Suva

Suva ROOT CERTIFICATION AUTHORITY

CERTIFICATE POLICY/CERTIFICATION PRACTICE STATEMENT

Effective Date: October 07, 2010
Version: 1.0

OID: 1.3.6.1.4.1.8024.0.3.600.0

Important Note About this Document

This document is the Certificate Policy/Certification Practice Statement herein after referred to as the Certificate Policy & Certification Practice Statement (CPCPS), adopted by Suva, (Suva). The Suva Certificate Policy & Certification Practice Statement contains an overview of the practices and procedures that Suva employs for its operation as a Digital Certification Authority.

This Document covers aspects of the Suva Public Key Infrastructure that relate to ALL Certification Authorities established by Suva.

Contact Information:

Suva
Abteilung Informatik
Fluhmattstr. 1
Postfach 4358
CH-6002 Luzern

Version Control

Date	Version	Comment	Author
May, 21 2010	0.1	Initial Version	R. Brutschin
June, 14 2010	0.2	Updates in Kapitel 5.4ff	R. Emmenegger
June, 29 2010	0.3	Div. kleinere Updates	R. Emmenegger
June, 30 2010	0.4	Div. kleinere Updates	R. Emmenegger
July, 1 2010	0.5	Update Abbilung in Kapitel 1.3	R. Emmenegger
July, 12 2010	0.6	Kap. 4.7 ' for public facing websites' added	R. Emmenegger
July, 21 2010	0.7	Suva durch Suva ersetzt	R. Emmenegger
July, 28 2010	0.8	Kap. 9.13 ergänzt	R. Emmenegger
Oktober, 07 2010	0.9	Dokument finalisiert	R. Emmenegger

Table of Contents

1 INTRODUCTION

1.1 Overview

The Suva Certificate Policy & Certification Practice Statement sets out 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 Suva Public Key Infrastructure.

The Certificate Policy & Certification Practice Statement outlines the trustworthiness and integrity of the Suva Root Certification Authority's operations. A fundamental concept underpinning the operation of the Suva Public Key Infrastructure is trust. Trust must be realised in each and every aspect of the provision of Certification Services and Operations including Digital Certificate Holder applications, issuance, renewal, revocation or expiry.

Suva ensures the integrity of its Public Key Infrastructure's operational hierarchy by binding Participants to contractual agreements. This Certificate Policy & Certification Practice Statement is not intended to create a contractual relationship between Suva and any Participant in the Suva Public Key Infrastructure. This Certificate Policy & Certification Practice Statement merely provides a general overview of the Suva Public Key Infrastructure including Digital Certificate Profiles as defined in Appendix A.

The Suva Public Key Infrastructure 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 Suva Public Key Infrastructure must do so pursuant to definitive contractual documentation.

This Certificate Policy & Certification Practice Statement undergoes a regular review process and is subject to amendment.

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

Any and all references to a Certificate Policy within every aspect the Suva Public Key Infrastructure refers to policies contained in the current and in-force Certificate Policy & Certification Practice Statement.

1.2 Document Name and Identification

The Object Identifier (OID) assigned to this Certificate Policy & Certification Practice Statement (CP & CPS) is: 1.3.6.1.4.1.8024.0.3.600.0

1.3 Public Key Infrastructure Participants

The Suva Certificate Policy & Certification Practice Statement outlines the roles and responsibilities of all parties involved in the generation and use of Digital Certificates and the operation of all Suva approved:

- Issuing Certification Authority services.
- Registration Authority services.

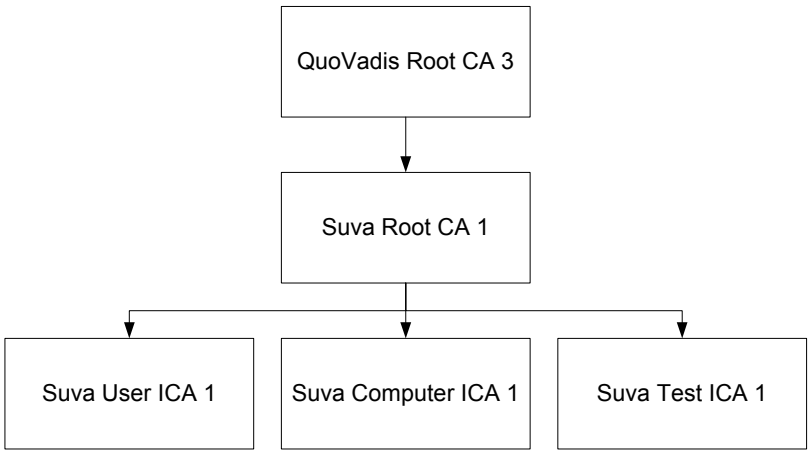
Suva, in its capacity as the Root Certification Authority, holds the Suva Root Certificate. The Suva Root Certification Authority represents the apex of the Suva Public Key Infrastructure. The Suva Root Certificate is signed by the QuoVadis Root Certificate to ensure widespread trust of certificates issued within the Suva PKI. The Suva Root Certification Authority digitally creates, signs and issues Issuing Certification Authority Certificates with its Root Certificate. Issuing Certificates are only issued to Approved Issuing Certification Authorities which are subsidiaries or affiliates of the Suva. An Approved Issuing Certification Authority utilizes its Issuing

Certificate to create, sign and issue Certificate Holder Digital Certificates. Approved Registration Authorities act as the interface between Issuing Certification Authorities and an Applicant Digital Certificate Holder. Approved Registration Authorities perform due diligence on potential Digital Certificate Holders and only successful applicant Digital Certificate Holders are approved and receive a Certificate Holder Digital Certificate.

Authorized Issuing Certification Authorities 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.
Generally, device Certificates will be issued to "internally and publicly facing" devices and applications. Exceptions of device Certificates that must NOT be issued by a Suva Corporate CA are listed in the contract (Root Signing Agreement) between QuoVadis and Suva. These are publicly facing certificates issued to public websites.

If you are not familiar with Common Terms usually employed in a Public Key Infrastructure please refer to the Key Terms and Definitions in Appendix B

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



Suva provides identification and authentication services for Digital Certificate Holders, servers, and personal computer or network devices. The registration procedures set out in this Certificate Policy & Certification Practice Statement and in Appendix A define the credentials necessary to establish the identity of an individual or entity.

- Suva has established the Suva Root Certification Authority under which a number of subordinate services operate. These subordinate services within the Suva Public Key Infrastructure are managed and operated by Suva

All subordinate services that operate under the Suva Root Certification Authority, i.e. that are within the Suva "chain of trust" are described in a separate Suva PKI 2008 concept.

Participants ("Participants") within the Suva Public Key Infrastructure include:

- Certification Authorities
- Registration Authorities
- Digital Certificate Holders including applicants for Digital Certificates prior to Digital Certificate issuance
- Authorized Relying Parties (including Suva Group Companies)

The practices described or referred to in this Certificate Policy & Certification Practice Statement:

- accommodate the diversity of the community and the scope of applicability within the Suva chain of trust; and
- adhere to the primary purpose of the Certificate Policy & Certification Practice Statement, of describing the uniformity and efficiency of practices throughout the Suva Public Key Infrastructure.

In keeping with their primary purpose, the practices described in outline in this Certificate Policy & Certification Practice Statement:

- are the minimum requirements necessary to ensure that Digital Certificate Holders and Authorized 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.

Within the Suva Certification Authority hierarchy there is one Root Certification Authority entity that represents the source of all trust within the Suva Public Key Infrastructure.

Suva digital certificates comply with the latest in Internet Standards (x509 v.3) as set out in RFC 5280.

Applications are as follows: authentication, signature and file encryption; secure electronic mail, business transactions, IPSEC applications, secure SSL/TLS applications not including public facing web site security, contracts signing applications, custom e-Commerce applications etc.

Digital Certificates may not be used and no participation is permitted in the Suva 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 or (iii) in connection with fraud, pornography, obscenity, hate, defamation, harassment, or other activity that is contrary to public policy.

1.3.1 Root Certification Authority

The Suva Root Certification Authority named "Suva Root Certification Authority" issues Issuing Certification Authority Certificates in accordance with this Suva Certificate Policy & Certification Practice Statement and related operational documents.

1.3.2 Suva and the Root Certificate Object Identifier

The Private Enterprise Object Identifier assigned by the QuoVadis to the Suva Root Certificate is declared in section 1.2.

