

ARX Certification Practice Statement

January 15, 2008

Version 1.0



Simple
Valuable
Affordable

Table of Contents

Terms and Acronyms Used in the CPS	4
1. General	5
1.1 ARX	5
1.2 ARX CPS	5
1.3 CPS Suitability, Amendments and Publication	5
1.4 Liability of ARX	6
1.5 Compliance with applicable standards	6
1.6 Digital Certificate Policy Overview	6
1.7 ARX PKI Hierarchy	6
1.8 ARX Certification Authority	6
1.10 Subscribers	6
1.11 Relying Parties	7
2. Technology	7
2.1 ARX CA Infrastructure	7
2.2 Digital Certificate Management	8
2.3 ARX Directories, Repository and Certificate Revocation Lists	8
2.4 Types of ARX Certificates	8
2.5 Extensions and Naming	8
2.6 Subscriber Private Key Generation Process	9
2.7 Subscriber Private Keys Protection and Backup	9
2.8 Subscriber Public Key Delivery to ARX	9
2.9 Delivery of Issued Subscriber Certificate to Subscriber's End Users	9
2.12 ARX Certificates Profile	9
3. Organization	11
3.1 Conformance to this CPS	11
3.2 Termination of CA Operations	11
3.3 Form of Records	11
3.4 Records Retention Period	11
3.5 Logs for Core Functions	12
3.6 Business Continuity Plans and Disaster Recovery	13
3.7 Availability of Revocation Data	13
3.8 Publication of Critical Information	13
3.9 Confidential Information	13
3.10 Personnel Management and Practices	14
3.11 Privacy Policy	15
3.12 Publication of information	15
4. Practices and Procedures	15
4.1 Certificate Application Requirements	15
4.2 Application Validation	16
4.4 Validation Requirements for Certificate Applications	16
4.5 Time to Confirm Submitted Data	17
4.6 Approval and Rejection of Certificate Applications	17
4.7 Certificate Issuance and Subscriber Consent	17
4.8 Certificate Validity	17
4.9 Certificate Acceptance by Subscribers	17
4.10 Verification of Digital Signatures	17
4.11 Reliance on Digital Signatures	17
4.12 Certificate Suspension	18
4.13 Certificate Revocation	18
5. Legal Conditions of Issuance	19

Digital Signatures That Keep Your Business Moving

5.1 ARX Representations	19
5.2 Information Incorporated by Reference into a ARX Digital Certificate	19
5.3 Displaying Liability Limitations, and Warranty Disclaimers	19
5.4 Publication of Certificate Revocation Data	19
5.5 Duty to Monitor the Accuracy of Submitted Information	19
5.6 Publication of Information	19
5.7 Interference with ARX Implementation	19
5.8 Standards	20
5.9 ARX Partnerships Limitations	20
5.11 Choice of Cryptographic Methods	20
5.12 Reliance on Unverified Digital Signatures	20
5.13 Rejected Certificate Applications	20
5.14 Refusal to Issue a Certificate	20
5.15 Subscriber Obligations	20
5.16 Representations by Subscriber upon Acceptance	21
5.17 Indemnity by Subscriber	22
5.19 Obligations of a Relying Party	22
5.20 Legality of Information	22
5.21 Subscriber Liability to Relying Parties	22
5.22 Duty to Monitor Agents	23
5.23 Use of Agents	23
5.24 Conditions of usage of the ARX Repository and Web site	23
5.25 Accuracy of Information	23
5.26 Obligations of ARX	23
5.27 Fitness for a Particular Purpose	24
5.28 Other Warranties	24
5.29 Non-Verified Subscriber Information	24
5.30 Exclusion of Certain Elements of Damages	24
5.33 Damage and Loss Limitations	25
5.34 Conflict of Rules	25
5.35 ARX Intellectual Property Rights	25
5.36 Infringement and Other Damaging Material	25
5.37 Ownership	25
5.38 Governing Law	26
5.39 Jurisdiction	26
5.40 Dispute Resolution	26
5.41 Successors and Assigns	26
5.42 Severability	26
5.43 Interpretation	26
5.44 No Waiver	27
5.45 Notice	27
5.46 Fees	27
6. General Issuance Procedure	27
6.1 General - ARX	27
6.2 Certificate Issuance	27
6.3 Content	28
6.4 Time to Confirm Submitted Data	28
6.5 Issuing Procedure	28

Terms and Acronyms Used in the CPS

Acronyms:

CA	Certificate Authority
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
EPKI	Enterprise Public Key Infrastructure Manager
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Standardization Sector
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure (based on X.509 Digital Certificates)
PKCS	Public Key Cryptography Standard
URL	Uniform Resource Locator
X.509	The ITU-T standard for Certificates and their corresponding authentication framework

Terms:

Applicant:	The Applicant is an Organization applying for Certificates on behalf of its End Users.
Certificate Policy:	The Certificate Policy is a statement of the issuer that corresponds to the prescribed usage of a digital certificate within an issuance context.
CoSign:	CoSign is a non-forgable, simple-to-use digital signature appliance.
End User/Individual:	The End User/Individual is an employee of an Organization or its affiliate.
Organization:	Organization is a Customer who had purchased a CoSign.
Relying Party Agreement:	The Relying Party Agreement is an agreement that must be read and accepted by a Relying Party prior to validating, relying on or using a Certificate and is available for reference at www.arx.com/documents/cps.php .
Relying Party:	The Relying Party is an entity that relies upon the information contained within the Certificate.
Subscriber Agreement:	The Subscriber Agreement is an agreement that must be read and accepted by an Applicant before applying for Certificates. The Subscriber Agreement is specific to the Digital Certificate product type and is available for reference at www.arx.com/documents/cps.php .
Subscriber:	The Subscriber is an Organization whose End-Users have been issued certificates.

1. General

This document is the ARX Certification Practice Statement (CPS) and outlines the legal, commercial and technical principles and practices that ARX employ in providing certification services that include, but are not limited to, approving, issuing, using and managing of Digital Certificates and in maintaining a X.509 Certificate based public key infrastructure (PKIX) in accordance with the Certificate Policies determined by ARX. It also defines the underlying certification processes for Subscribers and describes ARX's repository operations. The CPS is also a means of notification of roles and responsibilities for parties involved in Certificate based practices within the ARX PKI.

1.1 ARX

ARX is a Certification Authority (CA) that issues high quality and highly trusted standard digital certificates to entities including private and public companies and individuals in accordance with this CPS. In its role as a CA, ARX performs functions associated with public-key operations that include receiving requests, issuing, revoking and renewing a digital certificate and the maintenance, issuance and publication of Certificate Revocation Lists (CRLs) for users within the ARX PKI.

1.2 ARX CPS

The ARX CPS is a public statement of the practices of ARX and the conditions of issuance, revocation and renewal of a certificate issued under ARX's own hierarchy. Pursuant to the division of the tasks of a CA, this CPS is largely divided in the following sections: Technical, Organizational, Practices and Legal.

The ARX Certificate Policy Authority maintains this CPS, related agreements and Certificate policies referenced within this document. The Certificate Policy Authority may be contacted at the address below:

ARX Certificate Policy Authority
855 Folsom St. Suite 939
San Francisco, CA. 49107
USA
Attention: Legal Practices
Email: legal@arx.com

This CPS, related agreements and Certificate policies referenced within this document are available online at: www.arx.com/documents/cps.php.

