

Head office

Stockholm, Sweden
Drottninggatan 61
S-111 21 Stockholm

Root Certification Authority

Technical Certificate Policy

and

Certification Practice Statement

(Certificate profiles)

Date: 18.03.2010

Version 1.3

History

Version	Date	Author	Description/Comment
1.0	25.05.2008	Axel Janhoff, MC	Initial Version.
1.0a	05.06.2008	Dr. Ralf Hesse, MC	Revisions.
1.0b	16.06.2008	Dr. Ralf Hesse, MC	Changes in identity management.
1.0c	02.09.2008	Dr. Ralf Hesse, MC	Certificate profile altered, only the advanced certificate profile contains the RFC822 E-Mail.
1.0d	04.11.2008	Dr. Ralf Hesse, MC	Distinguished name composition pattern revised.
1.1	28.01.2009	Dr. Ralf Hesse, MC	Certificate profile for S/Mime signature altered. Better compatibility with Outlook. New profile for authentication certificates.
1.1a	28.09.2009	Axel Janhoff, MC	Update certificate profiles.
1.1b	08.10.2009	Axel Janhoff, MC	Update certificate profiles.
1.2	17.02.2010	Axel Janhoff, MC	Two new certificate authorities added (SW-Auth, SW-Email).
1.3	18.03.2010	Axel Janhoff, MC	Update certificate profiles. Warranty statements added.

1. INTRODUCTION	10
1.1. General Information	10
1.1.1. Overview	10
1.1.2. Terms and Abbreviations	10
1.2. Identification	13
1.3. Public Key Infrastructure Participants	14
1.3.1. Root Certification Authority	15
1.3.2. SG Obligations	15
1.3.3. Issuing Certification Authority Obligations	15
1.3.4. Issuing Certification Authorities	16
1.3.5. Registration Authority Obligations	16
1.3.6. Certificate Holders	17
1.3.6.1. Obligations and Responsibilities	17
1.3.6.2. Accepted Limitation of Liability	17
1.3.7. Relying Parties	17
1.3.7.1. Obligations and Responsibilities	18
1.3.7.2. Reasonable Reliance	18
1.3.7.3. Accepted Limitation of Liability	18
1.3.7.4. Assumptions about a Certificate Holder	18
1.3.7.5. Certificate Compromise	18
1.3.8. Other Participants	19
1.4. Certificate Usage	19
1.4.1. Appropriate Certificate Usage	19
1.4.2. Prohibited Certificate Usage	19
1.5. Certificate Validity Period	19
1.6. Policy Administration	19
1.6.1. Organisation Administering the TCP/CPS	19
1.6.2. TCP/CPS Applicability	19
1.6.3. TCP/CPS Revisions	19
1.6.3.1. Revisions without Notification	20
1.6.3.2. Revisions with Notification	20
1.6.4. TCP/CPS Publication and Notification	20
1.6.5. Contact Person	20
1.6.6. Person Determining the TCP/CPS Suitability	20
1.6.7. TCP/CPS Approval Procedures	20
1.6.8. Publication of TCP/CPS	21
1.6.9. Frequency of Publication	21
1.6.10. Access Control	21
2. PUBLICATION AND REPOSITORY RESPONSIBILITIES	22
2.1. Repositories	22
2.2. Publication of Certificate Information	22

2.3.	Time or Frequency of Publication	22
2.4.	Access Controls on Repositories	22
3.	IDENTIFICATION AND AUTHENTICATION	23
3.1.	Naming	23
3.1.1.	Types of Names	23
3.1.2.	Need for Names to be meaningful	23
3.1.3.	Pseudonymous Certificate Holders	23
3.1.4.	Rules for Interpreting Various Name Forms	23
3.1.5.	Uniqueness of Names	24
3.1.6.	Recognition, Authentication and Role of Trademarks	24
3.2.	Initial Identity Validation	24
3.2.1.	Method to Prove Possession of Private Key	24
3.2.2.	Authentication of Individual Identity	24
3.2.3.	Non-Verified Certificate Holder Information	24
3.2.4.	Criteria for Interoperation	25
3.3.	Identification and Authentication for Renewal Requests	25
3.4.	Identification and Authentication for Revocation Requests	25
3.4.1.	Issuing Certification Authority	25
3.4.2.	Registration Authority	25
3.4.3.	Certificate Holder	25
4.	CERTIFICATE LIFE-CYCLE OPERATION REQUIREMENTS	26
4.1.	Certificate Application	26
4.1.1.	Who Can Submit a Certificate Application	26
4.1.2.	Enrolment Process and Responsibilities	26
4.2.	Certificate Application Processing	26
4.2.1.	Approval or Rejection of Certificate Applications	26
4.2.2.	Time to Process Certificate Applications	26
4.3.	Certificate Issuance	26
4.3.1.	Certification Authority Actions during Certificate Issuance	26
4.3.1.1.	SG Root Certification Authority	26
4.3.1.2.	SG Issuing Certification Authority Certificates	26
4.3.1.3.	SG Registration Authority Appointment	27
4.3.1.4.	Registration Authority Officers Certificate	27
4.3.1.5.	Certificate Holder Certificates	27
4.3.2.	Notification to Applicant Certificate Holder by the Certification Authority of Issuance of Certificate	27
4.4.	Certificate Acceptance	27
4.4.1.	Notice of Acceptance	27
4.4.2.	Conduct Constituting Certificate Acceptance	28
4.4.3.	Publication of the Certificate by the Certification Authority	28
4.4.4.	Notification of Certificate Issuance by the Certification Authority to Other Entities	28

4.5. Key Pair and Certificate Usage	28
4.5.1. Certificate Holder Private Key and Certificate Usage	28
4.5.2. Relying Party Public Key and Certificate Usage	28
4.6. Certificate Renewal	28
4.7. Certificate Modification	29
4.8. Certificate Revocation and Suspension	29
4.8.1. Circumstances for Revocation	29
4.8.2. Who Can Request Revocation	30
4.8.2.1. SignGuard Europe AB	30
4.8.2.2. Certificate Holder	30
4.8.3. Procedure for Revocation Request	30
4.8.4. Revocation Request Grace Period	30
4.8.5. Time within which the Certification Authority Must Process the Revocation Request	30
4.8.6. Revocation Checking Requirement for Relying Parties	30
4.8.7. Certificate Revocation List Issuance Frequency	30
4.8.8. Maximum Latency for Certificate Revocation List	30
4.8.9. On-Line Revocation/Status Checking Availability	31
4.8.10. On-Line Revocation Checking Requirement	31
4.8.11. Other Forms of Revocation Advertisements Available	31
4.8.12. Special Requirements Re-Key Compromise	31
4.8.13. Circumstances for Suspension	31
4.8.14. Who Can Request Suspension	31
4.8.15. Procedure for Suspension Request	31
4.8.16. Limits on Suspension Period	31
4.9. Certificate Status Services	31
4.9.1. Operational Characteristics	31
4.9.2. Service Availability	31
4.9.3. Optional Features	31
4.10. End of Subscription	31
4.11. Key Escrow and Recovery	32
4.11.1. Key Escrow and Recovery Policy and Practices	32
4.11.2. Session Key Encapsulation and Recovery Policy and Practices	32
5. FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS	33
5.1. Physical Controls	33
5.1.1. Site Location and construction	33
5.1.2. Physical Access	33
5.1.3. Power and Air-Conditioning	33
5.1.4. Water Exposures	33
5.1.5. Fire Prevention and Protection	33
5.1.6. Media Storage	33
5.1.7. Waste Disposal	33
5.1.8. Off-Site Backup	33
5.2. Procedural Controls	33
5.2.1. Trusted Roles	34

5.2.2.	Number of Persons Required per Task	34
5.2.3.	Identification and Authentication for Each Role	34
5.2.4.	Roles Requiring Separation of Duties	34
5.3.	Personnel Controls	34
5.3.1.	Qualifications, Experience and Clearance Requirements	34
5.3.2.	Background Check Procedures	35
5.3.3.	Training Requirements	35
5.3.4.	Retraining Frequency and Requirements	35
5.3.5.	Job Rotation Frequency and Sequence	35
5.3.6.	Sanctions for Unauthorized Actions	35
5.3.7.	Independent Contractor Requirements	35
5.3.8.	Documentation Supplied to Personnel	35
5.4.	Audit Logging Procedures	35
5.4.1.	Types of Events Recorded	35
5.4.2.	Frequency of Processing Log	36
5.4.3.	Retention Period for Audit Log	36
5.4.4.	Protection of Audit Log	36
5.4.5.	Audit Log Backup Procedures	36
5.4.6.	Audit Collection System	36
5.4.7.	Notification to Event-Causing Subject	36
5.4.8.	Vulnerability Assessment	36
5.5.	Records Archival	37
5.5.1.	Types of Records Archived	37
5.5.2.	Retention Period for Archive	37
5.5.3.	Protection of Archive	37
5.5.4.	Archive Backup Procedures	37
5.5.5.	Requirements for Time-Stamping of Records	37
5.5.6.	Archive Collection System	37
5.5.7.	Procedures to Obtain and Verify Archive Information	37
5.6.	Key Changeover	38
5.7.	Compromise and Disaster Recovery	38
5.7.1.	SG Business Continuity Plan	38
5.8.	Certification Authority and/or Registration Authority Termination	38
5.8.1.	User Keys and Certificates	39
5.8.2.	Successor Issuing Certification Authority	39
5.8.3.	Private Key Destruction Procedures	39
6.	TECHNICAL SECURITY CONTROLS	40
6.1.	Key Pair Generation and Installation	40
6.1.1.	Key Pair Generation	40
6.1.2.	Private Key Delivery to Certificate Holder	40
6.1.3.	Public Key Delivery to Certificate Issuer	40
6.1.4.	Certification Authority Public Key to Relying Parties	40
6.1.5.	Key Sizes	40
6.1.6.	Public Key Parameters Generation and Quality Checking	40
6.1.7.	Key Usage Purposes (as per X.509 Version 3 Key Usage Field)	40

6.2. Private Key Protection and Cryptographic Module Engineering Controls	41
6.2.1. Cryptographic Module Standards and Controls	41
6.2.2. Private Key Multi-Person Control	41
6.2.3. Private Key Escrow	41
6.2.4. Private Key Backup	41
6.2.5. Private Key Archive	41
6.2.6. Private Key Transfer Into or From a Cryptographic Module	41
6.2.7. Private Key Storage on Cryptographic Module	41
6.2.8. Method of Activating Private Key	41
6.2.9. Method of Deactivating Private Key	42
6.2.10. Method of Destroying Private Key	42
6.2.11. Cryptographic Module Rating	42
6.3. Other Aspects of Key Pair Management	42
6.3.1. Public Key Archival	42
6.3.2. Certificate Operational Periods and Key Pair Usage Periods	42
6.4. Activation Data	42
6.4.1. Activation Data Generation and Installation	42
6.4.2. Activation Data Protection	43
6.4.3. Other Aspects of Activation Data	43
6.5. Computer Security Controls	43
6.5.1. Specific Computer Security Technical Requirements	43
6.5.2. Computer Security Rating	43
6.6. Life Cycle Technical Controls	43
6.6.1. Life Cycle Security Controls	44
6.6.2. Network Security Controls	44
6.6.3. Hardware Cryptographic Module Engineering Controls	44
6.7. Time-Stamping	44
7. CERTIFICATE, CRL AND OCSP PROFILES	45
7.1. Certificate Profile	45
7.1.1. Certificate Content	45
7.1.2. Version Numbers	45
7.1.3. Certificate Extensions	45
7.1.4. Algorithm Object Identifiers	45
7.1.5. Name Forms	45
7.1.6. Name Constraints	45
7.1.7. Usage of Policy Constraints Extension	45
7.1.8. Policy Qualifiers Syntax and Semantics	45
7.1.9. Processing Semantics for the Critical Certificate Policies Extension	45
7.2. Certificate Revocation List Profile	45
7.2.1. Version Number	45
7.2.2. Certificate Revocation List and Certificate Revocation List Entry Extensions	45
7.3. Online Certificate Status Protocol Profile	46
7.3.1. Online Certificate Status Protocol Version Numbers	46
7.3.2. Online Certificate Status Protocol Extensions	46
7.3.3. Signing of OCSP requests	46

7.4. Lightweight Directory Access Protocol Profile	46
7.4.1. Lightweight Directory Access Protocol Version Numbers	46
7.4.2. Lightweight Directory Access Protocol Extensions	46
7.5. Root Certificates	46
7.5.1. SG Root CA Certificate	46
7.5.2. SG Root CA1 Certificate	47
8. COMPLIANCE AND OTHER ASSESSMENTS	49
8.1. Frequency, Circumstance and Standards of Assessment	49
8.2. Topics Covered by Assessment	49
8.3. Actions Taken as a Result of Deficiency	50
8.3.1. Issuing Certification Authorities	50
8.3.2. Registration Authorities	50
9. OTHER BUSINESS AND LEGAL MATTERS	51
9.1. Financial Responsibilities	51
9.1.1. Financial Records	51
9.1.2. Fiduciary Relationships	51
9.1.3. Other Assets	51
9.1.4. Insurance or Warranty Coverage for End-Entities	51
9.2. Confidentiality of Business Information	51
9.2.1. Scope of Confidential Information	51
9.2.2. Information Not Within the Scope of Confidential Information	51
9.3. Responsibility to Protect Confidential Information	51
9.3.1. Privacy of Personal Information	51
9.3.1.1. Privacy Plan	51
9.3.2. Information Treated as Private	52
9.3.2.1. Registration Records	52
9.3.2.2. Certificate Revocation	52
9.3.3. Information Deemed Not Private	52
9.3.3.1. Certificate Contents	52
9.3.3.2. Certificate Revocation List	52
9.3.3.3. TCP/CPS	52
9.3.4. Responsibility to Protect Private Information	52
9.3.5. Notice and Consent to Use Private Information	52
9.3.6. Disclosure Pursuant to Judicial or Administrative Process	52
9.3.6.1. Release to Law Enforcement Officials	52
9.3.6.2. Release as Part of Civil Discovery	53
9.3.7. Other Information Disclosure Circumstances	53
9.4. Intellectual Property Rights	53
9.4.1. Object Identifiers	53
9.4.2. Licenses	53
9.4.3. IETF Guidelines	53
9.4.4. Breach	53

9.5. Representations and Warranties	53
9.5.1. Certification Authority Representations	53
9.5.2. SignGuards Liability	54
SG's liability for damages due to usage of certificates issued by SG Certificates Authorities is limited to 100,- € per issued certificate.	54
9.5.3. Certification Authority Warranties	54
9.5.4. Registration Authority Representations	54
9.5.5. Registration Authority Warranties	55
9.5.6. Certificate Holder Representations and Warranties	55
9.5.7. Relying Parties Representations and Warranties	55
9.5.8. Representations and Warranties of Other Participants	55
9.6. Term and Termination	55
9.6.1. Term	55
9.6.2. Termination	55
9.6.3. Effect of Termination and Survival	55
9.7. Individual Notices And Communications With Participants	55
9.8. Amendments	56
9.8.1. Procedure for Amendment	56
9.8.2. Notification Mechanism and Period	56
9.9. Record Keeping	56
9.10. Force Majeure	56
9.11. Other Provisions	56
9.12. Disclaimer / Legal Validity	56
10. APPENDIX A	57
10.1. Digital Certificate Profiles	57
10.2. Qualified Personal Certificate (QualifiedUserCA2008)	57
10.3. Advanced Personal Certificate (AdvancedUserCA2008)	58
10.4. Authenticated User (UserAuthCA2008)	59
10.5. Server Certificate (ServerCA)	59
10.6. Administrator Certificate (AdminCA)	59
10.7. Authentication software-certificate (SW-Auth)	60
10.8. E-Mail software-certificate (SW-Email)	61
10.9. Test CAs	62

1. INTRODUCTION

1.1. General Information

1.1.1. Overview

The SG Technical Certificate Policy and Certification Practice Statement (TCP/CPS) defines the policies, processes and procedures followed in the generation, issue, use and management of Digital Certificates and the roles, responsibilities and relationships of participants within the SG Public Key Infrastructure (SG-PKI).

The SG TCP/CPS outlines the trustworthiness and integrity of the SG Root Certification Authority's operations. A fundamental concept underpinning the operation of the SG-PKI is trust. Trust must be realised in every aspect of the provision of Certification Services and Operations including Digital Certificate Holder applications, issuance, renewal, revocation or expiry.

With the exception of Certification Authorities issuing Qualified Certificates in accordance with Swedish Regulations, at SG's discretion, trustworthy parties may be permitted to operate Issuing Certification Authority and Registration Authority services within the SG-PKI.

SG ensures the integrity of Public Key Infrastructure's operational hierarchy by binding Participants to contractual agreements. This TCP/CPS is not intended to create a contractual relationship between SG and any Participant in the SG-PKI. This TCP/CPS provides a general overview of the SG-PKI including Digital Certificate Profiles as defined in Appendix A.

The SG-PKI is designed and is operated to comply with the broad strategic direction of existing international standards for the establishment and operation of a Public Key Infrastructure Certification Authority. Any person seeking to rely on Digital Certificates or participate within the SG-PKI must do so pursuant to definitive contractual documentation.

This TCP/CPS undergoes a regular review process and is subject to amendments.

The structure of this TCP/CPS is based on Internet Public Key Infrastructure Certificate Policy and Certification Practices Framework, but does not seek to adhere or follow it exactly.

1.1.2. Terms and Abbreviations

In this SG CP/CPS the following Key terms and Abbreviations shall have the following meaning in the operation of the SG-PKI unless context otherwise requires:

"Applicant" means an Individual or Organisation that has submitted an application for the issue of a Digital Certificate.

"Authorised Relying Party" means an Individual or Organisation that has entered into a Relying Party Agreement authorizing that person or Organisation to exercise Reasonable Reliance on Digital Certificates, subject to the terms and conditions set forth in the applicable Relying Party Agreement.

"Authentication" means the procedures and requirements, including the production of documentation (if applicable) necessary to ascertain and confirm an Identity. Authentication procedures are designed and intended to provide against fraud, imitation and deception ("Authenticate" and "Authenticated" to be construed accordingly).

"Certification" means the process of creating a Digital Certificate for an entity and binding that entity's identity to the Digital Certificate.

"Certification Authority" means an entity trusted by one or more entities to create, assign or revoke Digital Certificates.

"Certification Authority Officer" means a responsible person involved in the day to day operations of a Certification Authority.

"Certificate Policy & Certification Practice Statement" (CP/CPS) is a publicly available document that details the SG-PKI and describes the practices employed in issuing Digital Certificates.