The Object Identifier assigned to the QuoVadis Root Certification Authority 3 Certificate is 1.3.6.1.4.1.8024.0.3.

1.3.3 Suva Obligations

Suva is obligated to operate the Suva Root Certification Authority, Suva Issuing Certification Authority and Suva Registration Authorities in accordance with this Suva Certificate Policy & Certification Practice Statement and other relevant operational policies and procedures with respect to the issuance and management of Digital Certificates.

1.3.4 Issuing Certification Authority Obligations

Within the Suva 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, may only rely on Suva Group Regis-

tration Authorities in the performance of Digital Certificate Holder Identification and Authentication requirements.

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 Suva Certificate Policy & Certification Practice Statement.
- They comply at all times with all compliance audit requirements.
- They follow a privacy policy in accordance with this Suva Certificate Policy & Certification Practice Statement.

1.3.5 Issuing Certification Authorities

Issuing Certification Authorities are Organizations Authorized by Suva to participate within the Suva Public Key Infrastructure to create, issue, sign, revoke and otherwise manage Digital Certificates in accordance with this Certificate Policy & Certification Practice Statement. Generally, Issuing Certification Authorities will be Authorized to issue and manage all types of Digital Certificates supported by this Suva Certificate Policy & Certification Practice Statement. These Organizations must be part of the Suva Group.

Issuing Certification Authorities are required to act in accordance with and to be bound by the terms of this Suva Certificate Policy & Certification Practice Statement. 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 Suva Policy Management Authority. Suva operates the Suva Root Certification Authority and Suva Issuing Certification Authorities in accordance with this Certificate Policy & Certification Practice Statement. Notwithstanding that the Issuing Certification Authority may delegate certain functions to a Suva Registration Authority; the Suva Issuing Certification Authority shall retain all responsibility for the management of Digital Certificates issued by it.

1.3.6 Registration Authority Obligations

Issuing Certification Authorities may, subject to the approval of Suva, designate specific Suva Registration Authorities to perform the Identification and Authentication and Digital Certificate request and revocation functions defined by this Suva Certificate Policy & Certification Practice Statement. All Suva Registration Authorities are required to fulfill their functions and obligations in accordance with this Suva Certificate Policy & Certification Practice Statement to be entered into between the Suva Registration Authority and the relevant Issuing Certification Authority.

Registration Authorities must perform certain functions in accordance with this Certificate Policy & Certification Practice Statement 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 this Suva Certificate Policy & Certification Practice Statement including, without limitation to the generality of the foregoing, compliance with any compliance audit requirements.
- Follow a privacy policy in accordance with this Suva Certificate Policy & Certification Practice Statement and other applicable documents Suva.

1.3.7 Certificate Holders

1.3.7.1 Obligations and Responsibilities

Digital Certificate Holders are required to act in accordance with this Certificate Policy & Certification Practice Statement and relevant 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 Suva 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 Suva 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 whatsoever.
- Take all reasonable measures to avoid the compromise of the security or integrity of Suva or the Suva Public Key Infrastructure.
- Forthwith upon termination, revocation or expiry of the Digital Certificate (howsoever caused), cease use of the Digital Certificate absolutely.
- At all times utilize the Digital Certificate in accordance with all applicable laws and regulations
- Use the signing keypairs 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 keypair in the event that Suva notifies the Digital Certificate Holder that the Suva Public Key Infrastructure has been compromised.

1.3.7.2 Accepted Limitation of Liability

Digital Certificates include a reference to the Certificate Policy & Certification Practice Statement, which includes statements detailing limitations of liability and disclaimers of warranty. In accepting a Digital Certificate, Digital Certificate Holders acknowledge and agree to all such limitations and disclaimers.

1.3.8 Relying Parties

Authorized Relying Parties are Individuals or Organizations who are authorized by contract to exercise Reasonable Reliance on Digital Certificates in accordance with the terms and conditions of this Suva Certificate Policy & Certification Practice Statement.

1.3.8.1 Obligations and Responsibilities

Authorized Relying parties are required to act in accordance with this Certificate Policy & Certification Practice Statement and Relying Party Agreement.

An Authorized Relying Party must utilize Digital Certificates and their corresponding Public Keys only for authorized and legal purposes and only in support of transactions or communications supported by the Suva Public Key Infrastructure.

An Authorized Relying Party shall not place reliance on a Digital Certificate unless the circumstances of that intended reliance constitute Reasonable Reliance and that Authorized 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.

1.3.8.2 Reasonable Reliance

An Authorized 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 Authorized Relying Party is otherwise in compliance with the terms and conditions of an applicable Authorized Relying Party Agreement and this Certificate Policy & Certification Practice Statement. For the purposes of this Certificate Policy & Certification Practice Statement 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 Authorized 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 Authorized Relying Party has, at the time of that reliance, used the Digital Certificate for purposes appropriate and permitted under this Suva Certificate Policy & Certification Practice Statement ;
- that the Authorized 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 Authorized Relying Party;
- that the Digital Certificate intended to be relied upon is valid and has not been revoked, the Authorized Relying Party being obliged to check the status of that Digital Certificate utilizing either the Suva Database, the Suva Certificate Revocation List or the Suva Online Certificate Status Protocol or otherwise in accordance with the provisions of this Suva Certificate Policy & Certification Practice Statement ;
- that the Authorized Relying Party has, at the time of that reliance, verified the Digital Signature, if any;
- that the Authorized 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 Authorized Relying Party ensures that the data signed has not been altered following signature by utilizing trusted application software,
- that the signature is trusted and the results of the signature are displayed correctly by utilizing trusted application software;
- that the identity of the Digital Certificate Holder is displayed correctly by utilizing trusted application software; and
- that any alterations arising from security changes are identified by utilizing trusted application software.

1.3.8.3 Accepted Limitation of Liability

Digital Certificates include a reference to the Certificate Policy & Certification Practice Statement, which includes statements detailing limitations of liability and disclaimers of warranty. In accepting a Digital Certificate, Digital Certificate Holders acknowledge and agree to all such limitations and disclaimers.

1.3.8.4 Assumptions about a Certificate Holder

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

1.3.8.5 Certificate Compromise

A party cannot rely on a Digital Certificate issued by Suva 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 Certificate Policy & Certification Practice Statement and the current set of revoked Digital Certificates published by Suva.

1.3.9 Other Participants

Other Participants in the Suva Public Key Infrastructure are required to act in accordance with this Certificate Policy & Certification Practice Statement and/or applicable Certificate Holder Agreement and/or Relying Party Agreement's or other relevant Suva documentation.

1.4 Certificate Usage

At all times utilize its Digital Certificate in accordance with this Suva Certificate Policy & Certification Practice Statement 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 Suva Certificate Policy & Certification Practice Statement is restricted to parties Authorized by contract to do so. Persons and entities other than those Authorized 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 Authorized 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 Authorized 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 Suva or any Suva Provider of any authority, rights, or privilege save as expressly set out in this Suva Certificate Policy & Certification Practice Statement or expressly set out in the Digital Certificate.

Any person participating within the Suva Public Key Infrastructure irrevocably agrees, as a condition to such participation, that the issuance of all products and services contemplated by this Suva Certificate Policy & Certification Practice Statement shall occur and shall be deemed to occur in Switzerland and that the performance of Suva' obligations hereunder shall be performed and be deemed to be performed in Switzerland.

1.4.2 Prohibited Certificate Usage

Digital Certificates may not be used and no participation is permitted in the Suva 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 Switzerland.

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 Suva Certificate Policy & Certification Practice Statement or the relevant Certificate Holder 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 Certification Practice Statement.

1.6 Policy Administration

1.6.1 Organization Administering the Certificate Policy & Certification Practice Statement

Suva operates the Policy Management Authority that is responsible for setting Certificate Policy & Certification Practice Statement and Certificate Profile direction for the overall public key infrastructure.

1.6.2 Certificate Policy & Certification Practice Statement Applicability

This Suva Certificate Policy & Certification Practice Statement is applicable to all Digital Certificates issued by the Suva Root Certification Authority and by Issuing Certification Authorities. Digital Certificates issued under this Suva Certificate Policy & Certification Practice Statement are intended to support secure electronic commerce and the secure exchange of information by electronic means.

1.6.3 Certificate Policy & Certification Practice Statement Revisions

The Suva Policy Management Authority is the responsible authority for changes to this Certificate Policy & Certification Practice Statement. There are two possible types of policy change:

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

1.6.3.1 Revisions without Notification

The only changes that may be made to this Suva Certificate Policy & Certification Practice Statement 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 Suva Public Key Infrastructure.

