

TECHNICAL SECURITY CONTROLS

WD0011 - Version 1.0.1
Effective Date: 17 July 2006

WIS@key S.A. © 2000-2007

WIS@key hereby grants non-exclusive permission to reproduce and distribute copies of this Certification Practice Statement for non-commercial purposes, provided the full source and copyright ownership are included. Any reproduction, distribution or other use beyond the foregoing permission requires authorisation by WIS@key and to such end may contact WIS@key in accordance with § 2.5.3.

1. TECHNICAL SECURITY CONTROLS	4
1.1. KEY PAIR GENERATION AND INSTALLATION	4
1.1.1. Key Pair Generation.....	4
1.1.2. Private Key Delivery to Entity.....	4
1.1.3. Public Key Delivery to Certificate Issuer	4
1.1.4. Root CA and Policy CA Public Key Delivery to Users.....	4
1.1.5. Key Sizes	5
1.1.6. Public Key Parameters Checking.....	5
1.1.7. Parameter Quality Checking	5
1.1.8. Private Key Protection Cryptographic Module Engineering Controls	5
1.1.9. Key Usage Purposes	5
1.2. PRIVATE KEY PROTECTION	6
1.2.1. Cryptographic Modules Standards and Controls	6
1.2.2. Private Key Multi-Person Control	6
1.2.3. Private Key Escrow.....	6
1.2.4. Private Key Backup	6
1.2.5. Private Key Entry into or from a Cryptographic Module	7
1.2.6. Private Key Storage on Cryptographic Module.....	7
1.2.7. Method of Activating Private Key	7
1.2.8. Method of deactivating private key	8
1.2.9. Method of Destroying Private Key	8
1.2.10. Usage Periods for the Public and Private Key	8
1.3. ACTIVATION DATA	8
1.3.1. Activation Data Generation and Installation.....	8
1.3.2. Activation Data Protection.....	9
1.4. COMPUTER SECURITY CONTROLS	9
1.5. LIFE CYCLE TECHNICAL CONTROLS	9
1.5.1. System Development Controls	9
1.5.2. Security management controls.....	10
1.5.3. Network Security Controls	10
1.5.4. Life Cycle Security Ratings.....	10
1.5.5. Time Stamping.....	10
2. CERTIFICATE, CRL AND OCSP PROFILES.....	11
2.1. CERTIFICATE PROFILE	11
2.1.1. Version Numbers	12
2.1.2. Certificate Extensions	12
2.1.3. Key usage.....	12
2.1.4. Certificate Policy Extensions.....	13
2.1.5. Subject Alternative Names	13
2.1.6. Issuer Alternative Name	13
2.1.7. Basic Constraints	13
2.1.8. Extended Key Usage.....	14
2.1.9. CRL Distribution Points	16
2.1.10. Authority Key Identifier	16
2.1.11. Subject Key Identifier	17

2.1.12.	Algorithm Object Identifiers.....	17
2.1.13.	Name Forms.....	17
2.1.14.	Name Constraints.....	17
2.1.15.	Certificate Policy Object Identifier.....	18
2.1.16.	Usage of Policy Constraints Extension.....	18
2.1.17.	Policy Qualifiers Syntax and Semantics.....	18
2.1.18.	Processing Semantics for the Critical Certificate Policies extension.....	18
2.2.	CRL PROFILE.....	18
2.2.1.	Version Number(s).....	19
2.2.2.	CRL Extensions.....	19
2.2.3.	CRL Entry Extensions.....	19
2.2.4.	OCSP Profile.....	20

1. TECHNICAL SECURITY CONTROLS

1.1. *Key Pair Generation and Installation*

1.1.1. **Key Pair Generation**

Key pairs for Issuing CA are generated in a hardware security module (HSM) which have gone through the WISeKey certification procedure.

Generation of End User key pairs should use minimum FIPS 140-1 or higher certified hardware or software using a random number seed generator that meets the requirements of FIPS 140-1 level 1.

Additional requirements on End User key generation may be specified in the Applicable Certificate Policy.

1.1.2. **Private Key Delivery to Entity**

Where key generation is provided the private key delivery may be done either at the moment of key generation (when the Subscriber is present); or delivered in a secure manner, such as through an encryption channel or within a secure device protected by the certificate services provider in which the key pair was generated (when the Subscriber is not present).