"Certificate Holder" means a Holder of a Digital Certificate chained to the SG Root Certificate, including without limitation, organisations, individuals and/or hardware and/or software devices. A Certificate Holder is (i) named in a Digital Certificate or responsible for the Device named in a Digital Certificate and (ii) holds a

Private Key corresponding to the Public Key listed in that Digital Certificate.

“Certificate Holder Agreement” means a contract between a Certificate Holder and an Issuing Certification Authority that contains, expressly or by reference, the terms and conditions of use within the SG-PKI.

“Certificate Chain” means a chain of Digital Certificates required to validate a Holder’s Digital Certificate back through its respective Issuing Certification Authority to the Root Certification Authority.

“Certificate Policy” means a certificate policy adopted by an Issuing Certificate Authority operating within the SG-PKI that defines all associated rules and indicates the applicability of a Certificate to a particular community and/or class of application with common security requirements;

“Certificate Revocation” means the process of removing a Digital Certificate from the management system and indicating that the Key Pair related to that Digital Certificate should no longer be used.

“Certificate Revocation List” means a list of Digital Certificates signed by the Issuing Certification Authority that have been revoked.

“Counterparty” means a person that is known to a Nominating Registration Authority or its respective Subsidiaries or Holding Companies and where the relationship with the Counterparty was established in accordance with recognised and documented Know Your Customer standards and with whom the Registration Authority is reliably able to identify the Counterparty through business records maintained by the Registration Authority or obtained from its respective Subsidiaries or Holding Companies.

“Cryptographic Module” means secure software, device or utility that (i) generates Key Pairs; (ii) stores cryptographic information; and/or (iii) performs cryptographic functions. “Digital Certificate” means a digital identifier within the SG Public Key Infrastructure that: (i) identifies the Issuing Certification Authority; (ii) identifies the Holder; (iii) contains the Holder’s Public and Private Keys; (iv) specifies the Digital Certificate’s Operational Term; (v) is digitally signed by the Issuing Certification Authority; and (vi) has prescribed Key Usages and Reliance Factor that governs its issuance and use whether expressly included or incorporated by reference to this CP/CPS.

“Digital Signature” means data appended to, or a cryptographic transmission of, a data unit that allows a recipient of the data to prove the source and integrity of the data unit.

“Digital Transmission” means the transmission of information in an electronic format.

“Device” means software, hardware or other electronic or automated means configured to act in a particular way without human intervention.

“Device Certificate” means a Digital Certificate issued to identify a Device.

“Distinguished Name” means the unique identifier for the Holder of a Digital Certificate.

“Federal Information Processing Standards” means the standards that deal with a wide range of computer system components including: hardware, storage media, data files, codes, interfaces, data transmission, networking, data management, documentation, programming languages, software engineering, performance and security.

“Identify” means a process to distinguish a subject or entity from other subjects or entities.

“Identity” means a set of attributes which together uniquely identify a subject or entity.

“Identification” means reliance on data to distinguish and Identify an entity or subject.

“Individual” means a natural person.

“Issuing Certification Authority” means a Certification Authority duly authorised to operate by SG to issue Digital Certificates to Certificate Holders within the SG-PKI.

“Issuing Certification Authority Agreement” an agreement entered into between SG and an Issuing Certification Authority to provide Issuing Certification Authority services within the SG Public Key Infrastructure.

“Issuing Certification Authority Certificate” A Digital Certificate issued by the SG Root Certification Authority to an Issuing Certification Authority enabling that Issuing Certification Authority to issue Digital Certificates to Certificate Holders.

“Key” means a sequence of symbols that controls the operation of a cryptographic transformation (e.g. encipherment, decipherment, cryptographic check function computation, signature generation, or signature verification).

“Key Pair” means two related Keys, one being a Private Key and the other a Public Key having the ability whereby one of the pair will decrypt the other.

“MC” means Mentana-Claimssoft AG, Griesbergstr.8, D-31162 Bad Salzdetfurth.

“Object Identifier” means the unique identifier registered under the ISO registration standard to reference a specific object or object class.

“Operational Term” means the term of validity of a Digital Certificate commencing on the date of its issue and terminating on the earlier of (i) the date disclosed in that Digital Certificate or (ii) the date of that Digital Certificate’s Revocation.

“Organisation” means an entity that is legally recognised in its jurisdiction of domicile (and can include a body corporate or un-incorporate, partnership, trust, non-profit making Organisation, or Government entity).

“Participants” means participants within the SG Public Key Infrastructure and include (i) Issuing Certification Authorities and their Subsidiaries and Holding Companies; (ii) Registration Authorities and their Subsidiaries and Holding Companies; (iii) Certificate Holders, (including Certificate Applicants); (iv) Authorised Relying Parties.

“Policy Management Authority” means the SG body responsible for overseeing and approving CP/CPS amendments and general management.

“Proprietary Marks” means any patents (pending or otherwise), trade marks, trade names, logos, registered designs, symbols, emblems, insignia, fascia, slogans, copyrights, know-how, information, drawings, plans and other identifying materials whether or not registered or capable of registration and all other proprietary rights whatsoever owned by or available to SG adopted or designated now or at any time hereafter by SG for use in connection with the SG Public Key Infrastructure.

“Private Key” means a Key forming part of a Key Pair that is required to be kept secret and known only to the person that holds it.

“Public Key” means a Key forming part of a Key Pair that can be made public.

“Public Key Infrastructure” means a system for publishing the public key values used in public key cryptography. Also a system used in verifying, enrolling, and certifying users of a security application.

“Qualified Certificate” A Digital Certificate whose primary purpose is to identify a person with a high level of assurance, where the Digital Certificate meets the qualification requirements defined by the applicable legal framework of the European Directive on Electronic Signature, Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, 1999.

“SG” means SignGuard Europe AB, Drottninggatan 61, S-11121 Stockholm

“SG Issuing Certification Authority” means SG in its capacity as an Issuing Certification Authority.

“SG Public Key Infrastructure” SG-PKI means the infrastructure implemented and utilized by SG for the generation, distribution, management and archival of Keys, Digital Certificates and Certificate Revocation Lists and the Repository to which Digital Certificates and Certificate Revocation Lists are to be posted.

“SG Root Certification Authority” means SG in its capacity as a Root Certification Authority.

“Registration Authority” means a Registration Authority designated by an Issuing Certification Authority to operate within the SG Public Key Infrastructure responsible for identification and authentication of Certificate Holders.

“Registration Authority Agreement” an agreement entered into between an Issuing Certification Authority and a Registration Authority pursuant to which that Registration Authority is to provide its services within the SG-PKI.

“Registration Authority Certificate” means a digital identifier issued by an Issuing Certification Authority (including SG in its capacity as an Issuing Certification Authority) in connection with the establishment of a

Registration Authority within the SG-PKI.

“Registration Authority Officer” means an Individual designated by a Registration Authority as being authorized to perform the functions of that Registration Authority.

“Relying Party” means a party that acts in reliance on a Digital Certificate.

“Relying Party Agreement” sets forth the terms and conditions under which an Individual or Organisation is entitled to exercise Reasonable Reliance on Digital Certificates.

“Repository” means one or more databases of Digital Certificates and other relevant information maintained by Issuing Certification Authorities.

“Root Certification Authority Certificate” means the self-signed Digital Certificate issued to the SG Root Certification Authority.

“Root Certification Authority” means SG as the source Digital Certification Authority being a self-signed Digital Certification Authority that signs Issuing Certification Authority Certificates.

“Secure Signature Creation Device” (SSCD) means a secure container specifically designed to carry and protect a digital certificate most commonly associated with a security rating, for example Federal Information Processing Standards (FIPS) Levels 1,2,3 etc.

“Token” means a Cryptographic Module consisting of a hardware object (e.g., a “smartcard”), often with a memory and microchip.

“Utility Certificate” means a Digital Certificate issued to a Responsible Person/s to be used in the day to day administration of the SG Public Key Infrastructure.

“Validation” means an online check, by Online Certificate Status Protocol (OCSP) request, or a check of the applicable Certificate Revocation List(s) (in the absence of Online Certificate Status Protocol capability) of the validity of a Digital Certificate and the validity of any Digital Certificate in that Digital Certificate’s Certificate Chain for the purpose of confirming that the Digital Certificate is valid at the time of the check (i.e., it is not revoked or expired).

Abbreviations used:

<u>CA</u>	Certification Authority
<u>CP</u>	Certificate Policy
<u>CPS</u>	Certification Practice Statement
<u>CRL</u>	Certificate Revocation List
<u>DN</u>	Distinguished Name
<u>LDAP</u>	Lightweight Directory Access Protocol
<u>ISO</u>	International Standards Organization
<u>OID</u>	Object Identifier
<u>PKI</u>	Public Key Infrastructure
<u>RA</u>	Registration Authority
<u>X.500</u>	The ITU-T (International Telecommunication Union-T) standard that establishes a distributed, hierarchical directory protocol organized by country, region, Organization, etc.
<u>X.501</u>	The ITU-T (International Telecommunication Union-T) standard for use of Distinguished Names in an X.500 directory.
<u>X.509</u>	The ITU-T standard for Certificates.X.509 Version 3, refers to Certificates containing or capable of containing extensions.

1.2. Identification

Name of this document: SignGuard Root Certification Authority - Technical Certificate Policy and Certificate Practice Statement, Version 1.3.

1.3. Public Key Infrastructure Participants

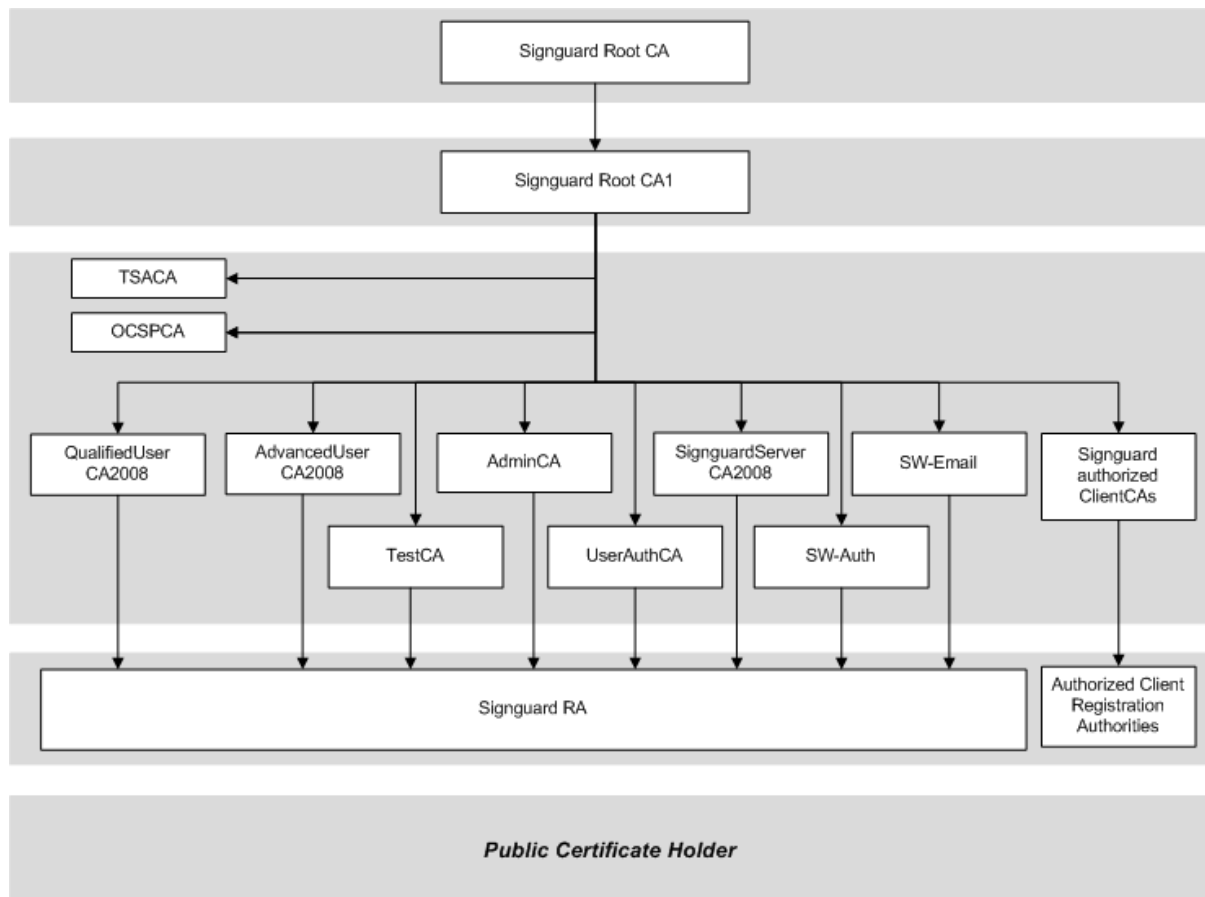
The SG TCP/CPS outlines the roles and responsibilities of all parties involved in the generation and use of Digital Certificates and the operation of all SG approved:

- Issuing Certification Authority services.
- Registration Authority services.

SG, in its capacity as the Root Certification Authority, holds the SG Root Certificates. The SG Root Certification Authority represents the top of the SG Public Key Infrastructure. The SG Root Certification Authority digitally creates, signs and issues Issuing Certification Authority Certificates with one of the Root Certificates identified above. Issuing Certificates are only issued to Approved Issuing Certification Authorities. An Approved Issuing Certification Authority utilises its Issuing CA Certificate to create, sign and issue Digital Certificates. Approved Registration Authorities act as the interface between Issuing Certification Authorities and an Applicant for a Digital Certificate. Approved Registration Authorities perform due diligence on potential Digital Certificate Holders and only successful applicants are approved and receive Digital Certificates.

An Authorised Issuing Certification Authority may also issue Device Certificates to itself, Subsidiaries or Holding Companies to Identify and Authenticate its Devices. Approved Registration Authorities perform due diligence on potential Device Certificate Holders and only successful Device Certificate applicants are approved and receive Device Certificates.

The diagram below illustrates the components of the SG Public Key Infrastructure:



SG provides identification and authentication services for Digital Certificate Holders, servers, and personal computer or network devices. The registration procedures set out in this TCP/CPS and in Appendix A define the credentials necessary to establish the identity of an individual or entity.

- For Qualified Digital Certificates according to the Swedish Digital Signature Law, all identification processes for individuals require applicants to present themselves for face-to-

face verification.

SG has established the SG Root Certification Authority under which a number of subordinate services operate. These subordinate services within the SG-PKI are:

- managed and operated by SG, or
- managed by clients but operated by SG (outsourced services), or
- managed and operated by clients (external services).

This TCP/CPS describes all subordinate services that operate under the SG Root Certification Authority, i.e. that are within the SG “chain of trust”.

Participants within the SG-PKI include:

- Certification Authorities
- Registration Authorities
- Digital Certificate Holders including applicants for Digital Certificates prior to Digital Certificate issuance
- Authorised Relying Parties

The practices described or referred to in this TCP/CPS:

- accommodate the diversity of the community and the scope of applicability within the SG chain of trust and
- adhere to the primary purpose of the TCP/CPS, of describing the uniformity and efficiency of practices throughout the SG Public Key Infrastructure.

In keeping with their primary purpose, the practices described in this TCP/CPS:

- are the minimum requirements necessary to ensure that Digital Certificate Holders and Authorised Relying Parties have a high level of assurance, and that critical functions are provided at appropriate levels of trust; and
- apply to all stakeholders, for the generation, issue, use and management of all Digital Certificates and Key Pairs.

SG digital certificates comply with the latest in Internet Standards (X509 v3) as set out in RFC 3280.

SG Certificates may not be used for: (i) any application requiring fail-safe applications performance such as: (a) the operation of nuclear power facilities, (b) air traffic control systems, (c) aircraft navigation systems, (d) weapons control systems, or (e) any other system whose failure could lead to injury, death or environmental damage; or (ii) transactions where applicable law prohibits the use of Digital Signatures for such transactions or where otherwise prohibited by law.

Applications are as follows: secure electronic mail, retail transactions, IPSEC applications, secure SSL/TLS applications, contracts signing applications, custom e-Commerce applications, digital signature applications etc.

1.3.1. Root Certification Authority

The SG Public Key Infrastructure contains one Root Certificate with a distinct common name for its Issuer and Subject. The SG Offline Root Certification Authority is named “SG Root CA”. Under this Offline Root Certificate, the SG Certification Authority issues an SG Working Root Certification Authority named “SG Root CA1”. This Root Certification Authority then issues Issuing Certification Authority Certificates and Time Stamping Authority Certificates in accordance with this SG TCP/CPS and related operational documents.

1.3.2. SG Obligations

SG is obligated to operate the SG Root Certification Authority, SG Issuing Certification Authority and SG Registration Authorities in accordance with this SG TCP/CPS and other relevant operational policies and procedures with respect to the issuance and management of Digital Certificates.

1.3.3. Issuing Certification Authority Obligations

Within the SG Public Key Infrastructure all Issuing Certification Authorities are responsible for the management of

Digital Certificates issued by them. Digital Certificate Management includes all aspects associated with the application, issue and revocation of Digital Certificates, including any required identification and authentication processes included in the Digital Certificate application process. Issuing Certification Authorities, if authorised to do so by SG, may rely on third party Registration Authorities in the performance of Digital Certificate Holder Identification and Authentication requirements. In circumstances where an Issuing Certification Authority has relied on a third party Registration Authority to perform Digital Certificate Holder Identification and Authentication the Issuing Certification Authority bears all responsibility and liability for the Identification and Authentication of its Digital Certificate Holders.

Notwithstanding the foregoing, Issuing Certification Authorities are required to conduct regular compliance audits of their Registration Authorities to ensure that they are complying with their obligations according to their respective Registration Authority Agreements (including the performance of Identification and Authentication requirements) and this SG TCP/CPS. Issuing Certification Authorities are required to ensure that all aspects of the services they offer and perform within the SG Public Key Infrastructure are in compliance at all times with this SG TCP/CPS.

- Without limitation to the generality of the foregoing, Issuing Certification Authorities are required to ensure that;
- Their Private Keys are used only in connection with the signature of Digital Certificates and Certificate Revocation Lists.
- All administrative procedures related to personnel and procedural requirements, and physical and technological security mechanisms, are maintained in accordance with this SG TCP/CPS.
- They comply at all times with all compliance audit requirements.
- They follow a privacy policy in accordance with this SG TCP/CPS and applicable Issuing Certification Authority Agreement.