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 Suva Certificate Policy & Certification Practice Statement or under policies that make reference to this Suva Certificate Policy & Certification Practice Statement requires thirty (30) days prior notice.

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

The Suva Policy Management Authority has authority to evaluate all changes and determine whether prior notification is required and whether the Suva Certificate Policy & Certification Practice Statement Object Identifier should be changed.

1.6.4 Certificate Policy & Certification Practice Statement Publication and Notification

New or amended Certificate Policy & Certification Practice Statements are published on the

web site http://pki.Suva.ch/repository. Issuing Certification Authorities are notified of changes to the Certificate Policy & Certification Practice Statement as and when they are approved.

1.6.5 Contact Person

This Certificate Policy & Certification Practice Statement is administered by the Policy Management Authority. Enquiries or other communications about this Certificate Policy & Certification Practice Statement should be addressed to:

Suva
Herr Markus Huber
Abteilung Informatik
Fluhmattstr. 1
Postfach 4358
CH-6002 Luzern

1.6.6 Person Determining the Certificate Policy & Certification Practice Statement Suitability

The Suva Policy Management Authority determines the suitability of the Certificate Policy & Certification Practice Statement.

1.6.7 Certificate Policy & Certification Practice Statement Approval Procedures

This Suva Certificate Policy & Certification Practice Statement is regularly reviewed and approved by the Suva Policy Management Authority. Notice of proposed changes are recorded in the change log at the beginning of this Suva Certificate Policy & Certification Practice Statement until they are approved, at which time the approved change will be recorded there permanently.

1.6.8 Publication of Certificate Policy & Certification Practice Statement

This Certificate Policy & Certification Practice Statement is published electronically in PDF format at http://pki.Suva.ch/repository

1.6.9 Frequency of Publication

Newly approved versions of this Certificate Policy & Certification Practice Statement, 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

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

1.7 Definitions and Acronyms

See Appendix B

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

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

The Suva 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 Suva Root Certification Authority and chained Issuing Certification Authorities may 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 (Section 10) of this Certificate Policy & Certification Practice Statement

2.3 Time or Frequency of Publication

Digital Certificate information is published promptly following generation and issue. Publication from the Active Directory Repository to the Certificate Revocation List is done in batch mode via an automated daily workflow process.

2.4 Access Controls on Repositories

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

3 IDENTIFICATION AND AUTHENTICATION

Suva 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 Suva Root Certification Authority 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 readily identifiable X.501 Distinguished Name (DN). The Distinguished Name includes the following fields:

- Common Name (CN) = First name/Last Name/ Suva Group User ID

The Common Name may contain the applicant's first and last name (surname). The Common Name is the only field authenticated during the Registration procedure. The User may choose whether to include the Locality, 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.

3.1.2 Need for Names to be Meaningful

Distinguished names must be meaningful, unambiguous and unique. Pseudonymous names may not be used. Suva 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 associ-

ation with the name of the Individual, Organization, 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 Organizations, the name shall meaningfully reflect the legal name of the Organization or the trading or business name of that Organization. In the case of a Device, the name shall state the name of the Device and the name of the Organization responsible for that Device.

3.1.3 Pseudonymous Certificate Holders

Suva Registration Authorities, their Subsidiaries or Holding Companies may not request Digital Certificates with Pseudonym to be issued by the Suva 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 Certificate Policy & Certification Practice Statement and the Digital Certificate Profiles detailed in Appendix A.

3.1.5 Uniqueness of Names

Suva 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 Suva 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.

3.2 Initial Identity Validation

Identity Validation is in compliance with this Certificate Policy & Certification Practice Statement 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 deemed 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.

3.2.2 Authentication of Organization Identity

The Identity of an Organization is required to be Authenticated with respect to each Digital Certificate that asserts (i) the Identity of an Organization; or (ii) an Individual or Device's affiliation with an Organization. Without limitation to the generality of the foregoing, the Identity of any Organization that seeks to act as a Registration Authority issuing certificates to its employees and/or employees of its respective Subsidiaries, Holding Companies or Counterparties is required to be Authenticated.

In order to Authenticate the Identity of an Organization, at a minimum, confirmation is required that: (i) the Organization legally exists in the name that will appear in the Organization field of any Digital Certificates issued under its name, or routinely does business under an alternative Organizational Unit identifier proposed by the Organization; and (ii) all other information contained in the Digital Certificate application is correct.

Where an Issuing Certification Authority or Registration Authority has a separate and pre existing commercial relationship with the Organization under review, the Issuing Certification Authority or Registration Authority may Authenticate the Identity of the Organization by reference to records kept in the ordinary course of business that, at a minimum, satisfy the requirements of this section. In all such cases, the Issuing Certification Authority or Registration Authority shall record the specific records upon which it relied for this purpose.

3.2.3 Authentication of Individual Identity

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

3.2.4 Validation of Authority

Where a Digital Certificate Holder's Name is associated with an Organizational Name to indicate the Digital Certificate Holder's status as a Counterparty, Employee or specifies an Authorization level to act on behalf of an Organization the Registration Authority will validate Applicant Digital Certificate Holders Authority by reference to business records maintained by the Registration Authority, its Subsidiaries, Holding Companies or Affiliates.

3.3 Identification and Authentication for Renewal Requests

Suva does not support renewal for public facing websites. 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.

3.3.1 Identification and Authentication for Routine Re-Key

Identification and Authentication for routine rekey is based on the same requirements as issuance of new certificates.

3.3.2 Identification and Authentication for Re-Key After Revocation

Identification and Authentication for Re-Key after revocation is based on the same requirements as issuance of new certificates.

3.4 Identification and Authentication for Revocation Requests

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

3.4.1 Certificate Holder

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

- Applying in person to the Registration Authority, Issuing Certification Authority or Suva supplying either original proof of identification in the form of a valid Passport, a national ID

card or a Suva internal Identification Card. A Suva internal Identification Card must have been accredited by a Suva internal department based on a Passport or a national ID card.
- Send a digitally signed email message to the Issuing Registration Authority, Issuing Certification Authority or Suva requesting that their Digital Certificate is revoked.
- Telephonically communicating a pre-existing shared secret associated with the Digital Certification Authority following appropriate Identification.

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 Suva Certificate Policy & Certification Practice Statement (including, without limitation, that information set out in Appendix A) 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 Enrollment Process and Responsibilities

Certain information concerning applications for Digital Certificates is set out in this Suva Certificate Policy & Certification Practice Statement. 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 Suva Public Key Infrastructure. Individuals and Organizations may generate a Digital Certificate application.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

See Appendix A for Identification and Authentication requirements for each Digital Certificate profile.

4.2.2 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 Certificate Policy & Certification Practice Statement and the Digital Certificate Profiles contained in Appendix A.

Suva, at its sole discretion not to be unreasonably withheld, may override any decision to Approve a Digital Certificate Holder Application.

4.2.3 Time to Process Certificate Applications

Registration and Issuing Certification Authorities operating within the Suva 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 Suva Certificate Policy & Certification Practice State-

ment.

4.3.1.1 Suva Root Certification Authority

The Root Certification Authority Certificate has been self generated and signed by the QuoVadis Root Certification Authority.

4.3.1.2 Suva Issuing Certification Authority Certificates

The Suva Root Certification Authority issues the Issuing Certification Authority Digital Certificate to the relevant Issuing Certification Authority.

4.3.1.3 Suva Registration Authority Appointment

Suva Registration Authorities are all wholly owned subsidiaries of Suva.

4.3.1.4 Registration Authority Officers Certificate

As part of the application process, Registration Authority's are required to nominate one or more persons within their Organization 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 Suva Public Key Infrastructure 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 Suva Certificate Policy & Certification Practice Statement.

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. This Certificate Policy & Certification Practice Statement sets out 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 Suva Certificate Policy & Certification Practice Statement 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 Authorized Issuing Certification Authority operating within the Suva Public Key Infrastructure, the Digital Certificate Holder expressly agrees with Suva 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 unauthorized person has ever had access to the Digital Certificate Holder's private key;

- All representations made by the Digital Certificate Holder to Suva 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 Suva of any material inaccuracies in such information;
- The Digital Certificate is being used exclusively for Authorized and legal purposes, consistent with this Certificate Policy & Certification Practice Statement.

