTAL OR CONSEQUENTIAL EVEN IF Echoworx HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Notwithstanding, except as expressly provided otherwise in this CP/CPS, applicable CP, or by statute or regulation, the CA's total liability per breach of any express warranties made under this CP/CPS and/or applicable CP is limited to direct damages having a maximum dollar amount (that is, a liability cap) of one dollar ($1.00). The liability cap set forth in this CP/CPS or applicable CP shall be the same regardless of the number of digital signatures, transactions or claims related to such certificate. Additionally, in the event the liability cap is exceeded, the available liability cap shall be apportioned first to the earliest claims to achieve final dispute resolution, unless otherwise ordered by a court of competent jurisdiction. In no event shall the CA be obligated to pay more than the aggregate liability cap for each certificate, regardless of the method of apportionment among claimants to the amount of the liability cap.

2.6. Financial Responsibility

By applying for and being issued certificates or otherwise relying upon such certificates, subscribers and relying parties agree to indemnify, defend and hold harmless the CA and its personnel, organizations, entities, subcontractors, suppliers, vendors, representatives and agents from any errors, omissions, acts, failures to act or negligence resulting in liability, losses, damages, suits or expenses of any kind, due to or otherwise proximately caused by the use or publication of a certificate that arises from the subscriber's failure to provide the CA with current, accurate and complete information at the time of certificate application or the subscriber's errors, omissions, acts, failures to act and negligence.

This CA and its registration authorities (RAs) are not the agents, fiduciaries, trustees or other representatives of subscribers or relying parties.

2.7. Interpretation and Enforcement

2.7.1. Governing Law

The laws of the province of Ontario in Canada shall govern the enforceability and construction of this CP/CPS document to ensure uniform procedures and interpretation for all users.

2.7.2. Severability, Survival, Merger, Notice

Severance or merger may result in changes to the scope, management and/or operations of this CA. In such an event, this CP/CPS may require modification as well. Changes to the operations will occur consistently with the CA's disclosed CP/CPS management processes.

2.7.3. Dispute Resolution

In the event of any dispute involving the services or provisions covered by this CP/CPS, the aggrieved party shall first notify the CA and all other relevant parties regarding the dispute. The CA will involve the appropriate personnel to resolve the dispute.

2.8. Fees

The CA may charge fees for their use of the CA's services on a negotiated per-user subscription basis in accordance with contracts between the CA and an application service provider on whose behalf end-entity certificates are issued to licensed users (subscribers) of Echoworx application software. Such fees are collected from the application service provider, not directly from the subscribing end-users. Additional fees may be levied for the setup, operation and maintenance of the issuing subordinate CA, subject to the terms and conditions of the contract between the CA and the application service provider.

2.9. Publication and Repository Requirements

This root CA's certificate policy and certification practices statement (CP/CPS) (this document) shall be published at:

https://www.echoworx.com/ca/root2/cps.pdf

Upon issuance, all public key certificates and certificate distribution lists (CRLs) issued (directly) by this CA are published at:

https://www.echoworx.com/ca/root2/cps.pdf

Revoked certificates may be removed upon publication of the CRL.

All subscribers and relying parties have access to this repository.

2.10. Compliance Audit Requirements

An annual audit is performed by an independent external auditor to assess the adequacy of this CA's business practices disclosure and the effectiveness of the CA's controls over its CA operations.

Topics covered by the annual audit include the following:

- CA business practices disclosure
- Service integrity (including key and certificate life cycle management controls)
- CA environmental controls

Significant deficiencies identified during the compliance audit will result in a determination of actions to be taken. This determination is made by the auditor with input from CA management. The CA is responsible for seeing that corrective action is taken within 60 days. Should a severe deficiency be identified that might compromise the integrity of the CA, CA management considers, with input from the auditor, whether suspension of the CA's operation is warranted.

Compliance audit results, if any, are communicated to the board of directors of the CA, CA management and the CA's policy authority, as well as others deemed appropriate by CA management.

2.11. Conditions of Certificate Applicability

Certificates issued under the CA's certificate policy are limited to use in connection with Echoworx licensed application software. Certificates issued by the CA may not be used for any other purpose unless expressly permitted otherwise.

2.12. CA Obligations

This CA is obligated to:

- Conform its operations to this CP/CPS, as the same may from time to time be modified by amendments published in the CA repository.
- Issue and publish certificates in a timely manner in accordance with the relevant certificate policy.
- Revoke certificates issued by this CA upon receipt of a valid request to revoke the certificate from a person authorized to request revocation.
- Publish CRLs on a timely basis in accordance with the applicable certificate policy and with provisions described in the Certificate Revocation section.
- Notify subscribers by an email (1) that certificates have been generated for them and (2) how the subscribers may retrieve the certificates.
- In the event this CA is not successful in validating the subscriber's application in accordance with the requirements for that class of certificate, this CA shall notify the subscriber that the application has been rejected.
- Notify subscribers by an email that the subscriber's certificate has been revoked.
- Notify other participants in the PKI of certificate issuance revocation through access to certificates and CRLs in the CA's repository.

2.13. RA Obligations

The RAs (or this CA's RA function) are obligated to:

- Verify the accuracy and authenticity of the information provided by the subscriber at the time of application, in accordance with the relevant certificate policy.
- Validate and securely send a revocation request to this CA upon receipt of a request to revoke a certificate, in accordance with the relevant certificate policy.
- Verify the accuracy and authenticity of the information provided by the subscriber at the time of renewal or re-key, in accordance with the relevant certificate policy.

2.14. Repository Obligations

The CA's repository function is obligated to publish certificates and certificate revocation lists in a timely manner.