1.3.4. Issuing Certification Authorities

Issuing Certification Authorities are Organisations authorised by SG to participate within the SG Public Key Infrastructure to create, issue, sign, revoke and otherwise manage Digital Certificates in accordance with their respective Issuing Certification Authority Agreement and this TCP/CPS. Generally, Issuing Certification Authorities will be authorised to issue and manage all types of Digital Certificates supported by this SG TCP/CPS.

- In accordance with the Swedish Digital Signature law, Qualified Certificates will only be issued from Issuing Certification Authorities owned and operated by SG and MC.

An Organisation wishing to participate in the SG Public Key Infrastructure, in the capacity of an Issuing Certification Authority, must supply to SG' satisfactory evidence of that Organisation's ability to operate in accordance with the performance standards; and other obligations that SG, in its sole discretion, requires of its Issuing Certification Authorities. Organisations wishing to act as Issuing Certification Authorities will be required to enter into and act in accordance with an Issuing Certification Authority Agreement and this CP and CPS. Without limitation to the generality of the foregoing, Issuing Certification Authorities are required to act in accordance with and to be bound by the terms of this SG CP and CPS. An Issuing Certification Authority may, but shall not be obliged to, detail its specific practices and other requirements in a Certificate Policy adopted by it following approval by the SG Policy Management Authority. SG operates the SG Root Certification Authority and SG Issuing Certification Authority in accordance with this TCP/CPS. Notwithstanding that the Issuing Certification Authority may delegate certain functions to a SG Registration Authority; the SG Issuing Certification Authority shall retain all responsibility for the management of Digital Certificates issued by it.

1.3.5. Registration Authority Obligations

Issuing Certification Authorities may, subject to the approval of SG, designate specific SG Registration Authorities to perform the Identification and Authentication and Digital Certificate request and revocation functions defined by this SG TCP/CPS. All SG Registration Authorities are required to fulfil their functions and obligations in accordance with this SG TCP/CPS and a Registration Authority Agreement to be entered into between the SG Registration Authority and the relevant Issuing Certification Authority.

SG Registration Authorities discharge their obligations in accordance with the practices outlined in overview in this TCP/CPS and applicable Registration Authority Agreement.

Registration Authorities must perform certain functions in accordance with this SG TCP/CPS and applicable Registration Authority Agreement which include but are not limited to;

- Process all Digital Certificate application requests.

- Maintain and process all supporting documentation related to Digital Certificate applications.
- Process all Digital Certificate Revocation requests.
- Comply with the provisions of its SG Registration Authority Agreement and the provisions of this SG TCP/CPS.
- Follow a privacy policy in accordance with this SG TCP/CPS and applicable SG Registration Authority Agreement.

1.3.6. Certificate Holders

1.3.6.1. Obligations and Responsibilities

Digital Certificate Holders are required to act in accordance with this TCP/CPS and Certificate Holder Agreement. A Digital Certificate Holder represents, warrants and covenants with and to the Registration Authority processing their application for a Digital Certificate that:

- Both as an applicant for a Digital Certificate and as a Digital Certificate Holder to submit complete and accurate information in connection with an application for a Digital Certificate.
- Comply fully with any and all information and procedures required in connection with the Identification and Authentication requirements relevant to the Digital Certificate issued. See Appendix A.
- Review the Digital Certificate that is issued and ensure that all the information set out therein is complete and accurate and to notify the Issuing Certification Authority, Registration Authority, or SG immediately in the event that the Digital Certificate contains any inaccuracies.
- Where Key Pairs are generated by an Applicant Digital Certificate Holder, the Applicant must promptly review, verify and accept or reject the information contained in the Digital Certificate signed by the Issuing Certification Authority.
- Secure the Private Key and take all reasonable and necessary precautions to prevent the theft, unauthorized viewing, tampering, compromise, loss, damage, interference, disclosure, modification or unauthorized use of its Private Key (to include password, hardware token or other activation data used to control access to the Participant's Private Key).
- Exercise sole and complete control and use of the Private Key that corresponds to the Digital Certificate Holder's Public Key.
- Immediately notify the Issuing Certification Authority, Registration Authority or SG in the event that their Private Key is compromised, or has reason to believe or suspects or ought reasonably to suspect that their Private Key has been lost, damaged, modified or accessed by another person, or compromised in any other way.
- Take all reasonable measures to avoid the compromise of the security or integrity of SG or the SG-PKI.
- Forthwith upon termination, revocation or expiry of the Digital Certificate (however caused), cease use of the Digital Certificate absolutely.
- At all times utilise the Digital Certificate in accordance with all applicable laws and regulations
- Use the signing key pairs for electronic signatures in accordance with the Digital Certificate profile and any other limitations known to, or which ought to be known to the Digital Certificate Holder.
- Discontinue the use of the digital signature key pair in the event that SG notifies the Digital Certificate Holder that the SG-PKI has been compromised.

1.3.6.2. Accepted Limitation of Liability

Digital Certificates include a brief statement detailing limitations of liability and disclaimers of warranty, with a reference to the full text of such warnings, limitations and disclaimers in this TCP/CPS. In accepting a Digital Certificate, Digital Certificate Holders acknowledge and agree to all such limitations and disclaimers.

1.3.7. Relying Parties

Authorised Relying Parties are Individuals or Organisations who are authorised by contract to exercise Reasonable Reliance on Digital Certificates in accordance with the terms and conditions of this SG TCP/CPS.

1.3.7.1. Obligations and Responsibilities

Authorised Relying parties are required to act in accordance with this SG TCP/CPS and Relying Party Agreement.

An Authorised Relying Party must utilise Digital Certificates and their corresponding Public Keys only for authorised and legal purposes and only in support of transactions or communications supported by the SG Public Key Infrastructure.

An Authorised Relying Party shall not place reliance on a Digital Certificate unless the circumstances of that intended reliance constitute Reasonable Reliance and that Authorised Relying Party is otherwise in compliance with the terms and conditions of their Relying Party Agreement. Any such Reliance is made solely at the risk of the relying Party.

1.3.7.2. Reasonable Reliance

An Authorised Relying Party shall not place reliance on a Digital Certificate unless the circumstances of that intended reliance constitute Reasonable Reliance (as set out below) and that Authorised Relying Party is otherwise in compliance with the terms and conditions of the Authorised Relying Party Agreement and this TCP/CPS. For the purposes of TCP/CPS and Relying Party Agreement, the term "Reasonable Reliance" means:

- that the attributes of the Digital Certificate relied upon are appropriate in all respects to the reliance placed upon that Digital Certificate by the Authorised Relying Party including, without limitation to the generality of the foregoing, the level of Identification and Authentication required in connection with the issue of the Digital Certificate relied upon.
- that the Authorised Relying Party has, at the time of that reliance, used the Digital Certificate for purposes appropriate and permitted under this TCP/CPS.
- that the Authorised Relying Party has, at the time of that reliance, acted in good faith and in a manner appropriate to all the circumstances known, or circumstances that ought reasonably to have been known to the Authorised Relying Party.
- that the Digital Certificate intended to be relied upon is valid and has not been revoked, the Authorised Relying Party being obliged to check the status of that Digital Certificate utilising either the SG Database, the SG Certificate Revocation List or the SG Online Certificate Status Protocol or otherwise in accordance with the provisions of this SG TCP/CPS.
- that the Authorised Relying Party has, at the time of that reliance, verified the Digital Signature, if any.
- that the Authorised Relying Party has, at the time of that reliance, verified that the Digital Signature, if any, was created during the Operational Term of the Digital Certificate being relied upon.
- that the Authorised Relying Party ensures that the data signed has not been altered following signature by utilising trusted application software.
- that the signature is trusted and the results of the signature are displayed correctly by utilising trusted application software.
- that the identity of the Digital Certificate Holder is displayed correctly by utilising trusted application software.
- that any alterations arising from security changes are identified by utilising trusted application software.

1.3.7.3. Accepted Limitation of Liability

Digital Certificates include a brief statement detailing limitations of liability and disclaimers of warranty, with a reference to the full text of such warnings, limitations and disclaimers in this TCP/CPS. In accepting a Digital Certificate, Relying Parties acknowledge and agree to all such limitations and disclaimers.

1.3.7.4. Assumptions about a Certificate Holder

A relying party shall make no assumptions about information that does not appear in a Digital Certificate.

1.3.7.5. Certificate Compromise

A party cannot rely on a Digital Certificate issued by SG if the party has actual or constructive notice of the compromise of the Digital Certificate or its associated private key. Such notice includes but is not limited to the

contents of the Digital Certificate and information incorporated in the Digital Certificate by reference, as well as the contents of this CP and CPS and the current set of revoked Digital Certificates published by SG (i.e. certificates have pointers to URLs where SG publishes status information, including Certificate Revocation Lists, CRLs).

1.3.8. Other Participants

Other Participants in the SG Public Key Infrastructure are required to act in accordance with this TCP/CPS and/or applicable Certificate Holder Agreement and/or Relying Party Agreement's or other relevant SG documentation.

1.4. Certificate Usage

At all times utilise its Digital Certificate in accordance with this SG TCP/CPS and all applicable laws and regulations.

1.4.1. Appropriate Certificate Usage

Digital Certificates may be used for identification, providing data confidentiality and data integrity, and for creating digital signatures.

The use of Digital Certificates supported by this SG TCP/CPS is restricted to parties authorised by contract to do so. Persons and entities other than those authorised by contract may not use Digital Certificates for any purpose. No reliance may be placed on a Digital Certificate by any Person unless that Person is an Authorised Relying Party.

A Digital Certificate does not convey evidence of authority of an Individual to act on behalf of any person or to undertake any particular act and Authorised Relying Parties are solely responsible for exercising due diligence and reasonable judgement before choosing to place any reliance whatsoever on a Digital Certificate. A Digital Certificate is not a grant, assurance, or confirmation from SG or any SG Provider of any authority, rights, or privilege save as expressly set out in this SG TCP/CPS or expressly set out in the Digital Certificate.

Any person participating within the SG-PKI irrevocably agrees, as a condition to such participation, that the issuance of all products and services contemplated by this SG TCP/CPS shall occur and shall be deemed to occur in Sweden and that the performance of SG obligations hereunder shall be performed and be deemed to be performed in Sweden.

1.4.2. Prohibited Certificate Usage

Digital Certificates may not be used and no participation is permitted in the SG Public Key Infrastructure (i) in circumstances that breach, contravene, or infringe the rights of others or (ii) in circumstances that offend, breach, or contravene any applicable law, statute, regulation, order, decree, or judgment of a court of competent jurisdiction or governmental order in Sweden or (iii) in connection with fraud, pornography, obscenity, hate, defamation or harassment.

No reliance may be placed on Digital Certificates and Digital Certificates may not be used in circumstances (i) where applicable law or regulation prohibits their use (ii) in breach of this SG TCP/CPS or the relevant User Agreement (iii) in any circumstances where the use of Digital Certificates could lead to death, injury, or damage to property; or (iv) as otherwise may be prohibited by the terms of issue.

1.5. Certificate Validity Period

The validity period of Digital Certificate Holder Certificates will be dependent on the class of Digital Certificate in question more fully disclosed in Section 10 of this TCP/CPS.

1.6. Policy Administration

1.6.1. Organisation Administering the TCP/CPS

SG operates the Policy Management Authority that is responsible for setting TCP/CPS and Certificate Profile direction for the overall public key infrastructure.

1.6.2. TCP/CPS Applicability

This SG TCP/CPS is applicable to all Digital Certificates issued by the SG Root Certification Authority and by Issuing Certification Authorities. Digital Certificates issued under this SG TCP/CPS are intended to support secure electronic commerce and the secure exchange of information by electronic means.

1.6.3. TCP/CPS Revisions

The SG Policy Management Authority is the responsible authority for changes to this TCP/CPS. There are two possible types of policy change:

- the issue of a new Certificate Policy & Certification Practice Statement (TCP/CPS); or
- a change to or alteration of a policy stated in an existing Certificate Policy & Certification Practice Statement (TCP/CPS).

If an existing TCP/CPS requires re-issue, the change process employed is the same as for as for initial publication, as described above. If a policy change is determined to have a material impact on a significant number of Digital Certificate Holders and relying parties of the TCP/CPS SG may, at its sole discretion, assign a new object identifier to the modified TCP/CPS.

1.6.3.1. Revisions without Notification

The only changes that may be made to this SG TCP/CPS without notification are editorial or typographical corrections or minor changes that do not, in the opinion of the Policy Management Authority, materially impact any participants within the SG-PKI.

1.6.3.2. Revisions with Notification

In this paragraph "level of trust" does not include those parts of the specification relating to the liabilities of the parties. Reference to "level of trust" applies solely to the technical/ administrative functions and any changes provided for under this clause shall not materially change this specification unless there is a significant business reason to do so.

Any change that increases the level of trust that can be placed in Digital Certificates issued under this SG CP and CPS or under policies that make reference to this SG TCP/CPS requires thirty (30) days prior notice.

Any change that decreases the level of trust that can be placed in Digital Certificates issued under this SG TCP/CPS or under policies that make reference to this SG TCP/CPS requires forty five (45) days prior notice. The SG TCP/CPS applicable to any Digital Certificate supported by this SG TCP/CPS shall be the SG TCP/CPS currently in effect; no provision is made for different versions of this SG TCP/CPS to remain in effect at the same time.

The SG Policy Management Authority has authority to evaluate all changes and determine whether prior notification is required and whether the SG TCP/CPS Object Identifier should be changed.

1.6.4. TCP/CPS Publication and Notification

New or amended SG TCP/CPS are published on the web site www.signguard.se/policies/policy.html. Issuing Certification Authorities are notified of changes to the SG TCP/CPS as and when they are approved.

1.6.5. Contact Person

This TCP/CPS is administered by the Policy Management Authority. Enquiries or other communications about this TCP/CPS should be addressed to SG.

SignGuard Europe AB
Policy Director
Drottninggatan 61
S-111 21 Stockholm

Organisation No. 556633-0220

Website: www.signguard.se

Electronic mail: policy@signguard.se

1.6.6. Person Determining the TCP/CPS Suitability

The SG Policy Management Authority determines the suitability of the TCP/CPS.

1.6.7. TCP/CPS Approval Procedures

This SG TCP/CPS is regularly reviewed and approved by the SG Policy Management Authority. Notice of proposed changes are recorded in the change log at the beginning of this SG TCP/CPS until they are approved, at which time the approved change will be recorded there permanently.

1.6.8. Publication of TCP/CPS

This TCP/CPS is published electronically in PDF format at www.signguard.se/policies/policy.html.

1.6.9. Frequency of Publication

Newly approved versions of this TCP/CPS, User Agreements and other relevant documents are published in accordance with the amendment, notification and other relevant provisions contained within those agreements.

1.6.10. Access Control

SG does operate access controls in connection with the availability of documentation. Access is generally available only to participants in the SG Public Key Infrastructure where necessary.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1. Repositories

The SG Repository serves as the primary repository. However, copies of the X.500 Directory may be published at such other locations as are required for the efficient operation of the SG Public Key Infrastructure.

The SG Root Certification Authority and chained Issuing Certification Authorities maintain in a Repository a list of all Digital Certificates issued and all Revoked Digital Certificates.

2.2. Publication of Certificate Information

The SG Root Certification Authority and chained Issuing Certification Authorities publish a Repository that lists all Digital Certificates issued and all the Digital Certificates that have been revoked. The location of the repository and Online Certificate Status Protocol responders are given in the individual Certificate Profiles more fully disclosed in Appendix A of this TCP/CPS.

2.3. Time or Frequency of Publication

Digital Certificate information is published promptly following generation and issue and within one hour of being revoked.

2.4. Access Controls on Repositories

Read only Access to Repositories is available to Relying Parties twenty four (24) hours per day, seven (7) days per week, except for reasonable maintenance requirements, where access is deemed necessary. Queries to the repository must specify individual certificate information. SG is the only entity that has write access to Repositories.

3. IDENTIFICATION AND AUTHENTICATION

SG implements rigorous authentication requirements, to ensure that the identity of the Digital Certificate Holder is proven. This may include face-to-face identity verification at the beginning of the Digital Certificate request procedure or at some point prior to Digital Certificate delivery to the Digital Certificate Holder. The registration procedure will depend on the type of Digital Certificate that is being applied for.

Issuing Certification Authorities may perform the Identification and Authentication required in connection with the issue of Digital Certificates, or they may delegate the responsibility to one or more Registration Authority's. The level of Identification and Authentication depends on the class of Digital Certificate being issued. See Appendix A for Digital Certificate profiles and the relevant Identification and Authentications requirements.

3.1. Naming

3.1.1. Types of Names

All Digital Certificate Holders require a distinguished name that is in compliance with the X.500 standard for Distinguished Names.

The SG Certification Authorities approves naming conventions for the creation of distinguished names for Issuing Certification Authority applicants. Different naming conventions may be used in different policy domains.

The Subject Name of all Digital Certificates issued to Individuals shall be the authenticated common name of the Digital Certificate holder. Each User must have a unique and identifiable X.501 Distinguished Name (DN). The Distinguished Name includes the following fields:

- Common Name (CN)
- Serial Number (SN) – applies only for the SW-Email CA

The Common Name (CN) may contain the applicant's first and last name (Surname). The Common Name, the Organisation and the Organisational Unit (where applicable) are the only fields authenticated during the Registration procedure. The User may choose whether to include State and Country but they are not verified in any way. Such attributes do not necessarily indicate the subscriber's country of citizenship, country of residence, or the country of issuance of the Digital Certificate.

The field Serial can but must not contain the Swedish Social Security Number of the User.

- For Qualified Certificates issued according to the Swedish Digital Signature law, all fields containing information - except the Email Address - must be verified by the appropriate Registration Authority by reference to appropriate documentation and face to face presentation of Government Issued ID, Passport, Swedish drivers' license or other approved SIS, Swedish Standards Institute, identification cards.

3.1.2. Need for Names to be meaningful

Distinguished names must be meaningful, unambiguous and unique. Pseudonymous names may be used. SG supports the use of Digital Certificates as a form of identification within a particular community of interest.

The contents of the Digital Certificate Subject and Name fields must have a meaningful association with the name of the Individual, Organisation, or Device. In the case of Individuals, the name should consist of the first name, last name, and any middle initial. In the case of Organisations, the name shall meaningfully reflect the legal name of the Organisation or the trading or business name of that Organisation. In the case of a Device, the name shall state the name of the Device and the name of the Organisation responsible for that Device.

3.1.3. Pseudonymous Certificate Holders

SG Registration Authorities, their Subsidiaries or Holding Companies may request Class 5 (Pseudonym) Digital Certificates to be issued by the SG Issuing Certification Authority to Employees of the Nominating Registration Authority, their Subsidiaries or Holding Companies.