1.3 CPS Suitability, Amendments and Publication

The ARX Certificate Policy Authority is responsible for determining the suitability of certificate policies illustrated within the CPS. The Authority is also responsible for determining the suitability of proposed changes to the CPS prior to the publication of an amended edition. Upon the Certificate Policy Authority accepting such changes deemed by the CA's Policy Authority to have significant impact on the users of this CPS an updated edition of the CPS will be published at the ARX repository (available at www.arx.com/documents/cps.php), with thirty days notice given of upcoming changes and suitable incremental version numbering used to identify new editions.

Revisions not denoted "significant" are those deemed by the CA's Policy Authority to have minimal or no impact on subscribers and relying parties using certificates and CRLs issued by the CA. Such revisions may be made without notice to users of the CPS and without changing the version number of this CPS.

Controls are in place to reasonably ensure that the ARX CPS is not amended and published without the prior authorization of the Certificate Policy Authority.

1.4 Liability of ARX

For legal liability of ARX under the provisions made in this CPS, please refer to Section 5.

1.5 Compliance with applicable standards

The practices specified in this CPS have been designed to meet or exceed the requirements of generally accepted and developing industry standards.

1.6 Digital Certificate Policy Overview

A digital certificate is formatted data that cryptographically binds an identified Subscriber's End-User with a public key. A digital certificate allows an End User/Individual taking part in an electronic transaction to prove their identity to other participants in such a transaction. Digital certificates are used in commercial environments as a digital equivalent of an identification card.

1.7 ARX PKI Hierarchy

UTN-USERFirst-Client Authentication and Email (serial number = 44 be 0c 8b 50 00 24 b4 11 d3 36 25 25 67 C9 89, expiry = 09 July 2019 17:36:58)

↳ CoSign Certificate Authority by ARX (serial number = 4E FA BB 32 A3 0D 00 A4 EB DC 13 03 C0 3C 5C BB, expiry = 09 July 2019 17:36:58)

↳ End User Certificate (serial number = x, expiry = 1 year from issuance)]

1.8 ARX Certification Authority

In its role as a Certification Authority (CA) ARX provides certificate services within the ARX PKI. The ARX CA will:

Conform its operations to the CPS (or other CA business practices disclosure), as the same may from time to time be modified by amendments published in the ARX repository www.arx.com/documents/cps.php.

Issue and publish certificates in a timely manner in accordance with the issuance times set out in this CPS.

Upon receipt of a valid request from the CoSign appliance to revoke a certificate, using the revocation methods detailed in this CPS, revoke a certificate issued for use within the ARX PKI.

Publish CRLs on a regular basis, in accordance with the applicable Certificate Policy and with provisions described in this CPS.

Distribute issued certificates in accordance with the methods detailed in this CPS.

Update CRLs in a timely manner as detailed in this CPS.

1.10 Subscribers

Subscribers of ARX certification services are Organizations that use PKI in relation with transactions and communications. Subscribers' End Users are parties that are identified in their certificates and have sole control of the private keys corresponding to the public keys listed in the certificates. Prior to verification of identity and issuance of End-Users' certificates, a Subscriber is an applicant for the services of ARX.

1.11 Relying Parties

Relying parties use PKI services in relation with ARX certificates and reasonably rely on such certificates and/or digital signatures when verified by reference to a public key listed in a Subscriber End User's certificate.

To verify the validity of a digital certificate the relying party must refer to the Certificate Revocation List (CRL) prior to relying on information in any certificate to ensure that ARX has not revoked the certificate. The CRL location is detailed within the certificate.

2. Technology

This section addresses certain technological aspects of the ARX infrastructure and PKI services.

2.1 ARX CA Infrastructure

The ARX CA Infrastructure uses trustworthy systems to provide certificate services. A trustworthy system is computer hardware, software and procedures that provide an acceptable resilience against security risks, a reasonable level of availability, reliability, correct operation, and enforce the security policy.

2.1.1 Root CA Signing Key Protection & Recovery

Protection of the CA Intermediate Root ("Sub Root") signing key pairs is ensured with the use of IBM 4578 cryptographic coprocessor devices, which are certified to FIPS 140-1 Level 4, for key generation, storage and use. The CA Sub Root signing key pairs are 2048 bit and were generated within the IBM 4578 device.

For CA Sub Root key recovery purposes, the Sub Root CA signing keys are encrypted and stored within a secure environment. The decryption key is split across m removable media and requires n of m to reconstruct the decryption key. Custodians in the form of two or more authorized officers are required to physically retrieve the removable media from the distributed physically secure locations.

Where CA Sub Root signing keys are backed up to another cryptographic hardware security module, such keys are transferred between devices in encrypted format only.

2.1.2 CA Root Signing Key Generation Process

ARX securely generates and protects its private key(s), and takes necessary precautions to prevent the compromise or unauthorized usage of it.

The ARX CA Sub Root key was generated in accordance with the guidelines detailed in the Root Key Generation Ceremony Reference of the Comodo CA CPS located at:

www.comodogroup.com/repository/Comodo_WT_CPS.pdf. The related activities and the personnel involved in the Sub Root Key Generation Ceremony are recorded for audit purposes. Subsequent Sub Root Key Generation Ceremonies are to follow the documented reference guide also.

2.1.3 CA Root Signing Key Archival

When any CA Sub Root Signing Key pair expires, they will be archived for at least 7 years. The keys will be archived in a secure cryptographic hardware module, as per their secure storage prior to expiration, as detailed herein.

2.1.4 CA Root Public Key Delivery to Subscribers

ARX makes its CA Sub Root Certificate available online at crt.arx.com/CoSignCertificateAuthoritybyARX.crt.

The full certificate chain (see section 1.7 of this CPS) is available to Subscriber's End-Users by means of the AIA (Authority Information Access) certificate extension.

2.2 Digital Certificate Management

ARX certificate management refers to functions that may include but are not limited to the following:

- ▶▶ Verification of the identity of an Applicant.
- ▶▶ Authorizing the issuance of certificates.
- ▶▶ Issuance of certificates.
- ▶▶ Revocation of certificates.
- ▶▶ Listing of certificates.
- ▶▶ Distributing certificates.
- ▶▶ Publishing certificates.
- ▶▶ Storing certificates.
- ▶▶ Retrieving certificates in accordance with their particular intended use.

2.3 ARX Directories, Repository and Certificate Revocation Lists

ARX manages and makes publicly available directories of revoked certificates using Certificate Revocation Lists (CRLs). All CRLs issued by ARX are X.509 v2 CRLs, in particular as profiled in IETF RFC 3280. Users and relying parties are strongly urged to consult the directories of revoked certificates at all times prior to relying on information featured in a certificate. ARX updates and publishes a new CRL every 24 hours or more frequently under special circumstances. The CRL for certificates can be accessed via the following URL: crl.arx.com/CoSignCertificateAuthorityARX.crl

ARX also publishes a repository of legal notices regarding its PKI services, including this CPS, agreements and notices, references within this CPS as well as any other information it considers essential to its services. The ARX legal repository may be accessed at www.arx.com/documents/cps.php.

2.4 Types of ARX Certificates

ARX currently offers digital certificates and related products that can be used in a way that addresses the needs of users for secure personal and business electronic signatures.

ARX may update or extend its list of products, including the types of certificates it issues, as it sees fit. The publication or updating of the list of ARX products creates no claims by any third party. Upon the inclusion of a new certificate product in the ARX hierarchy, an amended version of this CPS will be made public within two days on the official ARX websites.