2.15. Subscriber Obligations

Subscribers are obligated to:

- Provide information to the CA that is accurate and complete to the best of the subscribers' knowledge and belief regarding information in their certificates and identification and authentication information, and promptly notify the CA of any changes to this information.
- Safeguard their private key from compromise.
- Use certificates exclusively for legal purposes and in accordance with the relevant certificate policy and this CPS (or other CA business practices disclosure).
- Promptly request that the CA revoke a certificate if the subscriber has reason to believe there has been a compromise of their private key corresponding to the public key listed in the certificate.

2.16. Relying Party Obligations

Relying parties are obligated to:

- Restrict reliance on certificates issued by the CA to the purposes for those certificates, in accordance with the relevant certificate policy and with this CP/CPS.
- Verify the status of certificates at the time of reliance.
- Agree to be bound by the provisions of limitations of liability as described in this CP/CPS upon reliance on a certificate issued by the CA.

2.17. Acceptable Uses and Limits on Reliance

Certificates issued under the CA’s certificate policy are limited to use in connection with Echoworx licensed application software. Certificates issued by the CA may not be used for any other purpose unless expressly permitted otherwise.

3. Key Life Cycle Management

This section addresses the management of this CA's cryptographic keys throughout the operational life cycle of this CA, including how the public and private keys are generated and/or re-generated (that is, key changeover or re-keying); how the private key(s) are stored, protected and eventually destroyed; and how the public key(s) are distributed and archived.

3.1. Root CA Key Management

3.1.1. Root CA Key-Pair Generation

This root CA's signing key is 2048 bits in length. The private/public key-pair is generated in a Luna CA3 hardware security module (HSM) using the RSA algorithm with true random number generation (RNG) per Annex C of ANSI X9.17.

This root CA's private signing key material is generated, stored and used wholly within the Luna HSM; it is never exported for use in another device or onto any other media (except for being cloned onto an identical Luna HSM for backup purposes).

This root CA's private signing key shall only be used to sign only subordinate CA X.509 public key certificates and certificate revocation lists (CRLs).

The lifetime of the CA signing key-pair is twenty-five (25) years.

The Luna HSM is manufactured by Thales, which through mergers acquired the assets of Chrysalis ITS, Inc., the original developer of the Luna product line. This HSM device is compliant with FIPS 140-2 Level 3 and has been validated according to the Common Criteria Evaluation Assessment Level 4+ (EAL 4+) for environments that require the highest levels of physical and operational security.

3.1.2. Root CA Private-Key Protection

This root CA's private signing key is stored in a Luna CA3™ Hardware Security Module (HSM). This HSM device is compliant with FIPS 140-2 Level 3 and has been validated according to the Common Criteria Evaluation Assessment Level 4+ (EAL 4+) for environments that require the highest levels of physical and operational security.

There is a separation of physical and logical access to this root CA’s private signing key.

Multi-party controls ensure that at least two (2) individuals (one designated as a Security Officer and another designated as a Cryptographic Officer) provide dual control over physical access to the hardware modules at any time; m of n secret shares held by other, separate custodians (all executives of the CA operator, Echoworx or duly appointed thereby) on removable media (that is, Luna DataKeys™) are also required for logical access to the HSM management functions and activation of the private keys.

This root CA’s private signing key is backed up only on hardware certified to FIPS 140-2 Level 3 (Luna HSM) and is stored with multi-party controls enforced at all points of custody. These backup HSM are stored securely off-site in a secure safe-deposit box in the vault of two separate recognized financial institutions.

This root CA's private keys shall NOT be placed in escrow with an external third party.

3.1.3. Root CA Key Archival

This root CA's expired and/or revoked CA public key certificates shall be archived. A backup copy on removable media shall be stored securely in an off-site vault.

Archived keys are accessed only where historical evidence requires validation of archive keys. Only authorized Trusted Personnel are permitted to obtain access to archived keys.

3.1.4. Root CA Key Destruction

This root CA's private signing key shall be destroyed by re-initializing (zeroizing) all the Luna HSM upon which it is stored (that is, primary HSM and backup HSM). Each HSM shall be safeguarded as though it were still active until it can be physically destroyed.

The CA key destruction will not occur unless the business purpose or application has ceased to have value or legal obligations.

3.1.5. Root CA Public Key Distribution

Customers establishing an Echoworx application service shall be provided this root CA's public key in a self-signed certificate on a CDROM contained within the software installation kit.

This root CA's public key shall be delivered in a self-signed public key certificate included in Echoworx software application packages delivered to customers for distribution to subscribing end-users. The end-user software package shall be signed using Microsoft's Authenticode technology for which a code-signing key has been certified by a trusted third party.

This root CA's public key shall also be distributed in a self-signed public key certificate to leading providers of Internet software containing trusted key material, such as Microsoft's Internet Explorer and Mozilla Foundation's Firefox browser.

3.1.6. Root CA Key Changeover

The CA root signing private key has a lifetime of twenty-five (25) years and the corresponding public key certificate has a lifetime of twenty-five (25) years. Upon the end of the private key's lifetime, a new root CA signing key-pair may be generated and all subsequently issued certificates and CRLs are signed with the new private signing key. A corresponding new root CA public key certificate shall be securely provided to subscribers and relying parties.

3.2. Subscriber Key Management

For customers that subscribe to this root CA's managed key service for operating subordinate CAs, the following key management practices shall apply.

3.2.1. Subordinate CA Key Generation

The subordinate CA's signing key-pair shall be at least 2048 bits in length, using the RSA algorithm.