3.1.4. Rules for Interpreting Various Name Forms

Fields contained in Digital Certificates are in compliance with this TCP/CPS and the Digital Certificate Profiles

detailed in Appendix A.

3.1.5. Uniqueness of Names

SG Registration Authorities propose and approve distinguished names for Applicants, and as a minimum check that a proposed distinguished name is unique and verify that the name is not already listed in the SG X.500 Directory.

The Subject Name of each Digital Certificate issued by a Issuing Certification Authority shall be unique within each class of Digital Certificate issued by that Issuing Certification Authority and shall conform to all applicable X.500 standards for the uniqueness of names. The Issuing Certification Authority may, if necessary, insert additional numbers or letters to the Digital Certificate subject's common name in order to distinguish between two Digital Certificates that would otherwise have the same Subject Name.

3.1.6. Recognition, Authentication and Role of Trademarks

Issuing Certification Authorities are not obligated to seek evidence of trademark usage by any Organisation.

3.2. Initial Identity Validation

Identity Validation is in compliance with this TCP/CPS and the Digital Certificate Profiles detailed in Appendix A.

3.2.1. Method to Prove Possession of Private Key

Issuing Certification Authorities shall establish that each Applicant for a Digital Certificate is in possession and control of the Private Key corresponding to the Public Key contained in the Digital Certificate application. The Issuing Certification Authority shall do so in accordance with an appropriate secure protocol, such as the IETF PKIX Certificate Management Protocol.

Where Key Pairs are generated by an Applicant, the relevant Issuing Certification Authority and/or Registration Authority must satisfy themselves that the Applicant does in fact possess the Private Key that correspond to the Public Key received from the Applicant. This may typically be accomplished by exchanging digitally signed and encrypted e-mail messages with the Applicant.

The relevant Issuing Certification Authority and/or Registration Authority also take reasonable steps to ensure the Applicant is the true owner of the Key Pairs. Reasonable steps might typically consist of:

- the relevant Issuing Certification Authority and/or Registration Authority checking and arranging for any other Issuing Certification Authority and/or Registration Authority within the policy domain to check their records to ensure the Public Keys are not already listed against any current operational or revoked Digital Certificates; and
- if appropriate, obtaining a statutory declaration from the Applicant that they are the true owner of the Key Pairs.

If any doubt exists, the relevant Issuing Certification Authority and/or Registration Authority should not perform certification of the Key.

- For Qualified Certificates, in accordance with Swedish Digital Signature law, private keys are generated on secure signature smartcards in the presence of the Certificate Holder. The Certificate Holder is responsible for securing the smartcard with a Personal Identification Number directly on the Secure Signature Creation Device (SSCD).

3.2.2. Authentication of Individual Identity

An Individual's Identity is to be authenticated in accordance with all relevant application and other documentation.

3.2.3. Non-Verified Certificate Holder Information

The SG Issuing Certification Authority may accept any form of Non-Verified Holder Information for the Issue of Class 1 Digital Certificates.

An Issuing Certification Authority within the SG Public Key Infrastructure may accept the following Non Verified Digital Certificate Holder Information for all other classes of Digital Certificate:

- Email address

- Organisational Unit
 - Locality
- For Qualified Certificates, in accordance with the Swedish Digital Signature law, all certificate fields and registration information are verified by appropriate documentation.

3.2.4. Criteria for Interoperation

The SG-PKI operates in accordance with open standards under the X.509 criteria and as such Digital Certificates issued by the SG Issuing Certification Authority are fully interoperable with Digital Certificates issued by other Issuing Certification Authorities. The SG Root CA1 Private Key is used to sign the Public Keys of subordinate Issuing Certification Authorities, which may be enterprise Certification Authorities operated by SG customers.

3.3. Identification and Authentication for Renewal Requests

SG does not support renewal. Key Pairs must always expire at the same time as the associated Digital Certificate. If a renewal request is accepted, both new Digital Certificates and new Key Pairs are issued. Renewal is not permitted after Digital Certificate revocation. Application for a Digital Certificate following revocation is treated as though the person requesting renewal were a new Applicant.

3.4. Identification and Authentication for Revocation Requests

A request to revoke Keys and Digital Certificates may be submitted by persons authorised to do so under relevant contractual documentation.

3.4.1. Issuing Certification Authority

An Issuing Certification Authority can revoke a Digital Certificate it has issued by an authorised individual acting under the authority of the Policy Management Authority using a SG Utility Digital Certificate.

3.4.2. Registration Authority

A Registration Authority may request the revocation of Digital Certificates it has caused to be issued by requesting, in person, by digitally signed electronic mail or by authenticating to the SG Digital Certificate administration system that an authorised member of Issuing Certification Authority staff revokes the Digital Certificate/s in question.

3.4.3. Certificate Holder

A Digital Certificate Holder may request that their Digital Certificate be revoked by:

- Logging on to the SG Extranet: www.signguard.se with his/her credentials.

4. CERTIFICATE LIFE-CYCLE OPERATION REQUIREMENTS

4.1. Certificate Application

Digital Certificate applications are subject to various assessment procedures depending upon the type of Digital Certificate applied for.

4.1.1. Who Can Submit a Certificate Application

An application in a form prescribed by the Issuing Certification Authority must be completed by Applicants, which includes all registration information as described by this SG TCP/CPS (including Appendix A, Section 10) and the relevant User Agreement or other terms and conditions upon which the Digital Certificate is to be issued. All applications are subject to review, approval, and acceptance by the Issuing Certification Authority in its discretion.

4.1.2. Enrolment Process and Responsibilities

Certain information concerning applications for Digital Certificates is set out in this SG TCP/CPS. However, the issue of Digital Certificates by Issuing Certification Authorities will be pursuant to forms and documentation required by that Issuing Certification Authority. Notwithstanding the foregoing, the following steps are required in any application for a Digital Certificate: (i) Identity of the Holder or Device is to be established in accordance with Appendix A, (ii) a Key Pair for the Digital Certificate is to be generated in a secure fashion, (iii) the binding of the Key Pair to the Digital Certificate shall occur as set forth in this Certificate Policy & Certification Practice Statement, and (iv) the Issuing Certification Authority shall enter into contractual relations for the use of that Digital Certificate and the SG-PKI. Individuals and Organisations may generate a Digital Certificate application.

Each Issuing Certification Authority can adopt her own application forms and procedures that Applicants will be required to satisfy. Each Holder of a Digital Certificate is required to be bound by contract with respect to the use of that Digital Certificate. These contracts may be directly between the Issuing Certification Authority and the Holder or imposed upon that Holder through terms and conditions binding upon him. All agreements concerning the use of, or reliance upon, Digital Certificates issued within the SG-PKI must incorporate by reference the requirements of this SG TCP/CPS as it may be amended from time to time.

4.2. Certificate Application Processing

4.2.1. Approval or Rejection of Certificate Applications

A Registration Authority will approve or reject Digital Certificate Holder applications based upon the Digital Certificate Holders meeting the requirements of this TCP/CPS and the Digital Certificate Profiles contained in Appendix A.

SG may override any decision to approve a Digital Certificate Holder Application.

4.2.2. Time to Process Certificate Applications

Registration and Issuing Certification Authorities operating within the SG Public Key Infrastructure are under no obligation to process Digital Certificate Applications other than within a commercially reasonable time.

4.3. Certificate Issuance

4.3.1. Certification Authority Actions during Certificate Issuance

Digital Certificate issuance is governed by and should comply with the practices described in and any requirements imposed by the SG TCP/CPS.

4.3.1.1. SG Root Certification Authority

The Offline Root Certification Authority Certificate (SignguardRoot CA) has been self-generated and self-signed. The Working Root Certification Authority Certificate (SignguardRoot CA1) is signed by the Offline Root Certification Authority Certificate (SignguardRoot CA).

4.3.1.2. SG Issuing Certification Authority Certificates

Upon accepting the terms and conditions of the SG Issuing Certification Authority Agreement by the Issuing Certification Authority, successful completion of the Issuing Certification Authority application process as

prescribed by SG, and final approval of the application by the SG Root Certification Authority, the SG Root Certification Authority issues the Issuing Certification Authority Digital Certificate to the relevant Issuing Certification Authority.

4.3.1.3. SG Registration Authority Appointment

Upon accepting the terms and conditions of the SG Registration Authority Agreement, successful completion of the Registration Authority application process and final approval of the application by the nominating Issuing Certification Authority, the nominating Issuing Certification Authority a Registration Authority becomes duly appointed and appropriately trained and qualified staff members of the Registration Authority are eligible for Registration Authority Officer Digital Certificates.

4.3.1.4. Registration Authority Officers Certificate

As part of the application process, Registration Authorities are required to nominate one or more persons within their Organisation to take responsibility for the operation their Registration Authority's functions. Those nominated persons will each be issued with a Registration Authority Officers Digital Certificate.

4.3.1.5. Certificate Holder Certificates

Upon accepting the terms and conditions of the User Agreement or other relevant agreement by the Applying Digital Certificate Holder, the successful completion of the application process and final approval of the application by the Issuing Certification Authority, the Issuing Certification Authority issues the Digital Certificate to the Applicant or Device.

4.3.2. Notification to Applicant Certificate Holder by the Certification Authority of Issuance of Certificate

Issuing and Registration Authorities within the SG-PKI may choose to notify Applicant Digital Certificate Holders of Digital Certificate Issuance.

4.4. Certificate Acceptance

Digital Certificate acceptance is governed by and should comply with the practices described in and any requirements imposed by the SG TCP/CPS.

Until a Digital Certificate is accepted, it is not published in any Repository or otherwise made publicly available. By using a Digital Certificate, the Holder thereof certifies and agrees to the statements contained in the notice of approval. TCP/CPS defines what constitutes acceptance of a Digital Certificate. An Applicant that accepts a Digital Certificate warrants to the relevant Issuing Certification Authority that all information supplied in connection with the application process and all information included in the Digital Certificate issued to them is true, complete, and not misleading. Without limitation to the generality of the foregoing, the use of a Digital Certificate or the reliance upon a Digital Certificate signifies acceptance by that person of the terms and conditions of this SG TCP/CPS and Certificate Holder Agreement (as the same may, from time to time, be amended or supplemented) by which they irrevocably agree to be bound.

By accepting a Digital Certificate issued by an Authorised Issuing Certification Authority operating within the SG Public Key Infrastructure, the Digital Certificate Holder expressly agrees with SG and to all who reasonably rely on the information contained in the Digital Certificate that at the time of acceptance and throughout the operational period of the Digital Certificate, until notified otherwise by the Digital Certificate Holder that:

- No unauthorised person has ever had access to the Digital Certificate Holder's private key;
- All representations made by the Digital Certificate Holder to SG regarding the information contained in the Digital Certificate are true;
- All information contained in the Digital Certificate is true to the extent that the Digital Certificate Holder had knowledge or notice of such information, and does not promptly notify SG of any material inaccuracies in such information;
- The Digital Certificate is being used exclusively for authorised and legal purposes, consistent with this TCP/CPS.

4.4.1. Notice of Acceptance

BY ACCEPTING A DIGITAL CERTIFICATE, THE DIGITAL CERTIFICATE HOLDER ACKNOWLEDGES THAT THEY AGREE TO THE TERMS AND CONDITIONS CONTAINED IN THIS CP/CPS AND THE APPLICABLE CERTIFICATE HOLDER

AGREEMENT BY ACCEPTING A DIGITAL CERTIFICATE, THE DIGITAL CERTIFICATE HOLDER ASSUMES A DUTY TO RETAIN CONTROL OF THE DIGITAL CERTIFICATE HOLDER'S PRIVATE KEY, TO USE A TRUSTWORTHY SYSTEM AND TO TAKE REASONABLE PRECAUTIONS TO PREVENT ITS LOSS EXCLUSION MODIFICATION OR UNAUTHORISED USE.

BY ACCEPTING A DIGITAL CERTIFICATE, THE DIGITAL CERTIFICATE HOLDER AGREES TO INDEMNIFY AND HOLD SG AND ITS AGENTS AND CONTRACTORS HARMLESS FROM ANY ACTS OR OMISSIONS RESULTING IN LIABILITY, ANY LOSS OR DAMAGE, AND ANY SUITS, PROCEEDINGS OR CLAIMS, AND EXPENSES OF ANY KIND, INCLUDING REASONABLE ATTORNEYS FEES, THAT SG, ITS AGENTS AND/OR CONTRACTORS MAY INCUR, THAT ARE CAUSED BY THE USE OR PUBLICATION OF A DIGITAL CERTIFICATE AND THAT ARISE FROM (I) FALSEHOOD OR MISREPRESENTATION OF FACT BY THE DIGITAL CERTIFICATE HOLDER (OR A PERSON ACTING UPON INSTRUCTIONS FROM ANYONE AUTHORISED BY THE DIGITAL CERTIFICATE HOLDER); (II) FAILURE BY THE DIGITAL CERTIFICATE HOLDER TO DISCLOSE A MATERIAL FACT, IF THE MISREPRESENTATION OR OMISSION WAS MADE NEGLIGENTLY OR WITH INTENT TO DECEIVE SG OR ANY PERSON RECEIVING OR RELYING ON THE DIGITAL CERTIFICATE; (III) FAILURE TO PROTECT THE DIGITAL CERTIFICATE HOLDER'S PRIVATE KEY, TO USE A TRUSTWORTHY SYSTEM OR TO OTHERWISE TAKE THE PRECAUTIONS NECESSARY TO PREVENT THE COMPROMISE, LOSS, DISCLOSURE, MODIFICATION OR UNAUTHORISED USE OF THE DIGITAL CERTIFICATE HOLDER'S PRIVATE KEY; (IV) USE OF THE DIGITAL CERTIFICATE FOR A PURPOSE WHICH IS LIBELLOUS OR CONSTITUTES MALICIOUS FALSEHOOD OR DISPARAGEMENT OF GOODS OR SERVICES, OR IS OTHERWISE DEFAMATORY, IS IMMORAL, OBSCENE, PORNOGRAPHIC, IS ILLEGAL OR ADVOCATES ILLEGAL ACTIVITY, OR CONSTITUTES A VIOLATION OF PRIVACY OR INFRINGES THE INTELLECTUAL PROPERTY RIGHTS OF SG OR A THIRD PARTY.

4.4.2. Conduct Constituting Certificate Acceptance

The following constitutes acceptance of a Digital Certificate within the SG Public Key Infrastructure:

- Downloading, installing or otherwise taking delivery of a Digital Certificate.

4.4.3. Publication of the Certificate by the Certification Authority

All Digital Certificates issued within the SG-PKI are made available in public repositories by default, except where Digital Certificate Holders have requested that the Digital Certificate should not be published.

4.4.4. Notification of Certificate Issuance by the Certification Authority to Other Entities

Issuing and Registration Authorities within the SG Public Key Infrastructure may choose to notify other Entities of Digital Certificate Issuance.

4.5. Key Pair and Certificate Usage

4.5.1. Certificate Holder Private Key and Certificate Usage

Within the SG-PKI a Digital Certificate Holder may only use the Public and corresponding Private Key in a Digital Certificate for its lawful and indented use when the Digital Certificate Holder has accepted the User Agreement. The Digital Certificate Holder Accepts the User Agreement by accepting the Digital Certificate and by accepting the Digital Certificate unconditionally agrees to use the Digital Certificate in a manner consistent with the Key-Usage field extensions included in the Digital Certificate Profile.

4.5.2. Relying Party Public Key and Certificate Usage

A Party seeking to rely on a Digital Certificate issued within the SG Public Key Infrastructure agrees to and accepts the Relying Party Agreement by querying the existence or validity of; or by seeking to place or by placing reliance upon on a Digital Certificate.

Relying Parties are obliged to seek further independent assurances before any act of reliance is deemed reasonable and at a minimum must assess:

- The appropriateness of the use of the Digital Certificate for any given purpose and that the use is not prohibited by this TCP/CPS.
- That the Digital Certificate is being used in accordance with its Key-Usage field extensions.
- That the Digital Certificate is valid at the time of reliance by reference to Online Certificate Status Protocol and/or Certificate Revocation List checks.

4.6. Certificate Renewal

Certificate Renewal means the issuance of a new certificate without changing the public key or any other

information in the certificate.

The SG-PKI does not support Renewal and the following do not apply to this TCP/CPS:

- Circumstances for Digital Certificate Renewal.
- Who may request certification of a new public key.
- Processing Digital Certificate Renewal Requests.
- Notification of new Digital Certificate issuance to subscriber.
- Conduct constituting acceptance of a Renewed Digital Certificate.
- Publication of the Renewed Digital Certificate by the Digital Certification Authority.
- Notification of Digital Certificate issuance by the Certification Authority to other entities.

4.7. Certificate Modification

The SG-PKI does not support Digital Certificate Modification and the following do not apply to this TCP/CPS:

- Circumstance for Digital Certificate modification.
- Who may request Digital Certificate modification.
- Processing Digital Certificate modification requests.
- Notification of new Digital Certificates issuance to subscriber.
- Conduct constituting acceptance of modified Digital Certificate.
- Publication of the modified Digital Certificate.
- Notification of Digital Certificate issuance by the Certification Authority to other entities.

4.8. Certificate Revocation and Suspension

4.8.1. Circumstances for Revocation

Digital certificates shall be revoked when any of the information on a Digital Certificate changes or becomes obsolete or when the private key associated with the Digital Certificate is compromised or suspected to be compromised. A Digital Certificate will be revoked in the following instances upon notification:

- SG Digital Certification Authority key compromise
- Digital Certificate Holder profile creation error
- Key Compromise including unauthorised access or suspected unauthorised access to private keys lost or suspected lost keys, stolen or suspected stolen keys, destroyed or suspected destroyed keys or superseded.
- The Digital Certificate Holder has failed to meet their obligations under this SG TCP/CPS or any other agreement, regulation, or law that may be in force with respect to that Digital Certificate;
- Affiliation change
- Cessation of operation
- Incorrect information contained in Digital Certificate
- Digital Certificate Holder death
- Digital Certificate Holder request
- Issuing Registration Authority Request
- Breach of Certificate Holder agreement with SG

- Upon Authority request

In the event that an Issuing Certification Authority determines that its Digital Certificates or the SG-PKI could become compromised and that revocation of Digital Certificates is in the interests of the PKI, following remedial action, SG will authorise the reissue of Digital Certificates to Holders at no charge, unless the actions of the Holders were in breach of the SG TCP/CPS or other contractual documents.

4.8.2. Who Can Request Revocation

The following entities may request revocation of a Digital Certificate Holder Digital Certificate:

4.8.2.1. SignGuard Europe AB

SG may revoke any Digital Certificate issued within the SG-PKI at its sole discretion, and shall publish the list of revoked Digital Certificates in a publicly accessible Certificate Revocation List.