Suspended or revoked certificates are appropriately referenced in CRLs and published in ARX directories. ARX does not perform escrow of any Subscriber's End-Users' private keys.

2.4.1 ARX Secure Electronic Signature Certificates

ARX makes available Secure Electronic Signature Certificates that in combination with an appropriate application allow End Users to digitally sign documents and data for relying parties.

2.5 Extensions and Naming

2.5.1 Digital Certificate Extensions

ARX uses the International Telecommunications Union (ITU) standard X.509 version 3 for digital certificates to construct digital certificates for use within the ARX PKI. X.509 v3 allows a CA to add certain certificate

extensions to the basic certificate structure. ARX uses a number of certificate extensions for the purposes intended by X.509 v3 as per Amendment 1 to ISO/IEC 9594-8, 1995.

2.6 Subscriber Private Key Generation Process

The Subscriber's CoSign is responsible for the generation of the private key used in the certificate request. The ARX CA does not provide key generation, escrow, recovery or backup facilities.

Upon making a certificate request, the Subscriber's CoSign is responsible for the generation of an RSA key pair. The Subscriber's CoSign will be required to submit a public key and other details in the form of a Certificate Signing Request (CSR).

2.7 Subscriber Private Keys Protection and Backup

The Subscriber's CoSign is responsible for protection of the Organization End-Users' private keys. The ARX CA maintains no involvement in the generation, protection or distribution of such keys.

2.8 Subscriber Public Key Delivery to ARX

Secure Electronic Signature Certificate requests are generated by the CoSign appliance and submitted to the ARX CA in the form of a PKCS#10 Certificate Signing Request (CSR). The CoSign appliance makes its submission automatically.

2.9 Delivery of Issued Subscriber Certificate to Subscriber's End Users

Upon issuance of a Secure Electronic Signature Certificate, it is delivered directly to the requesting CoSign appliance.

2.12 ARX Certificates Profile

A Certificate profile contains fields as specified below:

2.12.1 Key Usage extension field

ARX certificates are general purpose and may be used without restriction on geographical area or industry. In order to use and rely on an ARX certificate the relying party must use X.509 v3 compliant software. ARX certificates include key usage extension fields to specify the purposes for which the certificate may be used and to technically limit the functionality of the certificate when used with X.509 v3 compliant software. Reliance on key usage extension fields is dependent on correct software implementations of the X.509 v3 standard and is outside of the control of ARX.

The possible key purposes identified by the X.509v3 standard are the following:

- a. Digital signature, for verifying digital signatures that have purposes other than those identified in b), f) or g), that is, for entity authentication and data origin authentication with integrity;
- b. Non-repudiation, for verifying digital signatures used in providing a non-repudiation service which protects against the signing entity falsely denying some action (excluding certificate or CRL signing, as in f) or g) below);
- c. Key encipherment, for enciphering keys or other security information, e.g. for key transport;
- d. Data encipherment, for enciphering user data, but not keys or other security information as in c) above;
- e. Key agreement, for use as a public key agreement key;
- f. Key certificate signing, for verifying a CA's signature on certificates, used in CA certificates only;

- g. CRL signing, for verifying a CA's signature on CRLs;
- h. Encipher only, public key agreement key for use only in enciphering data when used with key agreement;
- i. Decipher only, public key agreement key for use only in deciphering data when used with key agreement.

2.12.2 Extension Criticality Field

The Extension Criticality field denotes two separate uses for the Key Usage field. If the extension is noted as critical, then the key in the certificate is only to be applied to the stated uses. To use the key for another purpose in this case would break the issuer's policy. If the extension is not noted as critical, the Key Usage field is simply there as an aid to help applications find the proper key for a particular use.

2.12.3 Basic Constraints Extension

The Basic Constraints extension specifies whether the subject of the certificate may act as a CA or only as an end-user. Reliance on basic constraints extension field is dependent on correct software implementations of the X.509 v3 standard and is outside of the control of ARX.

2.12.4 Certificate Policy (CP)

Certificate Policy (CP) is a statement of the issuer that corresponds to the prescribed usage of a digital certificate within an issuance context. A policy identifier is a number unique within a specific domain that allows for the unambiguous identification of a policy, including a certificate policy.

The Specific ARX certificate profile is as per the table below:

ARX Secure Electronic Signature Certificate	
Signature Algorithm	sha1RSA
Issuer	CN CoSign Certificate Authority by ARX
	OU The CoSign Trust Network
	OU www.arx.com
	O ARX (Algorithmic Research)
	C US
Validity	1 year
Subject	CN
	O
	E
Authority Key Identifier	e4 d8 4e 6d 95 57 c3 6f 4a 15 4c 2f c2 b0 5b dc 0b 57 ef 9c
Key Usage (non-critical)	Digital Signature, Non-Repudiation, Key Encipherment, Data Encipherment (f0)
Netscape Certificate Type	SSL Client Authentication, SMIME (a0)
Basic Constraint	Subject Type=End Entity Path Length Constraint=None

Certificate Policies	http://www.arx.com/documents/cps.php
CRL Distribution Points	http://crl.arx.com/CoSignCertificateAuthoritybyARX.crl
Thumbprint Algorithm	sha1
Thumbprint	2B82 A358 F9E7 9813 924D 5F26 F4B5 EC36 6E91 6323

3. Organization

ARX operates within various operation sites. All sites operate under a security policy designed to, within reason, detect, deter and prevent unauthorized logical or physical access to CA related facilities.

This section of the CPS outlines the security policy, physical and logical access control mechanisms, service levels and personnel policy in use to provide trustworthy and reliable CA operations.

3.1 Conformance to this CPS

ARX conforms to this CPS and other obligations it undertakes through adjacent contracts when it provides its services.

3.2 Termination of CA Operations

In case of termination of CA operations for any reason whatsoever, ARX will provide timely notice and transfer of responsibilities to succeeding entities, maintenance of records, and remedies. Before terminating its own CA activities, ARX will take the following steps, where possible:

- ▶ Providing subscribers of valid certificates with ninety (90) days notice of its intention to cease acting as a CA;
- ▶ Revoking all certificates that are still un-revoked or un-expired at the end of the ninety (90) day notice period without seeking Subscriber's consent;
- ▶ Giving timely notice of revocation to each affected Subscriber;
- ▶ Making reasonable arrangements to preserve its records according to this CPS;
- ▶ Reserving its right to provide succession arrangements for the re-issuance of certificates by a successor CA that has all relevant permissions to do so and complies with all necessary rules, while its operation is at least as secure as ARX's.

The requirements of this article may be varied by contract, to the extent that such modifications affect only the contracting parties.

3.3 Form of Records

ARX retains records in electronic or in paper-based format for a period detailed in section 3.4 of this CPS. ARX may require Subscribers to submit appropriate documentation in support of a certificate application.

3.4 Records Retention Period

ARX retains the records of ARX digital certificates and the associated documentation for a term of no less than 7 years. The retention term begins on the date of expiration or revocation. Copies of certificates are

held, regardless of their status (such as expired or revoked). Such records may be retained in electronic, in paper-based format or any other format that ARX may see fit.

Such records are archived at a secure off-site location and are maintained in a form that prevents unauthorized modification, substitution or destruction.