The subordinate CA's signing key shall be hardware generated and stored in an HSM device is compliant with FIPS 140-2 Level 3 (for example, Luna HSM appliance).

The subordinate CA's signing key shall be used to sign subordinate CA public key certificates and certificate revocation lists (CRLs).

The lifetime of the subordinate CA signing key-pair shall not exceed ten (10) years.

3.2.2. Subordinate CA Key Storage, Backup, Recovery

The subordinate CA's signing key shall be stored in an HSM device compliant with FIPS 140-2 Level 3.

There shall be a separation of physical and logical access to the subordinate CA's root private key.

Multi-party controls shall ensure that at least two (2) individuals (one designated as a Security Officer and another designated as a Crypto Officer) provide dual control over physical access to the hardware modules at any time; m of n secret shares held by other, separate custodians on removable media (for example, Luna DataKeys) are also required for logical access to the HSM management functions and activation of the private keys.

The subordinate CA's private signing key is backed up only on hardware certified to FIPS 140-2 Level 3 (for example, Luna HSM) and is stored with multi-party controls enforced at all points of custody. These backup HSM shall be stored securely off-site in a secure safe-deposit box in the vault of a recognized financial institution.

Subordinate CA private keys shall NOT be placed in escrow with an external third party.

The subordinate CA's private signing key and expired (and revoked) CA public key certificates shall be archived.

3.2.3. Subordinate CA Key Archival

The subordinate CA's expired and/or revoked public key certificates shall be archived. A backup copy on removable media shall be stored securely in an off-site vault.

3.2.4. Subordinate CA Key Destruction

The subordinate CA's private signing key shall be destroyed by re-initializing (that is, zeroizing) all the HSM devices upon which it is stored (that is, primary HSM and backup HSM).

4. Certificate Life Cycle Management

This section addresses the management of this root CA's cryptographic keys throughout the operational life cycle of this root CA, including how the public and private keys are generated and/or re-generated (that is, key changeover or re-keying); how the private key(s) are stored, protected and eventually destroyed; and how the public key(s) are distributed and archived.

4.1. Initial Registration of Subordinate CA

The CA has established a single naming hierarchy utilizing the X.500 Distinguished Name form.

In all cases, names of subject subordinate CA entities must be meaningful. Generally, the name by which an organization is commonly known to the CA should be used.

All subordinate CA subjects are unambiguously identified in the naming hierarchy.

This root CA issues certificates within a closed PKI. Trademarks and related naming issues will generally not apply to certificates issued within this space.

Possession of a private key is proved by a public key certificate applicant by providing check values as defined in the certificate policy.

If organizational identity is considered important based upon the certificate policy, the organization identity is verified using a method approved by the certificate policy.

In submitting a certificate application, at least the following information must be submitted to this root CA: subscriber's public key, subscriber's distinguished name and other information required on the CA's certificate application form.

If required by the certificate policy, the CA verifies the authority of the subscriber to request a certificate by checking whether the subscriber is an employee of a particular organization or association through inquiry of the organization's HR department or the association's membership department.

The CA may verify the accuracy of the information included in the subscriber's certificate request through validation against a third-party database.

The CA shall check certificate requests for errors or omissions.

4.2. Registration Using an External RA

The CA requires that external registration authorities (RAs) physically present themselves, along with two forms of identification, to an employee of the CA.

The CA authorizes external RAs upon successful identification and authentication, and approval of the external RA enrolment and certificate application forms.

External RAs are responsible for identification and authentication of subscribers and must secure their private signing keys used for signing certificate applications, securely forward certificate applications to the CA and securely store any subscriber information collected.

The CA verifies the authenticity of certificate request submissions received from an external RA by validating the RA's digital signature on the submission.

4.3. Certificate Renewal

The certificate renewal process is similar to an application for a new certificate. However, the subscriber needs to provide only information that has changed.

4.4. Routine Re-Keying

Authentication of the subordinate CA's identity as defined in this root CA's identification and authentication requirements for initial registration need not be repeated unless required by the applicable certificate policy. Subscribers will be limited to re-keying no more than twice before repeating the authentication process defined in identification and authentication requirements for initial registration.

4.5. Re-Keying After Expiry or Revocation

For subordinate CAs whose certificates have been revoked or have expired, re-keying is permitted if the identification and authentication requirements for initial registration are repeated.

4.6. Certificate Issuance

Certificates are issued to the subordinate CAs upon successful processing of the application and the acceptance of the certificates by the subscribers. Certificate format, validity period, extension field and key usage extension field requirements are specified in accordance with this root CA's disclosed certificate profile.

4.7. Certificate Acceptance

Once a certificate has been generated, it is maintained in a secure remote repository until it is retrieved by the subscriber. Upon retrieval of the certificate from the secure remote repository, the certificate status is updated to reflect its status as accepted and valid.

4.8. Certificate Distribution

A single repository is operated for subscribers and relying parties that contains the certificates for all subordinate CAs. All certificates issued by this root CA and all certificate revocation lists (CRLs) relating thereto shall be published in this repository. The repository for this root CA is provided as a web directory accessible via the HTTP protocol and is located at:

https://www.echoworx.com/ca/root2/cps.pdf

4.9. Certificate Revocation

A certificate can be revoked for several reasons, including suspected or actual compromise of control of the private key that relates to the public key contained in the certificate, hardware or software failures that render the private key inoperable, or failure of a subscriber to meet the obligations of this certificate policy and certification practices statement (CP/CPS) and/or related certificate policy (CP). Other circumstances for revocation may be stipulated in the particular CP and may relate to changes in a subscriber's relationship with the CA, such as a change in customer status.