4.8.2.2. Certificate Holder

A Digital Certificate Holder within the SG-PKI may request revocation of their Digital Certificate.

4.8.3. Procedure for Revocation Request

SG will revoke a Digital Certificate upon receipt of a valid request. A revocation request should be promptly and directly communicated to the Issuing Certification Authority and the Registration Authority that approved or acted in connection with the issue thereof. The Digital Certificate Holder may be required to submit the revocation request via the SG Extranet. The Digital Certificate Holder, Registration Authority or Issuing Certification Authority may be required to provide a pass phrase that will be used to activate the revocation process. Digital Certificate revocation requests may also be issued by contacting the administrators of the Issuing Certification Authority or Registration Authority administrators directly. A revocation request may be communicated electronically if it is digitally signed with the Private Key of the Holder requesting revocation.

4.8.4. Revocation Request Grace Period

No grace period is permitted once a revocation request has been verified. Issuing Certification Authorities will revoke Digital Certificates as soon as reasonably practical following verification of a revocation request.

4.8.5. Time within which the Certification Authority Must Process the Revocation Request

The Issuing Certification Authority must revoke the Digital Certificate within one (1) hour of receipt of a valid revocation request.

4.8.6. Revocation Checking Requirement for Relying Parties

Digital Certificate revocation information is provided via the Certificate Revocation List in the SG X.500 Directory services.

4.8.7. Certificate Revocation List Issuance Frequency

The Certificate Revocation List is published at one (1) hour intervals twenty four (24) hours a day, seven (7) days a week. The Certificate Revocation List in the X.500 Directory is updated at the time of Digital Certificate Revocation.

When an Issuing Certification Authority provides Certificate Revocation Lists as a method of verifying the validity and status of Digital Certificates, the following requirements will apply:

- Authorised Relying Parties who rely on a Certificate Revocation List must in their validation requests check a current, valid Certificate Revocation List for the Issuing Certification Authority in the Digital Certificate path and obtain a current Certificate Revocation List; and
- Authorised Relying Parties who rely on a Certificate Revocation List must (i) check for an interim Certificate Revocation List before relying on a Digital Certificate, and (ii) log their validation requests.

Failure to do so negates the ability of the Authorised Relying Party to claim that it acted on the Digital Certificate with Reasonable Reliance.

4.8.8. Maximum Latency for Certificate Revocation List

The maximum latency for the Certificate Revocation list is one (1) hour.

4.8.9. On-Line Revocation/Status Checking Availability

The X.500 Directory provides Digital Certificate information services. SG seeks to provide availability for the X.500 Directory seven (7) days a week, twenty four (24) hours a day but is subject to routine maintenance.

4.8.10. On-Line Revocation Checking Requirement

When an Issuing Certification Authority provides an on line Digital Certificate status database as a method of verifying the validity and status of Digital Certificates, the Authorised Relying Party must validate the Digital Certificate in accordance with that method and log the validation request.

An entity that downloads a Certificate Revocation List from a repository shall verify the authenticity of the Certificate Revocation List by checking its digital signature and the associated Digital Certificate path.

Failure to do so negates the ability of the Authorised Relying Party to claim that it acted on the Digital Certificate with Reasonable Reliance.

4.8.11. Other Forms of Revocation Advertisements Available

There are no other forms of Revocation Advertisements available.

4.8.12. Special Requirements Re-Key Compromise

SG does not support Re-Keying.

4.8.13. Circumstances for Suspension

No suspension of Digital Certificates is permissible within the SG-PKI.

4.8.14. Who Can Request Suspension

No suspension of Digital Certificates is permissible within the SG-PKI.

4.8.15. Procedure for Suspension Request

No suspension of Digital Certificates is permissible within the SG-PKI.

4.8.16. Limits on Suspension Period

No suspension of Digital Certificates is permissible within the SG-PKI.

4.9. Certificate Status Services

4.9.1. Operational Characteristics

The Status of Digital Certificates issued within the SG-PKI is published in a Certificate Revocation List (usually: http://pki.signguard.se/ca/issuing_ca_name.crl) and/or is made available via Online Certificate Status Protocol (usually: http://ocsp.signguard.se/short_issuing_ca_name).

The URLs can be found in the within each certificate in the attributes "Authority Information Access" (for OCSP) and "CRL Distribution" (for CSP).For details also see Appendix A.

4.9.2. Service Availability

Digital Certificate status services are available twenty four (24) hours a day, seven (7) days a week with a availability of approximately 99,5%. Unavailability or downtimes due to technical maintenance and updates are possible.

4.9.3. Optional Features

No optional features available.

4.10. End of Subscription

Within the SG Public Key Infrastructure a Digital Certificate Holder may end a subscription by:

- Allowing a Digital Certificate to expire without renewing the Digital Certificate.
- Revoking a Digital Certificate without renewing it.

4.11. Key Escrow and Recovery

The SG-PKI does not support Key Escrow.

4.11.1. Key Escrow and Recovery Policy and Practices

The SG-PKI does not support Key Escrow.

4.11.2. Session Key Encapsulation and Recovery Policy and Practices

Not Applicable.

5. FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS

5.1. Physical Controls

SG manages and implements appropriate physical security controls to restrict access to the hardware and software used in connection with Issuing Certification Authority operations wherever those operations physically occur.

5.1.1. Site Location and construction

The site location of SG is in a secure environment in Hannover, Germany (www.hostway.de, www.hostway.com). SG operates their servers within a secure Hostway data-center that meets the standards of an independent security certification body, at a highly protected level. The location is equipped with redundant UPS and redundant Diesel Engines which guarantees continuous power delivery. The data-center is multiply connected to independent Internet backbones providers which also are directly connected to a second location in Frankfurt, Germany with own redundant Internet backbones connections. The location is guarded and run twenty four (24) hours a day and seven (7) days a week. The PKI servers are located in a closed rack. Direct access to the PKI servers is only possible for already known and authorised persons: The personally access will always have to be prior announced. An adequate ID-card always has to be presented to access the data-center.

5.1.2. Physical Access

SG permits entry to its secure operating area only to security cleared authorized personnel.

5.1.3. Power and Air-Conditioning

The data-centers secure operating area is connected to a standard power supply. All critical components are connected to uninterrupted power supply (UPS) units, to prevent abnormal shutdown in the event of a power failure. Automatic failover to standby diesel generators is provided.

5.1.4. Water Exposures

The data-center secure operating area provides protection against water.

5.1.5. Fire Prevention and Protection

The data-center secure operating area provides protection against fire.

5.1.6. Media Storage

All magnetic media containing SG-PKI information, including backup media, are stored in containers, cabinets or safes with fire protection capabilities and are located either within the SG service operations area or in a secure off-site storage area.

5.1.7. Waste Disposal

Paper documents and magnetic media containing trusted elements of SG or commercially sensitive or confidential information are securely disposed of by:

- in the case of magnetic media: physical damage to, or complete destruction of the asset or the use of an approved utility to wipe or overwrite magnetic media;
- in the case of printed material, shredding, or destruction by an approved service.

5.1.8. Off-Site Backup

Endorsed off-site storage agents are used for the storage and retention of backup software and data. The off-site storage:

- is available to authorized personnel twenty four (24) hours per day seven days per week for the purpose of retrieving software and data; and
- has appropriate levels of physical security in place.

5.2. Procedural Controls

Administrative processes are dealt with and described in detail in the various documents used within and supporting the SG-PKI.

Issuing Certification Authorities are required to ensure that administrative procedures related to personnel and procedural requirements, and physical and technological security mechanisms, are maintained in accordance with this TCP/CPS and other relevant operational documents.

5.2.1. Trusted Roles

In order to ensure that one person acting alone cannot circumvent the entire system, responsibilities are shared by multiple roles and individuals. Oversight may be in the form of a person who is not directly involved in issuing Digital Certificates examining system records or audit logs to ensure that other persons are acting within the realms of their responsibilities and within the stated security policy.

This is accomplished by creating separate roles and accounts on the service workstation, each of which has a limited amount of capability. This method allows a system of "checks and balances" to occur among the various roles.

5.2.2. Number of Persons Required per Task

At least two people are assigned to each trusted role to ensure adequate support at all times except verifying and reviewing audit logs. Some roles are assigned to different people to ensure no conflict of interest occurs and to prevent the possibility of accidental or intentional compromise of any component of the Digital Certification Authority infrastructure, most especially the Root Certification Authority and Operational Digital Certification Authority Private Keys, and customer Private Keys if held temporarily by SG during the registration process.

Digital Certification Authority key-pair generation and initialisation of each of the Digital Certification Authority (Root and Operational) shall require the active participation of at least two trusted individuals in each case. Such sensitive operations also require the active participation and oversight of senior management.

Issuing Certification Authorities will utilize commercially reasonable practices to ensure that one person acting alone cannot circumvent safeguards. Issuing Certification Authorities must ensure that no single Individual may gain access to a User's Private Key if stored by the Issuing Certification Authority. At a minimum, procedural or operational mechanisms must be in place for Issuing Certification Authority Key recovery in disaster recovery situations. To best ensure the integrity of the Issuing Certification Authority equipment and operation, Issuing Certification Authorities will use commercially reasonable efforts to identify a separate individual for each trusted role.

5.2.3. Identification and Authentication for Each Role

Persons filling trusted roles must undergo an appropriate security screening procedure, designated "Position of Trust".

Each individual performing any of the trusted roles shall use a SG issued Digital Certificate stored on an approved cryptographic smart card or token to identify themselves to the Digital Certificate server and Repository.

5.2.4. Roles Requiring Separation of Duties

Operations involving Root Certificate and Issuing Certification Authority roles are segregated between different employees. All operations involving maintenance of Audit Logs are segregated.

5.3. Personnel Controls

Background checks are conducted on all persons selected to take up a trusted role in accordance with the designated security screening procedure, prior to the commencement of their duties.

For purposes of mitigating the risk that one Individual acting alone could compromise the integrity of the SG Public Key Infrastructure or any Digital Certificate issued therein, SG shall perform relevant background checks of individuals and define tasks that the Individuals will be responsible to perform. SG shall determine the nature and extent of any background checks, in its sole discretion. The foregoing fully stipulates SG's obligations with respect to personnel controls and SG shall have no other duty or responsibility with respect to the foregoing. Without limitation, SG shall not be liable for employee conduct that is outside of their duties and for which SG has no control including, without limitation, acts of espionage, sabotage, criminal conduct, or malicious interference.

5.3.1. Qualifications, Experience and Clearance Requirements

SG requires that personnel meet a minimum standard with regards to Qualifications, Experience, Clearance and

Training.

5.3.2. Background Check Procedures

Background check procedures include but are not limited to checks and confirmation of:

- Previous employment
- Professional references
- Educational qualifications
- Criminal Records
- National ID-card or similar

Where the above checks and confirmations cannot be obtained due to a prohibition or limitation of law or other circumstances SG will utilise available substitute investigation techniques permitted by law that provide similar information, including background checks performed by applicable Government agencies.

5.3.3. Training Requirements

SG provides its personnel with on the job and professional training in order to maintain appropriate and required levels of competency to perform job responsibilities to the highest industry standard.

5.3.4. Retraining Frequency and Requirements

SG provides and maintains a program of retraining in order to maintain appropriate and required levels of competency to perform job responsibilities to the highest industry standard.

5.3.5. Job Rotation Frequency and Sequence

SG supports job rotation in order to maintain appropriate and required levels of competency across key roles.

5.3.6. Sanctions for Unauthorized Actions

Appropriate disciplinary actions are taken for unauthorised actions.

5.3.7. Independent Contractor Requirements

SG does not support the use of independent contractors to fulfil roles of responsibility.

5.3.8. Documentation Supplied to Personnel

SG provides personnel all required training materials needed to perform their job function and their duties under the job rotation program.

5.4. Audit Logging Procedures

5.4.1. Types of Events Recorded

All events involved in the generation of the Digital Certification Authority key pairs are recorded. This includes all configuration data used in the process.

Individuals who have access to particular key pairs and passwords will be audited. Key pair access will take the form of PIN protected smart cards or tokens. Access to databases will take the form of a user name and password. Access control in certain cases may take the form of one individual having access to the smartcard and another individual having access to the corresponding PIN to unlock the smart card or token. This ensures that a minimum of two people being present to perform certain tasks on the SG Digital Certification Authority.

The types of data recorded by SG include but are not limited to:

- All data involved in each individual Digital Certificate registration process will be recorded for future reference if needed.
- All data and procedures involved in the certification and distribution of Digital Certificates will be recorded.

- All data relevant to the publication of Digital Certificates and Certificate Revocation Lists will be recorded.
- All Digital Certificate revocation request details are recorded including reason for revocation.
- Logs recording all network traffic to and from trusted machines are recorded and audited.
- All aspects of the configuration of the backup site are recorded. All procedures involved in the backup process are recorded.
- All data recorded as mentioned in the above sections is backed up. Therefore there will be two copies of all record/audit material, stored in separate locations to protect against disaster scenarios.
- All aspects of the installation of new or updated software.
- All aspects of hardware updates.
- All aspects of shutdowns and restarts.
- Time and date of Log Dumps.

All Audit logs will be appropriately time stamped and their integrity protected.

5.4.2. Frequency of Processing Log

Audit logs are verified and consolidated at least monthly.

5.4.3. Retention Period for Audit Log

Audit logs are retained as archive records for a period no less than five (5) years for audit trail files, and no less than five (5) years for Key and Digital Certificate information. Audit logs are stored until at least five (5) years after the SG Issuing Certification Authority ceases operation.

5.4.4. Protection of Audit Log

The relevant audit data collected is regularly analysed for any attempts to violate the integrity of any element of the SG-PKI.

Only Digital Certification Authority Officers and auditors may view audit logs. SG decides whether particular audit records need to be viewed by others in specific instances and makes those records available. Consolidated logs are protected from modification and destruction.

All audit logs are protected in an encrypted format via a Key and Digital Certificate generated especially for the purpose of protecting the logs.

5.4.5. Audit Log Backup Procedures

Each Issuing Certification Authority performs an onsite backup of the audit log daily. The backup process includes weekly physical removal of the audit log copy from the Issuing Certification Authority's premises and storage at a secure off site location.

Backup procedures apply to the SG-PKI and the participants therein including the SG Root Certification Authority, Issuing Certification Authorities and Registration Authorities.

5.4.6. Audit Collection System

The security audit process of each Issuing Certification Authority runs independently of the Issuing Certification Authority software. Security audit processes are invoked at system start up and cease only at system shutdown.

5.4.7. Notification to Event-Causing Subject

Where an event is logged no notice is required to be given to the Individual, Organisation, Device or Application that caused the event.

5.4.8. Vulnerability Assessment

Both baseline and on-going threat and risk vulnerability assessments will be carried out on all parts of the SG Public Key Infrastructure environment, including the equipment, physical location, records, data, software,

personnel, administrative processes, communications and each Issuing Certification Authority. Vulnerability assessment procedures intend to identify SG Public Key Infrastructure threats and vulnerabilities, and determine a risk value based upon existing safeguards and control practices. Management can then make informed choices on determining how to best provide a secure environment with risk reduced to an acceptable level at an acceptable cost to management, clients, and shareholders.

5.5. Records Archival

5.5.1. Types of Records Archived

SG archives, and makes available upon authorized request, documentation related to and subject to the SG Document Access Policy. For each Digital Certificate, the records will address creation, issuance, use, revocation, expiration and renewal activities. These records will include all relevant evidence in the Issuing Certification Authority's possession including:

- Audit logs
- Digital Certificate requests and all related actions
- Contents of issued Digital Certificates
- Evidence of Digital Certificate acceptance and signed (electronically or otherwise) User Agreements
- Digital Certificate renewal requests and all related actions
- Revocation requests and all related actions
- Digital Certificate Revocation Lists posted
- Audit Opinions as discussed in this SG TCP/CPS and
- Name of the relevant SG Registration Authority.

5.5.2. Retention Period for Archive

SG Issuing Certification Authority archives will be retained and protected against modification or destruction for a period of five (5) years.

5.5.3. Protection of Archive

Archives shall be retained and protected against modification or destruction. Only Issuing Certification Authority Officers and auditors may view the archives in whole. The contents of the archives will not be released as a whole, except as required by law. SG may decide to release records of individual transactions upon request of any of the entities involved in the transaction or their recognized representatives. A reasonable handling fee per record (subject to a minimum fee) will be assessed to cover the cost of record retrieval. Requests for access to archived information should be sent electronically to SG.

5.5.4. Archive Backup Procedures

Adequate backup procedures must be in place so that in the event of the loss or destruction of the primary archives a complete set of backup copies will be readily available.

5.5.5. Requirements for Time-Stamping of Records

SG supports time stamping of all of its records. All events that are recorded within SG Service include the date and time of when the event took place. This date and time are based on the system time on which the Digital Certification Authority program is operating. SG uses procedures to review and ensure that all systems operating within the SG-PKI rely on a trusted time source.

5.5.6. Archive Collection System

The SG Archive System is internal. SG provides assistance to Issuing Certification Authorities and Registration Authorities within the SG-PKI to preserve their audit trails.

5.5.7. Procedures to Obtain and Verify Archive Information

Digital Certificate Holder Private Keys shall only be obtained by:

- A legitimate request from the Digital Certificate Holder where the identity of the Digital Certificate Holder is positively achieved or
- A legitimate and lawful judicial order that complies with requirements of TCP/CPS

5.6. Key Changeover

Key changeover is not automatic. Keys expire at the same time as their associated Digital Certificates and, with the exception of the SG Root Certification Authority which issues a new Digital Certificate and new Keys to itself, all parties within the SG Public Key Infrastructure are to obtain new keys by making an application for Digital Certificate renewal to the corresponding Registration Authority and subject to any relevant contractual documentation and fees.

5.7. Compromise and Disaster Recovery

SG has a Digital Certification Authority Operations Disaster & Recovery Plan (SG Business Continuity Plan). The purpose of this plan is to restore core business operations as quickly as practicable when systems and/or operations have been significantly and adversely impacted by fire, strikes, etc.

SG and each Issuing Certification Authority has in place an appropriate disaster recovery and business resumption plan that provides for the immediate continuation of Digital Certificate revocation services in the event of an unexpected emergency. SG regards its disaster recovery and business resumption plan as proprietary and that it contains sensitive confidential information. Accordingly, it is not intended to be made generally available.