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 CERTIFICATION POLICY & PRACTICE STATEMENT 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 UNAUTHORIZED USE.

4.4.2 Conduct Constituting Certificate Acceptance

The following constitutes acceptance of a Digital Certificate within the Suva 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 Suva Public Key Infrastructure are made available to relying parties.

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

Issuing and Registration Authorities within the Suva 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 Suva Public Key Infrastructure 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 Suva Public Key Infrastructure agrees to and accepts the Relying Party Agreement (http://pki.Suva.ch/repository) 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 asses:

- The appropriateness of the use of the Digital Certificate for any given purpose and that the use is not prohibited by this Certificate Policy & Certification Practice Statement.
- 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 or Certificate Revocation List Checks.

4.6 Certificate Re-Key

On expiration of the Certificate Validity Period, Digital Certificates are renewed on the basis of issuing a new Key Pair to the Digital Certificate Holder. Due diligence, key pair generation, delivery and management is performed in accordance with this Certificate Policy & Certification Practice Statement.

4.6.1 Circumstance for Certificate Re-Key

Digital Certificates may be renewed upon request.

4.6.2 Who May Request Re-Key

Digital Certificate Holders and Nominating Registration Authorities may request Digital Certificate Re-Keys.

4.6.3 Processing Certificate Re-Key Request

Digital Certificate Re-Key requests are processed in the same manner as requests for new Digital Certificates and in accordance with the provisions of this Certificate Policy & Certification Practice Statement. In order to process a Re-Key request the Digital Certificate Holder is required to confirm that the:

- Details contained in the original Digital Certificate application have not changed.
- Authenticate their identity to the Registration Authority.

Using the Digital Certificate to be renewed the Digital Certificate Holder may digitally sign an electronic message to the Nominating Registration Authority requesting that the Digital Certificate be renewed and confirming that the original application details have not changed.

4.6.4 Notification of New Certificate Issuance to Certificate Holder

Issuing and Registration Authorities within the Suva Public Key Infrastructure may choose to notify Digital Certificate Holders of Digital Certificate Issuance.

4.6.5 Conduct Constituting Acceptance of a Re-Key Certificate

The following constitutes acceptance of a Digital Certificate Re-Key within the Suva Public Key Infrastructure:

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

4.6.5.1 Publication of the Re-Key Certificate by the Certification Authority

All Digital Certificate Re-Keys issued within the Suva Public Key Infrastructure are made available to relying parties.

4.6.6 Notification of Certificate Re-Key by the Certification Authority to Other Entities

Issuing and Registration Authorities within the Suva Public Key Infrastructure may choose to notify other entities of Digital Certificate Re-Key.

4.7 Certificate Renewal

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

- The Suva Public Key Infrastructure does not support Renewal for public facing websites.

4.8 Certificate Modification

- The Suva Public Key Infrastructure does not support Digital Certificate Modification

4.9 Certificate Revocation and Suspension

4.9.1 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:

- Suva Digital Certification Authority key compromise
- Digital Certificate Holder profile creation error
- Key Compromise including unauthorized access or suspected unauthorized 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 Suva Certificate Policy & Certification Practice Statement or any other agreement, regulation, or law that may be in force with respect to that Digital Certificate;
- Where a Digital Certificate Holder's employer or company that operates the Nominating Registration Authority, or its respective Subsidiaries, Holding Companies or Counterparties requests revocation because;
- Of a change in the employment relationship with the Digital Certificate Holder
- The Digital Certificate Holder is no longer authorized to act on behalf of the employer or its respective Subsidiaries, Holding Companies or Counterparties.
- The Digital Certificate Holder otherwise becomes unsuitable or unauthorized to hold a Digital Certificate on behalf of the employer or its respective Subsidiaries, Holding Companies or Counterparties.
- Affiliation change
- Cessation of operation
- Incorrect information contained in Digital Certificate
- Digital Certificate Holder bankruptcy
- Digital Certificate Holder liquidation
- Digital Certificate Holder death
- Digital Certificate Holder request
- Issuing Registration Authority Request
- Breach of Certificate Holder agreement with Suva

In the event that an Issuing Certification Authority determines that its Digital Certificates or the Suva Public Key Infrastructure could become compromised and that revocation of Digital Certificates is in the interests of the Public Key Infrastructure, following remedial action, Suva will authorize the reissue of Digital Certificates to Holders at no charge, unless the actions of the Holders were in breach of the Suva Certificate Policy & Certification Practice Statement or other contractual documents.

4.9.2 Who Can Request Revocation

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

4.9.2.1 Suva

Suva may revoke any Digital Certificate issued within the Suva Public Key infrastructure at its sole discretion, and shall publish the list of revoked Digital Certificates in a publicly accessible Certificate Revocation List.

4.9.2.2 Issuing Certification Authorities

Issuing Certification Authorities operating within the Suva Public Key Infrastructure may revoke Digital Certificates that it has issued.

4.9.2.3 Registration Authorities

Registration Authorities operating within the Suva Public Key Infrastructure may request revocation of Digital Certificates that it requested to be issued.

4.9.2.4 Certificate Holder

A Digital Certificate Holder within the Suva Public Key Infrastructure may request revocation of their Digital Certificate.

4.9.3 Procedure for Revocation Request

Suva 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 Suva Support Line or directly over an Internet connection. 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 (or the Organization, where applicable). Alternatively, the Holder (or Organization, where applicable) may request revocation by contacting the Issuing Certification Authority and providing adequate proof of identification in accordance with this Suva Certificate Policy & Certification Practice Statement or an equivalent method.

4.9.4 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.

4.9.5 Time within which the Certification Authority Must Process the Revocation Request

The Issuing Certification Authority normally revokes Digital Certificates within 24 hours of receipt of a valid revocation request. In exceptional circumstances a "special Revocation Request" may be actioned manually with immediate effect.

4.9.6 Revocation Checking Requirement for Relying Parties

Digital Certificate revocation information is provided via the Certificate Revocation List.

4.9.7 Certificate Revocation List Issuance Frequency

The Certificate Revocation List of an Issuing CA is published weekly with a ten day validity period. The Certificate Revocation List of the Suva Root CA is issued once a year and published 3 months before the next update of the current CRL. The Certificate Revocation List in a directory is updated short-term after 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:

- Authorized 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
- Authorized 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 Authorized Relying Party to claim that it acted on the Digital Certificate with Reasonable Reliance.

4.9.8 Maximum Latency for Certificate Revocation List

The maximum latency for the Certificate Revocation list is 24 hours.

4.9.9 On-Line Revocation/Status Checking Availability

The directory provides Digital Certificate information services. Suva seeks to provide availability for the directory 7 days a week, 24 hours a day, subject to routine maintenance.

4.9.10 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 Authorized 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 Authorized Relying Party to claim that it acted on the Digital Certificate with Reasonable Reliance.

4.9.11 Other Forms of Revocation Advertisements Available

There are no other forms of Revocation Advertisements available.

4.9.12 Special Requirements Re-Key Compromise

Should a private key become compromised, the related certificate shall immediately be revoked. Should the private CA key become compromised, all certificates issued by that CA shall be revoked.

4.9.13 Circumstances for Suspension

No suspension of Digital Certificates is permissible within the Suva Public Key Infrastructure.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

The Status of Digital Certificates issued within the Suva Public Key Infrastructure is published in an LDAP X.500 directory or in a database.

4.10.2 Service Availability

Digital Certificate status services are available 24 hours a day: 7 days a week 365 days of the year.

4.10.3 Optional Features

Key Archive is an optional feature and must be requested by the Digital Certificate Holder before the Digital Certificate is generated.

4.11 End of Subscription

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

- Allowing a Digital Certificate to expire.
- Revoking a Digital Certificate.

4.12 Key Escrow and Recovery

The Suva Public Key infrastructure does support Key Escrow. Digital Certificates used for encryption only are securely archived and accessible under dual control for the purposes of decrypting information only. Signature keys are never archived.

4.12.1 Session Key Encapsulation And Recovery Policy And Practices

Not Applicable.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical Controls

Suva 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 Suva is in a secure office environment in Luzern.

5.1.2 Physical Access

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

5.1.3 Power and Air-Conditioning

The Suva 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 generators is provided.

5.1.4 Water Exposures

The Suva secure operating area provides protection against water.

5.1.5 Fire Prevention and Protection

The Suva secure operating area provides protection against fire.