Revocation may be requested by the subscriber (that is, subordinate CA), registration authority (if applicable) or this root CA. Requests by RA personnel to revoke a certificate require sufficient RA system access rights. Requests by subscribers to revoke their own certificates require one of the following:

- A digitally signed message from the subscriber to the RA
- Personal presentation of the subscriber to the RA with a personal photo ID card
- Presentation of the pass phrase created by the subscriber at the point of initial application
- Other means as provided in the CP

A subscriber can request a certificate revocation by an email, or by telephone to the certification authority (refer to the Contact Information section). Certificate revocation requests made by an email or a telephone are processed on a daily basis by the CA after the validity of such requests is ascertained. Validation procedures for telephone and email revocation requests are defined in the CP. Validated certificate revocation requests will be processed no more than 48 hours after receipt. The CP may define a shorter time period for the processing of revocation requests.

Revocation requests for reasons other than key compromise must be placed within a maximum of 72 hours of the event necessitating revocation. In the case of suspected or known private key compromise, a revocation request should be made immediately upon identification of the event.

This root CA's certificate revocation process supports the secure and authenticated revocation of one or more certificates of one or more entities and provides a means of rapid communication of such revocation through the issuance of CRLs published on an as-needed basis. The CA's system and processes provide the capability to revoke (1) the set of all certificates issued by the CA that have been signed with a single CA private signing key or (2) groups of certificates issued by the CA that have been signed with different CA private signing keys.

Upon revocation of the subscriber's certificate, the subscriber is notified by an email.

When a revocation request has been processed by an external registration authority, the external RA is also notified upon the revocation of a subscriber's certificate.

Upon the revocation of a subscriber's certificate, the newly revoked certificate is recorded in a CRL that is published within 24 hours.

4.10. Certificate Suspension

This root CA does not support suspension of (subordinate CA) public key certificates issued thereby.

4.11. Certificate Status

The CA publishes CRLs on an as-needed basis, as certificates are revoked. That is, the CRL is issued with a 'next issuance' date coincident with the expiry date of this root CA's certificate so, upon revocation of one or more subordinate CA certificates, an interim CRL shall be issued within 24 hours.

As stated in the CP, the onus for CRL checking is placed upon relying parties. This CA does not support online certificate status checking (OCSP).

A subscriber is notified of the revocation of his or her certificate by an email, a postal mail, or a telephone. The CP may define other forms of revocation advertisements.

The CA archives and retains all certificates and CRLs issued by the CA for a period not less than ten (10) years.

4.12. Certificate Profiles

This section specifies the profiles of certificates that may be issued directly by this root CA, including its own self-signed certificate.

4.12.1. Root CA Certificate Profile

Issuer (Root) CA Certificate Profile		
Basic Fields	**Value**	
Version	**0x2** *(Version 3)*	
Serial Number	**0** (Integer)	
Signature Algorithm	***SHA1withRSA-Encryption***	
Issuer	DN: C=CA, ST=Ontario, L=Toronto, O=Echoworx Corporation, OU=Certification Services, CN=Echoworx Root CA2	
Validity	**GeneralizedTime** (25 Years) **Not valid before:** *issue date - 1day* **Not valid after:** *issue date + 25yrs + 1day*	
Subject	DN: C=CA, ST=Ontario, L=Toronto, O=Echoworx Corporation, OU=Certification Services, CN=Echoworx Root CA2	
Subject Public Key	***subjectPublicKeyInfo***	
Issuer Unique ID	***BitString***	
Subject Unique ID	***BitString***	
X.509v3 Certificate Extensions		
Extended Attributes[1]	**Critical**	**Value**
Basic Constraints id-ce-basic-constraints	Y	**True**
Key Usage id-ce-keyUsage	N	**keyCertificateSign** **cRLSign**
Subject Key Identifier id-ce-subjectKeyIdentifier	N	*octetString (optional)*
Authority Key Identifier id-ce-authorityKeyIdentifier	N	*octetString (optional)*
Certificate Policy id-ce-certificatePolicy	N	1.3.6.1.4.1.15505.10.1.3.1
Certification Practices Statement id-ce-certificatePolicies + id-qt-cps	N	https://www.echoworx.com/ca/root2/cps.pdf
[1] Refer to RFC-3280 for the definition and specific OID values for extended attributes.		

Table 4: Issuer (Root) CA Certificate Profile

4.12.2. Subordinate CA Certificate Profile

Subject (Subordinate) CA Certificate Profile		
Basic Fields	**Value**	
Version	**0x2** *(Version 3)*	
Serial Number	***UniqueIdentifier*** (Integer)	
Signature Algorithm	***SHA2withRSA-Encryption***	
Issuer	DN: C=CA, ST=Ontario, L=Toronto, O=Echoworx Corporation, OU=Certification Services, CN=Echoworx Root CA2	
Validity	**GeneralizedTime** (10 Years) **Not valid before:** *issue date - 1day* **Not valid after:** *issue date + 10yrs + 1day*	
Subject	DN: C=*CountryCode*, ST=*StateOrProvince*, L=*Locality*, O=*Organization*, OU=*OrganizationalUnit*, CN=*CommonName*	
Subject Public Key	***subjectPublicKeyInfo***	
Issuer Unique ID	***BitString***	
Subject Unique ID	***BitString***	
X.509v3 Certificate Extensions		
Extended Attributes	**Critical**	**Value**
Basic Constraints id-ce-basic-constraints	Y	**True**
Key Usage id-ce-keyUsage	N	**keyCertificateSign** **cRLSign**
Subject Key Identifier id-ce-subjectKeyIdentifier	N	*octetString (optional)*
Authority Key Identifier id-ce-authorityKeyIdentifier	N	*octetString (optional)*
NetScape Certificate Type nsCertType	N	**Object Signing,** **Object Signing CA,** **SSL CA,** **S/MIME CA**
CRL Distribution Points id--ce-crlDistributionPoints	N	https://www.echoworx.com/ca/root2/crl.pem
Certificate Policy id-ce-certificatePolicy	N	1.3.6.1.4.1.15505.10.1.4.c[.e] *where:* *c (class) := 1 (A), 2 (B) or 3 (C)* *e (escrow) := 1 (escrowAllowed) if applicable*
Certification Practices Statement id-ce-certificatePolicies + id-qt-cps	N	https://www.echoworx.com/ca/root2/cps.pdf *(optional; example URL only)*