SG and each Issuing Certification Authority has in place an appropriate Key compromise plan detailing its activities in the event of a compromise of a SG Issuing Certification Authority Private Key. Such plans include procedures for:

- Revoking all Digital Certificates signed with that SG Issuing Certification Authority's Private Key and
- Promptly notifying SG and all of the Holders of Digital Certificates issued by that SG Issuing Certification Authority

5.7.1. SG Business Continuity Plan

The SG Business Continuity Plan is strictly confidential and provides for:

- Incident and compromise handling procedures
- Computing resources, software, and/or corrupted data handling procedures
- Entity private key compromise procedures
- Entity Public Key Revocation procedures
- Business continuity capabilities and procedures after a disaster

5.8. Certification Authority and/or Registration Authority Termination

When it is necessary to terminate an Issuing Certification Authority or Registration Authority service, the impact of the termination will be minimised as much as possible in light of the prevailing circumstances and is subject to the applicable Issuing Certification Authority and/or the Registration Agreements.

SG and each Issuing Certification Authority specify the procedures it will follow when terminating all or a portion of its Digital Certificate issuance and management operations. The procedures must, at a minimum:

- ensure any disruption caused by the termination of an Issuing Certification Authority is minimised
- ensure that archived records of the Issuing Certification Authority are retained
- ensure that prompt notification of termination is provided to Digital Certificate Holders, Authorised Relying Parties, and other relevant parties in the SG Public Key Infrastructure
- ensure that a process for revoking all Digital Certificates issued by an Issuing Certification Authority at the time of termination is maintained and

- notify relevant Government and Certification bodies under applicable laws and related regulations
- For Qualified Certificates, in accordance with Swedish Digital Signature law, a notice of termination of the Issuing Certification Authority must be communicated in accordance with pre-established procedures and regulations.

5.8.1. User Keys and Certificates

Where practical, Key and Digital Certificate revocation should be timed to coincide with the progressive and planned rollout of new Keys and Digital Certificates by a successor Issuing Certification Authority.

5.8.2. Successor Issuing Certification Authority

To the extent that it is practical and reasonable the successor Issuing Certification Authority should assume the same rights, obligations and duties as the terminating Issuing Certification Authority. The successor Issuing Certification Authority should issue new Keys and Digital Certificates to all subordinate service providers and Users whose Keys and Digital Certificates were revoked by the terminating Issuing Certification Authority due to its termination, subject to the individual service provider or User making an application for a new Digital Certificate, and satisfying the initial registration and Identification and Authentication requirements, including the execution of a new service provider or User Agreement.

5.8.3. Private Key Destruction Procedures

All Digital Certificate Holders have an obligation to protect their private keys from compromise. Private keys shall be destroyed in a way that prevents their loss, theft, modification, unauthorised disclosure or unauthorized use.

Upon termination of the Issuing Certification Authority, SG personnel shall destroy the SG Digital Certification Authority private key by deleting, overwriting or physical destruction.

6. TECHNICAL SECURITY CONTROLS

The SG Digital Certification Authority private keys are protected within a hardware security module with Federal Information Processing Standard-140 level 4 capabilities. Access to the modules within the SG CA environment is restricted by the use of Smart Cards or Tokens and associated pass phrases. These Smart Cards, Token and pass phrases are allocated among the multiple members of the SG management team. Such allocation ensures that no one member of the team holds total control over any component of the system.

6.1. Key Pair Generation and Installation

6.1.1. Key Pair Generation

All Key Pairs will be generated in a manner that SG, in its sole discretion, deems to be secure. SG retains the right to generate the Digital Certificate Holder's public and private key pair. The Digital Certificate Holder is required to provide all the necessary identification and authentication information when the Digital Certificate is being requested. Once all the registration information is collected by the SG Digital Certification Authority the Digital Certificate Holders public and private key pair is generated within a secure environment. SG Digital Certificate Holders can generate their own private key prior to submitting a Digital Certificate request. Key Generation methods and requirements differ according to the type of Digital Certificate requested.

Digital Certificate Holder Key Generation should be performed on an approved cryptographic Token. Any pseudo random numbers used for Key generation material will be generated by an FIPS approved method.

6.1.2. Private Key Delivery to Certificate Holder

Once the Digital Certificate Holder Certificate request has been signed the Certificate Holder's Digital Certificate and Private Key will be distributed in person or via a secure channel whereby only the Digital Certificate Holder will have access to his/her Private Key.

In all cases, a Private Key will be generated and remain within the Cryptographic Module. If the owner of the Cryptographic Module generates the Key, then there is no need to deliver the Private Key.

6.1.3. Public Key Delivery to Certificate Issuer

Public Keys must be delivered in a secure and trustworthy manner, such as a Digital Certificate request message. Delivery may also be accomplished via non electronic means. These means may include, but are not limited to, floppy disk (or other storage medium) sent via registered mail or courier, or by delivery of a Token for local Key generation at the point of Digital Certificate issuance or request. Off line means will include Identity checking and will not inhibit proof of possession of a corresponding Private Key. Any other methods used for Public Key delivery will be stipulated in a User Agreement or other agreement. In those cases where Key Pairs are generated by the Issuing Certification Authority on behalf of the Holder, the Issuing Certification Authority will implement secure mechanisms to ensure that the Token on which the Key Pair is held is securely sent to the proper Holder, and that the Token is not activated prior to receipt by the proper Holder.

6.1.4. Certification Authority Public Key to Relying Parties

Public Keys of SG Root Authority and each Issuing Certification Authority shall be publicly available.

6.1.5. Key Sizes

Key lengths within the SG-PKI are determined by Digital Certificate Profiles more fully disclosed in section 10. The SG Issuing Certification Authority uses an RSA minimum key length of 1.024 bit. The standard key length used is 2048 bit.

6.1.6. Public Key Parameters Generation and Quality Checking

The parameters used to create Public Keys are generated by the relevant Registration Authority application, except for self-generated User keys in which case the parameters are generated by the User's client application.

The quality of Public Key parameters is automatically checked by the Registration Authority that generates the Key, except for self-generated User Keys in which case the parameters are quality checked by the Registration Authority prior to submitting a Digital Certificate request to the appropriate Issuing Certification Authority.

6.1.7. Key Usage Purposes (as per X.509 Version 3 Key Usage Field)

Keys may be used for the purposes and in the manner described in the SG TCP/CPS - Digital Certificate Profiles.

Issuing Certification Authorities Private Keys are used for Digital Certificate signing and Certificate Revocation List signing. It may also be used to authenticate the issuing Certification Authority to a Repository.

6.2. Private Key Protection and Cryptographic Module Engineering Controls

All participants in the SG-PKI are required to take all appropriate and adequate steps to protect their Private Keys in accordance with the requirements of this SG TCP/CPS. Without limitation to the generality of the foregoing, all participants in the SG-PKI must (i) secure their Private Key and take all reasonable and necessary precautions to prevent the loss, damage, disclosure, modification, or unauthorised use of their Private Key (to include password, Token or other activation data used to control access to the Private Key); and (ii) exercise sole and complete control and use of their Private Key that corresponds to their Public Key.

6.2.1. Cryptographic Module Standards and Controls

The generation and maintenance of the Root and Issuing Certification Authorities private keys are facilitated through the use of an advanced cryptographic device known as a Hardware Security Module. The Hardware Security Module used by Issuing Certification Authorities in the SG-PKI is designed to provide Federal Information Processing Standard-140 Level 4 security standards in both the generation and the maintenance in all Root and Operational Digital Certification Authority private keys.

- For Qualified Certificates, in accordance with Swedish Digital Signature law, the Certificate Holder Private Keys are generated and stored on a Secure Signature Creation Device that meets or exceeds EAL 4 standards.

6.2.2. Private Key Multi-Person Control

Subject to the requirements of sections 5.2 and 5.3 of the current and in force SG TCP/CPS the SG-PKI uses trusted multi-person control for both access control and authorisation control.

6.2.3. Private Key Escrow

Private Keys will not be escrowed.

6.2.4. Private Key Backup

Issuing Certification Authority Private Keys are stored in an encrypted database, which is backed up under further encryption with backup copies maintained on site and in secure off-site storage. All Issuing Certificate Authority Keys are held in a secure cryptographic device and is equally secured when it is stored outside a secure cryptographic device.

6.2.5. Private Key Archive

Private Keys used for encryption shall not be archived, unless the Digital Certificate Holder or Registration Authority specifically contracts for such services. Private Keys for signing will not be archived.

Where a single key pair is generated for signing and encryption, the Private Key will only be archived on the specific request of the Digital Certificate Holder and the corporate entity with which that Digital Certificate Holder is affiliated.

Under no circumstances will private keys for Qualified Digital Certificates be archived.

6.2.6. Private Key Transfer Into or From a Cryptographic Module

If a Cryptographic Module is used, the Private Key must be generated in it and remain there in both encrypted and decrypted forms, and be decrypted only at the time at which it is being used. Private Keys must never exist in plain text form outside the cryptographic module. In the event that a Private Key is to be transported from one Cryptographic Module to another, the Private Key must be encrypted during transport.

6.2.7. Private Key Storage on Cryptographic Module

Private Keys held on a Cryptographic Module are stored in an encrypted form and password protected.

6.2.8. Method of Activating Private Key

A Digital Certificate Holder must be authenticated to the Cryptographic Module before the activation of the Private Key. This Authentication may be in the form of a password. When deactivated, Private Keys must be kept in encrypted form only.

6.2.9. Method of Deactivating Private Key

Cryptographic Modules that have been activated must not be left unattended or otherwise open to unauthorized access. After use, they must be deactivated, using, for example, a manual logout procedure or a passive timeout. When not in use, hardware Cryptographic Modules should be removed and stored, unless they are within the Holder's sole control.

6.2.10. Method of Destroying Private Key

Private Keys should be destroyed when they are no longer needed, or when the Digital Certificates to which they correspond expire or are revoked.

6.2.11. Cryptographic Module Rating

Cryptographic modules in use with the SG Public Key Infrastructure comply with industry standards.

- For Qualified Certificates, in accordance with Swedish Digital Signature law, the Certificate Holder Private Keys are generated and stored on a Secure Signature Creation Device that meets or exceeds EAL 4 standards.

6.3. Other Aspects of Key Pair Management

6.3.1. Public Key Archival

Public Keys will be recorded in Digital Certificates that will be archived in the Repository. No separate archive of Public Keys will be maintained.

The validity period of Digital Certificate Holder Digital Certificates will be dependent on the class of Digital Certificate in question.

6.3.2. Certificate Operational Periods and Key Pair Usage Periods

Usage periods for Public Keys and Private Keys shall match the usage periods for the Digital Certificate that binds the Public Key to an Individual, Organisation, or Device. Please see the variable Issuing Certificate Authority 'Valid From' and 'Valid To' fields in the Certificate Profiles outlined in Appendix A.

The maximum validity periods for Digital Certificates issued within the SG-PKI are:

- SG Root CA certificate: 25 years
- SG Root CA1 certificate: 10 years
- All Issuing CA certificates: 10 years
- Qualified Personal Certificates (According to Swedish Digital Signature law): 2 years
- All other Digital Certificates: Variable, but less than the remainder of the appropriate Issuing Certificate Authority Certificate

6.4. Activation Data

6.4.1. Activation Data Generation and Installation

Two factor Authentication shall be used to protect access to a Private Key. No activation data other than access control mechanisms is required to operate Cryptographic Modules.

A unique User Personal Identification Code may be generated by a Registration Authority during key pair creation, to protect the transport of a User's Keys and Digital Certificates to the User.

If activation data must be transmitted, it shall be via a channel of appropriate protection, and distinct in time and place from the associated Cryptographic Module.

6.4.2. Activation Data Protection

No activation data other than access control mechanisms is required to operate Cryptographic Modules. Personal Identification Codes may be supplied to Users in two portions using different delivery methods, for example by e-mail, SG Extranet and by standard post, to provide increased security against third party interception of the Personal Identification Code. Activation Data should be memorized, not written down. Activation Data must never be shared. Activation data must not contain Digital Certificate Holders personal information.

6.4.3. Other Aspects of Activation Data

Where a Personal Identification Code is used, the User is required to enter the Personal Identification Code and identification details such as their distinguished name before they are able to access and install their Keys and Digital Certificates.

6.5. Computer Security Controls

6.5.1. Specific Computer Security Technical Requirements

Each Issuing Certification Authority must establish an approved System Security Policy that incorporates computer security technical requirements that are specific to that Issuing Certification Authority's operations.

The SG Issuing Certification Authority has established an System Security Policy that incorporates computer security technical requirements that are specific to SG and configured to allow the minimal amount of connectivity identified as being necessary to accomplish Digital Certification Authority and Registration Authority functions.

Computer security technical requirements are achieved utilising a combination of hardened security modules and software, operating system security features, Public Key Infrastructure and Certificate Authority Software and physical safeguards, including security Policies and Procedures that include but are not limited to:

- Access controls to Certificate Authority services and PKI roles, see Section 5.1
- Enforced separation of duties for Certificate Authority Services and PKI roles, see Section 5.2
- Identification and Authentication of personnel that fulfil roles of responsibility in the SG-PKI, see Section 5.3
- Use of cryptography for session communication and database security, mutually authenticated and encrypted SSL/TLS is used for all communications
- Archival of Certificate Authority history and audit data, see Sections 5.4 and 5.6
- Use of X.509 Digital Certificates for all administrators

6.5.2. Computer Security Rating

SG has established an approved System Security Policy that incorporates computer security ratings that are specific to SG.

SG computer security ratings are achieved and maintained by real time security monitoring and analysis, monthly security reviews by the SG Chief Security Officer.

6.6. Life Cycle Technical Controls

All hardware and software procured for operating Issuing Certification Authority within the SG Public Key Infrastructure must be purchased in a manner that will mitigate the risk that any particular component was tampered with, such as random selection of specific components. Equipment developed for use within the SG Public Key Infrastructure shall be developed in a controlled environment under strict change control procedures.

A continuous chain of accountability, from the location where all hardware and software that has been identified as supporting an Issuing Certification Authority within the SG Public Key Infrastructure must be maintained by causing it to be shipped or delivered via controlled methods. Issuing Certification Authority equipment shall not have installed applications or component software that is not part of the Issuing Certification Authority configuration. All subsequent updates to Issuing Certification Authority equipment must be purchased or developed in the same manner as the original equipment and be installed by trusted and trained personnel in a defined manner.

SG has established a System Security Policy that incorporates computer security ratings that are specific to SG and deal with, including but not limited to:

6.6.1. Life Cycle Security Controls

SG employs a configuration management methodology for the installation and ongoing maintenance of the Certificate Authority systems. The Certificate Authority software, when first loaded will provide a method for SG to verify that the software on the system:

- Originated from the software developer
- Has not been modified prior to installation
- Is the version intended for use

The SG Chief Security Officer periodically verifies the integrity of the Certificate Authority software and monitors the configuration of the Certificate Authority systems.

6.6.2. Network Security Controls

All access to Issuing Certification Authority equipment via a network is protected by network firewalls and filtering routers. Firewalls and filtering routers used for Issuing Certification Authority equipment limits services to and from the Issuing Certification Authority equipment to those required to perform Issuing Certification Authority functions.

Issuing Certification Authority equipment is protected against known network attacks. Any and all unused network ports and services are turned off to ensure it is protected against known network attacks. Any network software present on the Issuing Certification Authority equipment is software required for the functioning of the Issuing Certification Authority application. All Root Certification Authority equipment is maintained and operated in stand-alone (offline) configurations.

6.6.3. Hardware Cryptographic Module Engineering Controls

Cryptographic modules used by the SG Root Certification Authority, Issuing Certification Authorities, and Registration Authorities are certified to Internet Engineering Task Force (IETF) Standards, and are either FIPS 140-2 Level 3 or EAL 4 compliant.

6.7. Time-Stamping

The SG Time-stamping Authority uses PKI and trusted time sources to provide reliable standards-based time-stamps. The SG Time-stamp Policy defines the operational and management practices of the SG Time-stamp Authority such that Participants and Relying Parties may evaluate their confidence in the operation of the time-stamping services.

The SG Time-stamp Policy aims to deliver time-stamping services used in support of qualified electronic signatures, (i.e. in line with article 5.1 of the European Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures), as well as under applicable Swedish laws and regulations. However SG Time-stamps may be equally applied to any application requiring proof that a datum existed before a particular time.

The structure and content of the SG Time-stamp Policy is in accordance with ETSI TS 102.023, Electronic Signatures and Infrastructures (ESI); Policy Requirements for Time-stamping Authorities. The SG Time-stamp Policy is administered and approved by the SG Policy Management Authority and should be read in conjunction with this TCP/CPS.

7. Certificate, CRL and OCSP Profiles

7.1. Certificate Profile

All SG Digital Certificates conform to Digital Certificate and Certificate Revocation List profiles as described in RFC 3280 and utilize the ITU-T X.509 Version 3 Digital Certificate standard.

For the purposes of this SG TCP/CPS, Digital Certificates, other than the SG Root Certificates and Issuing Certificates, all other Digital Certificate profiles within the SG-PKI are detailed in Appendix A.

7.1.1. Certificate Content

A SG Digital Certificate only certifies the information contained therein.

7.1.2. Version Numbers

Digital Certificates in the SG-PKI are X.509 Version 3

7.1.3. Certificate Extensions

Digital Certificate Extensions are defined in the Digital Certificate Profiles detailed in Appendix A.

7.1.4. Algorithm Object Identifiers

No specific definitions.

7.1.5. Name Forms

See 3.1.1

7.1.6. Name Constraints

See 3.1.1

7.1.7. Usage of Policy Constraints Extension

No specific definitions.

7.1.8. Policy Qualifiers Syntax and Semantics

Digital Certificates issued within the SG-PKI contain one of the Object Identifiers for this TCP/CPS.

7.1.9. Processing Semantics for the Critical Certificate Policies Extension

No specific definitions.

7.2. Certificate Revocation List Profile

If utilized, Certificate Revocation Lists are issued in the X.509 Version 2 format in accordance with the PKIX Digital Certificate and Certificate Revocation List Profile.

7.2.1. Version Number

Issuing Certification Authorities within the SG-PKI issue X.509 Version 2 Certificate Revocation Lists in accordance with the PKIX Digital Certificate and Certificate Revocation List Profile.

7.2.2. Certificate Revocation List and Certificate Revocation List Entry Extensions

All User PKI- software must correctly process all Certificate Revocation List extensions identified in the Digital Certificate and Certificate Revocation List profile.

7.3. Online Certificate Status Protocol Profile

Online Certificate Status Protocol is enabled for all Digital Certificates within the SG-PKI.

7.3.1. Online Certificate Status Protocol Version Numbers

Version 1 of the Online Certificate Status Protocol, as defined by RFC 2560, is supported within the SG-PKI.

