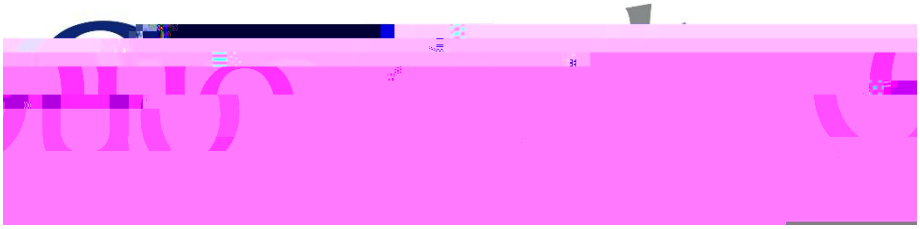

QUOVADIS ROOT CERTIFICATION AUTHORITY
CERTIFICATE POLICY/
CERTIFICATION PRACTICE STATEMENT

OIDs: 1.3.6.1.4.1.8024.0.1
1.3.6.1.4.1.8024.0.3

Effective Date: April 15, 2014

Version: 4.17

$VVHVVRU¶V 5HODWLRQVKLS 7R $VVHVVHG (QWLW\

9. OTHER BUSINESS AND LEGAL MATTERS 43

10. APPENDIX A 54

1. INTRODUCTION

1.1. Overview

¶

	5HJXODWLRQV DW 4XR9DGLV¶ GLVFUH
	5HJXODWLRQV DW 4XR9DGLV¶ GLVFUHWLRQ V

7UXVWHG &HUWLILFDWHV 3%DVHOLQH 5HTUQ

1.3.1.2 Issuing CAs and Their Obligations

1.3.3. Certificate Holders
1.3.3.1. Obligations And Responsibilities

1.4. Certificate Usage

1.4.1. Appropriate Certificate Usage

3.1.3. Pseudonymous Certificate Holders

3.1.4. Rules For Interpreting Various Name Forms

3.1.5. Uniqueness Of Names

4. CERTIFICATE LIFE-CYCLE OPERATION REQUIREMENTS

4.1. Certificate Application

4.1.1. Who Can Submit A Certificate Application

4.1.2. Enrolment Process And Responsibilities

4.3.1.1. QuoVadis Root Certification Authority

4.3.1.2. QuoVadis Issuing Certification Authority Certificates

4.3.1.3. QuoVadis Registration Authority Appointment

4.3.1.4. Registration Authority Officer's Certificate

¶

4.3.1.5. Certificate Holder Certificates
W K H $ S S O L F D Q W ¶ V

4.3.2. Notification To Applicant Certificate Holder By The Certification Authority Of Issuance Of Certificate

4.4. Certificate Acceptance

4.4.1. Notice Of Acceptance

¶ 6

x

4.10.2. Service Availability

4.10.3. Optional Features

4.11. End Of Subscription

4.12. Keyty

5.1.2. Physical Access

5.1.3. Power and Air-Conditioning

5.1.4. Water Exposures

5.1.5. Fire Prevention a

x

5.2.2. Number of Persons Required Per Task

x

5.3.3. Training Requirements

5.3.4. Retraining Frequency And Requirements

5.3.5. Job Rotation Frequency And Sequence

5.3.6. Sanctions for Unauthorised Actions

5.3.7. Independent Contractor Requirements

5.3.8. Documentation Supplied To Personnel

5.4. Audit Logging Procedures
5.4.1. Types Of Events Recorded

x

5.5.2. Retention Period For Archive

6.5. Computer Security Controls

6.5.2. Computer Security Rating

6.6. Life Cycle Technical Controls

6.6.1. System Development Controls

6.6.2. Security Management Controls

6.6.3. Life Cycle Security Controls

FIELDS	CONTENT	DEMARCATION

7.4.1. Lightweight Directory Access Protocol Version Numbers

7.4.2. Lightweight Directory Access Protocol Extensions

7.5. Digital Certificate Fields and Root CA Certificate Hashes

7.5.1. Digital Certificate Fields

7.5.2 QuoVadis Root Certificate Hashes

7.5.2.1. QuoVadis Root CA Certificate Hashes

Field	Certificate Profile

7.5.2.2. QuoVadis Root CA 1 G3 Certificate Hashes

Field	Certificate Profile

7.5.2.3. QuoVadis Root CA 3 Certificate Hashes

Field	Certificate Profile

7.5.2.4. QuoVadis Root CA 3 G3 Certificate Hashes

Field	Certificate Profile

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS
8.1. Frequency, Circumstance And Standards Of Assessment
8.1.1. QuoVadis Certification Authority

Standards / Law

8.2. Identity And Qualifications Of Assessor

8.3. Assessor's Relationship To Assessed Entity

8.5.2. Registration Authorities

RQ LV QRW WDNHQ LQ DFFRUGDQFH Z

¶VRU 5HJLVWUDWLRQ $XWKRULW\¶V

9.4.6. Disclosure Pursuant To Judicial Or Administrative Process
9.4.6.1. Release To Law Enforcement Officials

9.5.3. IETF Guidelines

9.5.4. Breach

9.6. Representations And Warranties
9.6.1. Certification Authority Representations
9.6.1.1 Root Certification Authority Representations