Table 5: Subject (Subordinate) CA Certificate Profile

4.12.3. End-Entity Certificate Profiles

This root CA does not directly issue end-entity certificates.

4.13. CRL Profile

CRL Certificate Profile	
Basic Fields	**Value**
Version	**0x1** *(Version 2)*
Serial Number	**UniqueIdentifier** (Integer)
Signature Algorithm	***SHA1withRSA-Encryption***
Issuer	DN: C=CA, ST=Ontario, L=Toronto, O=Echoworx Corporation, OU=Certification Services, CN=Echoworx Root CA2
This update	**GeneralizedTime** *Time of CRL issuance*
Next update	**GeneralizedTime** *Time of CA certificate expiry (not valid after date)* (t**hat is**, no fixed publication schedule; only interim CRLs issued on an as-need basis)
List of Revoked Certificates	
Certificate identification information	

Table 6: CRL Certificate Profile

4.14. Integrated Circuit Card (ICC) Life Cycle Management

This root CA does not issue smart cards to subscribers. Subscribers may, at their own discretion, purchase smart cards and readers for purposes of key generation and storage.

5. CA Environmental Controls

This section addresses the business and security controls for assuring integrity and trust in this root CA, including how this CP/CPS document is administered; cessation of operations; handling of sensitive and confidential information; intellectual property; physical security; business continuity and event journaling.

5.1. CP and CPS Administration

Some revisions to this certificate policy and certification practices statement (CP/CPS) and/or related certification policy (CP) documents may be deemed by the CA's policy authority to have minimal or no impact on subscribers and relying parties using certificates and CRLs issued by this root CA. Such revisions may be made without notice to users of the CP/CPS and without changing the version number of this CP/CPS. Revisions to the certificate policies supported by this CP/CPS, as well as revisions to the CP/CPS which are deemed by the CA's policy authority to have significant impact on the users of this CP/CPS, may be made with 30 days' notice to the users and a change in version number for this CP/CPS.

This root CA's policy authority will provide notification of upcoming changes on the CA's website 30 days prior to significant revisions to this CPS.

This CP/CPS and any subsequent changes are approved by the CA's policy authority.

5.2. CA Termination

This root CA can only be terminated by the Echoworx board of directors. In the event this root CA is terminated, all subordinate CA certificates issued under the CA will be revoked and the CA will cease to issue certificates. The CA shall provide no less than a 30-day notice to all business units utilizing the services of the CA. Upon termination, the records of the CA shall be archived and transferred to a designated custodian.

5.3. Confidentiality

Information which is not considered by this root CA to be public domain information is to be kept confidential.

Confidential information includes:

- Subscribers' private signing keys are confidential and are not provided to the CA or RA.
- Information specific to the operation and control of the CA, such as security parameters and audit trails, is maintained confidentially by the CA and is not released outside of the CA organization unless required by law.
- Information about subscribers held by the CA or RAs, excluding that which is published in certificates, CRLs, certificate policies or this CP/CPS, is considered confidential and shall not be released outside of the CA except as required by certificate policy or otherwise required by law.
- Generally, the results of annual audits are kept confidential, unless disclosure is deemed necessary by CA management.

Non-confidential information includes:

- Information included in certificates and CRLs and issued by the CA is not considered confidential.
- Information in the certificate policies supported by this CA is not considered confidential.
- Information in the CA's disclosed CP/CPS is not considered confidential.
- When the CA revokes a certificate, a revocation reason is included in the CRL entry for the revoked certificate. This revocation reason code is not considered confidential and can be shared with all other subscribers and relying parties. However, no other details concerning the revocation are normally disclosed.

The CA shall comply with legal requirements to release information to law enforcement officials.

The CA may disclose to another party information pertaining to the owner of such information upon the owner's request.

5.4. Intellectual Property Rights

Public key certificates and CRLs issued by the CA are the property of Echoworx. This CP/CPS document is the property of Echoworx.

5.5. Security Management

A current information security policy exists, which is approved and endorsed by senior management. It is published as a corporate document and is communicated to the appropriate staff groups via security awareness program.

The policy defines the objectives, scope, intent and principals of information security and measures to ensure compliance with security standards and regulatory requirements.

In particular, the security policy contains an approach to address and meet requirements of the following areas of information security:

- Compliance with regulatory, legislative and contractual requirements
- Guidance for security training requirements of staff
- Computer security to reduce weaknesses and exposures and, for example, to prevent software viruses or malicious software
- Business continuity and responsibility of management and staff
- Compliance enforcement and consequences of policy violations

Information security is managed to establish sustainable compliance with business objectives and with requirements. This includes direction, governance and a review and authorization process.

Management of security addresses also:

- Procedures to sustain physical and logical security in CA facilities and systems despite third-party access
- Risk assessments to identify security implications and security control requirements
- The addressing of security requirements and responsibilities with contracts between parties or in cases of delegation of CA roles and responsibilities

5.6. Asset Classification and Management

Owners are assigned to major CA assets with responsibility to establish and maintain appropriate controls.