3.5 Logs for Core Functions

For audit purposes, ARX maintains electronic or manual logs of the following events for core functions. All logs are backed up on removable media and the media held at a secure off-site location on a daily basis. These media are only removed by ARX staff on a visit to the data centre, and when not in the data centre are held either in a safe in a locked office within the development site, or off-site in a secure storage facility.

An audit log is maintained of each movement of the removable media. Logs are archived by the system administrator on a weekly basis and event journals reviewed on a weekly basis by CA management. Both current and archived logs are maintained in a form that prevents unauthorized modification, substitution or destruction. When the removable media reaches the end of its life it is wiped by a third party secure data destruction facility and the certificates of destruction are archived.

All logs include the following elements:

- ▶▶ Date and time of entry
- ▶▶ Serial or sequence number of entry
- ▶▶ Method of entry
- ▶▶ Source of entry
- ▶▶ Identity of entity making log entry

3.5.1 CA & Certificate Lifecycle Management

CA Root signing key functions, including key generation, backup, recovery and destruction

Subscriber's End-User's certificate life cycle management, including successful and unsuccessful certificate requests, certificate issuances, certificate re-issuances and certificate renewals

Subscriber's End-User's certificate revocation requests, including revocation reason

Certificate Revocation List updates, generations and issuances

Custody of keys and of devices and media holding keys

Compromise of a private key

3.5.2 Security Related Events

System downtime, software crashes and hardware failures

CA system actions performed by ARX personnel, including software updates, hardware replacements and upgrades

Cryptographic hardware security module events, such as usage, de-installation, service or repair and retirement

Successful and unsuccessful ARX PKI access attempts

Secure CA facility visitor entry and exit

3.5.3 Certificate Application Information

The documentation and other related information presented by the applicant as part of the application validation process

Storage locations, whether physical or electronic, of presented documents

3.5.4 Log Retention Period

ARX maintains logs for a period of 7 years, or as necessary to comply with applicable laws.

3.6 Business Continuity Plans and Disaster Recovery

To maintain the integrity of its services ARX implements, documents and periodically tests appropriate contingency and disaster recovery plans and procedures. Such plans are revised and updated as may be required at least once a year.

ARX operates a fully redundant CA system. The backup CA is readily available in the event that the primary CA should cease operation. All of its critical computer equipment is housed in a co-location facility run by a commercial data-centre, and all of the critical computer equipment is duplicated within the facility. Incoming power and connectivity feeds are duplicated. The duplicate equipment is ready to take over the role of providing the implementation of the CA, and allows us to specify a maximum system outage time (in case of critical systems failure) of 1 hour.

Backup of critical CA software is performed weekly and is stored offsite.

Backup of critical business information is performed daily and is stored offsite.

ARX operations are distributed across several sites world wide. All sites offer facilities to manage the lifecycle of a certificate, including but not limited to the application, issuance, revocation and renewal of such certificates.

As well as a fully redundant CA system, ARX maintains provisions for the activation of a backup CA and a secondary site should the primary site suffer a total loss of systems. This disaster recovery plan states that ARX will endeavor to minimize interruptions to its CA operations.

3.7 Availability of Revocation Data

ARX publishes Certificate Revocation Lists (CRLs) to allow relying parties to verify a digital signature made using an ARX issued digital certificate. Each CRL contains entries for all revoked un-expired certificates issued and is valid for 24 hours. ARX issues a new CRL every 24 hours and includes a monotonically increasing sequence number for each CRL issued. Under special circumstances, ARX may publish new CRLs prior to the expiry of the current CRL. All expired CRLs are archived (as described in section 3.4 of this CPS) for a period of 7 years or longer if applicable. ARX does not support OCSP (Online Certificate Status Protocol).

3.8 Publication of Critical Information

ARX publishes this CPS, certificate terms and conditions, the relying party agreement and copies of all subscriber agreements in the official ARX repository at www.arx.com/documents/cps.php. The ARX Certificate Policy Authority maintains the ARX repository. All updates, amendments and legal promotions are logged in accordance with the logging procedures referenced in section 3.5 of this CPS.

3.9 Confidential Information

ARX observes applicable rules on the protection of personal data deemed by law or the ARX privacy policy (see section 3.11 of this CPS) to be confidential.

3.9.1 Types of Information deemed as Confidential

ARX keeps the following types of information confidential and maintains reasonable controls to prevent the exposure of such records to non-trusted personnel.

Subscriber agreements.

Certificate application records and documentation submitted in support of certificate applications whether successful or rejected.

Transaction records and financial audit records.

External or internal audit trail records and reports, except for WebTrust audit reports that may be published at the discretion of ARX.

Contingency plans and disaster recovery plans.

Internal tracks and records on the operations of ARX infrastructure, certificate management and enrolment services and data.

3.9.2 Types of Information not deemed as Confidential

Subscribers acknowledge that revocation data of all certificates issued by the ARX CA is public information is published every 24 hours. Subscriber application data marked as “Public” in the relevant subscriber agreement and submitted as part of a certificate application is published within an issued digital certificate in accordance with section 2.12.4 of this CPS.

3.9.3 Access to Confidential Information

All personnel in trusted positions handle all information in strict confidence.

3.9.4 Release of Confidential Information

ARX is not required to release any confidential information, unless as otherwise required by law, without an authenticated, reasonably specific request by an authorized party specifying:

- ▶▶ The party to whom ARX owes a duty to keep information confidential.
- ▶▶ The party requesting such information.
- ▶▶ A court order, if any.

3.10 Personnel Management and Practices

Consistent with this CPS ARX follows personnel and management practices that provide reasonable assurance of the trustworthiness and competence of their employees and of the satisfactory performance of their duties.

3.10.1 Trusted roles

Trusted roles relate to access to the ARX account management system, with functional permissions applied on an individual basis. Senior members of the management team decide permissions, with signed authorizations being archived.

Trusted personnel must identify and authenticate themselves to the system before access is granted. Identification is via a username, with authentication requiring a password and digital certificate.

3.10.2 Personnel controls

All trusted personnel have background checks before access is granted to ARX’s systems. Training of personnel is undertaken via a mentoring process involving senior members of the team to which they are attached.

3.11 Privacy Policy

ARX has implemented a privacy policy, which complies with this CPS. The ARX privacy policy is published at the ARX repository at www.arx.com/documents/cps.php.

3.12 Publication of information

The ARX certificate services and the ARX repository are accessible through several means of communication:

On the web: www.arx.com/documents/cps.php

By email from legal@arx.com

and by mail from:

ARX Inc.
Attention: Legal Practices,
855 Folsom St. Suite 939
San Francisco, CA. 49107
USA
Tel: (415) 839 8161
Fax: (415) 723 7110

4. Practices and Procedures

This section describes the certificate application process, including the information required to make and support a successful application.

4.1 Certificate Application Requirements

All Certificate Applicants (organizations) must complete the enrollment process, which includes:

- ▶ Submit to ARX a certificate application, including application information as detailed in this CPS, and agree to the terms of the relevant subscriber agreement
- ▶ Provide proof of identity through the submission of official documentation as requested by ARX during the enrolment process

Certificate applications are submitted to ARX. The following list details the process involved in processing certificate applications.