Where delivery is required, the activation data required for the use of the private key should be distributed separately to the device in which the Private Key is delivered.

1.1.3. **Public Key Delivery to Certificate Issuer**

The Public keys are generally delivered to the CA as PKCS#10 certificate requests. The signature on the PKCS#10 request should be verified to confirm that the user is in possession of the private key associated with the delivered public key.

The end user may also submit a certificate request with the public key through a secure web interface or other approved mechanism such Windows AutoEnrolment.

1.1.4. **Root CA and Policy CA Public Key Delivery to Users**

The entire Certificate Chain, including the Root CA and Subordinate CAs is generally distributed to End Users for Certificate path validation purposes.

The certificate hash (thumbprint) and the Certificate of the WISeKey Root CA certificate and WISeKey Policy CAs are available on the WISeKey Web site (www.WISeKey.com/repository/). Relying parties must confirm the validity of their copy of the Root CA and Policy CAs certificate using this thumbprint.

1.1.5. Key Sizes

The modulus of the [NAME OF OPERATOR] Issuing CA is at least 1024 bits in length and uses the RSA algorithm.

End User Key Pairs are recommended to be at least 1024 bits in length and use the RSA algorithm. End User key sizes and algorithms are defined in the applicable Certificate Policy.

1.1.6. Public Key Parameters Checking

The parameters used in the generation of public keys are in accordance with the requirements of FIPS 140-1.

1.1.7. Parameter Quality Checking

Parameter quality checking is in accordance with FIPS 140-1.

1.1.8. Private Key Protection Cryptographic Module Engineering

Controls

The combination of procedural, physical and logical controls that are used to protect the [NAME OF OPERATOR] CA described in this CPS.

In addition all subscribers are required to adopt suitable precautions to protect their Private Key, and to avoid its disclosure, modification, loss, or unauthorised use.

1.1.9. Key Usage Purposes

The Issuing CA Cryptographic Keys may be used for:

- Issuance of certificates to End entities (user or server).
- Issuance of Certificate Revocation Lists
- Signing of Online Certificate Status Responses

The key usage purposes of Issuing CAs are limited to their activities as Subordinate PKI Entities and may therefore not be used for any other purposes. Key usage is also defined by the CA level (Standard, Advanced or Qualified).

The End User key usage purposes are defined in the applicable certificate policy.

1.2. Private Key Protection

1.2.1. Cryptographic Modules Standards and Controls

[NAME OF OPERATER] uses hardware security modules that are accredited and certified for use by WISeKey, or modules that are certified FIPS 140-2 Level 2 or higher for all Issuing CAs.

1.2.2. Private Key Multi-Person Control

The DPAA has implemented security procedures and technical measures so that all sensitive CA cryptographic operations require the presence and active involvement of multiple Trusted Persons. The activation of the CA private signing key is performed using multiparty control.

If necessary, based on a risk assessment, the activation of the CA private signing key is performed using multi-factor authentication (for example, a combination of smart card and password, biometric and password).

1.2.3. Private Key Escrow

The Issuing CA may provide key archival and recovery services of End User confidentiality keys only subject to End User consent. Should the PAA approve the provision of this service, the corresponding Certificate Policy will define the terms of such provision.

Key recovery should require the presence and participation of several authorised [NAME OF OPERATOR] officers and should be properly documented.

Private key escrow is NOT provided under any circumstances for end user signing keys that are indicated as non-repudiable per the applicable Certificate Policy.

1.2.4. Private Key Backup

The Issuing CA Private Cryptographic Key should only be backed up for disaster recovery purposes.

As part of standard operation procedure encrypted backup copies of CA Private Keys, that require the participation of multiple Trusted Persons before reconstruction in a secure cryptographic device, are kept onsite and offsite for business continuity and disaster

recovery.

All hardware cryptographic modules used for CA Private Key activation, storage and protection must meet the requirements defined in this CPS.

The CA Private Key is backed up, stored, and recovered by authorised personnel using multiparty control in a physically secured environment. If the CA's private signing key is backed up, backup copies of the CA Private Keys should be subject to the equivalent or greater level of security controls as keys currently in use.