PDNLQJ UHDVRQDEOH HIIRUWV WR HQVXUH LW FRQGXFWV DQ HIILFLHQW D

10. APPENDIX A
10.1. Digital Certificate Profiles

¶

10.1.1. QuoVadis Certificate Class

QuoVadis Certificate Class	Description	QuoVadis Certificate Class OID	Assurance Level	Requires token?
	3 ´			

10.3. QV Advanced

$GYDQFHG 'LJLWDO &HUWLILFDWHV SURYLGH UHOLDEOH YHWWLQJ R

REGISTRATION PROCESS

,I WKH &HUWLILFDWH +ROGHU LV D SK\VLFDO SHUVRQ HYLGHQFH RI

10.4.1. ElDI-V/GeBüV Certificates

PURPOSE
REGISTRATION PROCESS

10.4.2 SuisseID Identity and Authentication Certificates

PURPOSE
REGISTRATION PROCESS
3 6 X L V V H , ' 6 S H F L I L F D W L R Q ´ G R F X P H Q W 8 Q O H V V V W D W H G R W K H U Z L \

Extensions		

10.5.5. SuisseID Qualified Certificates

PURPOSE

Extensions		
URL	http://www.quovadisglobal.com/repository	

10.6.1.1. Grid End User Certificate

PURPOSE
REGISTRATION PROCESS
DIGITAL CERTIFICATE DELIVERY

10.6.1.2. Grid Server Certificate

PURPOSE		
REGISTRATION PROCESS		
DIGITAL CERTIFICATE DELIVERY		
FIELDS	**CONTENT**	**DEMARCATION**

11. APPENDIX B
11.1. Definitions and Acronyms

"Certificate Revocation List" PHDQV D OLVW RI GLJLWDOO\ VLJQHG FHUWLILFDWHV WKDW LGHQWLILHV FHUWLILFDWHV WKDW KDYH EHHQ UHYRNHG

"Counterparty" PHDQV D SHUVRQ WKDW LV QRW D 1RPLQDWLQJ 5HJLVWUDWLRQ

"Cryptographic Module" PHDQV VHFXUH VRIWZDUH GHYLFH RU XWLOLW\ WKDW L

"Digital Certificate" PHDQV D GLJLWDO LGHQWLILHU ZLWKLQ WKH 4XR9DGLV

"Digital Signature" PHDQV GDWD DSSHQGHG WR RU D FU\SWRJUDSKLF WUDQVPLVVLR

"Digital Transmission" PHDQV WKH WUDQVPLVVLRQ RI LQIRUPDWLRQ LQ DQ HOHFWURQ

"Device" PHDQV VRIWZDUH KDUGZDUH RU RWKHU HOHFWURQLF RU DXWRPDWHG

"Device Certificate" PHDQV D 'LJLWDO &HUWLILFDWH LVVXHG WR LGHQWLI\ D 'HYLFH

"Distinguished Name" PHDQV WKH XQLTXH LGHQWLILHU IRU WKH +ROGHU RI D 'LJLWDO

"Federal Information Processing Standards"

- Operational Term´ PHDQV WKH WHUP RI YDOLGLW\ RI D 'LJLWDO &HUWLILFDWH FRP
¶V
- Organisation´ PHDQV DQ HQWLW\ WKDW LV OHJDOO\ UHFRJQLVHG LQ LWV MXULVG
- Participants´ PHDQV SDUWLFLSDQWV ZLWKLQ WKH 4XR9D
- PKCS´ PHDQV 3XEOLF
- Policy Management Authority´ PHDQV WKH 4XR9DGLV ERG\ UHVSRQVLEOH IRU RYHUVH
- Proprietary Marks´ PHDQV DQ\ SDWHQWV SHQGLQJ RU RWKHUZLVH WUDGH PDUN

3Repository´ PHDQV RQH RU PRUH GDWDEDVHV RI 'LJLWDO &HUWLILFDWHV DQG R

3Reserved IP Address´ PHDQV D

3Root Certification Authority Certificate´

3Root Certification Authority´ PHDQV 4XR9DGL

"Secure Signature Creation Device" (SSCD)

1. Secure signature-creation devices must, by appropriate technical and procedural means, ensure at the least that:
   (a) the signature-creation-data used for signature generation can practically occur only once, and that their secrecy is reasonably assured;
   (b) the signature-creation-data used for signature generation cannot, with reasonable assurance, be derived and the signature is protected against forgery using currently available technology;
   (c) the signature-creation-data used for signature generation can be reliably protected by the legitimate signatory
   against the use of others.
2. Secure signature-creation devices must not alter the data to be signed or prevent such data from being presented to the signatory prior to the signature process.

3Subscriber