The customer (an organization) will enter into an agreement with ARX that will specify the following:

- ▶ The customer's role will include requesting and authorizing certificate requests on behalf of the customer organization's End Users.
- ▶ Such requests and authorizations will be sent directly by the CoSign appliance installed by the customer to the ARX PKI.
- ▶ The certificate request shall demonstrate to ARX ownership of the private key half of the End-User's key pair through the submission of a valid PKCS#10 Certificate Signing Request (CSR).

- ▶ The CoSign appliance will issue the above mentioned requests and authorizations only as a response to an action in an IT system it synchronizes with.
- ▶ The customer is committed to allow only authorized and properly trained individuals (administrators) to manage those IT systems.
- ▶ The customer acknowledges that the acts of defining a new user, deleting a user, or modifying user details in the aforementioned IT systems by an administrator constitutes a request and authorization by the customer for a new certificate to be issued or revoked as appropriate.
- ▶ The customer takes on the responsibility to make sure that user records created and managed in its IT system are accurate (specifically user name and email address) and are directly and properly mapped to persons.
- ▶ The customer is responsible to implement a credential management policy which aims to ensure that only the authorized person has access to the credentials required to access the CoSign appliance for the purpose of generating digital signatures using their issued certificate.
- ▶ Specifying and implementing a procedure and policy for validating the identity of persons and of credential issuance in order to comply with the above requirements, is the sole responsibility of the customer.

4.2 Application Validation

Prior to issuing certificates, ARX employs controls to validate the identity of the Subscriber information featured in the application.

4.2.1 Secure Electronic Signature Certificates

The customer will first supply to ARX the following documents and/or information:

- ▶ The name to be used in the Organization portion of the distinguished name in the subject attribute in all certificates issued to its users
- ▶ The email address domain(s) suffix to be used in all email addresses included in all certificates issued to its users.
- ▶ Documentation to prove the ownership of the above domain names and of rights to use the Organization name requested.

ARX will validate the supplied documents, and will then issue a credential to the customer which will be loaded into the customer's CoSign appliance for the purpose of authenticating the CoSign to the ARX CA as belonging to the specific customer and authorized to issue requests on its behalf.

4.4 Validation Requirements for Certificate Applications

In all types of ARX certificates, the Subscriber has a continuous obligation to monitor the accuracy of the submitted information and notify ARX of any changes that would affect the validity of any certificate. Failure to comply with the obligations as set out in the subscriber agreement will result in the revocation of the Subscriber's Digital Certificates without further notice to the Subscriber and the Subscriber shall pay any Charges payable but that have not yet been paid under the Agreement.

4.4.1 Serial Number Assignment

ARX assigns certificate serial numbers that appear in ARX certificates. Assigned serial numbers are unique.

4.5 Time to Confirm Submitted Data

ARX makes reasonable efforts to confirm certificate application information and issue digital certificates within reasonable time frames.

4.6 Approval and Rejection of Certificate Applications

Following successful completion of all required validations of a certificate application ARX approves an application for digital certificates.

If the validation of a certificate application fails, ARX rejects the certificate application. ARX reserves its right to reject applications to issue certificates to applicants if, on its own assessment, by issuing certificates to such parties the good and trusted name of ARX might get tarnished, diminished or have its value reduced and under such circumstances may do so without incurring any liability or responsibility for any loss or expenses arising as a result of such refusal.

Applicants whose applications have been rejected may subsequently re-apply.

4.7 Certificate Issuance and Subscriber Consent

ARX issues certificates upon approval of a certificate application. A digital certificate is deemed to be valid at the moment a subscriber accepts it (refer to section 4.9 of this CPS). Issuing digital certificates means that ARX accepts the certificate application.

4.8 Certificate Validity

Certificates are valid upon issuance by ARX and acceptance by the subscriber. Generally, the certificate validity period will be 1, 2 or 3 years, however ARX reserves the right to offer validity periods outside of this standard validity period.

4.9 Certificate Acceptance by Subscribers

An issued certificate is delivered directly to the CoSign appliance. A subscriber is deemed to have accepted a certificate when:

- ▶▶ The subscriber uses the certificate.
- ▶▶ 30 days pass from the date of the issuance of a certificate.

4.10 Verification of Digital Signatures

Verification of a digital signature is used to determine that:

- ▶▶ The private key corresponding to the public key listed in the signer's certificate created the digital signature.
- ▶▶ The signed data associated with this digital signature has not been altered since the digital signature was created.

4.11 Reliance on Digital Signatures

The final decision concerning whether or not to rely on a verified digital signature is exclusively that of the relying party. Reliance on a digital signature should only occur if:

- ▶▶ The digital signature was created during the operational period of a valid certificate and it can be verified by referencing a validated certificate.

- ▶ The relying party has checked the revocation status of the certificate by referring to the relevant Certificate Revocation Lists and the certificate has not been revoked.
- ▶ The relying party understands that a digital certificate is issued to a subscriber for a specific purpose and that the private key associated with the digital certificate may only be used in accordance with the usages suggested in the CPS and named as Object Identifiers in the certificate profile.

Reliance is accepted as reasonable under the provisions made for the relying party under this CPS and within the relying party agreement. If the circumstances of reliance exceed the assurances delivered by ARX under the provisions made in this CPS, the relying party must obtain additional assurances.

Warranties are only valid if the steps detailed above have been carried out.

4.12 Certificate Suspension

ARX does not utilize certificate suspension.

4.13 Certificate Revocation

Revocation of a certificate is to permanently end the operational period of the certificate prior to reaching the end of its stated validity period. ARX will revoke a digital certificate if:

- ▶ There has been loss, theft, modification, unauthorized disclosure, or other compromise of the private key associated with the certificate.
- ▶ The Subscriber, Subscriber's end user or ARX has breached a material obligation under this CPS.
- ▶ Either the Subscriber's or ARX's obligations under this CPS are delayed or prevented by a natural disaster, computer or communications failure, or other cause beyond the person's reasonable control, and as a result another person's information is materially threatened or compromised.
- ▶ There has been a modification of the information pertaining to the Subscriber or end user that is contained within the certificate.
- ▶ The Subscriber requested that the certificate be revoked.

4.13.1 Request for Revocation

When the Subscriber's administrator deletes a user, or modifies a user details in its IT systems, it constitutes a revocation request. Returning the CoSign appliance to factory settings will create revocation requests for all certificates stored in it.

ARX employs the following procedure for authenticating a revocation request:

- ▶ The revocation request must be sent by the CoSign appliance of the Organization associated with the certificate request.
- ▶ ARX CA infrastructure will then perform the revocation of the certificate. Logging of the revocation will be maintained in accordance with the logging procedures covered in this CPS.

4.13.2 Effect of Revocation

Upon revocation of a certificate, the operational period of that certificate is immediately considered terminated. The serial number of the revoked certificate will be placed within the Certificate Revocation List (CRL) and remains on the CRL until some time after the end of the certificate's validity period. An updated CRL is published on the ARX website every 24 hours; however, under special circumstances the CRL may be published more frequently.

5. Legal Conditions of Issuance

This part describes the legal representations, warranties and limitations associated with ARX digital certificates.

5.1 ARX Representations

ARX makes to all subscribers and relying parties certain representations regarding its public service, as described below. ARX reserves its right to modify such representations as it sees fit or required by law.