5.1.6 Media Storage

All magnetic media containing Suva Public Key Infrastructure information, including backup media are stored in containers, cabinets or safes with fire protection capabilities and are located either within the Suva 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 Suva 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; 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 offsite storage agents are used for the storage and retention of backup software and data. The offsite storage is available to authorized personnel 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 Suva Public Key Infrastructure.

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 Certificate Policy & Certification Practice Statement 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.

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 Suva during the registration process.

Digital Certification Authority key-pair generation and initialization of each of the Digital Certification Authority/ies (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 Suva issued Digital Certificate stored on an approved cryptographic smart card 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 M of N employees.

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

5.3.1 Qualifications, Experience, and Clearance Requirements

Suva 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

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

5.3.3 Training Requirements

Suva 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 state of the art industry standard.

5.3.4 Retraining Frequency and Requirements

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

5.3.5 Job Rotation Frequency and Sequence

Not Applicable

5.3.6 Sanctions for unauthorized Actions

Appropriate disciplinary actions are taken for unauthorized actions.

5.3.7 Independent Contractor Requirements

Suva does not support the use of independent contractors to fulfill roles of responsibility.

5.3.8 Documentation Supplied to Personnel

Suva 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.

The types of data recorded by Suva 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.
- 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.
- Time and date of Transaction Archive 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 as needed.

5.4.3 Retention Period for Audit Log

Audit logs are retained as archive records for a period no less than 6 (six) years for audit trail files, and no less than 11 (eleven) years for Key and Digital Certificate information. Audit logs are stored until at least 6 (six) years after the Suva Issuing Certification Authority ceases operation.

5.4.4 Protection of Audit Log

The relevant audit data collected is regularly analyzed for any attempts to violate the integrity of any element of the Suva Public Key Infrastructure.

The Suva PKI Owner and Auditors may view audit logs as a whole. The Suva PKI Owner 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.

5.4.5 Audit Log Backup Procedures

Each Issuing Certification Authority creates a new onsite backup archive of the audit log if the audit log has reached the defined size. 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 Suva Public Key Infrastructure and the participants therein including the Suva 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, Organization, Device or Application that caused the event.

5.4.8 Vulnerability Assessment

Both baseline and ongoing threat and risk vulnerability assessments will be carried out on all parts of the Suva 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 Suva 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, Suvas, and shareholders.

5.5 Records Archival

5.5.1 Types of Records Archived

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 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 Suva Certificate Policy & Certification Practice Statement ; and
- Name of the relevant Suva Registration Authority.

5.5.2 Retention Period for Archive

Suva Issuing Certification Authority archives will be retained and protected against modification or destruction for a period of 6 (six) years.

5.5.3 Protection of Archive

Archives shall be retained and protected against modification or destruction. Only the Suva PKI Owner 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. The Suva PKI Owner 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 the Suva PKI Owner.

5.5.4 Archive Backup Procedures

Adequate backup procedures must be in place.

5.5.5 Requirements For Time-Stamping of Records

No set requirements.

5.5.6 Archive Collection System

The Suva Archive Collection System is internal. Suva provides assistance to Issuing Certification Authorities and Registration Authorities within the Suva Public Key Infrastructure 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 this Certificate Policy & Certification Practice Statement.

5.6 Key Changeover

Key changeover is not automatic. Keys expire at the same time as their associated Digital Certificates and all parties within the Suva 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.

5.7 Compromise and Disaster Recovery

Suva has a Digital Certification Authority Operations Disaster & Recovery 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.

Suva 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. Suva 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.

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

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

5.7.1 Digital Certification Authority Operations Disaster & Recovery Plan

The Digital Certification Authority Operations Disaster & Recovery 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 minimized as much as possible in light of the prevailing circumstances and is subject to the applicable Issuing Certification Authority and/or the Registration Agreements.
Suva 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 minimized;
- ensure that archived records of the Issuing Certification Authority are retained;
- ensure that prompt notification of termination is provided to Digital Certificate Holders, Authorized Relying Parties, and other relevant parties in the Suva 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.

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, unauthorized disclosure or unauthorized use.

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

6 Technical Security Controls

The Suva 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 Suva environment including the Root and Operational Digital Certification Authorities' private keys are restricted by the use of token/smartcards and associated pass phrases.

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

All Key Pairs will be generated in a manner that Suva, in its sole discretion, deems to be secure.

Digital Certificate Holder Key Generation may be performed in hardware or software depending on the Certificate type.

All Keys for Issuing Certification Authorities, Registration Authorities and Registration Authority Officers must be randomly generated on an approved cryptographic token. Any pseudo random numbers used for Key generation material will be generated by a 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.

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, 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 Suva and each Issuing Certification Authority shall be publicly available.

6.1.5 Key Sizes

Key lengths within the Suva Public Key Infrastructure are determined by Digital Certificate Profiles more fully disclosed in section 10. The Suva Issuing Certification Authority uses an RSA minimum key length of 2,048 bit modulus.

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 Suva 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 V3 Key Usage Field)

Keys may be used for the purposes and in the manner described in the Suva Certificate Policy & Certification Practice Statement – 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 Suva Public Key Infrastructure are required to take all appropriate and adequate steps to protect their Private Keys in accordance with the requirements of this Suva Certificate Policy & Certification Practice Statement. Without limitation to the generality of the foregoing, all participants in the Suva Public Key Infrastructure must (i) secure their Private Key and take all reasonable and necessary precautions to prevent the loss, damage, disclosure, modification, or unauthorized 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 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 Suva Public Key Infrastructure is designed to provide Federal Information Processing Standard-140 Level 4 security standards in the maintenance in all Root and Operational Digital Certification Authority private keys.

6.2.2 Private Key (N Out of M) Multi-Person Control

Subject to the requirements of sections 5.2 & 5.3 of the current and in force Suva Certificate Policy & Practice statement the Suva Public Key Infrastructure uses trusted multi-person control for both access control and authorization control.

6.2.3 Private Key Escrow

Private Keys shall not be escrowed.

6.2.4 Private Key Backup

Issuing Certification Authority Private Keys are stored in an encrypted file, which is backed up under further encryption with backup copies maintained on site and in secure offsite 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.

Certificate Holders may choose to backup their Private Keys by backing up their hard drive or

the encrypted file containing their Keys.

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.

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 Suva Public Key Infrastructure comply with industry 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, Organization, 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 Suva Public Key Infra-

structure are:

- Root CA certificate — 20 years
- All Issuing CA certificates — 10 years
- Employee Signing Certificates — 5 years
- Employee Encryption Certificates — 5 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. One of these factors must be randomly and automatically generated. 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 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.

Computer security technical requirements are achieved utilizing 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 Public Key Infrastructure roles, see Section 5.1
- Enforced separation of duties for Certificate Authority Services and Public Key Infrastructure roles, see Section 5.2
- Identification and Authentication of personnel that fulfil roles of responsibility in the Suva Public Key Infrastructure, 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

- Secure access by certificate administrators using a combination of specific IP address, BIOS and Windows passwords.

6.5.2 Computer Security Rating

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

6.6 Life Cycle Technical Controls

All hardware and software procured for operating Issuing Certification Authority within the Suva 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 Suva Public Key Infrastructure shall be developed in a controlled environment under strict change control procedures.

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

6.6.1 System Development Controls

The Suva Certificate Authority follows the Certificate Issuing and Management Components (CIMC) Family of Protections Profiles that defines the requirements for components that issue, revoke and manage public key certificates, such as X.509 public key certificates. The CIMC is based on the common Criteria/ISO IS15408 standards.

6.6.2 Security Management Controls

The Suva Certificate Authority follows the Certificate Issuing and Management Components (CIMC) Family of Protections Profiles that defines the requirements for components that issue, revoke and manage public key certificates, such as X.509 public key certificates. The CIMC is based on the common Criteria/ISO IS15408 standards.

6.6.3 Life Cycle Security Controls

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

6.6.4 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 (off line) configurations.

6.6.5 Hardware Cryptographic Module Engineering Controls

Cryptographic module used by the Suva Root Certification Authority, Issuing Certification Au-

thorities, and Registration Authorities are certified to Internet Engineering Task Force (IETF) Standards, and are either FIPS 140-2 or EAL 4 compliant.

6.7 Time-Stamping

Not applicable.