If the CA Private Key is exported from a secure cryptographic module and moved to secure storage for purposes of offline processing or backup and recovery, then the Private Key is exported in a secure key management scheme including any of the following:

- a. As ciphertext protected using multiple control,
- b. As encrypted key fragments using multiple control and split knowledge/ownership
- c. In another secure cryptographic module such as a key transportation device using multiple control

End Users may, under their sole and absolute responsibility, backup their Private Keys in the event the key storage device allows it, which shall be explicitly determined in the applicable policy.

1.2.5. Private Key Entry into or from a Cryptographic Module

CA key pair generation always takes place within a hardware cryptographic module. Keys stored outside of a module are always in encrypted form, whether for transport between modules, or backup/disaster recovery purposes, as defined in this CPS.

1.2.6. Private Key Storage on Cryptographic Module

Recovery and storage of the CA Private Key is conducted in the same secure schema used in the backup process, using multiple controls as defined in this CPS.

The private key may be cloned to multiple in multiple cryptographic module(s) complying with the requirements in this CPS, where additional cryptographic performance is required.

1.2.7. Method of Activating Private Key

The Issuing CA's Private key activation requires entry and validation of a PIN/passphrase compliant with specified security parameters.

Private Key activation data for all Entities in the Infrastructure, including Certificate Subscribers, and CAs, must be protected in an affordable and reasonable manner that

avoids loss, theft, unauthorised use and disclosure.

1.2.8. Method of deactivating private key

The PKI Services and CA private keys are used in a secure environment using a Hardware Security Module that manages activation and deactivation in accordance with strict role separation and security procedures.

End Users control the use and deactivation of private keys and the secure storage devices on which they are stored, and must comply with the applicable Certificate Policy

1.2.9. Method of Destroying Private Key

The Issuing CA Private Key in the HSM may be destroyed by returning the HSM to its factory initialised state. Smartcards and other cryptographic tokens used by the Issuing CA will be physically destroyed prior to disposal.

Destruction of End User private keys shall be in accordance with [NAME OF OPERATOR] internal policies and the relevant certificate policy, provided such measures are sufficiently secure to avoid misuse or compromise.

1.2.10. Usage Periods for the Public and Private Key

The Issuing CA key pair and certificate will expire after a maximum 10 years from the moment of their generation.

The usage period of the key pair and certificates for End Users will be defined in the applicable Certificate Policy.

1.3. Activation Data

1.3.1. Activation Data Generation and Installation

The activation data generation and installation for Issuing CAs is required to comply with minimum rules described in the CPS, such as multiple controls, used to protect tokens containing WISEKey Certificate Services CA Private Keys.

Keys are generated in accordance with the requirements of CPS and the Key Ceremony Document. The creation and distribution of Secret Shares is logged.

End User activation data generation is under the control of the End User, and is specified in the applicable certificate policy.

1.3.2. **Activation Data Protection**

The activation data of the Issuing CA is required to be protected in accordance with CertifyID Policy Authority operational rules.

All Issuing CAs are responsible for maintaining appropriate physical, and security control of their Key Shares, and all Key Share holders must sign a Key Shareholder Agreement to this effect.

End User activation data protection is specified by the applicable Certificate Policy.

1.4. Computer Security Controls

[NAME OF OPERATOR] is required to comply with WISeKey technical documentation stipulating the required computer security technical controls.

All CA software, data files, and operations are maintained on trustworthy systems that meet a minimum level of security as specified in the [NAME OF OPERATOR] security policy. Unauthorised access to these servers are prohibited, and unauthorised access attempts are logged. Only trusted persons having valid business reasons are permitted to use these servers.

Firewalls are employed where necessary to segregate and protect the CA Services Infrastructure network from other network elements, and prevent intrusion attempts.

Passwords use to access the CA Services Infrastructure systems must follow [NAME OF OPERATOR] password policy.

1.5. Life Cycle Technical Controls

1.5.1. **System Development Controls**

The CA software used by the Issuing CA for certificate issuance and lifecycle management has been developed in accordance with the requirements of ITSEC (Information Technology Security Evaluation Criteria). Common Criteria EAL 3 or higher.