5.2 Information Incorporated by Reference into a ARX Digital Certificate

ARX incorporates by reference the following information in every digital certificate it issues:

- ▶▶ Terms and conditions of the digital certificate.
- ▶▶ Any other applicable certificate policy as may be stated on an issued ARX certificate, including the location of this CPS.
- ▶▶ The mandatory elements of the standard X.509v3.
- ▶▶ Any non-mandatory but customized elements of the standard X.509v3.
- ▶▶ Content of extensions and enhanced naming that are not fully expressed within a certificate.
- ▶▶ Any other information that is indicated to be so in a field of a certificate.

5.3 Displaying Liability Limitations, and Warranty Disclaimers

ARX certificates may include a brief statement describing limitations of liability, limitations in the value of transactions to be accomplished, validation period, and intended purpose of the certificate and disclaimers of warranty that may apply. Subscribers must agree to ARX Terms & Conditions before signing-up for certificates.

5.4 Publication of Certificate Revocation Data

ARX reserves its right to publish a CRL (Certificate Revocation List) as may be indicated.

5.5 Duty to Monitor the Accuracy of Submitted Information

In all cases and for all types of ARX certificates the subscriber has a continuous obligation to monitor the accuracy of the submitted information and notify ARX of any such changes.

5.6 Publication of Information

Published critical information may be updated from time to time as prescribed in this CPS.

Such updates shall be indicated through appropriate version numbering and publication date on any new version.

5.7 Interference with ARX Implementation

Subscribers, relying parties and any other parties shall not interfere with, or reverse engineer the technical implementation of ARX PKI services including the key generation process, the public web site and the ARX repositories except as explicitly permitted by this CPS or upon prior written approval of ARX. Failure to comply with this as a Subscriber will result in the revocation of the Subscriber's Digital Certificates without

further notice to the Subscriber or end users and the Subscriber shall pay any Charges payable but that have not yet been paid under this Agreement. Failure to comply with this as a relying party will result in the termination of the agreement with the relying party, the removal of permission to use or access the ARX repository and any Digital Certificate or Service provided by ARX.

5.8 Standards

ARX assumes that user software that is claimed to be compliant with X.509 v3 and other applicable standards enforces the requirements set out in this CPS. ARX cannot warrant that such user software will support and enforce controls required by ARX, whilst the user should seek appropriate advice.

5.9 ARX Partnerships Limitations

Partners of the ARX network shall not undertake any actions that might imperil, put in doubt or reduce the trust associated with the ARX products and services. Failure to comply with this will result in the termination of the agreement with the relying party, the removal of permission to use or access the ARX repository and any Digital Certificate or Service provided by ARX.

5.11 Choice of Cryptographic Methods

Parties are solely responsible for having exercised independent judgment and employed adequate training in choosing security software, hardware, and encryption/digital signature algorithms, including their respective parameters, procedures, and techniques as well as PKI as a solution to their security requirements.

5.12 Reliance on Unverified Digital Signatures

Parties relying on a digital certificate must verify a digital signature at all times by checking the validity of a digital certificate against the relevant CRL published by ARX. Relying parties are alerted that an unverified digital signature cannot be assigned as a valid signature of the Subscriber or end user.

Relying on an unverifiable digital signature may result in risks that the relying party, and not ARX, assume in whole.

By means of this CPS, ARX has adequately informed relying parties on the usage and validation of digital signatures through this CPS and other documentation published in its public repository available at <http://www.arx.com/documents/cps.php> or by contacting via out of bands means via the contact address as specified in the Document Control section of this CPS.

5.13 Rejected Certificate Applications

The private key associated with a public key, which has been submitted as part of a rejected certificate application, may not under any circumstances be used to create a digital signature if the effect of the signature is to create conditions of reliance upon the rejected certificate.

5.14 Refusal to Issue a Certificate

ARX reserves its right to refuse to issue a certificate to any party as it sees fit, without incurring any liability or responsibility for any loss or expenses arising out of such refusal.

ARX reserves the right not to disclose reasons for such a refusal.

5.15 Subscriber Obligations

Unless otherwise stated in this CPS, Subscribers shall exclusively be responsible:

Vertical watermark text: Digital Signatures That Keep Your Business Moving

- ▶ To allow only authorized and properly trained individuals (administrators) to manage its IT systems.
- ▶ Provide correct and accurate information in its communications with ARX.
- ▶ Alert ARX if at any stage whilst the certificate is valid, any information originally submitted has changed since it had been submitted to ARX.
- ▶ Read, understand and agree with all terms and conditions in this ARX CPS and associated policies published in the ARX Repository at www.arx.com/documents/cps.php.
- ▶ Refrain from tampering with an ARX certificate or the CoSign appliance.
- ▶ Use ARX certificates for legal and authorized purposes in accordance with the suggested usages and practices in this CPS.
- ▶ Cease using an ARX certificate if any information in it becomes misleading obsolete or invalid.
- ▶ Cease using an ARX certificate if such certificate is expired and remove it from any applications and/or devices it has been installed on.
- ▶ Refrain from using the subscriber's private key corresponding to the public key in an ARX issued certificate to issue digital certificates or subordinate CAs.
- ▶ Make reasonable efforts to prevent the compromise, loss, disclosure, modification, or otherwise unauthorized use of the private key corresponding to the public key published in an ARX certificate.
- ▶ Request the revocation of a certificate (by deleting or modifying the relevant user) in case of an occurrence that materially affects the integrity of an ARX certificate.

5.16 Representations by Subscriber upon Acceptance

Upon accepting a certificate, the Subscriber represents to ARX and to relying parties that at the time of acceptance and until further notice:

- ▶ Digital signatures created using the private key corresponding to the public key included in the certificate is the digital signature of the Subscriber End User and the certificate has been accepted and is properly operational at the time the digital signature is created.
- ▶ No unauthorized person has ever had access to the subscriber's private keys.
- ▶ All representations made by the Subscriber to ARX regarding the information contained in the certificates are accurate and true.
- ▶ All information contained in the certificate is accurate and true to the best of the Subscriber's knowledge or to the extent that the Subscriber had notice of such information whilst the Subscriber shall act promptly to notify ARX of any material inaccuracies in such information.
- ▶ The certificate is used exclusively for authorized and legal purposes, consistent with this CPS.
- ▶ It or its end users will use an ARX certificate only in conjunction with the entity named in the organization field of a digital certificate (if applicable).
- ▶ The Subscriber is an Organization subscriber and not a CA, and will not use the private key corresponding to any public key listed in the certificates for purposes of signing any certificate (or any other format of certified public key) or CRL, as a CA or otherwise, unless expressly agreed in writing between Subscriber and ARX.
- ▶ The Subscriber agrees with the terms and conditions of this CPS and other agreements and policy statements of ARX.

- ▶ The Subscriber abides by the laws applicable in his/her country or territory including those related to intellectual property protection, viruses, accessing computer systems etc.
- ▶ The Subscriber complies with all export laws and regulations for dual usage goods as may be applicable.

5.17 Indemnity by Subscriber

By accepting a certificate, the Subscriber agrees to indemnify and hold ARX, as well as its agent(s) and contractors harmless from any acts or omissions resulting in liability, any loss or damage, and any suits and expenses of any kind, including reasonable attorneys' fees, that ARX, and the above mentioned parties may incur, that are caused by the use or publication of a certificate, and that arises from:

- ▶ Any false or misrepresented data supplied by the Subscriber or agent(s).
- ▶ Any failure of the Subscriber to disclose a material fact, if the misrepresentation or omission was made negligently or with intent to deceive the CA, ARX, or any person receiving or relying on the certificate.
- ▶ Failure to protect the Subscriber's confidential data including their private key, or failure to take reasonable precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorized use of the subscriber's confidential data.
- ▶ Breaking any laws applicable in his/her country or territory including those related to intellectual property protection, viruses, accessing computer systems etc.