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate Profile

All Suva Digital Certificates conform to Digital Certificate and Certificate Revocation List profiles as described in RFC 5280 and utilize the ITU-T X.509 version 3 Digital Certificate Standard.
For the purposes of this Suva Certificate Policy & Certification Practice Statement , Digital Certificates, other than the Suva Root Certificate and Issuing Certificates, all other Digital Certificate profiles within the Suva PKI are detailed in Appendix A.

7.1.1 Certificate Content

A Suva Digital Certificate only certifies the information contained therein.

7.1.2 Version Numbers

Digital Certificates in the Suva Public Key Infrastructure are x.509 Version 3.

7.1.3 Certificate Extensions

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

7.1.4 Algorithm Object Identifiers

No Stipulation.

7.1.5 Name Forms

See 3.1.1

7.1.6 Name Constraints

See 3.1.1

7.1.7 Certificate Policy & Certification Practice Statement Object Identifier

The Object Identifier (OID) assigned to this Certificate Policy & Certification Practice Statement (CP & CPS) is listed in section 1.2.

7.1.8 Usage of Policy Constraints Extension

No Stipulation.

7.1.9 Policy Qualifiers Syntax and Semantics

Digital Certificates issued within the Suva Public Key Infrastructure contain the Object Identifier for this Certificate Policy & Certification Practice Statement.

7.1.10 Processing Semantics for the Critical Certificate Policies Extension

No Stipulation.

7.2 Certificate Revocation List Profile

If utilized, Certificate Revocation Lists are issued in the X.509 version 2 format in accordance with the Public Key Infrastructure X Digital Certificate and Certificate Revocation List Profile.

7.2.1 Version Number

Issuing Certification Authorities within the Suva Public Key Infrastructure issue X.509 version 2

Certificate Revocation Lists in accordance with the Public Key Infrastructure X (PKIX) Digital Certificate and Certificate Revocation List Profile.

7.2.2 Certificate Revocation List and Certificate Revocation List Entry Extensions

All User Public Key Infrastructure 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 may be enabled for all Digital Certificates within the Suva Public Key Infrastructure.

7.3.1 Online Certificate Status Protocol Version Numbers

No Stipulation.

7.3.2 Online Certificate Status Protocol Extensions

No Stipulation.

7.4 Root and Issuing Certification Authority Profiles and Certificate Fields

7.4.1 QuoVadis Root Certificate Profile

See Certificate Specification Document "Suva Corporate CA Certificate Specification".

7.4.2 Suva Root Certificate Profile

See Certificate Specification Document "Suva Corporate CA Certificate Specification".

7.4.3 Suva Root CRL Profile

See Certificate Specification Document "Suva Corporate CA Certificate Specification".

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency, Circumstance and Standards of Assessment

8.1.1 Suva Certification Authority

Suva is subject to audits in respect of its various certificate authorities activities by QuoVadis Limited.

8.1.2 Issuing Certification Authorities

Issuing Certification Authorities (including Suva) will undergo an audit in order to determine compliance with this Suva Certificate Policy & Certification Practice Statement, at least annually. These audits shall include the review of all relevant documents maintained by the Issuing Certification Authority regarding their operations within the Suva Public Key Infrastructure and under this Suva Certificate Policy & Certification Practice Statement, and other related operational policies and procedures.

8.1.3 Registration Authorities

Every Registration Authority within the Suva Public Key Infrastructure is subject to a compliance review as needed performed by or on behalf of Suva in order to determine compliance by those entities with their operational requirements within the Suva Public Key Infrastructure. The obligations of Issuing Certification Authorities and Registration Authorities within the Suva Public Key Infrastructure is established by contract between those entities.

8.2 Identity and Qualifications of Assessor

The audit services described in Section 8.1.1 are to be performed by independent, recognised, credible, and established audit firms or information technology consulting firms provided they are qualified to perform and experienced in performing information security audits, specifically

having significant experience with Public Key Infrastructure's and cryptographic technologies.

8.3 Assessor's Relationship to Assessed Entity

The auditor is related to the Certification Authority by contract.

8.4 Topics Covered by Assessment

The topics covered by an audit of an Issuing Certification Authority will include but may not be limited to:

- Security Policy and Planning;
- Physical Security;
- Technology Evaluation;
- Services Administration;
- Personnel Vetting;
- Contracts; and
- Privacy Considerations.

8.5 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 Suva with input from Auditors.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

No individual fees for the certificates or the use of certificate management services related to these certificates (e.g. issuing, updating, revoking, suspending, reactivating) are charged. The Suva PKI is designed to serve Suva employees under rules specified by this Certificate Practice Statement.

9.1.1 Certificate Issuance or Renewal Fees

Not Applicable.

9.1.2 Certificate Access Fees

Not Applicable.

9.1.3 Revocation or Status Information Access Fees

Not Applicable.

9.1.4 Fees for Other Services

Not Applicable.

9.1.5 Refund Policy

Not Applicable.

9.2 Financial Responsibilities

9.2.1 Financial Records

Suva is responsible for maintaining its financial books and records in a commercially reasonable manner.

9.2.2 Fiduciary Relationships

Primary participants in the Suva certificate programs are limited to Suva group employees and directors, and are therefore related to the Certification Authorities.

Relying Parties may be third parties with whom no agency or fiduciary relationship is established.

9.2.3 Insurance Cover

Suva maintains in full force and effect a liability insurance policy.

Within the Suva Public Key Infrastructure the Root Certification Authority and all Issuing and Registration Authorities are required to demonstrate that they have the financial resources necessary to discharge their obligations under this Certificate Policy & Certification Practice Statement and any other relevant and associated documentation or agreements.

Suva and each Issuing and/or Registration Authority shall maintain appropriate insurances necessary to provide for their respective liabilities as participants within the Suva Public Key Infrastructure. Failure to establish and maintain insurances may be the basis for the revocation of their respective Digital Certificates.

9.2.4 Other Assets

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

9.2.5 Insurance or Warranty Coverage for End-Entities

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

9.3 Confidentiality of Business Information

9.3.1 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 Suva Certificate Policy & Certification Practice Statement.

9.3.2 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.

9.4 Responsibility to Protect Confidential Information

9.4.1 Privacy of Personal Information

Suva, 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 Certificate Policy & Certification Practice Statement 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. Suva complies with the Federal Act on Data Protection of June 19, 1992 (SR 235.1).

9.4.2 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.

9.4.2.1 Registration Records

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

9.4.2.2 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 Suva Public Key Infrastructure, in which case prior disclosure of the termination may be given.

9.4.3 Information Deemed Not Private

9.4.3.1 Certificate Contents

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

9.4.3.2 Certificate Revocation List

Digital Certificates published are not considered to be confidential information.

9.4.3.3 Certificate Policy & Certification Practice Statement

This Suva Certificate Policy & Certification Practice Statement is a public document and is not confidential information and is not treated as Private.

9.4.4 Responsibility to Protect Private Information

Information supplied to Suva as a result of the practices described in this Certificate Policy & Certification Practice Statement may be covered by national government or other privacy legislation or guidelines. Suva 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.

9.4.5 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 Suva 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.

9.4.6 Disclosure Pursuant To Judicial or Administrative Process

9.4.6.1 Release to Law Enforcement Officials

As a general principle, no document or record belonging to Suva 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 Suva to be under appeal when served on Suva (Suva 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.

9.4.6.2 Release as Part of Civil Discovery

As a general principal, no document or record belonging to Suva 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 Suva to be under appeal when served on Suva (Suva 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.

9.4.7 Other Information Disclosure Circumstances

Suva, 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 Certificate Policy & Certification Practice Statement.

9.5 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 Suva.

9.5.1 Object Identifiers

Copyright in the Object Identifiers for the Suva infrastructure vests solely in Suva.

9.5.2 Licenses

Suva is in possession of, or holds licences for the use of hardware and software in support of the Suva Public Key Infrastructure as outlined in this Certificate Policy & Certification Practice Statement.

9.5.3 IETF Guidelines

The use of the Public Key Infrastructure X IETF Guidelines is acknowledged.

9.5.4 Breach

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

9.6 Representations and Warranties

9.6.1 Certification Authority Representations

Suva discharges its obligations by:

- providing the operational infrastructure and certification services;
- making reasonable efforts to ensure it conducts an efficient and trustworthy operation. "Reasonable efforts" includes but does not limit Suva to operating in compliance with:
- documented operational procedures; and
- within applicable law and regulation;
- approving the establishment of all Issuing Certification Authorities (save in respect of the Suva Digital Certification Authority);
- maintaining this Certificate Policy & Certification Practice Statement and enforcing the practices described within it and in all relevant collateral documentation;
- publishing its Root Certification Authority Hash at http://pki.Suva.ch/repository 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;
- investigating any suspected compromise which may threaten the integrity of the Suva Public Key Infrastructure;
- revoking Issuing Certification Authority Certificates and posting such revoked Certificates in the Certificate Revocation List; and
- conducting compliance audits of Issuing Certification Authorities.