Inventories are maintained for important CA assets.

Information classification is implemented reflecting business and information protection needs and provides guidance for labelling and handling to enable compliance with the classification scheme.

5.7. Personnel Security

Security roles and responsibilities, as specified in the organization's security policy, are documented in the job descriptions.

Verification checks on key permanent and contract staff are performed at the time of job application. The CA's policies and procedures specify the background checks and clearance procedures required for the personnel filling the trusted roles and other personnel, including janitorial staff.

Employees sign a confidentiality (non-disclosure) agreement as part of their initial terms and conditions of employment.

Contracted personnel controls include the following:

- Bonding requirements on contract personnel
- Contractual requirements including indemnification for damages due to the actions of the contractor personnel
- Audit and monitoring of contractor personnel

Employee and contracted staff receive appropriate training to raise awareness and achieve compliance with corporate security policies. This training is aligned with clear role-based compliance and training requirements.

A formal disciplinary process exists and is followed for employees who have violated organizational security policies and procedures. The CA's policies and procedures specify the sanctions against personnel for unauthorized actions, unauthorized use of authority and unauthorized use of systems.

Appropriate and timely actions are taken when an employee is terminated so that controls and security are not impaired by such an occurrence.

5.8. Physical Security Controls

All critical CA operations take place within a physically secure facility with at least four layers of security to access sensitive hardware or software. Sensitive system components are physically separated from the organization's other systems so that only authorized employees of the CA can access them.

Physical access to the CA system is strictly controlled and is subject to continuous (24/7) electronic surveillance monitoring. Only trustworthy individuals with a valid business reason are provided such access. The access control system is always functional and, in addition to conventional combination locks, electronic badge readers are used.

All CA systems have industry standard power and air conditioning systems to provide a suitable operating environment.

All CA systems have reasonable precautions taken to minimize the impact of water exposure.

All CA systems have industry standard fire prevention and protection mechanisms in place.

Media storage under the control of the CA is subject to the normal media storage requirements of the company.

Waste is disposed of in accordance with the organization’s normal waste disposal requirements. Cryptographic devices are physically destroyed or zeroized in accordance with the manufacturers’ guidance prior to disposal.

Off-site backups are stored in a secure storage facility by a bonded third-party storage facility.

5.9. Business Continuity Management Controls

The CA has a business continuity and disaster recovery plan to restore the CA’s business operations in a reasonably timely manner following interruption to, or failure of, critical business processes. The CA’s business continuity plan defines 72 hours as an acceptable system outage time in the event of a major natural disaster or CA private key compromise.

Copies of essential business information and CA system software are performed whenever there is a change made to this root CA's off-line system.

The CA maintains a recovery site, which is approximately 15 km apart from the CA’s primary site.

Effectiveness of business and disaster recovery plans are tested at least once a year with appropriate methods.

Controls are in place to detect a compromised CA private signing key or a suspected compromise. Its occurrence is considered a disaster and appropriate measures are taken as defined in the disaster recovery plan.

5.10. Event Logging

As part of this root CA’s system backup procedures, audit trail files are backed up to media prior to shutdown of intermittent operation of the off-line root CA system and thereafter archived by the system administrator.

Event journals are reviewed at least on a monthly basis by CA management. The review must be documented including findings, notifications to senior management, actions taken and issue resolution.

The logged events must be inspected to identify incidents with high severity and to eliminate “false positives”. Events that are considered “high severity” could cause a risk for system availability or represent a security breach or an attempted breach, such as multiple incorrect logons of a user account, attempts of unauthorized access to systems and resources and unauthorized alterations of critical and security related system parameters.

The event logs of Hardware Security Modules are monitored with on-line monitoring software in short time intervals. Detected events are rated and significant events will trigger an email notification sent to alert the CA operations team. The CA operations team reviews the situation in real-time, and performs the necessary steps to notify about and to resolve the problem. Access to the logs is secure and available only to the CA operations team.

6. References

[RFC3280]

Housley, R. et al., *Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile*, Network Working Group Request for Comments: 3280, The Internet Society, April 2002

https://www.rfc-archive.org/getrfc.php?rfc=3280

[WebTrust]

AICPA/CICA WebTrust$^{SM/TM}$ *Program for Certification Authorities, version 1.0,* American Institute of Certified Public Accountants, Inc. and *Canadian Institute of Chartered Accountants,* 2000/08/25