7.3.2. Online Certificate Status Protocol Extensions

No specific definitions.

7.3.3. Signing of OCSP requests

OCSP requests shall be made to the appropriate URLs as described in 4.9.1 and Appendix A. OCSP requests to CAs except for the Qualified Users CA may need to be signed, i.e. a relying party who wants to validate certificates by OCSP needs to make an agreement with SG beforehand.

7.4. Lightweight Directory Access Protocol Profile

SG will host a repository in the form of an Lightweight Directory Access Protocol directory for the purpose of storing and making available all X.509 V.3 Digital Certificates issued under the SG Certification Authority, with public access to download these Digital Certificates for Digital Certificate Holder and relying party requirements and receiving (from the SG Digital Certification Authority), storing and making publicly available regularly updated Certificate Revocation List V.2 information, for the purpose of Digital Certificate validation.

7.4.1. Lightweight Directory Access Protocol Version Numbers

LDAP V.3 in accordance with RFC-3377

7.4.2. Lightweight Directory Access Protocol Extensions

No specific definitions.

7.5. Root Certificates

7.5.1. SG Root CA Certificate

Field	SiguardRootCA (Offline)
Version	V3
Serial Number	00 80 ed 67 06 b2 b2 18 2c
Signature Algorithm	SHA1RSA
Subject Public Key	30:82:01:0a:02:82:01:01:00:91:f3:aa:cc:0d:c9:e7:3b:97:a3:5f:c7:1c:e3: f1:01:07:ac:6d:d9:e7:ff:31:a1:f4:15:4d:c0:e6:46:aa:30:46:34:00:03:09: d9:ec:5d:59:f1:9b:86:5b:77:ca:e6:cf:ce:bc:b3:95:7c:9a:7f:fb:3f:01:e2: d7:0d:d9:ab:73:3b:7d:73:b0:b7:66:e0:de:10:74:c7:33:4c:95:51:61:3c: a2:15:41:4c:d3:69:0b:75:d9:7e:ed:69:fd:73:e1:dd:b9:36:e6:67:57:78:f8: 76:15:e1:31:9f:aa:72:7f:85:9a:26:7a:50:49:32:72:9f:2f:c3:4a:f4:cc:25: da:c4:6e:2e:aa:ae:0a:c1:b7:8f:02:6a:f0:14:a4:71:cf:05:ec:b8:57:07:b8: c4:af:5b:eb:1b:58:aa:78:28:b5:21:a7:7c:53:31:80:b6:d2:9f:eb:d1:9e:b1: 74:ff:02:2d:46:4b:af:3e:ba:0f:cd:13:c6:59:f9:a7:24:92:02:82:bb:ff:b6:ee: 06:ce:4a:b3:6b:e7:da:ab:2d:92:ff:14:e2:78:94:27:e6:d3:d8:96:45:8d:34: 9b:99:e0:b1:c6:f5:4b:c0:ab:c8:d7:4a:de:f2:5b:fc:cb:fa:1a:5c:7e:cf:7d: 54:66:be:25:65:3c:a5:19:7e:7f:fd:b5:02:03:01:00:01
Fingerprint	23:4d:79:45:70:b3:a4:be:71:b0:0d:96:bb:72:eb:08:f7:87:ef:44
Validity:	
Not Before	02.06.2008 20:17:38
Not After	27.05.2033 20:17:38

Issuer:	
Common Name (CN)	Siguard RootCA
Organisational Unit (OU)	RootCA
Location (L)	Gothenburg
Country (C)	SE
Subject:	
Common Name (CN)	Siguard RootCA
Organisational Unit (OU)	RootCA
Location (L)	Gothenburg
Country (C)	SE
Extensions:	
Authority Key Identifier	92:16:94:28:02:16:d8:19:40:a4:38:e6:eb:69:a8:d4:2b:0b:76:7d (Subject Key Identifier of Issuing CA)
Subject Key Identifier	92:16:94:28:02:16:d8:19:40:a4:38:e6:eb:69:a8:d4:2b:0b:76:7d (Message Digest of Public Key)
Key Usage	Key Cert Sign, CRL Sign Offline, CRL Sign
Certificate Policies	http://www.siguard.se/policies/policies.html
Authority Information Access	ldap://pki.siguard.se/cn=SiguardRootCA,dc=siguard,dc=se
CRL Distribution	ldap://pki.siguard.se/cn=SiguardRootCA,dc=siguard,dc=se http://pki.siguard.se/ca/SiguardRootCA.der.crl
Thumbprint Algorithm	SHA1

7.5.2. SG Root CA1 Certificate

Field	SiguardRootCA1 (Online)
Version	V3
Serial Number	01
Signature Algorithm	SHA1RSA
Subject Public Key	30:82:01:0a:02:82:01:01:00:d8:5e:24:99:b7:1e:51:d6:ca:a1:63:fe:e1: 45:04:0f:cb:23:9e:42:72:ab:11:23:f1:f6:51:51:0b:f8:00:a6:0e:eb:51: 6e:04:af:ae:fe:e8:80:9d:e0:f8:32:9e:d0:24:05:38:80:89:81:e5: 63:3a:de:1d:43:8c:b3:e6:c2:a0:23:35:bb:1d:53:77:64:6d:66:fb:2c: 82:93:60:01:46:76:7f:e5:4f:cc:a3:40:ec:7a:36:1b:b4:43:3e:c4:85: 55:1b:72:13:66:26:6c:74:47:2e:91:ca:f2:0e:59:04:f4:51:db:86: 9b:7f:a5:3c:01:54:19:0c:22:c5:7c:37:a8:73:ce:7d:02:0b:7a:5c: 68:98:6f:5a:5a:74:00:52:85:24:41:02:5c:76:21:b5:79:8a:20:7e:5f:a2: 58:d1:ad:17:9d:7c:04:44:1c:fc:00:5e:9e:5a:dc:3f:72:f0:40:72: 60:84:10:ac:61:47:b3:2d:b9:91:1c:65:47:c8:4a:55:fc:c1:4b:7a:cd: 85:ec:46:97:1f:23:3f:a7:cd:9c:a1:4b:c3:a3:62:d8:14:56:5b:22:a3:f7:da:df:32: df:8d:34:bc:fa:96:4f:b8:68:47:34:44:e7:6a:7e:66:a1: b5:26:7b:13:3b:de:5d:10:88:98:7f:b1:50:fb:02:03:01:00:01
Fingerprint	c2:86:0e:15:2b:1c:08:f1:d2:a6:5a:cf:9d:6d:06:7f:05:dd:7d:91
Validity:	
Not Before	02.06.2008 20:20:42
Not After	31.05.2018 20:20:42
Issuer:	
Common Name (CN)	Siguard RootCA
Organisation (O)	Siguard Europe AB
Location (L)	Gothenburg
Country (C)	SE

Subject:	
Common Name (CN)	Signtguard RootCA1
Organisation(O)	Signtguard Europe AB
Location (L)	Gothenburg
Country (C)	SE
Extensions:	
Authority Key Identifier	92:16:94:28:02:16:d8:19:40:a4:38:e6:eb:69:a8:d4:2b:0b:76:7d (Subject Key Identifier of Issuing CA)
Subject Key Identifier	ad:9d:ca:e0:f3:3d:d7:20:17:7d:87:23:78:d4:e4:49:da:30:4f:9e (Message Digest of Public Key)
Key Usage	Key Cert Sign, CRL Sign Offline, CRL Sign
Certificate Policies	http://www.signtguard.se/policies/policies.html
Authority Information Access	ldap://pki.signtguard.se/cn=SigntguardRootCA,dc=signtguard,dc=se
CRL Distribution	ldap://pki.signtguard.se/cn=SigntguardRootCA,dc=signtguard,dc=se http://pki.signtguard.se/ca/SigntguardRootCA1.der.crl
Thumprint Algorithm	SHA1

8. Compliance and Other Assessments

8.1. Frequency, Circumstance and Standards of Assessment

SG may be subject to audits in respect of its various accreditations and certifications as follows:

Standard / Law	
Common PKI Specification	The Common PKI specification takes into account all business relevant electronic signatures up to the qualified electronic signature (T7 and TeleTrust, Germany)
ESI ("Directive")	Electronic Signatures and Infrastructures (ESI) regulations from EU Telecommunication Standards Institute (ETSI)
ETSI [ETSI TS 102.023]	TS 101 023 v.1.2.1 January 2003 EU Standards Body Technical Specification - Policy Requirements for time-stamping authorities
ETSI [ETSI TS 102.042]	TS 101 042 v.1.3.4 December 2007 EU Standards Body Technical Specification - Policy Requirements for certification authorities issuing qualified certificates TS
ETSI [ETSI TS 102.456]	TS 101 456 v.1.4.3 May 2007 EU Standards Body Technical Specification - Policy Requirements for certification authorities issuing qualified certificates TS
ETSI [ETSI TS 102.862]	TS 101 862, v1.3.2 June 2004, Qualified Certificate Profile
IETF RFC 3647	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework corrigenda IETF RFC 3647 (including Erratum issued by IETF April 2004)
IETF RFC 4059	Internet X.509 Public Key Infrastructure Warranty Certificate Extension
PKCS#10 (RFC2986)	Certificate Request Syntax Specification
PKCS#15 / ISO 7816-15	Cryptographic Token Information Format Standard
SEIS S10	Swedish Certificate Policy for high assurance general ID-certificate with private key protected in an electronic ID-Card
SS 62 77 99 (ISO /IEC 27002:2005)	Guidelines and general principals for implementing, maintaining and improving information security management in an organisation

8.2. Topics Covered by Assessment

The topics that can be covered by an audit of a Issuing Certification Authority could include but may not be limited to:

- Security Policy and Planning
- Physical Security
- Technology Evaluation
- Services Administration

- Personnel Vetting
- Contracts and
- Privacy Considerations

8.3. Actions Taken as a Result of Deficiency

Actions taken as the result of deficiency will be determined by the nature and extent of the deficiency identified. Any determination will be made by SG with input from Auditors. SG at its sole discretion will determine an appropriate course of action and time frame to rectify the deficiency.

- For Qualified Certificates, in accordance with the Swedish Digital Signature law, the course of action and time frame for rectification of any deficiency as set by the accrediting authority.

8.3.1. Issuing Certification Authorities

If irregularities are found or reported, the Issuing Certification Authority in question must submit a report to the SG Root Certification Authority detailing actions the Issuing Certification Authority will take in response to the irregularity.

Where the Issuing Certification Authority fails to take appropriate action in response to an irregularity, the SG Root Certification Authority may (i) indicate the irregularities, but allow the Issuing Certification Authority to continue operations for a limited period of time; (ii) allow the Issuing Certification Authority to continue operations for a maximum of thirty (30) days pending correction of any problems prior to revocation of that Issuing Certification Authority's Issuing Certificate; (iii) limit the class of any Digital Certificates issued by the Issuing Certification Authority; or (iv) revoke the Issuing Certification Authority's Issuing Certificate. Any decision regarding which of these actions to take will be based on the severity of the irregularities. Any remedy may include permanent or temporary cessation of the Issuing Certification Authority's services, but all relevant factors must be considered prior to making a decision. A special audit may be required to confirm the implementation and effectiveness of any remedy.

In circumstances where any irregularities are found with respect to SG, in its capacity as an Issuing Certification Authority, the principles described above will be followed by the SG Root Certification Authority.

8.3.2. Registration Authorities

If irregularities are found or reported, the SG Root Certification Authority, or if applicable the Issuing Certification Authority, will address the issues raised with the relevant entity. Any action to be taken will be determined by SG by reference to its determination as to the severity or materiality of the irregularity. In the event that SG determines that remedial action is required, the relevant entity will be advised by SG as to the procedures and action required to remedy the irregularity. Remedial action determined by SG shall be limited to the operations and procedures required to be taken in order to ensure that the Registration Authority operates in compliance with the SG TCP/CPS. In the event that SG determines that remedial action is required, and such action is not taken in accordance with SG's determination, SG may (i) allow the Nominating Issuing Certification Authority to continue operations for a further period of time whilst the irregularities are addressed; (ii) allow the Nominating Certification Authority and its Registration Authority to continue operations for a maximum of thirty (30) days pending full implementation of the actions required by SG prior to termination of that Issuing Certification Authority's agreement with SG and the associated revocation of any Digital Certificate issued to them; (iii) limit the class of any Digital Certificates issued by the Nominating Issuing Certification Authority; or (iv) terminate that Issuing Certification Authority's agreement with SG and revoke the Issuing Certificate. Any decision regarding which of these actions to take will be based on SG's opinion of the severity and materiality of the irregularities.

9. Other Business and Legal Matters

9.1. Financial Responsibilities

9.1.1. Financial Records

SG is responsible for maintaining its financial books and records in a commercially reasonable manner and shall engage the services of an international accounting firm to provide financial services, including periodic audits.

9.1.2. Fiduciary Relationships

SG is not the agent, fiduciary or other representative of any Digital Certificate Holder and/or Relying Party and must not be represented by the Digital Certificate Holder and/or Relying Party to be so. Digital Certificate Holders and/or Relying Parties have no authority to bind SG by contract or otherwise, to any obligation.

Participation in the SG Public Key Infrastructure does not make any participant an agent, fiduciary, trustee, or other representative of any entity, legal or otherwise. Nothing contained in this SG TCP/CPS or in any corresponding User or Relying Party Agreement shall be deemed to constitute SG, SG-PKI Participants or any of their agents, directors, employees, consultants, suppliers, contractors, partners or Counterparties a fiduciary, endorser, promoter, agent, partner, representative, or Counterparty of any entity, and the use of or reliance upon Digital Certificates or other forms of participation within the SG-PKI is to be construed accordingly.

9.1.3. Other Assets

Issuing Certification Authorities and Registration Authorities shall maintain sufficient assets and financial resources to perform their duties within the SG-PKI and be reasonably able to bear liability to Digital Certificate Holders and Relying Parties.

9.1.4. Insurance or Warranty Coverage for End-Entities

SG will give advice to and support the SG Certificate Holders and SG Relying Parties on questions relating to the different types of insurance available.

SG Certificate Holders are entitled to apply to commercial insurance providers for financial protection against accidental occurrences such as theft, corruption, loss or unintentional disclosure of the private key that corresponds to the public key in their SG Digital Certificate.

SG Relying parties are entitled to apply to commercial insurance providers for protection against financial loss.

9.2. Confidentiality of Business Information

9.2.1. Scope of Confidential Information

Any personal or corporate information held by Issuing Certification Authorities related to a Digital Certificate Holder's application and the issuance of Digital Certificates is considered confidential and will not be released without the prior consent of the relevant Holder, unless required otherwise by law or to fulfil the requirements of this SG TCP/CPS.

The Issuing Certification Authority does not have access to the Private Keys of any of the entities it certifies or whose Digital Certificate requests it processes.

9.2.2. Information Not Within the Scope of Confidential Information

Information appearing on Digital Certificates or stored in the Repository is not considered confidential, unless statutes or special agreements so dictate.

9.3. Responsibility to Protect Confidential Information

9.3.1. Privacy of Personal Information

9.3.1.1. Privacy Plan

SG, Issuing Certification Authorities, Registration Authorities, Digital Certificate Holders, Relying Parties and all others using or accessing any personal data in connection with matters dealt with this CP/CPS shall comply with the Council Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and any amending and/or implementing legislation enacted from time to time, and any other relevant legislation relating to data protection, and any equivalent legislation or regulations in any relevant jurisdiction.

9.3.2. Information Treated as Private

All information about Digital Certificate Holders that is not publicly available through the content of issued Digital Certificates, Digital Certificate directories and online Repositories is treated as private.

9.3.2.1. Registration Records

All registration records are considered confidential information and treated as private.

9.3.2.2. Certificate Revocation

The reason for a Digital Certificate being revoked, (if applicable), is considered to be confidential information, with the sole exception of the revocation of an Issuing Certification Authority Digital Certificate due to:

- the compromise of the Issuing Certification Authority's Private Key, in which case a disclosure may be made that the Private Key has been compromised;
- the termination of a Issuing Certification Authority within the SG-PKI, in which case prior disclosure of the termination may be given.

9.3.3. Information Deemed Not Private

9.3.3.1. Certificate Contents

The content of Digital Certificates issued by SG is public information and deemed not private.

9.3.3.2. Certificate Revocation List

Digital Certificates published in the X.500 Directory are not considered to be confidential information.

9.3.3.3. TCP/CPS

This SG TCP/CPS is a public document and is not confidential information and is not treated as private.

9.3.4. Responsibility to Protect Private Information

Information supplied to SG as a result of the practices described in this TCP/CPS may be covered by national government or other privacy legislation or guidelines. SG will not divulge any private Digital Certificate Holder information to any third party for any reason, unless compelled to do so by law or competent regulatory authority.

9.3.5. Notice and Consent to Use Private Information

In the course of accepting a Digital Certificate, all Digital Certificate Holders have agreed to allow their personal data submitted in the course of registration to be processed by and on behalf of the SG Digital Certification Authority, and used as explained in the registration process. They have also been given an opportunity to decline from having their personal data used for particular purposes. They have also agreed to let certain personal data to appear in publicly accessible directories and be communicated to others.

- For Qualified Certificates issued in accordance with Swedish Digital Signature laws, Certificate Holders expressly consent to personal data in the form of the data included in the Certificate Fields being transferred outside of Sweden and published in a repository which makes this information publicly available to persons searching the repository with the appropriate query string.

9.3.6. Disclosure Pursuant to Judicial or Administrative Process

9.3.6.1. Release to Law Enforcement Officials

As a general principle, no document or record belonging to SG is released to law enforcement agencies or officials except where a properly constituted instrument, warrant, order, judgment, or demand is produced requiring production of the information, having been issued by a court of competent jurisdiction, and not known to SG to be under appeal when served on SG (SG being under no obligation to determine the same), and which has been determined by a Court of competent jurisdiction to be valid, subsisting, issued in accordance with general principles of law and otherwise enforceable. With respect to the SG Root Certification Authority: or the laws of the jurisdiction of the relevant Issuing Certification Authority and enforceable in that jurisdiction.

9.3.6.2. Release as Part of Civil Discovery

As a general principal, no document or record belonging to SG is released to any person except where a properly constituted instrument, warrant, order, judgment, or demand is produced requiring production of the information, having been issued by a court of competent jurisdiction, and not known to SG to be under appeal when served on SG (SG being under no obligation to determine the same), and which has been determined by a Court of competent jurisdiction to be valid, subsisting, issued in accordance with general principles of law and otherwise enforceable. With respect to the SG Root Certification Authority: or the laws of the jurisdiction of the relevant Issuing Certification Authority and enforceable in that jurisdiction.