9.6.2 Certification Authority Warranties

Suva 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 Suva 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 Suva takes to verify the information contained in a Digital Certificate vary according to the nature and identity of the Digital Certificate Holder, and the applica-

tions for which the Digital Certificate will be marked as trusted. Suva 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 Suva takes to verify the information contained in a Digital Certificate vary according to the nature and identity of the Digital Certificate Holder, and the applications for which the Digital Certificate will be marked as trusted. Suva 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 Suva in connection with this Suva Certificate Policy & Certification Practice Statement to Subscribers and Authorized Relying Parties are incorporated, by reference or otherwise, in the relevant User Agreement or applicable terms and conditions. Warranties, if any, provided by Suva to Subscribers and/or Authorized Relying Parties shall be set out in a warranty protection plan duly approved by the Policy Management Authority and adopted by Suva.

9.6.3 Registration Authority Representations

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

- all Certificate Policies under which they issue Digital Certificates;
- documented operational procedures; and
- applicable law and regulation.

9.6.4 Registration Authority Warranties

Authorized Registration Authorities operating within the Suva 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 Suva 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.

9.6.5 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, Authorized and legal purpose consistent with this Certificate Policy & Certification Practice Statement.

9.6.6 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 Certificate Policy & Certification Practice Statement and Relying Party agreement.

9.6.7 Representations and Warranties of Other Participants

Participants within the Suva Public Key Infrastructure Represent and Warrant to accept and perform any and all duties and obligations as specified by this Certificate Policy & Certification Practice Statement.

9.7 Disclaimers of Warranties

To the extent permitted by applicable law, this Certificate Policy & Certification Practice Statement , Digital Certificate Holder Agreement, Relying Party Agreement and any other contractual documentation applicable within the Suva Public Key Infrastructure shall disclaim Suva' possible warranties, including any warranty of merchantability or fitness for a particular purpose.

To the extent permitted by applicable law, Suva makes no express or implied representations or warranties pursuant to this Certificate Policy & Certification Practice Statement. Suva expressly disclaims any and all express or implied warranties of any type to any person, including any implied warranty of title, non infringement, merchantability, or fitness for a particular purpose.

9.8 Liabilities

9.8.1 Suva Liability

Suva shall be liable to Digital Certificate Holders or relying parties for direct loss arising from any breach of this Certificate Policy & Certification Practice Statement or for any other liability it may incur in contract, tort or otherwise, including liability for negligence up to an aggregated maximum limit specified below in section 9.8.3.1 for any one event or series of related events (in any one twelve month period). Suva shall not in any event be liable for any loss of profits, loss of sales or turnover, loss or damage to reputation, loss of contracts, loss of customers, loss of the use of any software or data, loss or use of any computer or other equipment save as may arise directly from breach of this Certificate Policy & Certification Practice Statement, wasted management or other staff time, losses or liabilities under or in relation to any other contracts, indirect loss or damage, consequential loss or damage, special loss or damage, and for the purpose of this paragraph, the term "loss" means a partial loss or reduction in value as well as a complete or total loss.

9.8.2 Suva Limitations of Liability

Suva shall not in any event be liable for any loss of profits, loss of sales or turnover, loss or damage to reputation, loss of contracts, loss of customers, loss of the use of any software or data, loss or use of any computer or other equipment save as may arise directly from breach of this Certificate Policy & Certification Practice Statement , wasted management or other staff time, losses or liabilities under or in relation to any other contracts, indirect loss or damage, consequential loss or damage, special loss or damage, and for the purpose of this paragraph, the term "loss" means a partial loss or reduction in value as well as a complete or total loss.

Suva' liability to any person for damages arising under, out of or related in any way to this Suva Certificate Policy & Certification Practice Statement, User Agreement, the applicable contract or any related agreement, whether in contract, warranty, tort or any other legal theory, shall, subject as hereinafter set out, be limited to actual damages suffered by that person. Suva shall not be liable for indirect, consequential, incidental, special, exemplary, or punitive damages with respect to any person, even if Suva has been advised of the possibility of such damages, regardless of how such damages or liability may arise, whether in tort, negligence, equity, contract, statute, common law, or otherwise. As a condition to participation within the Suva Public Key Infrastructure (including, without limitation, the use of or reliance upon Digital Certificates), any person that participates within the Suva Public Key Infrastructure irrevocably agrees that they shall not apply for or otherwise seek either exemplary, consequential, special, incidental, or punitive damages and irrevocably confirms to Suva their acceptance of the foregoing and the fact that Suva has relied upon the foregoing as a condition and inducement to permit that person to participate within the Suva Public Key Infrastructure.

For the avoidance of doubt, Suva shall bear no liability or responsibility to any person that participates in the Suva Public Key Infrastructure unless that person is a Holder.

9.8.3 Excluded Liability

Suva shall bear absolutely no liability for any loss whatsoever involving or arising from any one (or more) of the following circumstances or causes:

- If the Digital Certificate held by the claiming party or otherwise the subject of any claim has been compromised by the unauthorized disclosure or unauthorized use of the Digital Certificate or any password or activation data used to control access thereto;
- If the Digital Certificate held by the claiming party or otherwise the subject of any claim was issued as a result of any misrepresentation, error of fact, or omission of any person, entity, or Organization;
- If the Digital Certificate held by the claiming party or otherwise the subject of any claim had expired or been revoked prior to the date of the circumstances giving rise to any claim;
- If the Digital Certificate held by the claiming party or otherwise the subject of any claim has been modified or altered in any way or been used otherwise than as permitted by the terms of this Suva Certificate Policy & Certification Practice Statement and/or the relevant User Agreement or any applicable law or regulation;
- If the Private Key associated with the Digital Certificate held by the claiming party or otherwise the subject of any claim has been compromised; or
- If the Digital Certificate held by the claiming party was issued in a manner that constituted a breach of any applicable law or regulation.
- Computer hardware or software, or mathematical algorithms, are developed that tend to make public key cryptography or asymmetric cryptosystems insecure, provided that Suva uses commercially reasonable practices to protect against breaches in security resulting from such hardware, software, or algorithms;
- Power failure, power interruption, or other disturbances to electrical power, provided Suva uses commercially reasonable methods to protect against such disturbances;
- Failure of one or more computer systems, communications infrastructure, processing, or storage media or mechanisms, or any sub components of the preceding, not under the exclusive control of Suva and/or its subcontractors or service providers; or
- One or more of the following events: a natural disaster or Act of God (including without limitation flood, earthquake, or other natural or weather related cause); a labour disturbance; war, insurrection, or overt military hostilities; adverse legislation or governmental action, prohibition, embargo, or boycott; riots or civil disturbances; fire or explosion; catastrophic epidemic; trade embargo; restriction or impediment (including, without limitation, export controls); any lack of telecommunications availability or integrity; legal compulsion including, any judgments of a court of competent jurisdiction to which Suva is, or may be, subject; and any event or occurrence or circumstance or set of circumstances that is beyond the control of Suva.

9.8.3.1 Certificate Loss Limits

Without prejudice to any other provision of this Section 9, Suva' liability for breach of its obligations pursuant to this Suva Certificate Policy & Certification Practice Statement shall, absent fraud or wilful misconduct on the part of Suva, be subject to a monetary limit determined by the type of Digital Certificate held by the claiming party and shall be limited absolutely to the monetary amounts set out below.

Loss Limits/ Reliance Limits	Maximum per Certificate
Standard Certificates	$20,000.00
Device Certificate	$20,000.00

In no event shall Suva' liability exceed the loss limits set out in the table above. The loss limits apply to the life cycle of a particular Digital Certificate to the intent that the loss limits reflect

Suva' total potential cumulative liability per Digital Certificate per year (irrespective of the number of claims per Digital Certificate). The foregoing limitation applies regardless of the number of transactions or causes of action relating to a particular Digital Certificate in any one year of that Digital Certificate's life cycle.