http://www.webtrust.org/homepage-documents/item65306.pdf

7. Appendix

7.1. Root CA2 Certificate

Echoworx Root CA2 Certificate	
MD5 Fingerprint	A9:81:C0:B7:3A:92:50:BC:91:A5:21:FF:3D:47:87:9F
SHA1 Fingerprint	CB:65:82:64:EA:8C:DA:18:6E:17:52:FB:52:C3:97:36:7E:A3:87:BE
PEM Form	-----BEGIN CERTIFICATE----- MIIE5zCCA8+gAwIBAgIBADANBgkqhkiG9w0BAQUFADCBjTELMAkGA1UEBhMCQ0Ex EDAOBgNVBAgTB09udGFyaW8xEDAOBgNVBAcTB1Rvcm9udG8xHTAbBgNVBAoTFEVj aG93b3J4IENvcnBvcmF0aW9uMR8wHQYDVQQLExZDZXJ0aWZpY2F0aW9uIFNlcnZp Y2VzMRowGAYDVQQDExFFY2hvd29yeCBSb290IENBMjAeFw0wNTEwMDYxMDQ5MTNa Fw0zMDEwMDcxMDQ5MTNaMIGNMQswCQYDVQQGEwJDQTEQMA4GA1UECBMHT250YXJp bzEQMA4GA1UEBxMHVG9yb250bzEdMBsGA1UEChMURWNob3dvcnggQ29ycG9yYXRp b24xHzAdBgNVBAsTFkNlcnRpZmljYXRpb24gU2VydmljZXMxGjAYBgNVBAMTEUVj aG93b3J4IFJvb3QgQ0EyMIIBIDANBgkqhkiG9w0BAQEFAAOCAQ0AMIIBCAKCAQEA utU/5BkV15UBf+s+JQruKQxr77s3rjp/RpOtmhHILIiO5gsEWP8MMrfrVEiidjI6 Qh6ans0KAWc2Dw0/j4qKAQzOSyAZgjcdypNTBZ7muv212DA2Pu41rXqwMrlBrVi/ KTghfdLlNRu6JrC5y8HarrnRFSKF1Thbzz921kLDRoCi+FVs5eVuK5LvIfkhNAqA byrTgO3T9zfZgk8upmEkANPDL1+8y7dGPB/d6lk0I5mv8PESKX02TlvwgRSIiTHR k8++iOPLBWlGp7ZfqTEXkPUZhgrQQvxcrwCUo6mk8TqgxCDP5FgPoHFiPLef5szP ZLBJDWp7GLyE1PmkQI6WiwIBA6OCAVAwggFMMA8GA1UdEwEB/wQFMAMBAf8wCwYD VR0PBAQDAgEGMB0GA1UdDgQWBBQ74YEboKs/OyGC1eISrq5QqxSlEzCBugYDVR0j BIGyMIGvgBQ74YEboKs/OyGC1eISrq5QqxSlE6GBk6SBkDCBjTELMAkGA1UEBhMC Q0ExEDAOBgNVBAgTB09udGFyaW8xEDAOBgNVBAcTB1Rvcm9udG8xHTAbBgNVBAoT FEVjaG93b3J4IENvcnBvcmF0aW9uMR8wHQYDVQQLExZDZXJ0aWZpY2F0aW9uIFNl cnZpY2VzMRowGAYDVQQDExFFY2hvd29yeCBSb290IENBMoIBADBQBgNVHSAESTBH MEUGCysGAQQB+REKAQMBMDYwNAYIKwYBBQUHAgEWKGh0dHA6Ly93d3cuZWNob3dv cnguY29tL2NhL3Jvb3QyL2Nwcy5wZGYwDQYJKoZIhvcNAQEFBQADggEBAG+nrPi/ 0RpfEzrj02C6JGPUar4nbjIhcY6N7DWNeqBoUulBSIH/PYGNHYx7/lnJefiixPGE 7TQ5xPgElxb9bK8zoAApO7U33OubqZ7M7DlHnFeCoOoIAZnG1kuwKwD5CXKB2a74 HzcqNnFW0IsBFCYqrVh/rQgJOzDA8POGbH0DeD0xjwBBooAolkKT+7ZItJF1Pb56 QpDL9G+16F7GkmnKlAIYT3QTS3yFGYChnJcd+6txUPhKi9sSOOmAIaKHnkH9Scz+ A2cSi4A3wUYXVatuVNHpRb2lygfH3SuCX9MU8Ure3zBlSU1LALtMqI4JmcQmQpIq zIzvO2jHyu9PQqo= -----END CERTIFICATE-----

Echoworx Root CA2 Certificate	
Text Form	Certificate: Data: Version: 3 (0x2) Serial Number: 0 (0x0) Signature Algorithm: sha1WithRSAEncryption Issuer: C=CA, ST=Ontario, L=Toronto, O=Echoworx Corporation, OU=Certification Services, CN=Echoworx Root CA2 Validity Not Before: Oct 6 10:49:13 2005 GMT Not After: Oct 7 10:49:13 2030 GMT Subject: C=CA, ST=Ontario, L=Toronto, O=Echoworx Corporation, OU=Certification Services, CN=Echoworx Root CA2 Subject Public Key Info: Public Key Algorithm: rsaEncryption RSA Public Key: (2048 bit) Modulus (2048 bit): 00:ba:d5:3f:e4:19:15:d7:95:01:7f:eb:3e:25:0a: ee:29:0c:6b:ef:bb:37:ae:3a:7f:46:93:ad:9a:11: c8:2c:88:8e:e6:0b:04:58:ff:0c:32:b7:eb:54:48: a2:76:32:3a:42:1e:9a:9e:cd:0a:01:67:36:0f:0d: 3f:8f:8a:8a:01:0c:ce:4b:20:19:82:37:1d:ca:93: 53:05:9e:e6:ba:fd:b5:d8:30:36:3e:ee:35:ad:7a: b0:32:b9:41:ad:58:bf:29:38:21:7d:d2:e5:35:1b: ba:26:b0:b9:cb:c1:da:ae:b9:d1:15:22:85:d5:38: 5b:cf:3f:76:d6:42:c3:46:80:a2:f8:55:6c:e5:e5: 6e:2b:92:ef:21:f9:21:34:0a:80:6f:2a:d3:80:ed: d3:f7:37:d9:82:4f:2e:a6:61:24:00:d3:c3:2f:5f: bc:cb:b7:46:3c:1f:dd:ea:59:34:23:99:af:f0:f1: 12:29:7d:36:4e:5b:f0:81:14:88:89:31:d1:93:cf: be:88:e3:cb:05:69:46:a7:b6:5f:a9:31:17:90:f5: 19:86:0a:d0:42:fc:5c:af:00:94:a3:a9:a4:f1:3a: a0:c4:20:cf:e4:58:0f:a0:71:62:3c:b7:9f:e6:cc: cf:64:b0:49:0d:6a:7b:18:bc:84:d4:f9:a4:40:8e: 96:8b Exponent: 3 (0x3) X509v3 extensions: X509v3 Basic Constraints: critical CA:TRUE X509v3 Key Usage: Certificate Sign, CRL Sign X509v3 Subject Key Identifier: 3B:E1:81:1B:A0:AB:3F:3B:21:82:D5:E2:12:AE:AE:50:AB:14:A5:13 X509v3 Authority Key Identifier: keyid:3B:E1:81:1B:A0:AB:3F:3B:21:82:D5:E2:12:AE:AE:50:AB:14:A5:13 DirName:/C=CA/ST=Ontario/L=Toronto/O=Echoworx Corporation/OU=Certification Services/CN=Echoworx Root CA2 serial:00 X509v3 Certificate Policies: Policy: 1.3.6.1.4.1.15505.10.1.3.1