Under no circumstance may [NAME OF OPERATOR] use other CA software than the one originally used and approved by WISeKey.

Usage of Issuing CA Private Key with any other software platform is strictly forbidden and any attempt will result in the immediate revocation of the Issuing CA certificate.

The applications used within the CA Infrastructure are expected to be developed, implemented and maintained in line with appropriate development methodology and

change management standards.

Software developed for the CA Infrastructure is checked to ensure that the appropriate version is being used, and that its integrity is intact, before being deployed on the platform.

1.5.2. Security management controls

The [NAME OF OPERATOR] implements monitoring and configuration control policies for the CA Infrastructure systems where necessary.

1.5.3. Network Security Controls

In order to prevent unauthorised access and malicious activity, all CA and Certificate management functions are performed over secured networks in accordance with the [NAME OF OPERATOR] Security Policy. Furthermore, highly sensitive information is protected using encryption channels, and authentication performing using digital signatures where required.

The Issuing CA is maintained on-line and uses firewalls for connections to un-trusted networks including the Internet. The configuration and access control to these network security devices is strictly controlled and limited to authorised personnel only.

1.5.4. Life Cycle Security Ratings

No stipulation

1.5.5. Time Stamping

Not applicable.

2. Certificate, CRL and OCSP Profiles

2.1. Certificate Profile

The DPAA may establish several Certificate Profiles to accommodate the different types of Certificates issued by the Issuing CA. In all cases, such Certificates are compliant with the WISEKey Certificate Services technical specifications and should be documented in an internal Certificate Profile framework.

Issuing CAs shall have the profile and contain the fields specified in the related policy framework document. The Certificates shall conform to (a) ITU-T Recommendation X.509 (1997): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, June 1997 and, where not superseded by the preceding standards (b) Internet X.509 Public Key Infrastructure - Certificate and CRL Profile.

The end entity Certificates issued by the issuing CA shall contain the following fields:

:

- Version—Set to v3
- Serial number—Unique values for each Certificate in the CA domain i.e. unique values for the issuer DN
- Signature algorithm identifier – Object identifier of the algorithm used by the CA to sign the Certificate
- Issuer DN — Certificate issuer's distinguished name, identification of the Certificate issuer
- Valid From — Greenwich Mean Time (Zulu) time base. Synchronised to a trusted time source.
- Valid To — Greenwich Mean Time (Zulu) time base. Synchronised to a trusted time source.
- Subject DN — Certificate subject's distinguished name
- Subject Public Key —A single Public Key algorithm (RSA) is supported for the subject Public Key. Public key information: algorithm identifier (that is, RSA with SHA-1) and Public Key encoded in accordance with the WISEKey Certificate Standards.

The End Entity Certificates issued by the issuing CA will respect all constraints contained in the Issuing CA certificate. The CA software that has been certified for use by the CA operator will enforce such constraints, and the customer is expected to use only this software. The CA operator should not attempt to contour these constraints.

Advanced Issuing CAs in the WISEKey Certificate Services framework are constrained as

follows:

- Server or SSL certificates, can only be issued with the organisation's registered domains.
- Client certificates e.g, authentication, email etc. can only be issued containing email addresses belonging to the organisation's registered domains.
- End entities under Advanced Issuing CAs are constrained to contain a subset of the following extended key usages:
 - Client Authentication
 - Secure Email
 - Certificate replication with Exchange
 - SSL Certificates (Server Authentication)
 - OCSP Signing
 - Windows SmartCard Logon
 - File Encryption

[NAME OF OPERATOR] shall issue Certificates having the profile set forth in this CPS 7.1.

In addition, the [NAME OF OPERATOR] is explicitly prohibited from issuing certificates for Subordinate CAs.

2.1.1. Version Numbers

All Certificates shall be X.509 Version 3 Certificates. The WISeKey Certificate Services Infrastructure shall issue Version 3 CA Certificates and X.509 Version 3 Certificate Subscriber Certificates.

2.1.2. Certificate Extensions

The WISeKey Certificate Services Infrastructure shall populate X.509 Version 3 Certificates with the extensions required by the internal Certificate Policy framework.