9.3.7. Other Information Disclosure Circumstances

SG, Issuing Certification Authorities and Registration Authorities are under no obligation to disclose information other than is provided for by a legitimate and lawful judicial order that complies with requirements of this TCP/CPS.

9.4. Intellectual Property Rights

All Intellectual Property Rights including all copyright in all Digital Certificates and all documents (electronic or otherwise) belong to and will remain the property of SG.

Private Keys and Public Keys are the property of the applicable rightful Private Key holder. Digital Certificates issued and all Intellectual Property Rights including all copyright in all Digital Certificates and all documents (electronic or otherwise) belong to and will remain the property of SG.

This SG TCP/CPS and the Proprietary Marks are the intellectual property of SG.

SG retains exclusive title to, copyright in, and the right to license this SG TCP/CPS.

9.4.1. Object Identifiers

Copyright in the Object Identifiers for the SG infrastructure belong solely to SG.

9.4.2. Licenses

SG is in possession of, or holds licences for the use of hardware and software in support of the SG-PKI as outlined in this TCP/CPS.

9.4.3. IETF Guidelines

The use of the PKIX IETF Guidelines is acknowledged.

9.4.4. Breach

SG excludes all liability for breach of any other intellectual property rights.

9.5. Representations and Warranties

9.5.1. Certification Authority Representations

SG discharges its obligations by:

- providing the operational infrastructure and certification services, including X.500 Directory and service provider software;
- making reasonable efforts to ensure it conducts an efficient and trustworthy operation. "Reasonable efforts" includes but does not limit SG to operating in compliance with:

- documented operational procedures; and
- within applicable law and regulation;
- approving the establishment of all Issuing Certification Authorities and on approval, executing a Issuing Certification Authority Agreement (save in respect of the SG Digital Certification Authority);
- maintaining this TCP/CPS and enforcing the practices described within it and in all relevant collateral documentation;
- publishing its Root Certification Authority Hash at www.signguard.de and other nominated web sites;
- Issuing Certification Authority Certificates to Issuing Certification Authorities that comply with X.509 standards and are suitable for the purpose required;
- Issuing Certification Authority Certificates that are factually correct from the information known to it at the time of issue, and that are free from data entry errors;
- publishing issued Issuing Certification Authority Certificates without alteration in the X.500 Directory;
- investigating any suspected compromise which may threaten the integrity of the SG Public Key Infrastructure;
- revoking Issuing Certification Authority Certificates and posting such revoked Certificates in the X.500 Directory Certificate Revocation List; and
- conducting compliance audits of Issuing Certification Authorities.

9.5.2. SignGuards Europes Liability

SG's liability for damages due to usage of certificates issued by SG Certificates Authorities is limited to 100, 00 € per issued certificate.

9.5.3. Certification Authority Warranties

SG hereby warrants (a) it has taken reasonable steps to verify that the information contained in any Digital Certificate is accurate at the time of issue (b) Digital Certificates shall be revoked if SG believes or is notified that the contents of the Digital Certificate are no longer accurate, or that the key associated with a Digital Certificate has been compromised in any way. The nature of the steps SG takes to verify the information contained in a Digital Certificate vary according to the Digital Certificate fee charged, the nature and identity of the Digital Certificate Holder, and the applications for which the Digital Certificate will be marked as trusted. SG makes no other warranties, and all warranties, express or implied, statutory or otherwise, are excluded to the greatest extent permissible by applicable law, including without limitation all warranties as to merchantability or fitness for a particular purpose.

The nature of the steps SG takes to verify the information contained in a Digital Certificate vary according to the Digital Certificate fee charged, the nature and identity of the Digital Certificate Holder, and the applications for which the Digital Certificate will be marked as trusted. SG makes no other warranties, and all warranties, express or implied, statutory or otherwise, are excluded to the greatest extent permissible by applicable law, including without limitation all warranties as to merchantability or fitness for a particular purpose.

Each Issuing Certification Authority is required to ensure that warranties, if any, provided by SG in connection with this SG TCP/CPS to Subscribers and Authorised Relying Parties are incorporated, by reference or otherwise, in the relevant User Agreement or applicable terms and conditions. Warranties, if any, provided by SG to Subscribers and/or Authorised Relying Parties shall be set out in a warranty protection plan duly approved by the Policy Management Authority and adopted by SG.

9.5.4. Registration Authority Representations

Registration Authorities in performing their functions will operate their certification services in accordance with:

- any Issuing Certification Authority Agreement
- any applicable Registration Authority Agreement
- all Certificate Policies under which they issue Digital Certificates

- documented operational procedures and
- applicable law and regulation

9.5.5. Registration Authority Warranties

Authorised Registration Authorities operating within the SG Public Key Infrastructure hereby warrant that (a) they take reasonable steps to verify that the information contained in any Digital Certificate is accurate at the time of issue (b) Digital Certificates shall be revoked if SG believes or is notified that the contents of the Digital Certificate are no longer accurate, or that the key associated with a Digital Certificate has been compromised in any way.

9.5.6. Certificate Holder Representations and Warranties

Digital Certificate Holders Represent and Warrant:

- To use only the Digital Certificate Holders own valid, legal and operational Key pairs to create a Digital Signature.
- That the Private Key is protected and has never been accessed by another person.
- All representations made by the Digital Certificate Holder in the Digital Certificate Application are true.
- All information in the Digital Certificate is true and accurate.
- The Digital Certificate is being used for its intended, authorised and legal purpose consistent with this TCP/CPS.

9.5.7. Relying Parties Representations and Warranties

Relying Parties Represent and Warrant:

- To collect enough information about a Digital Certificate and its Corresponding Holder to make an informed decision as to the extent they can rely on the Digital Certificate.
- That the relying part is solely responsible for making the decision to rely on a Digital Certificate.
- That the relying Party shall bear the legal consequences of any failure to perform Relying Party obligations under the terms of this TCP/CPS and Relying Party agreement.

9.5.8. Representations and Warranties of Other Participants

Participants within the SG-PKI Represent and Warrant to accept and perform any and all duties and obligations as specified by this TCP/CPS.

9.6. Term and Termination

9.6.1. Term

This TCP/CPS becomes effective upon publication in the SG Repository. Amendments to this TCP/CPS become effective upon publication in the SG Repository.

9.6.2. Termination

This TCP/CPS shall remain in force until it is amended or replaced by a new version.

9.6.3. Effect of Termination and Survival

The provisions of this SG TCP/CPS shall survive the termination or withdrawal of a User from the SG-PKI with respect to all actions based upon the use of or reliance upon a Digital Certificate or other participation within the SG-PKI. Any such termination or withdrawal shall not act so as to prejudice or affect any right of action or remedy that may have accrued to any person up to and including the date of withdrawal or termination.

9.7. Individual Notices And Communications With Participants

Electronic mail, postal mail, fax, and web pages will all be valid means of SG providing any of the notices required by this SG TCP/CPS, unless specifically provided otherwise. Electronic mail, postal mail, and fax will all be valid

means of providing any notice required pursuant to this SG CP/CPS to SG unless specifically provided otherwise (for example in respect of revocation procedures).

9.8. Amendments

9.8.1. Procedure for Amendment

Amendments to this TCP/CPS are made and approved by the SG Policy Management Authority. Amendments shall be in the form of an Amended TCP/CPS or a replacement Certificate Policy & Certification Practice Statement. Updated versions of this TCP/CPS supersede and designated or conflicting provisions of the referenced version of the TCP/CPS.

9.8.2. Notification Mechanism and Period

The SG Policy Management Authority reserve the right to amend this TCP/CPS without notification for amendments that are not material, including corrections of typographical errors, changes to URLs and changes to contact details. The decision to designate amendments as material or non-material to this TCP/CPS is at the sole discretion of the SG Policy Management Authority.

9.9. Record Keeping

SG shall keep records material to the issue of Digital Certificates for a minimum of 5 (five) years.

9.10. Force Majeure

SG accepts no liability for any breach of warranty, delay or failure in performance that results from events beyond its control such as acts of God, acts of war, acts of terrorism, epidemics, power or telecommunication services failure, fire, and other natural disasters.

9.11. Other Provisions

No specific definition.

9.12. Disclaimer / Legal Validity

This general disclaimer is part of this SG TCP/CPS. If any of the terms and conditions should be determined invalid by reasons of the relevant laws then the remaining terms and conditions shall remain in full effect.

10. APPENDIX A

10.1. Digital Certificate Profiles

Within the SG Public Key Infrastructure an Issuing Certification Authority can only issue Digital Certificates with approved Digital Certificate Profiles. All Digital Certificate Profiles within the SG Public Key Infrastructure are detailed below.

The procedure for Digital Certificate Holder registration, Digital Certificate generation and distribution is described below for each type of Digital Certificate issued. Additionally specific Certificate Policies and SG liability arrangements not described in this TCP/CPS may be drawn up under contract for individual customers.

Please note that where a Qualified Digital Certificate is issued within the meaning of European Union Directive 1999/93/EC, the individual applying for the Qualified Digital Certificate must undergo a face to face identification and verification procedure, or use a pre-existing identification where a digital trust worth identification can be provided.

The Certificate Profiles that follow indicate the fields which are variable on initial registration by the Certificate Holder (SE) and those which are fixed by the Issuing Certification Authority either based on policy or by IETF Standard, applicable law or regulation.

10.2. Qualified Personal Certificate (QualifiedUserCA2008)

Field	Content
Version	V3
Serial Number	Unique, system generated number
Signature Algorithm	SHA1RSA
Subject Public Key Information	RSA (1024 or 2048)
Validity:	
Not Before	Date: DD.MM.YYYY HH:MM:SS
Not After	Date: DD.MM.YYYY HH:MM:SS
Issuer:	
Common Name (CN)	Signguard QualifiedUserCA2008
Organisational Unit (OU)	QualifiedUserCA2008
Organisation (O)	Signguard Europe AB
Country (C)	SE
Subject:	
Common Name (CN)	First Name and Last Name
Organisational Unit (OU)	Not Used
Organisation(O)	Not Used
Country (C)	ISO 3166-1 Country Code
Serial (Serial)	Optional
Extensions:	
Authority Key Identifier	SHA-1 Message Imprint of Public Key of Issuing CA
Subject Key Identifier	SHA-1 Message Imprint of Subjects Public Key
Key Usage	Non Repudiation
Certificate Policies	http://www.signguard.se/policies/policies.html
Authority Information Access	http://ocsp.signguard.se/QualifiedUserCA2008/
CRL Distribution	http://pki.signguard.se/ca/QualifiedUserCA2008.der.crl
Thumbprint Algorithm	SHA1

NCSA Policy URL	http://www.signguard.se/policy/policies.html
QC Statement	0.4.0.1862.1.1 (PKIX QC Compliance)
Subject Alternative Name	Not Used
Warrenty	1.3.6.1.5.5.7.1.16 (PKIX Warranty Certificate Extension)

10.3. Advanced Personal Certificate (AdvancedUserCA2008)

Field	Content
Version	V3
Serial Number	Unique, system generated number
Signature Algorithm	SHA1RSA
Validity:	
Not Before	Date: DD.MM.YYYY HH:MM:SS
Not After	Date: DD.MM.YYYY HH:MM:SS
Issuer:	
Common Name (CN)	Signguard AdvancedUserCA2008
Organisational Unit (OU)	AdvancedUserCA2008
Organisation (O)	Signguard Europe AB
Country (C)	SE
Subject:	
Common Name (CN)	First Name and Last name
Organisational Unit (OU)	Optional
Organisation(O)	Optional
Country (C)	ISO 3166-1 Country Code
Serial (Serial)	Optional
Subject Public Key Information	RSA (1024 or 2048)
Extensions:	
Authority Key Identifier	SHA-1 Message Imprint of Public Key of Issuing CA
Subject Key Identifier	SHA-1 Message Imprint of Subjects Public Key
Key Usage	Digital Signature Key Encipherment
Enhanced Key Usage	Client Authentication Secure Email Encrypting file system (all optional)
Certificate Policies	http://www.signguard.se/policies/policies.html
Authority Information Access	http://ocsp.signguard.se/AdvancedUserCA2008/
CRL Distribution	http://pki.signguard.se/ca/AdvancedUserCA2008.der.crl
Subject Alternative Name	Email address: user@domain.tld
Thumbprint Algorithm	SHA1
Warranty	1.3.6.1.5.5.7.1.16 (PKIX Warranty Certificate Extension)

10.4. Authenticated User (UserAuthCA2008)

Field	Content
Version	V3
Serial Number	Unique, system generated number
Signature Algorithm	SHA1RSA
Validity:	
Not Before	Date: DD.MM.YYYY HH:MM:SS
Not After	Date: DD.MM.YYYY HH:MM:SS
Issuer:	
Common Name (CN)	Signguard UserAuthCA2008
Organisational Unit (OU)	Signguard UserAuthCA2008
Organisation (O)	Signguard Europe AB
Country (C)	SE
Subject:	
Common Name (CN)	First Name and Last name
Organisational Unit (OU)	Optional
Organisation(O)	Optional
Country (C)	ISO 3166-1 Country Code
Serial (Serial)	Optional
Subject Public Key Information	RSA (1024 or 2048)
Extensions:	
Authority Key Identifier	SHA-1 Message Imprint of Public Key of Issuing CA
Subject Key Identifier	SHA-1 Message Imprint of Subjects Public Key
Key Usage	Digital Signature Key Encipherment
Enhanced Key Usage	Client Authentication
Certificate Policies	http://www.signguard.se/policy/policies.html
Authority Information Access	http://ocsp.signguard.se/AdvancedUserCA2008/
CRL Distribution	http://pki.signguard.se/ca/QualifiedUserCA2008.der.crl
Subject Alternative Name	Email address: user@domain.tld
Thumbprint Algorithm	SHA1
Warranty	1.3.6.1.5.5.7.1.16 (PKIX Warranty Certificate Extension)

10.5. Server Certificate (ServerCA)

Has yet to be defined and is for future usage.

10.6. Administrator Certificate (AdminCA)

Field	Content
Version	V3
Serial Number	Unique, system generated number
Signature Algorithm	Sha1RSA

Validity:	
Not Before	Date: DD.MM.YYYY HH:MM:SS
Not After	Date: DD.MM.YYYY HH:MM:SS
Issuer:	
Common Name (CN)	Signguard AdminUserCA
Organisational Unit (OU)	AdminUserCA
Organisation (O)	Signguard Europe AB
Country (C)	SE
Subject:	
Common Name (CN)	First Name and Last name
Organisational Unit (OU)	Not Used
Organisation(O)	Signguard Europe AB
Country (C)	SE
Subject Public Key Information	RSA 2048
Extensions:	
Authority Key Identifier	SHA-1 Message Imprint of Public Key of Issuing CA
Subject Key Identifier	SHA-1 Message Imprint of Subjects Public Key
Key Usage	Digital Signature Non Repudation Key Encipherment Data Encipherment Key Agreement (all optional)
Enhanced Key Usage	Client Authentication Secure Email Encrypting file system (all optional)
Certificate Policies	http://www.signguard.se/policies/policies.html
Authority Information Access	http://ocsp.signguard.se/admin/
CRL Distribution	http://pki.signguard.se/ca/AdminCA.der.crl
Subject Alternative Name	Email address: user@domain.tld (optional)
Thumbprint Algorithm	SHA1
Warranty	1.3.6.1.5.5.7.1.16 (PKIX Warranty Certificate Extension)

10.7. Authentication software-certificate (SW-Auth)

Field	Content
Version	V3
Serial Number	Unique, system generated number
Signature Algorithm	SHA1RSA
Validity:	
Not Before	Date: DD.MM.YYYY HH:MM:SS
Not After	Date: DD.MM.YYYY HH:MM:SS
Issuer:	
Common Name (CN)	Signguard SW-Auth
Organisational Unit (OU)	Signguard SW-Auth
Organisation (O)	Signguard Europe AB
Country (C)	SE
Subject:	

Common Name (CN)	First Name and Last name
Organisational Unit (OU)	Optional
Organisation(O)	Optional
Country (C)	ISO 3166-1 Country Code
Serial (Serial)	Optional
Subject Public Key Information	RSA (1024 or 2048)
Extensions:	
Authority Key Identifier	SHA-1 Message Imprint of Public Key of Issuing CA
Subject Key Identifier	SHA-1 Message Imprint of Subjects Public Key
Key Usage	Digital Signature Key Encipherment
Enhanced Key Usage	Client Authentication
Certificate Policies	http://www.signguard.se/policies/policies.html
Authority Information Access	http://ocsp.signguard.se/swauthuser
CRL Distribution	http://pki.signguard.se/ca/SW-Auth.der.crl
Subject Alternative Name	Email address: user@domain (optional)
Thumbprint Algorithm	SHA1
Warranty	1.3.6.1.5.5.7.1.16 (PKIX Warranty Certificate Extension)

10.8. E-Mail software-certificate (SW-Email)

Field	Content
Version	V3
Serial Number	Unique, system generated number
Signature Algorithm	SHA1RSA
Validity:	
Not Before	Date: DD.MM.YYYY HH:MM:SS
Not After	Date: DD.MM.YYYY HH:MM:SS
Issuer:	
Common Name (CN)	Signguard SW-Email
Organisational Unit (OU)	SW-Email
Organisation (O)	Signguard Europe AB
Country (C)	SE
Subject:	
Common Name (CN)	First Name and Last name
Organisational Unit (OU)	Optional
Organisation(O)	Optional
Country (C)	ISO 3166-1 Country Code
Serial (Serial)	Optional
Subject Public Key Information	RSA (1024 or 2048)
Extensions:	
Authority Key Identifier	SHA-1 Message Imprint of Public Key of Issuing CA
Subject Key Identifier	SHA-1 Message Imprint of Subjects Public Key

Key Usage	Digital Signature Key Encipherment
Enhanced Key Usage	Client Authentication Secure Email Encrypting file system (all optional)
Certificate Policies	http://www.signguard.se/policies/policies.html
Authority Information Access	http://ocsp.signguard.se/swemail/
CRL Distribution	http://pki.signguard.se/ca/SW-Email.der.crl
Subject Alternative Name	Email address: user@domain.tld
Thumbprint Algorithm	SHA1
Warranty	1.3.6.1.5.5.7.1.16 (PKIX Warranty Certificate Extension)

10.9. Test CAs

All Test CAs from the SG Public Key Infrastructure (SignGuardServer TestCA and TESTCA) are for internal use only!

If needed or on request, SG will publish the Digital Certificate Profiles of these Test Certification Authorities.