Echoworx Root CA2 Certificate	
	CPS: https://www.echoworx.com/ca/root2/cps.pdf Signature Algorithm: sha1WithRSAEncryption 6f:a7:ac:f8:bf:d1:1a:5f:13:3a:e3:d3:60:ba:24:63:d4:6a: be:27:6e:32:21:71:8e:8d:ec:35:8d:7a:a0:68:52:e9:41:48: 81:ff:3d:81:8d:1d:8c:7b:fe:59:c9:79:f8:a2:c4:f1:84:ed: 34:39:c4:f8:04:97:16:fd:6c:af:33:a0:00:29:3b:b5:37:dc: eb:9b:a9:9e:cc:ec:39:47:9c:57:82:a0:ea:08:01:99:c6:d6: 4b:b0:2b:00:f9:09:72:81:d9:ae:f8:1f:37:2a:36:71:56:d0: 8b:01:14:26:2a:ad:58:7f:ad:08:09:3b:30:c0:f0:f3:86:6c: 7d:03:78:3d:31:8f:00:41:a2:80:28:96:42:93:fb:b6:48:b4: 91:75:3d:be:7a:42:90:cb:f4:6f:b5:e8:5e:c6:92:69:ca:94: 02:18:4f:74:13:4b:7c:85:19:80:a1:9c:97:1d:fb:ab:71:50: f8:4a:8b:db:12:38:e9:80:21:a2:87:9e:41:fd:49:cc:fe:03: 67:12:8b:80:37:c1:46:17:55:ab:6e:54:d1:e9:45:bd:a5:ca: 07:c7:dd:2b:82:5f:d3:14:f1:4a:de:df:30:65:49:4d:4b:00: bb:4c:a8:8e:09:99:c4:26:42:92:2a:cc:8c:ef:3b:68:c7:ca: ef:4f:42:aa

Table 7: Echoworx Root CA2 Certificate

7.2. Definition of Terms

Term	Definition
Administrator	An individual who performs administrative functions within an Echoworx Security Services deployment.
Certificate	An electronic document that is made up of a public key and a digital signature.
Certificate Authority (CA)	An entity that issues digital certificates to end-entities.
Echoworx Security Services (ESS)	The Echoworx applications that interoperate with a Certificate Authority to enable certificate issuance and management in an environment for use with end-user applications for encryption and/or digital signing of documents and email.
Key Authority	An administrative user whose function is to act as part of a trusted group authorized to retrieve subscriber keys that have been escrowed.
Key Escrow	Key Escrow is a means of securely holding subscriber key material for retrieval by an authorized third party.
MIME	MIME stands for Multipurpose Internet Mail Extensions. MIME is the standard used for defining the format of internet mail messages (that is, email).
Policy Object Identifier (Policy OID)	A Policy OID is a unique number used to name and identify the Policy under which a certificate is issued. The inclusion of an issuance policy object identifier in an issued certificate indicates that the certificate was issued in a manner that meets the issuance requirements associated with the defined issuance policy object identifier.
Private Key	A digital key held by an individual or end-entity used for decrypting documents that have been encrypted for them with a corresponding public key and/or for digitally signing documents.
Public Key	A digital key that corresponds to a private key belonging to an individual that is used for encrypting a document for that individual and/or for verifying their digital signature on a document.
Public Key Infrastructure (PKI)	A PKI is a technical infrastructure that is used to bind a private key to an identity through the issuance of a digital certificate by a trusted third party (a CA).

Term	Definition
Root CA	A certification authority that sits at the top of a CA hierarchy or PKI.
S/MIME	S/MIME stands for Secure Multipurpose Internet Mail Extensions, and is a standard for the application of public key cryptography to email messages encapsulated in the MIME format.
Subordinate CA	A Certificate Authority that is part of a CA hierarchy below a Root CA.
Subscriber	An individual who subscribes for a service.

Table 8: Definition of Terms

ECHOWORX™

IT PAYS TO BE SECURE

Echoworx protects the privacy of people and businesses throughout the world by making email data protection easier. Our customizable email encryption platform helps organizations easily share protected email, statements, and documents from anywhere and from any device. Our passionate encryption experts transform communication chaos into order for world leading organizations who understand — it pays to be secure.

Encryption is an investment in brand, maximizing competitive advantage.

Clients in 30 countries use Echoworx and more than 5,000 business, public sector, and institutional deployments are serviced through our data centers in the U.S., Canada, Germany, Ireland, and the U.K.

For more information www.echoworx.com/contact-us