2.1.3. Key usage

The criticality field of this extension is generally set to FALSE. The KeyUsage extensions are generally populated as follows:

WISeKey Certificate Services	Certificate Key Usage
Root CA	digitalSignature (0), KeyCertSign (5), cRLSign (6)

Policy CA	digitalSignature (0), KeyCertSign (5), cRLSign (6)
Standard Issuing CA	digitalSignature (0), KeyCertSign (5), cRLSign (6)
Advanced Issuing CA	KeyCertSign (5), cRLSign (6)

End entity certificates key usages should follow the key usage extensions stipulated in the [NAME OF OPERATOR] internal Certificate Profile framework.

2.1.4. Certificate Policy Extensions

WISeKey Certificate Services Infrastructure Certificates MAY use the Certificate Policies extension.

If the CertificatePolicies extension is populated, then it should contain the applicable object identifier for the [NAME OF OPERATOR] CP in accordance with the internal Certificate Profile framework.

The CertificatePolicies extension may also contain the applicable object identifier for the WISeKey Certificate Services Certificate Policy to which this certificate is mapped.

Policy qualifiers are generally absent.

This extension's criticality field is set to FALSE.

2.1.5. Subject Alternative Names

The subject alternative name may be present in Certificates in the WISeKey Certificate Services PKI. This field should generally be encoded as an RFC822 string. This extension's criticality field is set to FALSE.

2.1.6. Issuer Alternative Name

The issuer alternative name may be present in Certificates in the WISeKey Certificate Services PKI and if so then it should be a copy of the subject alternative name from the issuer's Certificate. This field should generally be encoded as an RFC822 string. This extension's criticality field is set to FALSE.

2.1.7. Basic Constraints

All CA Certificates in the WISeKey Services Infrastructure have their BasicConstraints extension with the value of cA set to TRUE. The criticality of the Basic Constraints extension

should be set to TRUE for CA Certificates.

In general, End Entity, or Certificate Subscriber Certificates should not contain the BasicConstraints extension. If they do contain the Basic Constraints extension then the value of cA should be set to FALSE.

For CA Certificates in the WISeKey Certificate Services Infrastructure should the “pathLenConstraint” field of the BasicConstraints extension should give the maximum number of CA Certificates that may follow this Certificate in a certification path.

Root CA Certificates do not contain the “pathLenConstraint” field, indicating that there are no restrictions on the of number of non-self-issued intermediate certificates that may follow this certificate in a valid certification path.

Standard Policy CA Certificates have a “pathLenConstraint” field value of “1” indicating that only one non self-issued intermediate CA certificate may follow this certificate in the certification path.

Advanced Policy CA Certificates need not contain the “pathLenConstraint” field, thus indicating that there are no restrictions on the of number of non-self-issued intermediate certificates that may follow this certificate in a valid certification path.

Qualified Policy CA Certificates need not contain the “pathLenConstraint” field, thus indicating that there are no restrictions on the of number of non-self-issued intermediate certificates that may follow this certificate in a valid certification path.

Standard Issuing CA Certificates MUST have a “pathLenConstraint” field value of “0” indicating that only end entity certificates may follow this Certificate in the certification path.

Advanced Issuing CA Certificates MUST have a “pathLenConstraint” field value of “0” indicating that only end entity certificates may follow this Certificate in the certification path.

2.1.8. Extended Key Usage

The Certificates in the WISeKey Certificate Services Infrastructure may use extended key usage fields as specified in the internal Certificate Policy framework.

End entity certificates can only be issued with a subset of the Extended Key Usage Constraints that are present in the Issuing CA’s certificate.

Standard and Advanced Issuing CAs in the WISeKey Certificate Services Framework generally include extended key usages to restrict usages of the keys of End Entities or Certificate Subscribers. The key usage constraints that are permitted under the Issuing CA classes can be found within the relevant Policy CA CPS documents. However they are typically as follows:

CA Class	Permitted IETF PKIX Extended Key Usages
Standard	id-kp-serverAuth id-kp-clientAuth id-kp-emailProtection id-kp-OCSPSigning
Advanced	id-kp-serverAuth id-kp-clientAuth id-kp-emailProtection id-kp-OCSPSigning
Qualified	id-kp-serverAuth id-kp-clientAuth id-kp-emailProtection id-kp-OCSPSigning id-kp-timeStamping id-kp-codeSigning

Additionally, WISeKey Issuing CAs that are issued to CAs located at Customer Sites are restricted with Extended Key Usage Constraints and Application Policy Constraints Extensions.