9.8.4 Mitigation of Suva' Liability

Suva has introduced a number of measures to reduce or limit its liabilities in the event that the safeguards in place to protect its resources fail to:

- inhibit misuse of those resources by Authorized personnel; or
- prohibit access to those resources by unauthorized individuals.

These measures include but are not limited to:

- identifying contingency events and appropriate recovery actions in a Contingency & Disaster Recovery Plan;
- performing regular system data backups;
- performing a backup of the current operating software and certain software configuration files;
- storing all backups in secure local and offsite storage;
- maintaining secure offsite storage of other material needed for disaster recovery;
- periodically testing local and offsite backups to ensure that the information is retrievable in the event of a failure;
- periodically reviewing its Contingency & Disaster Recovery Plan, including the identification, analysis, evaluation and prioritization of risks;
- periodically testing uninterrupted power supplies.

9.8.5 Claims against Suva Liability

9.8.5.1 Notification Period

Suva shall have no obligation pursuant to any claim for breach of its obligations hereunder unless the claiming party gives notice to Suva within ninety (90) days after the claiming party knew or ought reasonably to have known of a claim, and in no event more than three years after the expiration of the Digital Certificate held by the claiming party.

9.8.5.2 Mitigating Acts and Disclosure of Supporting Information

As a precondition to Suva' payment of any claim under the terms of this Suva Certificate Policy & Certification Practice Statement, a claiming party shall do and perform, or cause to be done and performed, all such further acts and things, and shall execute and deliver all such further agreements, instruments, and documents as Suva may reasonably request in order to investigate a claim of loss made by a claiming party.

9.9 Indemnities

Indemnity provisions and obligations are contained within relevant contractual documentation.

9.10 Term and Termination

9.10.1 Term

This Certificate Policy & Certification Practice Statement becomes effective upon publication in the Suva Repository. Amendments to this Certificate Policy & Certification Practice Statement become effective upon publication in the Suva Repository.

9.10.2 Termination

This Certificate Policy & Certification Practice Statement shall remain in force until it is amended or replaced by a new version.

9.10.3 Effect of Termination and Survival

The provisions of this Suva Certificate Policy & Certification Practice Statement shall survive

the termination or withdrawal of a User from the Suva Public Key Infrastructure with respect to all actions based upon the use of or reliance upon a Digital Certificate or other participation within the Suva Public Key Infrastructure. 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.

9.11 Individual Notices and Communications with Participants

Electronic mail, postal mail, fax, and web pages will all be valid means of Suva providing any of the notices required by this Suva Certificate Policy & Certification Practice Statement, unless specifically provided otherwise. Electronic mail, postal mail, and fax will all be valid means of providing any notice required pursuant to this Suva Certificate Policy & Certification Practice Statement to Suva unless specifically provided otherwise (for example in respect of revocation procedures).

9.12 Amendments

9.12.1 Procedure for Amendment

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

9.12.2 Notification Mechanism and Period

The Suva Policy Management Authority reserve the right to amend this Certificate Policy & Certification Practice Statement 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 Certificate Policy & Certification Practice Statement is at the sole discretion of the Suva Policy Management Authority.

9.12.3 Circumstances under Which Object Identifiers must be Changed

Unless the Suva Policy Management Authority determine otherwise the Object Identifier to this Certificate Policy & Certification Practice Statement shall not change.

9.13 Dispute Resolution Provisions

Any controversy or claim between two or more participants in the Suva Public Key Infrastructure (for these purposes, Suva shall be deemed a "participant" within the Suva Public Key Infrastructure) arising out of or relating to this Suva Certificate Policy & Certification Practice Statement shall be referred to an arbitration tribunal.

The participants agree that the Handelsgericht Zürich will function as arbitration tribunal.

9.14 Governing Law

The Relationships between the Participants are dealt with under the system of laws applicable under the terms of the contracts entered into. In general these can be summarised as follows;

- Dispute between Root Certification Authority and Issuing Certification Authority is dealt with under Swiss Law.
- Dispute between Issuing Certification Authority and Registration Authority is dealt with under the applicable law of the Issuing Certification Authority.
- Dispute between Issuing Certification Authority and Authorized Relying Party is dealt with under the applicable law of the Issuing Certification Authority.

9.15 Compliance with Applicable Law

This Certificate Policy & Certification Practice Statement is subject to applicable law.

9.16 Miscellaneous Provisions

Not Applicable.

9.16.1 Record Keeping

Suva shall keep records material to the issue of Digital Certificates for a minimum of 11 years.

9.16.2 Entire Agreement

Not Applicable.

9.16.3 Assignment

Not Applicable.

9.16.4 Severability

Any provision of this Suva Certificate Policy & Certification Practice Statement that is determined to be invalid or unenforceable will be ineffective to the extent of such determination without invalidating the remaining provisions of this Suva Certificate Policy & Certification Practice Statement or affecting the validity or enforceability of such remaining provisions.

9.16.5 Enforcement (Attorneys' Fees and Waiver of Rights)

The failure or delay of Suva to exercise or enforce any right, power, privilege, or remedy whatsoever, howsoever or otherwise conferred upon it by this Suva Certificate Policy & Certification Practice Statement; shall not be deemed to be a waiver of any such right or operate so as to bar the exercise or enforcement thereof at any time or times thereafter, nor shall any single or partial exercise of any such right, power, privilege or remedy preclude any other or further exercise thereof or the exercise of any other right or remedy. No waiver shall be effective unless it is in writing. No right or remedy conferred by any of the provisions of this Suva Certificate Policy & Certification Practice Statement is intended to be exclusive of any other right or remedy, except as expressly provided in this Suva Certificate Policy & Certification Practice Statement, and each and every right or remedy shall be cumulative and shall be in addition to every other right or remedy given hereunder or now or hereafter existing in law or in equity or by statute or otherwise.

9.16.6 Force Majeure

Suva 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.

9.17 Other Provisions

No Stipulation.

10 APPENDIX A

10.1 Digital Certificate Profiles and Certificate Enrollment Services

Within the Suva Public Key Infrastructure an Issuing Certification Authority can only issue Digital Certificates with approved Digital Certificate Profiles.

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 Suva liability arrangements not described in this Certificate Policy & Certification Practice Statement may be drawn up under contract for individual customers.

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

See Certificate Specification Document "Suva Corporate CA Certificate Specification".

11 APPENDIX B - Definitions and Interpretation

In this Suva Certificate Policy & Certification Practice Statement the following Key terms and Abbreviations shall have the following meaning in the operation of the Suva Public Key Infrastructure unless context otherwise requires:

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

"**Authorized Relying Party**" means an Individual or Organization that has entered into a Relying Party Agreement authorizing that person or Organization 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**" is a publicly available document that details the Suva Public Key Infrastructure and describes the practices employed in issuing Digital Certificates.

"**Certificate Holder**" means a Holder of a Digital Certificate chained to the Suva Root Certificate, including without limitation, Organizations, 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 Suva Public Key Infrastructure.

"**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 Suva Public Key Infrastructure 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 Suva 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 Certificate Policy & Certification Practice Statement .

"**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 Authorized to operate by Suva to issue Digital Certificates to Certificate Holders within the Suva Public Key Infrastructure.

"**Issuing Certification Authority Certificate**" A Digital Certificate issued by the Suva 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.

"**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.

"**Organization**" 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 Organization, or Government entity).

"**Participants**" means participants within the Suva 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) Authorized Relying Parties.

"**Policy Management Authority**" means the Suva body responsible for overseeing and approving Certificate Policy & Certification Practice Statement 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 Suva adopted or designated now or at any time hereafter by Suva for use in connection with the Suva 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.

"**Suva Issuing Certification Authority**" means Suva in its capacity as an Issuing Certification Authority.

"**Suva Public Key Infrastructure**" means the infrastructure implemented and utilized by Suva 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.

"**Suva Root Certification Authority**" means Suva in its capacity as a Root Certification Authority.

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

"**Registration Authority Certificate**" means a digital identifier issued by an Issuing Certifica-

tion Authority (including Suva in its capacity as an Issuing Certification Authority) in connection with the establishment of a Registration Authority within the Suva Public Key Infrastructure.

"**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 Organization 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 Suva Root Certification Authority.

"**Root Certification Authority**" means Suva as the source Digital Certification Authority being a self-signed Digital Certification Authority that signs Issuing Certification Authority Certificates.

"Secure Signature Creation Device" 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 "smart card"), 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 Suva Public Key Infrastructure.

"**Validation**" means an online check, by Online Certificate Status Protocol 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).