5.19 Obligations of a Relying Party

A party relying on an ARX certificate accepts that in order to reasonably rely on an ARX certificate they must:

- ▶ Minimize the risk of relying on a digital signature created by an invalid, revoked, expired or rejected certificate; the relying party must have reasonably made the effort to acquire sufficient knowledge on using digital certificates and PKI.
- ▶ Study the limitations to the usage of digital certificates and be aware through the Relying Party agreement the maximum value of the transactions that can be made using an ARX digital certificate.
- ▶ Read and agree with the terms of the ARX CPS and relying party agreement.
- ▶ Verify an ARX certificate by referring to the relevant CRL and the CRLs of intermediate CA and root CA.
- ▶ Trust an ARX certificate only if it is valid and has not been revoked or has expired.
- ▶ Rely on an ARX certificate, only as may be reasonable under the circumstances listed in this section and other relevant sections of this CPS.

5.20 Legality of Information

Subscribers shall solely be responsible for the legality of the information they present for use in certificates issued under this CPS, in any jurisdiction in which such content may be used or viewed.

5.21 Subscriber Liability to Relying Parties

Without limiting other Subscriber obligations stated in this CPS, Subscribers are liable for any misrepresentations they make in certificates to third parties that reasonably rely on the representations contained therein and have verified one or more digital signatures with the certificate.

5.22 Duty to Monitor Agents

The Subscriber shall control and be responsible for the data that an agent supplies to ARX. The Subscriber must promptly notify the issuer of any misrepresentations and omissions made by an agent. The duty of this article is continuous.

5.23 Use of Agents

For certificates issued at the request of a Subscriber's agent, both the agent and the Subscriber shall jointly and severally indemnify ARX, and its agents and contractors.

5.24 Conditions of usage of the ARX Repository and Web site

Parties (including Subscribers and relying parties) accessing the ARX Repository (www.arx.com/documents/cps.php) and official web site(s) agree with the provisions of this CPS and any other conditions of usage that ARX may make available. Parties demonstrate acceptance of the conditions of usage of the CPS by using an ARX issued certificate.

Failure to comply with the conditions of usage of the ARX Repositories and web site may result in terminating the relationship between ARX and the party.

5.25 Accuracy of Information

ARX, recognizing its trusted position, makes all reasonable efforts to ensure that parties accessing its Repositories receive accurate, updated and correct information. ARX, however, cannot accept any liability beyond the limits set in this CPS.

Failure to comply with the conditions of usage of the ARX Repositories and web site may result in terminating the relationship between ARX and the party.

5.26 Obligations of ARX

To the extent specified in the relevant sections of the CPS, ARX promises to:

- ▶▶ Comply with this CPS and its internal or published policies and procedures.
- ▶▶ Comply with applicable laws and regulations.
- ▶▶ Provide infrastructure and certification services, including but not limited to the establishment and operation of the ARX Repository and web site for the operation of PKI services.
- ▶▶ Provide Trust mechanisms, including a key generation mechanism, key protection, and secret sharing procedures regarding its own infrastructure.
- ▶▶ Provide prompt notice in case of compromise of its private key(s).
- ▶▶ Provide and validate application procedures for certificates that it may make publicly available.
- ▶▶ Issue digital certificates in accordance with this CPS and fulfill its obligations presented herein.
- ▶▶ Publish accepted certificates in accordance with this CPS.
- ▶▶ Provide support to subscribers and relying parties as described in this CPS.
- ▶▶ Revoke certificates according to this CPS.
- ▶▶ Provide for the expiration and renewal of certificates according to this CPS.
- ▶▶ Make available a copy of this CPS and applicable policies to requesting parties.

The subscriber also acknowledges that ARX has no further obligations under this CPS.

5.27 Fitness for a Particular Purpose

ARX disclaims all warranties and obligations of any type, including any warranty of fitness for a particular purpose, and any warranty of the accuracy of unverified information provided, save as contained herein and as cannot be excluded at law.

5.28 Other Warranties

ARX does not warrant:

- ▶▶ The accuracy, authenticity, completeness or fitness of any unverified information contained in certificates or otherwise compiled, published, or disseminated by or on behalf of ARX except as it may be stated in the product description below in this CPS and in the ARX insurance policy.
- ▶▶ In addition, shall not incur liability for representations of information contained in a certificate except as it may be stated in the relevant product description in this CPS.
- ▶▶ Does not warrant the quality, functions or performance of any software or hardware device.
- ▶▶ Although ARX is responsible for the revocation of a certificate, it cannot be held liable if it cannot execute it for reasons outside its own control.
- ▶▶ The validity, completeness or availability of directories of certificates issued by a third party (including an agent) unless specifically stated by ARX.

5.29 Non-Verified Subscriber Information

Notwithstanding limitation warranties under the product section of this CPS, ARX shall not be responsible for non-verified Subscriber end user information submitted to ARX, or the ARX directory or otherwise submitted with the intention to be included in a certificate,.

5.30 Exclusion of Certain Elements of Damages

In no event (except for fraud or willful misconduct) shall ARX be liable for:

- ▶▶ Any indirect, incidental or consequential damages.
- ▶▶ Any loss of profits.
- ▶▶ Any loss of data.
- ▶▶ Any other indirect, consequential or punitive damages arising from or in connection with the use, delivery, license, performance or non-performance of certificates or digital signatures.
- ▶▶ Any other transactions or services offered within the framework of this CPS.
- ▶▶ Any other damages except for those due to reliance, on the information featured on a certificate, on the verified information in a certificate.
- ▶▶ Any liability incurred in this case or any other case if the fault in this verified information is due to fraud or willful misconduct of the applicant.
- ▶▶ Any liability that arises from the usage of a certificate that has not been issued or used in conformance with this CPS.
- ▶▶ Any liability that arises from the usage of a certificate that is not valid.

- ▶ Any liability that arises from usage of a certificate that exceeds the limitations in usage and value and transactions stated upon it or on the CPS.
- ▶ Any liability that arises from security, usability, integrity of products, including hardware and software a subscriber uses.
- ▶ Any liability that arises from compromise of a subscriber's private key.

ARX does not limit or exclude liability for death or personal injury.

5.33 Damage and Loss Limitations

In no event (except for fraud or willful misconduct) will the aggregate liability of ARX to all parties including without any limitation a subscriber, an applicant, a recipient, or a relying party for all digital signatures and transactions related to such certificate exceeds the applicable liability cap for such certificate.

5.34 Conflict of Rules

When this CPS conflicts with other rules, guidelines, or contracts, this CPS, dated January 15, 2007, shall prevail and bind the subscriber and other parties except as to other contracts either:

- ▶ Predating the first public release of the present version of this CPS.
- ▶ Expressly superseding this CPS for which such contract shall govern as to the parties thereto, and to the extent permitted by law.

5.35 ARX Intellectual Property Rights

ARX or its partners or associates own all intellectual property rights associated with its databases, web sites, ARX digital certificates and any other publication originating from ARX including this CPS.

5.36 Infringement and Other Damaging Material

ARX Subscribers represent and warrant that when submitting to ARX and using a domain and distinguished name (and all other certificate application information) they do not interfere with or infringe any rights of any third parties in any jurisdiction with respect to their trademarks, service marks, trade names, company names, or any other intellectual property right, and that they are not seeking to use the domain and distinguished names for any unlawful purpose, including, without limitation, tortious interference with contract or prospective business advantage, unfair competition, injuring the reputation of another, and confusing or misleading a person, whether natural or incorporated.

Although ARX will provide all reasonable assistance, certificate Subscribers shall defend, indemnify, and hold ARX harmless for any loss or damage resulting from any such interference or infringement and shall be responsible for defending all actions on behalf of ARX.

5.37 Ownership

Certificates are the property of ARX. ARX gives permission to reproduce and distribute certificates on a nonexclusive, royalty-free basis, provided that they are reproduced and distributed in full. ARX reserves the right to revoke the certificate at any time.

Private and public keys are property of the subscribers who rightfully issue and hold them.

All secret shares (distributed elements) of the ARX private key remain the property of ARX.

5.38 Governing Law

This CPS is governed by, and construed under the laws of the state of Delaware, U.S.A. This choice of law is made to ensure uniform interpretation of this CPS, regardless of the place of residence or place of use of ARX digital certificates or other products and services. The laws of the state of Delaware applies in all ARX commercial or contractual relationships in which this CPS may apply or quoted implicitly or explicitly in relation to ARX products and services where ARX acts as a provider, supplier, beneficiary receiver or otherwise.

5.39 Jurisdiction

Each party, including ARX partners, subscribers and relying parties, irrevocably agrees that the courts of the state of Delaware have exclusive jurisdiction to hear and decide any suit, action or proceedings, and to settle any disputes, which may arise out of or in connection with this CPS or the provision of ARX PKI services.

5.40 Dispute Resolution

Before resorting to any dispute resolution mechanism including adjudication or any type of Alternative Dispute Resolution (including without exception mini-trial, arbitration, binding expert's advice, co-operation monitoring and normal expert's advice) parties agree to notify ARX of the dispute with a view to seek dispute resolution.

5.41 Successors and Assigns

This CPS shall be binding upon the successors, executors, heirs, representatives, administrators, and assigns, whether express, implied, or apparent, of the parties. The rights and obligations detailed in this CPS are assignable by the parties, by operation of law (including as a result of merger or a transfer of a controlling interest in voting securities) or otherwise, provided such assignment is undertaken consistent with this CPS articles on termination or cessation of operations, and provided that such assignment does not effect a novation of any other debts or obligations the assigning party owes to other parties at the time of such assignment.

5.42 Severability

If any provision of this CPS or the application thereof, is for any reason and to any extent found to be invalid or unenforceable, the remainder of this CPS (and the application of the invalid or unenforceable provision to other persons or circumstances) shall be interpreted in such manner as to affect the original intention of the parties.

Each and every provision of this CPS that provides for a limitation of liability, disclaimer of or limitation upon any warranties or other obligations, or exclusion of damages is intended to be severable and independent of any other provision and is to be enforced as such.

5.43 Interpretation

This CPS shall be interpreted consistently within the boundaries of business customs, commercial reasonableness under the circumstances and intended usage of a product or service. In interpreting this CPS, parties shall also take into account the international scope and application of the services and products of ARX as well as the principle of good faith as it is applied in commercial transactions.

The headings, subheadings, and other captions in this CPS are intended for convenience and reference only and shall not be used in interpreting, construing, or enforcing any of the provisions of this CPS.

Appendices and definitions to this CPS are for all purposes an integral and binding part of the CPS.

5.44 No Waiver

This CPS shall be enforced as a whole, whilst failure by any person to enforce any provision of this CPS shall not be deemed a waiver of future enforcement of that or any other provision.

5.45 Notice

ARX accepts notices related to this CPS by means of digitally signed messages or in paper form. Upon receipt of a valid, digitally signed acknowledgment of receipt from ARX, the sender of the notice shall deem their communication effective. The sender must receive such acknowledgment within five (5) days, or else written notice must then be sent in paper form through a courier service that confirms delivery or via certified or registered mail, postage prepaid, return receipt requested, addressed as follows:

ARX Inc.
855 Folsom St. Suite 939
San Francisco, CA. 49107
USA
Attention: Legal Practices
Email: legal@arx.com

This CPS, related agreements and Certificate policies referenced within this document are available online at www.arx.com/documents/cps.php.

5.46 Fees

ARX charges fees for some of the certificate services it offers.

ARX does not charge fees for the revocation of a certificate or for a Relying Party to check the validity status of an ARX issued certificate using Certificate Revocation Lists.

ARX retains its right to affect changes to such fees.

6. General Issuance Procedure

6.1 General - ARX

ARX offers certificates to make use of an appropriate application for Digital Signatures. Prior to the issuance of a certificate ARX will validate an application in accordance with this CPS which may involve the request by ARX to the applicant for relevant official documentation supporting the application.

ARX certificates are issued to Organizations' End Users.

The validity period of ARX certificates will be 1 year. ARX reserves the right to, at its discretion, issue certificates that may fall outside of these set periods.

6.2 Certificate Issuance

A certificate request can be done according to the following means:

The Organization submits to ARX a certificate application, including application information as detailed in this CPS, and agree to the terms of the relevant subscriber agreement. The applicant also provides proof

of identity through the submission of official documentation as requested by ARX during the enrollment process. ARX will validate the supplied documents, and will then issue a credential to the customer which will be loaded into the customer's CoSign appliance for the purpose of authenticating the CoSign to the ARX CA as belonging to the specific customer and authorized to issue requests on its behalf.

6.3 Content

Typical content of information published in an ARX certificate may include but is not limited to the following elements of information:

6.3.1 Secure Electronic Signature Certificates

- ▶▶ End user's e-mail address.
- ▶▶ End user's name.
- ▶▶ Code of applicant's country.
- ▶▶ Organization name, organizational unit name, street address, city, state.
- ▶▶ Applicant's public key.
- ▶▶ Issuing certification authority (ARX).
- ▶▶ ARX digital signature.
- ▶▶ Type of algorithm.
- ▶▶ Validity period of the digital certificate.
- ▶▶ Serial number of the digital certificate.

6.4 Time to Confirm Submitted Data

ARX makes reasonable efforts to confirm certificate application information and issue digital certificates within a reasonable time frame. The time frame is greatly dependent on the Subscriber providing the necessary details and / or documentation in a timely manner.

From time to time, events outside of the control of ARX may delay the issuance process, however ARX will make every reasonable effort to meet issuance times and to make applicants aware of any factors that may affect issuance times in a timely manner.

6.5 Issuing Procedure

Document Control

This document is version 1.0 of the ARX CPS, created on January 15, 2007 and signed off by the ARX Certificate Policy Authority

ARX Inc.
855 Folsom St. Suite 939
San Francisco, CA. 49107
USA
Attention: Legal Practices
Email: legal@arx.com
Tel: (415) 839 8161
Fax: (415) 723 7110

Copyright Notice

Copyright ARX 2007. All rights reserved.

No part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means (electronic, mechanical, photocopying, recording or otherwise) without prior written permission of ARX Inc.

Requests for any other permission to reproduce this ARX document (as well as requests for copies from ARX) must be addressed to:

ARX Inc.
855 Folsom St. Suite 939
San Francisco, CA. 49107
USA

Digital Signatures That Keep Your Business Moving