CertifyID CA Class/BB Edition	Possible Purpose and Usage	Extended Key Usage Restrictions
STANDARD STANDARD PLUS	Secure Email Client Authentication Windows Smartcard Logon Key Recovery File Recovery Directory Service Email Repl	[[ApplicationPolicyConstraintsExtension] Client Authentication (1.3.6.1.5.5.7.3.2) Secure E-mail (1.3.6.1.5.5.7.3.4) Key Recovery (1.3.6.1.4.1.311.10.3.11) Key Recovery Agent (1.3.6.1.4.1.311.21.6) Smart Card logon (1.3.6.1.4.1.311.20.2.2) Private Key Archival (1.3.6.1.4.1.311.21.5) Certificate Request Agent (1.3.6.1.4.1.311.20.2.1) Encrypting File System (1.3.6.1.4.1.311.10.3.4) File Recovery (1.3.6.1.4.1.311.10.3.4.1) Directory Service E-Mail Replication (1.3.6.1.4.1.311.21.19)

ADVANCED	Secure Email Client Authentication Windows Smartcard Logon Server Authentication Key Recovery OCSPSigning [Ref: attd] File Recovery Directory Service E-Mail Replication	[ApplicationPolicyConstraintsExtension] Client Authentication (1.3.6.1.5.5.7.3.2) Server Authentication (1.3.6.1.5.5.7.3.1) Secure E-mail (1.3.6.1.5.5.7.3.4) Key Recovery (1.3.6.1.4.1.311.10.3.11) Key Recovery Agent (1.3.6.1.4.1.311.21.6) Smart Card logon (1.3.6.1.4.1.311.20.2.2) Private Key Archival (1.3.6.1.4.1.311.21.5) Certificate Request Agent (1.3.6.1.4.1.311.20.2.1) Encrypting File System (1.3.6.1.4.1.311.10.3.4) Id-pkix-OCSPSigning (1.3.6.1.5.5.7.3.9) Id-pkix-OCSPNoCheck (1.3.6.1.5.5.7.48.1.5) File Recovery (1.3.6.1.4.1.311.10.3.4.1) Directory Service E-Mail Replication (1.3.6.1.4.1.311.21.19)
QUALIFIED	All application policies are possible, but unlikely to be granted to a client.	No restrictions are pre-set. The exact constraints are determined based on the CA implementation and audit. Generally, however, the following application policies are NOT allowed (also see table below): Code Signing (1.3.6.1.5.5.7.3.3) Microsoft Trust List Signing (1.3.6.1.4.1.311.10.3.1) Qualified Subordination (1.3.6.1.4.1.311.10.3.10) Time Stamping (1.3.6.1.5.5.7.3.8)

2.1.9. CRL Distribution Points

The WISeKey Certificate Service Infrastructure certificates generally always include the cRLDistributionPoints extension.

2.1.10. Authority Key Identifier

WISeKey Certificate Services Infrastructure Certificates are generally populated with the Authority Key Identifier extension of X.509 Version 3 and all Root CA, Policy CA, Issuing CA and End Entity Certificates should contain this extension. When present in a Certificate, the Authority Key Identifier extension should contain the 160-bit SHA-1 hash of the Public Key of the CA issuing the Certificate.

The extension's critical field is generally set to FALSE.

2.1.11. Subject Key Identifier

The keyIdentifier is calculated based on the Public Key of the Subject of the Certificate whenever the a Certificate is populated with the subjectKeyIdentifier extension.

The extension's critical field is generally set to FALSE.

2.1.12. Algorithm Object Identifiers

Certificates are signed with sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5) or md5WithRSAEncryption (OID: 1.2.840.113549.1.1.4) in accordance with the governing CPS and Certificate Policy framework.

2.1.13. Name Forms

The WISeKey Certificate Services Infrastructure respects the name forms outlined in the IETF PKIX X.509 V3 Standard . In particular:

- For Root CA, Policy CA, and all other CA Certificates the Subject Distinguished Name should always be present.
- For Root CA, Policy CA, and Issuing CA Certificates, the Subject Distinguished Name must contain at least the CN attribute, other attributes are optional. The Organisation attribute should be present and should clearly and uniquely identify the CA operator.

2.1.14. Name Constraints

For Root CA and Policy CA Certificates name constraints are generally not used and their use is discouraged.

For Issuing CA Certificate name constraints are generally used, and their use is encouraged.

CertifyID CA Edition	Extended Key Usage Restrictions
STANDARD	[NameConstraintsPermitted] Relative Distinguished Name Constraint (DIRECTORYNAME =) DNS name constraints (DNS =) RFC 822 and E-mail constraints (EMAIL =)

STANDARD PLUS	[No Name Constraints Apply, however extended audit conditions apply]
ADVANCED	[NameConstraintsPermitted] Relative Distinguished Name Constraint (DIRECTORYNAME =) DNS name constraints (DNS =) RFC 822 and E-mail constraints (EMAIL =)
QUALIFIED	No restrictions are pre-set. Name constraints need not be applied, and their necessity is determined based on the CA implementation and audit.

2.1.15. Certificate Policy Object Identifier

The Certificate Policies extension MAY be used, and Certificates can possess the object identifier of the Certificate Policy corresponding to the Certificate Type as specified in the governing CPS and within the Certificate Policy Framework.

Where this extension is used, this extension's criticality field is set to FALSE.

2.1.16. Usage of Policy Constraints Extension

Policy constraints are generally not used and their use is discouraged.

2.1.17. Policy Qualifiers Syntax and Semantics

Policy qualifiers are generally not used.

2.1.18. Processing Semantics for the Critical Certificate Policies extension

Not used.

2.2. CRL Profile

The Root CA has established a CRL profile for CRLs issued by the Root and Subordinate CAs in the network. In all cases, such CRL profiles are compliant with the WISEKey Certificate Services technical specifications and are documented in an internal Certificate

Profile framework. The CRL follows the RFC 2459 standard.

WISeKey Certificate Service CRLs generally contain the following fields:

- Version — v2
- Signature Algorithm — Identifies algorithm used to sign CRL. Allowed signature algorithms are sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5) or md5WithRSAEncryption (OID: 1.2.840.113549.1.1.4) in accordance with the WISeKey Certificate Services Technical Standards.
- Issuer — directoryName of issuer Entity who has signed and issued the CRL. The CRL Issuer Name is in accordance with the Issuer Distinguished Name requirements specified in the CPS and Certificate Policy framework.
- This update — Date and Time of CRL issue. Encoded as G Greenwich Mean Time (Zulu) time. WISeKey Certificate Service Infrastructure CRLs are effective upon issue.
- Revoked Certificates — Listing of revoked Certificates, including the Serial Number of the revoked.
- Next update— Date by which the next CRL will be issued. This field is generally not included, however it may be included. If included the frequency of CRL issuance will be
- governed by the internal Certificate Policy framework.

2.2.1. Version Number(s)

The WISeKey Certificate Services Infrastructure issues only Version 2 CRLs.

The WISeKey Certificate Services Infrastructure also supports online Certificate status and revocation checking services.

2.2.2. CRL Extensions

- AuthorityKeyIdentifier — this extension field must be present in the CRL. When present, the Authority Key Identifier extension always includes the issuing CA's subject distinguished name and serial number. When the Certificate issuer contains the Subject Key Identifier extension, the Authority Key Identifier also contains the 160-bit SHA-1 hash of the Public Key of the CA issuing the Certificate.
- CRLNumber – this extension field must be present in the CRL. The number is a monotonically increasing integer value that uniquely identifies an instance of the CRL.

2.2.3. CRL Entry Extensions

CRL Entry extensions are permitted in compliance with Internet X.509 Public Key Infrastructure - Certificate and CRL Profile.

2.3. OCSP Profile

The WISeKey Services Infrastructure supports the use online Certificate status and revocation checking services based on the RFC 2560 - X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP.