



KIBS Certification Practice Statement For Qualified Certificates

Version 1.0

Effective Date: February, 2010

KIBS AD Skopje
Kuzman Josifovski Pitu 1
1000, Skopje,
Republic of Macedonia
Phone number: +389 2 3297401
<http://ca.kibs.com.mk>

KIBS Certification Practices Statement for Qualified Certificates

Published date: February, 2010

Trademark Notices

KIBS is the registered mark of KIBS AD Skopje. ADACOM is the registered mark of ADACOM SA. VeriSign is the registered trademarks of VeriSign, Inc. The VeriSign logo, VeriSign Trust Network and NetSure are trademarks and service marks of VeriSign, Inc. Other trademarks and service marks in this document are the property of their respective owners.

Without limiting the rights reserved above, and except as licensed below, no part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), without prior written permission of KIBS AD Skopje.

Requests for any other permission to reproduce this KIBS Certification Practices Statement (as well as requests for copies from KIBS.) must be addressed to KIBS AD, Kuzman Josifovski Pitu 1, 1000, Skopje, Republic of Macedonia, phone: ++38923297401, fax: +389 23297497, e-mail: ca-info@kibs.com.mk.

Table of Contents

1.	INTRODUCTION.....	9
1.1	Overview	10
1.2	Document name and Identification	11
1.3	PKI Participants	11
1.3.1	Certification Authorities	11
1.3.2	Registration Authorities	11
1.3.3	Subscribers	11
1.3.4	Relying Parties	12
1.3.5	Other Participants	12
1.4	Certificate Usage	12
1.4.1	Appropriate Certificate Usages	12
1.4.2	Prohibited Certificate Uses.....	13
1.5	Policy Administration	13
1.5.1	Organization Administering the Document	13
1.5.2	Contact Person	13
1.5.3	Person Determining CP Suitability for the Policy	14
1.5.4	CPS Approval Procedure.....	14
1.6	Definitions and Acronyms	14
2.	PUBLICATION AND REPOSITORY RESPONSIBILITIES	15
2.1	Repositories	15
2.2	Publication of Certificate Information	15
2.3	Time or Frequency of Publication	15
2.4	Access Controls on Repositories	16
3.	IDENTIFICATION AND AUTHENTICATION	17
3.1	Naming.....	17
3.1.1	Type of Names.....	17
3.1.2	Need for Names to be Meaningful.....	18
3.1.3	Anonymity or pseudonymity of Subscribers	18
3.1.4	Rules for Interpreting Various Name Forms.....	18
3.1.5	Uniqueness of Names	18
3.1.6	Recognition, Authentication, and Role of Trademarks	18
3.2	Initial Identity Validation.....	18
3.2.1	Method to Prove Possession of Private Key.....	18
3.2.2	Authentication of Individual Identity	19
3.2.3	Non-Verified Subscriber information	19
3.2.4	Validation of Authority.....	19
3.3	Identification and Authentication for Re-key Requests.....	19
3.3.1	Identification and Authentication for Routine Re-key	20
3.3.2	Identification and Authentication for Re-key After Revocation.....	20
3.4	Identification and Authentication for Revocation Request	20
4.	CERTIFICATE LIFE-CYCLE OPERATIONAL	21
4.1	Certificate Application	21
4.1.1	Who Can Submit a Certificate Application?	21
4.1.2	Enrollment Process and Responsibilities.....	21
4.2	Certificate Application Processing	22
4.2.1	Performing Identification and Authentication Functions.....	22
4.2.2	Approval or Rejection of Certificate Applications	22
4.2.3	Time to Process Certificate Applications.....	22
4.3	Certificate Issuance.....	22
4.3.1	CA Actions during Certificate Issuance.....	22

4.3.2	Notifications to Subscriber by the CA of Issuance of Certificate.....	22
4.4	Certificate Acceptance	23
4.4.1	Conduct Constituting Certificate Acceptance	23
4.4.2	Publication of the Certificate by the CA	23
4.4.3	Notification of Certificate Issuance by the CA to Other Entities	23
4.5	Key Pair and Certificate Usage	23
4.5.1	Subscriber Private Key and Certificate Usage	23
4.5.2	Relying Party Public Key and Certificate Usage	23
4.6	Certificate Renewal.....	24
4.6.1	Circumstances for Certificate Renewal	24
4.6.2	Who May Request Renewal	24
4.6.3	Processing Certificate Renewal Requests.....	24
4.6.4	Notification of New Certificate Issuance to Subscriber.....	24
4.6.5	Conduct Constituting Acceptance of a Renewal Certificate.....	24
4.6.6	Publication of the Renewal Certificate by the CA	24
4.6.7	Notification of Certificate Issuance by the CA to Other Entities	24
4.7	Certificate Re-Key.....	24
4.7.1	Circumstances for Certificate Re-Key	24
4.7.2	Who May Request Certification of a New Public Key.....	25
4.7.3	Processing Certificate Re-Keying Requests	25
4.7.4	Notification of New Certificate Issuance to Subscriber.....	25
4.7.5	Conduct Constituting Acceptance of a Re-Keyed Certificate	25
4.7.6	Publication of the Re-Keyed Certificate by the CA.....	25
4.7.7	Notification of Certificate Issuance by the CA to Other Entities	25
4.8	Certificate Modification	25
4.8.1	Circumstances for Certificate Modification.....	25
4.8.2	Who May Request Certificate Modification.....	25
4.8.3	Processing Certificate Modification Requests.....	25
4.8.4	Notification of New Certificate Issuance to Subscriber.....	25
4.8.5	Conduct Constituting Acceptance of Modified Certificate.....	26
4.8.6	Publication of the Modified Certificate by the CA.....	26
4.8.7	Notification of Certificate Issuance by the CA to Other Entities	26
4.9	Certificate Revocation and Suspension.....	26
4.9.1	Circumstances for Revocation.....	26
4.9.2	Who Can Request Revocation	27
4.9.3	Procedure for Revocation Request	27
4.9.4	Revocation Request Grace Period.....	27
4.9.5	Time within which CA must process the Revocation Request	27
4.9.6	Revocation Checking Requirements for Relying Parties	27
4.9.7	CRL Issuance Frequency	28
4.9.8	Maximum Latency for CRLs.....	28
4.9.9	On-Line Revocation/Status Checking Availability.....	28
4.9.10	On-Line Revocation Checking Requirements	28
4.9.11	Other Forms of Revocation Advertisements Available	28
4.9.12	Special Requirements regarding Key Compromise	28
4.9.13	Circumstances for Suspension	28
4.9.14	Who Can Request Suspension.....	28
4.9.15	Procedure for Suspension Request	28
4.9.16	Limits on Suspension Period	29
4.10	Certificate Status Services.....	29
4.10.1	Operational Characteristics.....	29
4.10.2	Service Availability.....	29
4.10.3	Optional Features.....	29

4.11	End of Subscription	29
4.12	Key Escrow and Recovery	29
4.12.1	Key Escrow and Recovery Policy and Practices	29
4.12.2	Session Key Encapsulation and Recovery Policy and Practices	29
5.	FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS.....	30
5.1	Physical Controls.....	30
5.1.1	Site Location and Construction	30
5.1.2	Physical Access	30
5.1.3	Power and Air Conditioning	30
5.1.4	Water Exposures	30
5.1.5	Fire Prevention and Protection	31
5.1.6	Media Storage	31
5.1.7	Waste Disposal	31
5.1.8	Off-Site Backup.....	31
5.2	Procedural Controls	31
5.2.1	Trusted Roles.....	31
5.2.2	Number of Persons Required per Task.....	32
5.2.3	Identification and Authentication for Each Role	32
5.2.4	Roles Requiring Separation of Duties.....	32
5.3	Personnel Controls.....	32
5.3.1	Qualifications, Experience.....	33
5.3.2	Background Check Procedures.....	33
5.3.3	Training Requirements.....	33
5.3.4	Retraining Frequency and Requirements.....	34
5.3.5	Job Rotation Frequency and Sequence	34
5.3.6	Sanctions for Unauthorized Actions.....	34
5.3.7	Independent Contractor Requirements.....	34
5.3.8	Documentation Supplied to Personnel	34
5.4	Audit Logging Procedures	34
5.4.1	Types of Events Recorded	34
5.4.2	Frequency of Processing Log	35
5.4.3	Retention Period for Audit Log.....	35
5.4.4	Protection of Audit Log	35
5.4.5	Audit Log Backup Procedures.....	36
5.4.6	Audit Collection System (Internal vs. External)	36
5.4.7	Notification to Event-Causing Subject.....	36
5.4.8	Vulnerability Assessments.....	36
5.5	Records Archival.....	36
5.5.1	Types of Records Archived	36
5.5.2	Retention Period for Archive.....	36
5.5.3	Protection of Archive	37
5.5.4	Archive Backup Procedures.....	37
5.5.5	Requirements for Time-Stamping of Records	37
5.5.6	Archive Collection System	37
5.5.7	Procedures to Obtain and Verify Archive Information.....	37
5.6	Key Changeover	37
5.7	Compromise and Disaster Recovery	38
5.7.1	Incident and Compromise Handling Procedures.....	38
5.7.2	Computing Resources, Software, and/or Data Are Corrupted.....	38
5.7.3	Entity Private Key Compromise Procedures.....	38
5.7.4	Business Continuity Capabilities after a Disaster	38
5.8	CA or RA Termination.....	39

6.	TECHNICAL SECURITY CONTROLS	41
6.1	Key Pair Generation and Installation	41
6.1.1	Key Pair Generation.....	41
6.1.2	Private Key Delivery to Subscriber	41
6.1.3	Public Key Delivery to Certificate Issuer.....	41
6.1.4	CA Public Key Delivery to Relying Parties	41
6.1.5	Key Sizes	41
6.1.6	Public Key Parameters Generation and Quality Checking.....	42
6.2	Private Key Protection and Cryptographic Module Engineering Controls	42
6.2.1	Cryptographic Module Standards and Controls	42
6.2.2	Private Key (m out of n) Multi-Person Control.....	42
6.2.3	Private Key Escrow	42
6.2.4	Private Key Backup	43
6.2.5	Private Key Archival.....	43
6.2.6	Private Key Transfer Into or From a Cryptographic Module	43
6.2.7	Private Key Storage on Cryptographic Module	43
6.2.8	Method of Activating Private Key	43
6.2.9	Method of Deactivating Private Key	44
6.2.10	Method of Destroying Private Key	44
6.2.11	Cryptographic Module Rating	45
6.3	Other Aspects of Key Pair Management.....	45
6.3.1	Public Key Archival	45
6.3.2	Certificate Operational Periods and Key Pair Usage Periods	45
6.4	Activation Data.....	46
6.4.1	Activation Data Generation and Installation	46
6.4.2	Activation Data Protection	46
6.4.3	Other Aspects of Activation Data	46
6.5	Computer Security Controls.....	47
6.5.1	Specific Computer Security Technical Requirements.....	47
6.5.2	Computer Security Rating	47
6.6	Life Cycle Technical Controls.....	47
6.6.1	System Development Controls.....	47
6.6.2	Security Management Controls.....	47
6.6.3	Life Cycle Security Controls	48
6.7	Network Security Controls	48
6.8	Time-Stamping	48
7.	CERTIFICATE, CRL, AND OCSP PROFILES	49
7.1	Certificate Profile	49
7.1.1	Version Number(s)	49
7.1.2	Certificate Extensions.....	49
7.1.3	Algorithm Object Identifiers.....	52
7.1.4	Name Forms	52
7.1.5	Name Constraints.....	52
7.1.6	Certificate Policy Object Identifier	52
7.1.7	Usage of Policy Constraints Extension	52
7.1.8	Policy Qualifiers Syntax and Semantics.....	52
7.1.9	Processing Semantics for the Critical Certificate Policies Extension	52
7.2	CRL Profile	53
7.2.1	Version Number(s)	53
7.2.2	CRL and CRL Entry Extensions	53
7.3	OCSP Profile	53
7.3.1	Version Number(s)	53

8.	COMPLIANCE AUDIT AND OTHER ASSESSMENTS.....	54
8.1	Frequency and Circumstances of Assessment	54
8.2	Identity/Qualifications of Assessor	54
8.3	Topics Covered by Assessment	54
8.4	Actions Taken as a Result of Deficiency.....	54
8.5	Communications of Results.....	55
9.	OTHER BUSINESS AND LEGAL MATTERS.....	56
9.1	Fees.....	56
9.1.1	Certificate Issuance or Renewal Fees.....	56
9.1.2	Certificate Access Fees.....	56
9.1.3	Revocation or Status Information Access Fees	56
9.1.4	Fees for Other Services	56
9.1.5	Refund Policy.....	56
9.2	Financial Responsibility.....	56
9.2.1	Insurance Coverage.....	56
9.2.2	Other Assets	56
9.3	Confidentiality of Business Information.....	56
9.3.1	Scope of Confidential Information	56
9.3.2	Information Not Within the Scope of Confidential Information	57
9.3.3	Responsibility to Protect Confidential Information.....	57
9.4	Privacy of Personal Information.....	57
9.4.1	Privacy Plan	57
9.4.2	Information Treated as Private	57
9.4.3	Information Not Deemed Private.....	57
9.4.4	Responsibility to Protect Private Information.....	57
9.4.5	Notice and Consent to Use Private Information	57
9.4.6	Disclosure Pursuant to Judicial or Administrative Process.....	57
9.4.7	Disclosure upon Owner’s Request	58
9.4.8	Other Information Disclosure Circumstances	58
9.5	Intellectual Property rights	58
9.5.1	Property Rights in Certificates and Revocation Information.....	58
9.5.2	Property Rights in the CPS.....	58
9.5.3	Property Rights in Names.....	58
9.5.4	Property Rights in Keys and Key Material	58
9.6	Representations and Warranties	59
9.6.1	CA Representations and Warranties	59
9.6.2	RA Representations and Warranties	59
9.6.3	Subscriber Representations and Warranties.....	59
9.6.4	Relying Party Representations and Warranties	60
9.6.5	Representations and Warranties of Other Participants.....	60
9.7	Disclaimers of Warranties.....	60
9.8	Obligations for CAs issuing Qualified Certificates	60
9.9	Limitations of Liability	61
9.10	Indemnities	62
9.10.1	Indemnification by Subscribers	62
9.10.2	Indemnification by Relying Parties.....	62
9.11	Term and Termination	62
9.11.1	Term	62
9.11.2	Termination.....	62
9.11.3	Effect of Termination and Survival.....	63
9.12	Individual Notices and Communications with Participants	63
9.13	Amendments.....	63

9.13.1	Procedure for Amendment	63
9.13.2	Notification Mechanism and Period.....	63
9.13.3	Circumstances under Which OID Must be Changed	63
9.14	Dispute Resolution Provisions.....	63
9.14.1	Disputes among VeriSign, Affiliates, and Customers	63
9.14.2	Disputes with End-User Subscribers or Relying Parties.....	63
9.15	Governing Law	64
9.16	Compliance with Applicable Law	64
9.17	Miscellaneous Provisions	64
9.17.1	Entire Agreement	64
9.17.2	Assignment.....	64
9.17.3	Severability.....	64
9.17.4	Enforcement (Attorney's Fees and Waiver of Rights)	64
9.17.5	Force Majeure	64
9.18	Other Provisions.....	64
Appendix A. Table of Acronyms and definitions		65
Table of Acronyms		65
Definitions.....		65

1. INTRODUCTION

This document is the KIBS Certification Practice Statement for Qualified Certificates (hereinafter: CPS). It states the practices that KIBS Certification Authority (hereinafter: CA) employ in providing certification services for Qualified Certificates in accordance with the European and Macedonian law, that include, but are not limited to, issuing, managing, revoking, and renewing Qualified Certificates in accordance with the specific requirements of the VeriSign Trust Network Certificate Policies (hereinafter: CP) and the VeriSign Trust Network European Directive Policies (hereinafter: EDP) that supplements the CP.

The CP is the principal statement of policy governing the VeriSign Trust Network (hereinafter: VTN). It establishes the business, legal, and technical requirements for approving, issuing, managing, using, revoking, and renewing, digital certificates within the VTN and providing associated trust services. These requirements, called the “VTN Standards”, protect the security and integrity of the VTN, apply to all VTN Participants, and thereby provide assurances of uniform trust throughout the VTN. More information concerning the VTN and VTN Standards is available in the CP.¹

In addition the EDP supplements the CP with additional information as to how the VTN meets specific policy requirements set forth by the European Telecommunications Standards Institute (hereinafter: ETSI). The purpose of the EDP is to facilitate compliance with the Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for Electronic Signatures (hereinafter: Directive).

1. The Directive is intended to facilitate the use of Electronic Signatures and establishes requirements for “Qualified Certificates” that support certain types of Electronic Signatures. The EDP also describes the two certificate policies set forth in the ETSI Technical Specification 101 456 (the “ETSI Policy Document”).
2. The EDP defines two policies that supplement the CP referring to Qualified Certificates, referred to here as “Directive Level 1” (hereinafter: DL1) and “Directive Level 2” (hereinafter: DL2). DL1 and DL2 correspond, respectively, to the “QCP public” certificate policy and “QCP public + SSCD” certificate policy defined in the ETSI Policy Document.
3. Finally, the EDP supplements the certificate profile developed by ETSI (the “Qualified Certificate Profile”), which defines a technical format for Certificates that meet the requirements of the directive (“Qualified Certificates”). Certification Authorities issuing Qualified Certificates can use the Qualified Certificate Profile to assist them in issuing certificates that comply with annex I and II of the Directive. A copy of the EDP can be found at <https://www.adacom.com/repository/edp>.

KIBS has authority over a portion of the VTN called its “Subdomain” of the VTN. KIBS’s Subdomain includes entities subordinate to it such as its Customers, Subscribers, and Relying Parties.

While the CP and EDP set forth requirements that VTN Participants must meet, this CPS describes how KIBS meets these requirements within KIBS’s Subdomain of the VTN. More specifically, this CPS describes the practices that KIBS employs for:

- securely managing the core infrastructure that supports the VTN, and
- issuing, managing, revoking, and renewing VTN Qualified Certificates

¹ The current version of VTN CP, can be found at <https://ca.kibs.com.mk/repository/cps>

This CPS conforms to the Internet Engineering Task Force (IETF) RFC 3647 for Certificate Policy and Certification Practice Statement construction.

1.1 Overview

KIBS acts as a CA in the VTN and performs all Certificate lifecycle services of issuing, managing, revoking, and renewing Certificates. KIBS also offers

Web Site certificates (Secure Server IDs and Global Server IDs)

Web Site Certificates (Secure Server Ids and Global Server Ids) are offered by KIBS in a special cooperation with VeriSign and not under KIBS CA. For this line of business shall apply the VeriSign CPS, as published on <http://www.verisign.com/repository/cps/>.

This CPS is specifically applicable to:

- VeriSign's Public Primary Certification Authority (PCA), being the Root Certification Authority for KIBS Qualified Certificates,
- KIBS's Public CAs, consist the certificate chain for KIBS Qualified Certificates.

More generally, the CPS also governs the use of VTN services regarding Qualified Certificates within KIBS's Subdomain of the VTN by all individuals and entities within KIBS's Subdomain (collectively, KIBS Subdomain Participants).

KIBS offers Qualified Certificates (DL1 and DL2) within its Subdomain of the VTN. This CPS describes how KIBS meets the CP and EDP requirements for the Qualified Certificates it issues within its Subdomain. Thus, the CPS, as a single document, covers practices and procedures concerning the issuance and management of the Qualified Certificate provided by KIBS.

KIBS may publish Certificate Practices Statements that are supplemental to this CPS in order to comply with the specific policy requirements of the legislation, or other industry standards and requirements. These supplemental certificate practices shall be made available to subscribers for the certificates issued under the supplemental policies and their relying parties.

The CPS is only one of a set of documents relevant to KIBS's Subdomain of the VTN. These other documents include:

- Ancillary confidential security and operational documents² that supplement the CP and CPS by providing more detailed requirements, such as:
 - The VeriSign Physical Security Policy, which sets forth security principles governing the VTN infrastructure,
 - The VeriSign Security and Audit Requirements Guide, which describes detailed requirements for VeriSign and Affiliates concerning personnel, physical, telecommunications, logical, and cryptographic key management security, and
 - Key Ceremony Reference Guide, which presents detailed key management operational requirements.
 - The KIBS Physical Security Policy which sets forth security principles governing KIBS Subdomain,
- Ancillary agreements imposed by KIBS. These agreements bind Customers, Subscribers, and Relying Parties of KIBS. Among other things, the agreements flow down VTN Standards to these VTN Participants and, in some cases, state specific practices for how they must meet VTN Standards.

In many instances, the CPS refers to these ancillary documents for specific, detailed practices implementing VTN Standards.

² Although these documents are not publicly available their specifications are included in VeriSign's Annual WebTrust for Certification authorities audit and may be made available to customer under special Agreement

1.2 Document name and Identification

This document is the KIBS Certification Practice Statement for Qualified Certificates. VTN Certificates contain object identifier values corresponding to the applicable VTN Class of Certificate. Therefore, KIBS has not assigned this CPS an object identifier value.

Certificate Policy Object Identifiers are used in accordance with Section 7.1.6.

1.3 PKI Participants

1.3.1 Certification Authorities

The term Certification Authority (hereinafter: CA) is an umbrella term that refers to all entities authorized to issue public key certificates within the VTN. The CA term encompasses a subcategory of issuers called Primary Certification Authorities (hereinafter: PCA). PCAs act as roots of domains. Each PCA is a VeriSign entity. Subordinate to the PCAs are Certification Authorities that issue Certificates to end-user Subscribers or other CAs. KIBS is an issuing CA managing Qualified Certificates.

KIBS implements this CPS based on its internal requirements, which also complies with all the requirements of the VTN CP, and the ADACOM CPS.

One VTN CA technically outside the three hierarchies under each of the PCAs is the Secure Server Certification Authority. This CA does not have a superior CA, such as a root or a PCA. Rather, the Secure Server CA acts as its own root and has issued itself a self-signed root Certificate. It also issues Certificates to end-user Subscribers. Thus, the Secure Server Hierarchy consists only of the Secure Server CA.

In this CPS, references to CAs refer to CAs that comprises the certificate chain of KIBS Qualified Certificates. More specifically these CAs are:

- (VeriSign) Class 2 Public Primary Certification Authority – G3, as Root CA,
- KIBS Verba CA as Intermediate CA, and
- KIBS Qualified Certificate Services CA, as Issuing CA.

1.3.2 Registration Authorities

A Registration Authority (hereinafter: RA) is an entity that performs identification and authentication of certificate applicants for end-user certificates, initiates or passes along revocation requests for certificates for end-user certificates, and approves applications for renewal or re-keying certificates on behalf of a VTN CA. KIBS act as an RA for the Qualified Certificates it issues.

KIBS may enter into a contractual relationship with one or more third parties, especially regarding the validation of the Subscriber. In this case, the third party constitutes a Local Registration Authority (hereinafter: LRA). LRA performs its responsibilities in accordance with and is bound by the contractual terms and this CPS, as well.

1.3.3 Subscribers

A subscriber is the entity named as the end-user Subscriber of a certificate. End-user Subscribers may be individuals or organizations. For Qualified Certificates, end-user Subscribers may be only legally eligible individuals, in accordance with the Macedonian law.

In some cases certificates are issued directly to individuals or entities for their own use. However, there commonly exist other situations where the party requiring a certificate is different from the subject to whom the credential applies. For example, an organization may require certificates for

its employees to allow them to represent the organization in electronic transactions/business. In such situations the entity subscribing for the issuance of certificates (i.e. paying for them, either through subscription to a specific service, or as the issuer itself) is different from the entity which is the subject of the certificate (generally, the holder of the credential). Two different terms are used in this CPS to distinguish between these two roles: "Subscriber", is the entity which contracts with KIBS for the issuance of credentials and; "Subject", is the person to whom the credential is bound. The Subscriber bears ultimate responsibility for the use of the credential but the Subject is the individual that is authenticated when the credential is presented.

When 'Subject' is used, it is to indicate a distinction from the Subscriber. When "Subscriber" is used it may mean just the Subscriber as a distinct entity but may also use the term to embrace the two. The context of its use in this CPS will invoke the correct understanding.

CAs are technically also subscribers of certificates within the VTN, either as a PCA issuing a self signed Certificate to itself, or as a CA issued a Certificate by a superior CA. References to "end entities" and "subscribers" in this CPS, however, apply only to end-user Subscribers of Qualified Certificates .

1.3.4 Relying Parties

A Relying Party is an individual or entity that acts in reliance of a certificate and/or a digital signature issued under the VTN. A Relying party may, or may not also be a Subscriber within the VTN.

1.3.5 Other Participants

Not applicable.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Usages

Individual Certificates are normally used by individuals to sign and encrypt e-mail and to authenticate to applications (client authentication). While the most common usages for KIBS Qualified individual certificates are included in Table 1 below, a DL1 or DL2 certificate may be used for other purposes, provided that a Relying Party is able to reasonably rely on that certificate and the usage is not otherwise prohibited by law, the VTN CP, the VTN EDP, this CPS and the Subscriber Agreement. DL1 Certificates may be used to support digital signatures, where the applications making use of the digital signatures require Electronic Signatures that "are not [to be] denied legal effectiveness and admissibility as evidence in legal proceedings" in accordance with article 5(2) of the Directive. The uses for DL1 Certificates correspond to the uses for certificates identified in the QCP public Certificate policy in the ETSI Policy Document.

DL2 Certificates may be used to support digital signatures where the applications making use of the digital signatures require Advanced Electronic Signatures that "satisfy the requirements of a signature in relation to data in electronic form in the same manner as a hand-written signature satisfies those requirements in relation to paper based data" in accordance with article 5(1) of the Directive. The uses for DL2 Certificates correspond to the uses for Certificates identified in the QCP public+ SSCD Certificate policy in the ETSI Policy Document.

DL1 and DL2 Certificates are **High assurance Certificates** that provide a high level of assurance of the identity of the Subscriber.

Certificate Class	Assurance Level		Usage		
	Low assurance level	High assurance Level	Signing	Encryption	Client Authentication
DL1 Certificates		✓	✓	✓	✓
DL2 Certificates		✓	✓	✓	✓

Table 1. Individual Certificate Usage

1.4.2 Prohibited Certificate Uses

KIBS Certificates are not designed, intended, or authorized for use or resale as control equipment in hazardous circumstances or for uses requiring fail-safe performance such as the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control systems, or weapons control systems, where failure could lead directly to death, personal injury, or severe environmental damage.

DL1 and DL2 Certificates are intended for client applications and shall not be used as server or organizational Certificates or as CA Certificates.

CA Certificates may not be used for any functions except CA functions.

1.5 Policy Administration

1.5.1 Organization Administering the Document

KIBS AD Skopje
 Kuzman Josifovski Pitu 1,
 1000, Skopje
 Republic of Macedonia
 tel. ++389 2 3297401
 fax: +389 2 3297497
 E-mail: ca-info@kibs.com.mk

1.5.2 Contact Person

The Certificate Policy Manager

KIBS AD Skopje
 Kuzman Josifovski Pitu 1,
 1000, Skopje
 Republic of Macedonia
 tel. ++389 2 3297401
 fax: +389 2 3297497
 E-mail: ca-info@kibs.com.mk

1.5.3 Person Determining CP Suitability for the Policy

The organization identified in Section 1.5.1 and ADACOM is responsible for determining whether this CPS and other documents in the nature of certification practice statements that supplement or are subordinate to this CPS are suitable under the VTN CP, the ADACOM CPS and this CPS.

1.5.4 CPS Approval Procedure

Approval of this CPS and subsequent amendments are made by the KIBS Practices Development Group and the VeriSign Policy Management Authority (hereinafter: PMA). Amendments are either in the form of a document containing an amended form of the CPS or an update notice. Amended versions or updates are linked to the Practices Updates and Notices section of the KIBS Repository located at: <https://ca.kibs.com.mk/repository/cps>. Updates supersede any designated or conflicting provisions of the referenced version of the CPS.

1.6 Definitions and Acronyms

See Appendix A for a table of acronyms and definitions.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

KIBS is responsible for the repository functions for its own CAs. KIBS publishes the issued DL1 or DL2 Certificates in the repository in accordance with CPS § 2.2.

Upon revocation of an end-user Subscriber's Certificate, KIBS publishes notice of such revocation in the repository and issues Certificate Revocation List (hereinafter: CRL) pursuant to the provisions of the CPS.

2.2 Publication of Certificate Information

KIBS maintains a web-based repository that permits Relying Parties to make online inquiries regarding revocation and other Certificate status information. KIBS provides Relying Parties with information on how to find the appropriate repository to check Certificate status.

KIBS will at all times publish in the repository section of its web site, a current version of:

- The VTN CP
- The VTN EDP,
- This CPS,
- Subscriber Agreements,
- Relying Party Agreements,
- It's Privacy Policy.

KIBS publishes certain CA information in the repository section of KIBS's web site at <https://ca.kibs.com.mk/repository/rpa> as described below.

KIBS publishes Certificates in accordance with Table 2 below.

Certificate Type	Publication Requirements
VeriSign PCA	Available to Relying Parties through inclusion in current browser software.
KIBS Intermediate and Issuing CA Certificates	Available to Relying Parties as part of a Certificate Chain that can be obtained with the end-user Subscriber Certificate through the query functions described below.
End-User Subscriber Certificates	Available to relying parties through query functions in the KIBS repository at: https://ca.kibs.com.mk/repository/rpa . Also available through query of the KIBS LDAP directory server at ldap://ldap-ca.kibs.com.mk

Table 2 – Certificate Publication Requirements

2.3 Time or Frequency of Publication

Updates to this CPS are published in accordance Section 9.13. Updates to Subscriber Agreements and Relying Party Agreements are published as necessary. Certificates are published upon issuance. Certificate status information is published in accordance with the provisions of this CPS.

2.4 Access Controls on Repositories

Information published in the repository portion of the KIBS web site is publicly-accessible information. Read only access to such information is unrestricted. KIBS requires persons to agree to a Relying Party Agreement as a condition to accessing Certificates, Certificate status information, or CRLs. KIBS has implemented logical and physical security measures to prevent unauthorized persons from adding, deleting, or modifying repository entries according to the applicable KIBS security policies.

3. IDENTIFICATION AND AUTHENTICATION

3.1 Naming

Unless where indicated otherwise in the VTN CP, the VTN EDP, this CPS or the content of the digital certificate, names appearing in Certificates issued under VTN are authenticated.

3.1.1 Type of Names

KIBS CA Certificates contain X.501 Distinguished Names in the Issuer and Subject fields. KIBS CA Distinguished Names consist of the components specified in Table 3 below.

Attribute	Value					
	Issuer Field			Subject Field		
	Root CA	Intermediate CA	Issuing CA	Root CA	Intermediate CA	Issuing CA
Country (C) =	US	US	MK	US	MK	MK
Organization (O) =	VeriSign, Inc.	VeriSign, Inc.	Clearing House KIBS AD Skopje	VeriSign, Inc.	Clearing House KIBS AD Skopje	Clearing House KIBS AD Skopje
Organizational Unit (OU) =	<ul style="list-style-type: none"> VeriSign Trust Network © 1999 VeriSign, Inc. – For authorized use only 	<ul style="list-style-type: none"> VeriSign Trust Network © 1999 VeriSign, Inc. – For authorized use only 	VeriSign Trust Network	<ul style="list-style-type: none"> VeriSign Trust Network © 1999 VeriSign, Inc. – For authorized use only 	VeriSign Trust Network	<ul style="list-style-type: none"> VeriSign Trust Network Terms of use at https://ca.kibs.com.mk/repository/rpa (c)09 Class 2 Managed PKI Individual Subscriber CA
Common Name (CN) =	VeriSign Class 2 Public Primary Certification Authority – G3	<ul style="list-style-type: none"> VeriSign Class 2 Public Primary Certification Authority – G3 	KIBS Verba CA	VeriSign Class 2 Public Primary Certification Authority – G3	KIBS Verba CA	KIBS Qualified Certificate Services CA

Table 3 – Distinguished Name Attributes in CA Certificates

End-user Subscriber Certificates contain an X.501 distinguished name in the Subject name field and consist of the components specified in Table 4 below.

Attribute	Value
Country (C) =	2 letter ISO country code of the end-user
Organization (O) =	Name of the end-user Organization
Organizational Unit (OU) =	This is optional parameter, it can contain Organization Unit name , etc.

Attribute	Value
Common Name (CN) =	This attribute includes the Full Name of the end-user
E-Mail Address (E) =	E-mail address of the end-user

Table 4 – Distinguished Name Attributes in End User Subscriber Certificates

The Common Name (CN=) component of the Subject distinguished name of end-user Subscriber Certificates is authenticated. The common name value included in the Subject distinguished name of individual Certificates represents the individual's real personal name.

3.1.2 Need for Names to be Meaningful

DL1 and DL2 Certificates contain names with commonly understood semantics permitting the determination of the identity of the individual that is the Subject of the Certificate.

KIBS CA certificates contain names with commonly understood semantics permitting the determination of the identity of the CA that is the Subject of the Certificate.

3.1.3 Anonymity or pseudonymity of Subscribers

For KIBS Qualified Certificates (DL1 or DL2), the use of pseudonyms is not permitted.

3.1.4 Rules for Interpreting Various Name Forms

No stipulation.

3.1.5 Uniqueness of Names

KIBS ensures that Subject Distinguished Names of Subscriber are unique within the domain of a specific CA through automated components of the Subscriber enrollment process. It is possible for a Subscriber to have two or more certificates with the similar Subject Distinguished Name.

3.1.6 Recognition, Authentication, and Role of Trademarks

Certificate Applicants are prohibited from using names in their Certificate Applications that infringe upon the Intellectual Property Rights of others. KIBS, however, does not verify whether a Certificate Applicant has Intellectual Property Rights in the name appearing in a Certificate Application or arbitrates, mediates, or otherwise resolves any dispute concerning the ownership of any domain name, trade name, trademark, or service mark. KIBS is entitled, without liability to any Certificate Applicant, to reject or suspend any Certificate Application because of such dispute.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

The certificate applicant must demonstrate that it rightfully holds the private key corresponding to the public key to be listed in the Certificate.

The method to prove possession of a private key shall be PKCS #10, or another cryptographically equivalent demonstration.

3.2.2 Authentication of Individual Identity

For DL1 and DL2 Certificates the authentication of identity is based on the personal (physical) presence of the Certificate Applicant before an agent of the KIBS, or before a notary public or other official with comparable authority within the Certificate Applicant's jurisdiction. KIBS representatives, notary or other official authority, check the identity of the Certificate Applicant against a well-organized form of government – issued photographic identification, such as an identification card or a passport. When the authentication is based on the personal (physical) presence of the Certificate Applicant before an agent of the KIBS, KIBS attests a copy of the Applicant's identification card or a passport for archiving purposes. When the authentication is based on the personal (physical) presence of the Certificate Applicant before a notary public or other official with comparable authority, the Applicant has to submit to KIBS or the equivalent RA, an attested copy of his/her identification card or passport, referring the attestation date.

The attestation of the identification card or the passport must be in the Macedonian or English language. In case of an identification card or a passport issued in other than the above languages, the attestation must be in one of those languages or accompanied by an official translation in one of the above mentioned languages.

3.2.3 Non-Verified Subscriber information

Non-verified subscriber information includes the Organization Unit (OU) attributes.

3.2.4 Validation of Authority

Whenever an individual's name is associated with an Organization name in a certificate in such a way to indicate the individual's affiliation or authorization to act on behalf of the Organization KIBS RA:

- determines that the organization exists by using at least one third party identity proofing service or database, or alternatively, organizational documentation issued by or filed with the applicable government that confirms the existence of the organization, and
- Uses information contained in the business records or databases of business information (employee or customer directories) of an RA approving certificates to its own affiliated individuals or confirms by telephone, confirmatory postal mail, or comparable procedure to the organization, when appropriate, his/her authority to act on behalf of the Organization.

3.3 Identification and Authentication for Re-key Requests

Prior to the expiration of an existing Subscriber's Certificate, it is necessary for the Subscriber to obtain a new certificate to maintain continuity of Certificate usage. KIBS generally requires that the Subscriber generate a new key pair to replace the expiring key pair (technically defined as "rekey"). However, in certain cases (i.e. for web server certificates) Subscribers may request a new certificate for an existing key pair (technically defined as "renewal").

Generally speaking, both "Rekey" and "Renewal" are commonly described as "Certificate Renewal", focusing on the fact that the old Certificate is being replaced with a new Certificate and not emphasizing whether or not a new key pair is generated. For DL1 and DL2 Certificates this distinction is not important as a new key pair is always generated as part of KIBS's end-user Subscriber Certificate replacement process.

3.3.1 Identification and Authentication for Routine Re-key

Re-key procedures ensure that the person seeking to rekey an end-user Subscriber Certificate is in fact the Subscriber of the Certificate.

The Subscriber submits a rekey application to KIBS or the equivalent RA by submitting his existing certificate (digitally signing), and the RA, reconfirms in such way the identity of the Subscriber. For DL1 and DL2 certificates, the personal (physical) presence of the Certificate Applicant before an agent of KIBS, or before a notary public or other official with comparable authority within the Certificate Applicant's jurisdiction, is not required, unless the verified registration data included in the certificate or the identification documents (identification card or a passport) that have been submitted at the initial application has changed.

In any case, the applicant has to resubmit a copy of the certificate or the form of government (identification card or a passport) that had been submitted at the initial application.

3.3.2 Identification and Authentication for Re-key After Revocation

Re-key after revocation is not permitted.

3.4 Identification and Authentication for Revocation Request

Prior to the revocation of a Certificate, KIBS verifies that the revocation has been requested by the Certificate's Subscriber.

Acceptable procedures for authenticating the revocation requests of a Subscriber include one or more of the following:

- Having the Subscriber submit the Subscriber's Challenge Phrase , and revoking the Certificate automatically if it matches the Challenge Phrase on record
- Receiving a message from the Subscriber that requests revocation and contains a digital signature verifiable with reference to the Certificate to be revoked.
- Communication with the Subscriber providing reasonable assurances, ensuring that the person or organization requesting revocation is, in fact the Subscriber or has the dully authorization to do so. Such communication, depending on the circumstances, may include one or more of the following: telephone, facsimile, e-mail, postal mail, or courier service.

KIBS Administrators are entitled to request the revocation of end-user Subscriber Certificates within KIBS's Subdomain. KIBS authenticates the identity of Administrators via access control using SSL and client authentication before permitting them to perform revocation functions, or another VTN-approved procedure

4. CERTIFICATE LIFE-CYCLE OPERATIONAL

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application?

Application for Qualified Certificate may submit the natural (physical) person, who is the subject of the Certificate, provided that he/she is an adult and legally eligible according to the Macedonian law.

4.1.2 Enrollment Process and Responsibilities

4.1.2.1 End-user Certificate Subscribers

All end-user Certificate Subscribers manifest assent to the relevant Subscriber Agreement that contains representations and warranties described in Section 9.6.3 and undergo an enrollment process consisting of:

- completing and signing a Certificate Application and providing true and correct information,
- generating, or arranging to have generated, a key pair,
- delivering his, her, or its public key, directly or through an RA, to KIBS
- demonstrating possession of the private key corresponding to the public key delivered to KIBS.

The enrollment process for Qualified Certificates is in accordance with CP § 4.1, subject to the following clarifications:

- The Subscriber Agreements, to which Certificate Applicants manifest assent, are communicated in accordance with EDP § 2.1.1, 2.1.2,
- The Certificate Applicant shall present evidence of identity consistent with EDP § 3.1.9, and
- The enrollment information provided in the Certificate Application includes a physical address, or other attributes, that enable KIBS to contact the Certificate Applicant.

Records retained in accordance with CPS § 5.4.1. include the information used to authenticate the Certificate Applicant's identity (including any reference number on the documentation used for authentication and any limitations on its validity) and a record of the signed subscriber agreement in electronic form, wherein the Subscriber inter alia consents to the keeping of a record by the CA of information used in registration and include all other consents required in ETSI Policy Document.

In the case of an application for rekeying:

- Any changes in the terms of the Subscriber Agreement following the previous enrollment or re-enrollment are communicated in accordance with EDP § 2.1.1, 2.1.2, and
- Records retained under CPS § 5.5.1 also include the Subscriber's assent to any such changes.

4.1.2.2 CA and RA Certificates

ADACOM, as VeriSign's Affiliate, may issue additional RA certificates for the issuance DL1 and DL2 certificates.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

KIBS RA performs identification and authentication of all required Subscriber information in terms of Section 3.2.

4.2.2 Approval or Rejection of Certificate Applications

KIBS RA approves an application for a certificate only if the following criteria are met:

- Successful identification and authentication of all required Subscriber information in terms of Section 3.2,
- Payment has been received.

KIBS RA rejects a certificate application if:

- Identification and authentication of all required Subscriber information in terms of Section 3.2 cannot be completed, or
- The Subscriber fails to furnish supporting documentation upon request,
- The Subscriber fails to respond to notices within a specified time, or
- Payment has not been received, or
- The RA believes that issuing a certificate to the Subscriber may bring the VTN into disrepute.

4.2.3 Time to Process Certificate Applications

KIBS begins processing certificate applications within a reasonable time of receipt. A certificate application remains active until rejected.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

A Certificate is created and issued following the approval of a Certificate Application by KIBS or following receipt of an RA's request to issue the Certificate. ADACOM creates and issues to a Certificate Applicant a Certificate based on the information in a Certificate Application following approval of such Certificate Application.

The Qualified Certificates generated and issued in accordance with CP § 4.2.1 are issued by systems utilizing safeguards against forgery detailed in CP § 6 and EDP § 6 and that ensure that the Certificate is issued to the Certificate Applicant, or applicant for renewal or rekeying, holding the private key corresponding to the public key in the Certificate to be issued.

The issuance of Certificates under CPS § 3.3 is, as a technical matter, rekeying rather than a re-Certification of a previously-certified public key.

4.3.2 Notifications to Subscriber by the CA of Issuance of Certificate

KIBS either directly or through the RA, notify Subscribers that they have created such Certificates, and provide Subscribers with access to the Certificates by notifying them that their Certificates are available. Certificates are made available to end-user Subscribers, by informing them to download them from a web site, via an e-mail message sent to the Subscriber.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

The following conduct constitutes certificate acceptance:

- Downloading a Certificate or installing a Certificate from a message attaching it constitutes the Subscriber's acceptance of the Certificate.
- Failure of the Subscriber to object to the certificate or its content constitutes certificate acceptance.

4.4.2 Publication of the Certificate by the CA

KIBS publishes the Certificates it issues in a publicly accessible repository.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

Not applicable.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

Use of the private key corresponding to the public key in the certificate is only permitted once the Subscriber has agreed to the Subscriber agreement and accepted the certificate. The certificate shall be used lawfully in accordance with KIBS's Subscriber Agreement, the terms of the VTN CP and this CPS. Certificate use must be consistent with the KeyUsage field extensions included in the certificate.

Subscribers shall protect their private keys from unauthorized use and shall discontinue use of the private key following expiration or revocation of the certificate.

4.5.2 Relying Party Public Key and Certificate Usage

Relying parties shall assent to the terms of the ADACOM relying party agreement as a condition of relying on the certificate.

Reliance on a certificate must be reasonable under the circumstances. If the circumstances indicate a need for additional assurances, the Relying Party must obtain such assurances for such reliance to be deemed reasonable.

Before any act of reliance, Relying Parties shall independently assess:

- The appropriateness of the use of a Certificate for any given purpose and determine that the Certificate will, in fact, be used for an appropriate purpose that is not prohibited or otherwise restricted by this CPS. KIBS is not responsible for assessing the appropriateness of the use of a Certificate.
- That the certificate is being used in accordance with the KeyUsage field extensions included in the certificate.
- The status of the certificate and all the CAs in the chain that issued the certificate. If any of the Certificates in the Certificate Chain have been revoked, the Relying Party is solely responsible to investigate whether reliance on a digital signature performed by an end-user Subscriber Certificate prior to revocation of a Certificate in the Certificate chain is reasonable. Any such reliance is made solely at the risk of the Relying party.

Assuming that the use of the Certificate is appropriate, Relying Parties shall utilize the appropriate software and/or hardware to perform digital signature verification or other cryptographic operations they wish to perform, as a condition of relying on Certificates in connection with each such operation. Such operations include identifying a Certificate Chain and verifying the digital signatures on all Certificates in the Certificate Chain.

4.6 Certificate Renewal

Certificate renewal is the issuance of a new certificate to the subscriber without changing the public key or any other information in the certificate. Certificate renewal is not supported for DL1 and DL2 certificates.

4.6.1 Circumstances for Certificate Renewal

Not applicable.

4.6.2 Who May Request Renewal

Not applicable.

4.6.3 Processing Certificate Renewal Requests

Not applicable.

4.6.4 Notification of New Certificate Issuance to Subscriber

Not applicable.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Not applicable.

4.6.6 Publication of the Renewal Certificate by the CA

Not applicable.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

Not applicable.

4.7 Certificate Re-Key

Certificate rekey is the application for the issuance of a new certificate that certifies the new public key. For DL1 and DL2 Certificates, rekey is supported.

4.7.1 Circumstances for Certificate Re-Key

Prior to the expiration of an existing Subscriber's Certificate, it is necessary for the Subscriber to Re-key the certificate to maintain continuity of Certificate usage. A certificate may also be re-keyed after expiration.

4.7.2 Who May Request Certification of a New Public Key

Only the subscriber for an individual certificate may request certificate rekeying.

4.7.3 Processing Certificate Re-Keying Requests

Re-key procedures ensure that the person seeking to renew an end-user Subscriber Certificate is in fact the Subscriber (or authorized by the Subscriber) of the Certificate.

The Subscriber submits a rekey application to KIBS RA by submitting his existing certificate (digitally signing), and KIBS RA, reconfirms the identity of the Subscriber in accordance with the identification and authentication requirements, as described in section 3.3.1.

4.7.4 Notification of New Certificate Issuance to Subscriber

Notification of issuance of a re-keyed certificate to the Subscriber is in accordance with Section 4.3.2.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

Conduct constituting Acceptance of a re-keyed certificate is in accordance with Section 4.4.1.

4.7.6 Publication of the Re-Keyed Certificate by the CA

The re-keyed certificate is published in KIBS's publicly accessible repository.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

Not applicable.

4.8 Certificate Modification

4.8.1 Circumstances for Certificate Modification

Certificate modification refers to the application for the issuance of a new certificate due to changes in the information in an existing certificate (other than the subscriber's public key).

Certificate modification is considered a Certificate Application in terms of Section 4.1.

4.8.2 Who May Request Certificate Modification

See Section 4.1.1.

4.8.3 Processing Certificate Modification Requests

KIBS RA performs identification and authentication of all required Subscriber information in terms of Section 3.2.

4.8.4 Notification of New Certificate Issuance to Subscriber

See Section 4.3.2

4.8.5 Conduct Constituting Acceptance of Modified Certificate

See Section 4.4.1

4.8.6 Publication of the Modified Certificate by the CA

See Section 4.4.2

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

See Section 4.4.3.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

The KIBS Subscriber's agreement grants this obligation or/and right to the parties to apply for revocation of a Certificate. Only in the circumstances listed below, will an end-user Subscriber certificate be revoked by KIBS (or by the Subscriber) and published on a CRL.

An end-user Subscriber Certificate is revoked if:

- KIBS or a Subscriber has reason to believe or strongly suspects that there has been a Compromise of a Subscriber's private key,
- KIBS has reason to believe that the Subscriber has materially breached a material obligation, representation, or warranty under the applicable Subscriber Agreement,
- The Subscriber Agreement with the Subscriber has been terminated,
- KIBS has reason to believe that the Certificate was issued in a manner not materially in accordance with the procedures required by this CPS, the Certificate, was issued to a person other than the one named as the Subject of the Certificate, or the Certificate was issued without the authorization of the person named as the Subject of such Certificate,
- KIBS has reason to believe that a material fact in the Certificate Application is false,
- KIBS determines that a material prerequisite to Certificate Issuance was neither satisfied nor waived,
- In case that a Subscriber lose the legal eligibility, be declared in absence or death, taking into account that a certificate is at all case non transferable,
- In case of non appealable court's decision that order the revocation or cancelation of the certificate,
- In case that the private key of the CA has been compromised,
- The information within the Certificate, other than non-verified Subscriber Information, is incorrect or has changed, or the circumstances under which the certificate was issued have changed (i.e. in case where an employee has taken a certificate under this role and is no longer the employee of the company),
- The continued use of that certificate is harmful to the VTN.

When considering whether certificate usage is harmful to the VTN, KIBS considers, among other things, the following:

- The nature and number of complaints received,

- The identity of the complainant(s),
- Relevant legislation in force,
- Responses to the alleged harmful use from the Subscriber.

KIBS may also revoke an Administrator Certificate if the Administrator's authority to act as Administrator has been terminated or otherwise has ended.

KIBS Subscriber Agreements require end-user Subscribers to immediately notify KIBS of a known or suspected compromise of its private key.

After the approving of a revocation request by the CA, the revoked certificate cannot be re-entered into force.

4.9.2 Who Can Request Revocation

Individual Subscribers or a duly authorized person by them can request the revocation of their own individual Certificates.

KIBS is entitled to request or initiate the revocation of the Certificates issued to its own CAs. KIBS is entitled to request or initiate the revocation of the Certificates issued to its own RAs for Qualified Certificates.

4.9.3 Procedure for Revocation Request

4.9.3.1 Procedure for Requesting the Revocation of an End-User Subscriber Certificate

An end-user Subscriber requesting revocation is required to communicate the request to the KIBS by e-mail at ca-pomos@kibs.com.mk who in turn will initiate revocation of the certificate promptly.

4.9.3.2 Procedure for Requesting the Revocation of a CA or RA Certificate

KIBS may initiate CA or RA Certificate revocation.

4.9.4 Revocation Request Grace Period

Revocation requests shall be submitted as promptly as possible within a commercially reasonable time.

4.9.5 Time within which CA must process the Revocation Request

KIBS takes commercially reasonable steps to process revocation requests without delay.

Right after the approving of a revocation request, the CA informs the subject of the certificate for the revocation via e-mail for this event.

4.9.6 Revocation Checking Requirements for Relying Parties

Relying Parties shall check the status of Certificates on which they wish to rely. One method by which Relying Parties may check Certificate status is by consulting the most recent CRL from the CA that issued the Certificate on which the Relying Party wishes to rely. Alternatively, Relying Parties may meet this requirement by checking Certificate status using the KIBS web-based repository. CAs shall provide Relying Parties with information on how to find the appropriate CRL, web-based repository to check for revocation status.

4.9.7 CRL Issuance Frequency

CRLs for end-user Subscriber Certificates are issued at least once per day. CRLs for CA Certificates are issued at least annually, but also whenever a CA Certificate is revoked. If a Certificate listed in a CRL expires, it may be removed from later-issued CRLs after the Certificate's expiration. KIBS does not remove the Certificates that have been expired, from the later-issued CRLs after the Certificates' expiration. Nevertheless, KIBS grants the right to change this policy in the future, if required.

4.9.8 Maximum Latency for CRLs

CRLs are posted to the repository within a commercially reasonable time after generation. This is generally done automatically within minutes of generation.

4.9.9 On-Line Revocation/Status Checking Availability

Online revocation and other Certificate status information are available via a web-based repository. In addition to publishing CRLs, KIBS provides Certificate status information through query functions in the KIBS repository. Certificate status information is available at:

<https://secure-ca.kibs.com.mk/services/qcen/client/search.htm>

4.9.10 On-Line Revocation Checking Requirements

A relying party must check the status of a certificate on which he/she/it wishes to rely. If a Relying Party does not check the status of a Certificate on which the Relying Party wishes to rely by consulting the most recent relevant CRL, the Relying Party shall check Certificate status by consulting the KIBSs repository.

4.9.11 Other Forms of Revocation Advertisements Available

Not applicable.

4.9.12 Special Requirements regarding Key Compromise

KIBS uses commercially reasonable efforts to notify potential Relying Parties if it discovers, or have reason to believe, that there has been a Compromise of the private key of one of its own CAs.

4.9.13 Circumstances for Suspension

KIBS does not provide suspension services for the certificates it issues.

4.9.14 Who Can Request Suspension

Not applicable.

4.9.15 Procedure for Suspension Request

Not applicable.

4.9.16 Limits on Suspension Period

Not applicable.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

The Status of public certificates is available via CRL at KIBS's website, and LDAP directory.

4.10.2 Service Availability

Certificate Status Services are available 24x7 without scheduled interruption.

4.10.3 Optional Features

Not applicable.

4.11 End of Subscription

A subscriber may end a subscription for a KIBS certificate by:

- Allowing his/her/its certificate to expire,
- Revoking of his/her/its certificate before certificate expiration without replacing the certificates.

4.12 Key Escrow and Recovery

CA private keys and end-user Subscriber signature private keys are not escrowed.

4.12.1 Key Escrow and Recovery Policy and Practices

Not applicable.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Not applicable.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical Controls

KIBS has implemented a set of Security Policies, which supports the security requirements of this CPS. Compliance with these policies is included in KIBS's audit requirements described in Section 8. The KIBS Security Policies contain sensitive security information and is only available upon agreement with KIBS. An overview of the requirements is described below.

5.1.1 Site Location and Construction

KIBS RA operations are conducted within physically protected environment that deter, prevent, and detect unauthorized use of, access to, or disclosure of sensitive information and systems whether covert or overt.

CA operations are outsourced to ADACOM SA. ADACOM maintains disaster recovery storage locations for its CA operations. ADACOM disaster recovery storage location complies with the Off-site Storage Security Requirements set forth in the "ADACOM Disaster Recovery Plan".

5.1.2 Physical Access

KIBS RA systems are protected by five tiers of physical security, with access to the lower tier required before gaining access to the higher tier.

KIBS uses ADACOM CA systems that are protected by seven tiers of physical security, with access to the lower tier required before gaining access to the higher tier.

Progressively restrictive physical access privileges control access to each tier. Sensitive CA operational activity, any activity related to the lifecycle of the certification process such as authentication, verification, and issuance, occur within very restrictive physical tiers. Access to each tier requires the use of a proximity card employee badge. Physical access is automatically logged and video recorded. Some tiers enforce individual access control through the concurrent use of proximity cards and biometrics (two factor authentication). Unescorted personnel, including untrusted employees or visitors, are not allowed into such secured areas.

The physical security system employed by ADACOM includes tiers for key management security which serves to protect both online and offline storage of CSUs and keying material. Areas used to create and store cryptographic material enforce dual control, each through the concurrent use of proximity cards and biometrics. Online CSUs are protected through the use of locked cabinets. Offline CSUs are protected through the use of locked safes, cabinets and containers. Access to CSUs and keying material is restricted in accordance with ADACOM's segregation of duties requirements. The opening and closing of cabinets or containers in these tiers is logged for audit purposes.

5.1.3 Power and Air Conditioning

ADACOM's and KIBS's secure facilities are equipped with primary and backup:

- power systems to ensure continuous, uninterrupted access to electric power, and
- heating / ventilation / air conditioning systems to control temperature and relative humidity.

5.1.4 Water Exposures

ADACOM and KIBS have taken reasonable precautions to minimize the impact of water exposure to their systems.

5.1.5 Fire Prevention and Protection

ADACOM and KIBS have taken reasonable precautions to prevent and extinguish fires or other damaging exposure to flame or smoke. Fire prevention and protection measures have been designed to comply with local fire safety regulations.

5.1.6 Media Storage

All media containing production software and data, audit, archive, or backup information is stored within ADACOM's and KIBS's facilities and in a secure off-site storage facility with appropriate physical and logical access controls designed to limit access to authorized personnel and protect such media from accidental damage (e.g., water, fire, and electromagnetic).

5.1.7 Waste Disposal

Sensitive documents and materials are shredded before disposal. Media used to collect or transmit sensitive information are rendered unreadable before disposal. Cryptographic devices are physically destroyed or zeroized in accordance the manufacturers' guidance prior to disposal. Other waste is disposed of in accordance with ADACOM's and KIBS's normal waste disposal requirements.

5.1.8 Off-Site Backup

ADACOM and KIBS perform routine backups of critical system data, audit log data, and other sensitive information. Offsite backup media are stored in a physically secure manner using a secure off-site storage facility.

5.2 Procedural Controls

5.2.1 Trusted Roles

Trusted Persons include all employees that have access to or control authentication or cryptographic operations that may materially affect:

- the validation of information in Certificate Applications,
- the acceptance, rejection, or other processing of Certificate Applications, revocation requests, renewal requests, or enrollment information,
- the issuance, or revocation of Certificates, including personnel having access to restricted portions of its repository,
- the handling of Subscriber information or requests.

Trusted Persons include, but are not limited to:

- customer service personnel,
- cryptographic business operations personnel,
- security personnel,
- system administration personnel,
- designated engineering personnel, and
- executives that are designated to manage infrastructural trustworthiness.

KIBS considers the categories of personnel identified in this section as Trusted Persons having a Trusted Position. Persons seeking to become Trusted Persons by obtaining a Trusted Position must successfully complete the screening requirements set out in this CPS.

Contractors and consultants that have access to or control authentication or cryptographic operations are not allowed to conduct these operations unescorted.

5.2.2 Number of Persons Required per Task

KIBS has established, maintains, and enforces rigorous control procedures to ensure the segregation of duties based on job responsibility and to ensure that multiple Trusted Persons are required to perform sensitive tasks.

Policy and control procedures are in place to ensure segregation of duties based on job responsibilities. The most sensitive tasks require multiple Trusted Persons.

The validation and issuance of Qualified Certificates require the participation of at least 2 Trusted Persons, or a combination of at least one trusted person and an automated validation and issuance process.

5.2.3 Identification and Authentication for Each Role

For all personnel seeking to become Trusted Persons, verification of identity is performed through the personal (physical) presence of such personnel before Trusted Persons performing KIBS HR or security functions and a check of well-recognized forms of identification (e.g., passports and identification cards). Identity is further confirmed through the background checking procedures in CPS § 5.3.1.

KIBS ensures that personnel have achieved Trusted Status and departmental approval has been given before such personnel are:

- issued access devices and granted access to the required facilities,
- issued electronic credentials to access and perform specific functions on KIBS, RA, or other IT systems.

5.2.4 Roles Requiring Separation of Duties

Roles requiring Separation of duties include (but are not limited to):

- the validation of information in Certificate Applications,
- the acceptance, rejection, or other processing of Certificate Applications, revocation requests, or renewal requests, or enrollment information,
- the issuance, or revocation of Certificates, including personnel having access to restricted portions of the repository,
- the handling of Subscriber information or requests,
- the generation, issuing or destruction of a CA certificate.

5.3 Personnel Controls

Personnel seeking to become Trusted Persons must present proof of the requisite background, qualifications, and experience needed to perform their prospective job responsibilities competently and satisfactorily. Background checks are repeated at least every 5 years for personnel holding Trusted Positions.

5.3.1 Qualifications, Experience

KIBS requires that personnel seeking to become Trusted Persons present proof of the requisite background, qualifications, and experience needed to perform their prospective job responsibilities competently and satisfactorily.

5.3.2 Background Check Procedures

Prior to commencement of employment in a Trusted Role, KIBS conducts background checks which include the following:

- check of previous employment and professional reference (if available),
- confirmation of the highest or most relevant educational degree obtained,
- search of national criminal records.

To the extent that any of the requirements imposed by this section cannot be met due to a prohibition or limitation in local law or other circumstances, KIBS will utilize a substitute investigative technique permitted by law that provides substantially similar information.

The factors revealed in a background check that may be considered grounds for rejecting candidates for Trusted Positions or for taking action against an existing Trusted Person generally include (but are not limited to) the following:

- Misrepresentations made by the candidate or Trusted Person,
- Highly unfavorable or unreliable professional references,
- Certain criminal convictions.

Reports containing such information are evaluated by human resources and security personnel, who determine the appropriate course of action in light of the type, magnitude, and frequency of the behavior uncovered by the background check. Such actions may include measures up to and including the cancellation of offers of employment made to candidates for Trusted Positions or the termination of existing Trusted Persons.

The use of information revealed in a background check to take such actions is subject to the applicable laws.

5.3.3 Training Requirements

KIBS provides its personnel with training upon hire or the requisite on-the-job training needed for them to perform their job responsibilities competently and satisfactorily. KIBS maintains records of such training. KIBS periodically reviews and enhances its training programs as necessary.

KIBS's training programs are tailored to the individual's responsibilities and include the following as relevant:

- Basic PKI concepts,
- Job responsibilities,
- KIBS security and operational policies and procedures,
- Use and operation of deployed hardware and software,
- Incident and Compromise reporting and handling.

5.3.4 Retraining Frequency and Requirements

KIBS provides refresher training and updates to their personnel to the extent and frequency required to ensure that such personnel maintain the required level of proficiency to perform their job responsibilities competently and satisfactorily.

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 or other violations of KIBS policies and procedures. Disciplinary actions may include measures up to and including termination and are commensurate with the frequency and severity of the unauthorized actions.

5.3.7 Independent Contractor Requirements

In limited circumstances, independent contractors or consultants may be used to fill Trusted Positions. Any such contractor or consultant is held to the same functional and security criteria that apply to a KIBS employees in a comparable position.

Independent contractors and consultants who have not completed or passed the background check procedures specified in CPS § 5.3.2 are permitted access to KIBS 's secure facilities only to the extent they are escorted and directly supervised by Trusted Persons at all times.

5.3.8 Documentation Supplied to Personnel

KIBS provides its employees the requisite training and other documentation needed to perform their job responsibilities competently and satisfactorily.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

ADACOM manually or automatically logs the following significant events:

- CA key life cycle management events, including:
 - Key generation, backup, storage, recovery, archival, and destruction
 - Cryptographic device life cycle management events.
- CA and Subscriber certificate life cycle management events, including:
 - Certificate Applications, renewal, rekey, and revocation,
 - Successful or unsuccessful processing of requests,
 - Generation and issuance of Certificates and CRLs.
- Security-related events including:
 - Successful and unsuccessful PKI system access attempts,
 - PKI and security system actions performed by ADACOM personnel,
 - Security sensitive files or records read, written or deleted,
 - Security profile changes,
 - System crashes, hardware failures and other anomalies,
 - Firewall and router activity,
 - CA facility visitor entry/exit.

KIBS manually or automatically logs the following significant events:

- RAs log Certificate Application information including:
 - Kind of identification document(s) presented by the Certificate Applicant,
 - Record of unique identification data, numbers, or a combination thereof (e.g., Certificate Applicant's identification card number) of identification documents, if applicable,
 - Storage location of copies of applications and identification documents,
 - Identity of entity accepting the application,
 - Method used to validate identification documents, if any,
 - Name of receiving CA or submitting RA, if applicable.
- Subscriber certificate life cycle management events, including:
 - Certificate Applications, renewal, rekey, and revocation,
 - Successful or unsuccessful processing of requests
 - Generation and issuance of certificates.
- Security-related events including:
 - Successful and unsuccessful system access attempts,
 - Security system actions performed by KIBS personnel,
 - Security sensitive files or records read, written or deleted,
 - Security profile changes,
 - System crashes, hardware failures and other anomalies,
 - Firewall and router activity,
 - RA facility visitor entry/exit.

Log entries include the following elements:

- Date and time of the entry,
- Serial or sequence number of entry, for automatic journal entries,
- Identity of the entity making the journal entry,
- Kind of entry.

5.4.2 Frequency of Processing Log

Audit logs are examined on at least a weekly basis for significant security and operational events. In addition, KIBS reviews its audit logs for suspicious or unusual activity in response to alerts generated based on irregularities and incidents within KIBS CA and RA systems.

Audit log processing consists of a review of the audit logs and documentation for all significant events in an audit log summary. Audit log reviews include a verification that the log has not been tampered with, an inspection of all log entries, and an investigation of any alerts or irregularities in the logs. Actions taken based on audit log reviews are also documented.

5.4.3 Retention Period for Audit Log

Audit logs shall be retained onsite for at least two (2) months after processing and thereafter archived in accordance with Section 5.5.2.

5.4.4 Protection of Audit Log

Audit logs are protected with an electronic audit log system that includes mechanisms to protect the log files from unauthorized viewing, modification, deletion, or other tampering.

5.4.5 Audit Log Backup Procedures

Incremental backups of audit logs are created daily and full backups are performed weekly.

5.4.6 Audit Collection System (Internal vs. External)

Automated audit data is generated and recorded at the application, network and operating system level.

5.4.7 Notification to Event-Causing Subject

Where an event is logged by the audit collection system, no notice is required to be given to the individual, organization, device, or application that caused the event.

5.4.8 Vulnerability Assessments

Events in the audit process are logged, in part, to monitor system vulnerabilities. Logical security vulnerability assessments (hereinafter: LSVAs) are performed, reviewed, and revised following an examination of these monitored events. LSVAs are based on real-time automated logging data and are performed on a daily, monthly, and annual basis. An annual LSVAs will be an input into an entity's annual Compliance Audit.

5.5 Records Archival

5.5.1 Types of Records Archived

KIBS archives:

- All audit data collected in terms of Section 5.4,
- Certificate application information,
- Documentation supporting certificate applications,
- Certificate lifecycle information e.g. revocation, rekey and renewal application information.

KIBS retain the following evidence relating to the identity of Subscribers in connection with Certificate Applications for Qualified Certificates:

- The types of documents presented by Certificate Applicants in connection with their Certificate Applications;
- A record of unique identification data, numbers (e.g., a Certificate Applicant's passport or national identification card number) of identification documents, if applicable;
- The identity of the entity that receives and accepts Certificate Applications; and
- A validation plan showing the methods used to validate identification documents.

In addition, KIBS, retain records of the storage location of Certificate Applications and identification documents.

5.5.2 Retention Period for Archive

Records associated with a Qualified Certificate are retained for at least a time period of five (5) years after the date of revocation or expiry of that Qualified Certificate.

5.5.3 Protection of Archive

KIBS protects the archive so that only authorized Trusted Persons are able to obtain access to the archive. The archive is protected against unauthorized viewing, modification, deletion, or other tampering by storage within a Trustworthy System. The media holding the archive data and the applications required to process the archive data shall be maintained to ensure that the archive data can be accessed for the time period set forth in this CPS.

5.5.4 Archive Backup Procedures

KIBS performs full backup electronic archives of its issued Certificate information on a daily basis and weekly basis. Copies of paper-based records shall be maintained using an off-site secure facility.

5.5.5 Requirements for Time-Stamping of Records

Certificates, CRLs, and other revocation database entries contain time and date information.

5.5.6 Archive Collection System

KIBS archive collection systems are internal.

5.5.7 Procedures to Obtain and Verify Archive Information

Only authorized Trusted Personnel are able to obtain access to the archive. The integrity of the information is verified when it is restored.

5.6 Key Changeover

KIBS CA key pairs are retired from service at the end of their respective maximum lifetimes as defined in this CPS. KIBS CA Certificates may be renewed as long as the cumulative certified lifetime of the CA key pair does not exceed the maximum CA key pair lifetime. New CA key pairs are generated as necessary, for example to replace CA key pairs that are being retired, to supplement existing, active key pairs and to support new services.

Prior to the expiration of the CA Certificate for a Superior CA, key changeover procedures are enacted to facilitate a smooth transition for entities within the Superior CA's hierarchy from the old Superior CA key pair to new CA key pair(s). KIBS's CA key changeover process requires that:

- A Superior CA ceases to issue new Subordinate CA Certificates no later than 60 days before the point in time ("Stop Issuance Date") where the remaining lifetime of the Superior CA key pair equals the approved Certificate Validity Period for the specific type(s) of Certificates issued by Subordinate CAs in the Superior CA's hierarchy.
- Upon successful validation of Subordinate CA (or end-user Subscriber) Certificate requests received after the "Stop Issuance Date" Certificates will be signed with a new CA key pair.

The Superior CA continues to issue CRLs signed with the original Superior CA private key until the expiration date of the last Certificate issued using the original key pair has been reached.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

Backups of the following CA information are kept in off-site storage and made available in the event of a Compromise or disaster: Certificate Application data, audit data, and database records for all Certificates issued. Back-ups of CA private keys are generated and maintained in accordance with CP § 6.2.4. ADACOM maintains backups of the foregoing CA information for their own CAs.

5.7.2 Computing Resources, Software, and/or Data Are Corrupted

In the event of the corruption of computing resources, software, and/or data, such an occurrence is reported to ADACOM Security and ADACOM's incident handling procedures are enacted. Such procedures require appropriate escalation, incident investigation, and incident response. If necessary, ADACOM's key compromise or disaster recovery procedures will be enacted.

5.7.3 Entity Private Key Compromise Procedures

Upon the suspected or known Compromise of a ADACOM CA, ADACOM infrastructure or KIBS CA private key, ADACOM's Key Compromise Response procedures are enacted by the ADACOM Security Incident Response Team (hereinafter: ASIRT). This team, which includes Security, Cryptographic Business Operations, Production Services personnel, and other ADACOM management representatives, assesses the situation, develops an action plan, and implements the action plan with approval from ADACOM executive management.

If CA Certificate revocation is required, the following procedures are performed:

- The Certificate's revoked status is communicated to Relying Parties through the KIBS repository in accordance with CPS § 4.4.9,
- Commercially reasonable efforts will be made to provide additional notice of the revocation to all affected VTN Participants, and
- The CA will generate a new key pair in accordance with CPS § 4.7, except where the CA is being terminated in accordance with CPS § 4.9.

5.7.4 Business Continuity Capabilities after a Disaster

5.7.4.1 VeriSign

VeriSign has implemented a disaster recovery site more than 1600km from VeriSign's principal secure facilities. VeriSign has developed, implemented and tested a disaster recovery plan to mitigate the effects of any kind of natural or man-made disaster. This plan is regularly tested, verified, and updated to be operational in the event of a disaster.

Detailed disaster recovery plans are in place to address the restoration of information systems services and key business functions. VeriSign's disaster recovery site has implemented the physical security protections and operational controls required by the VeriSign Security and Audit Requirements Guide to provide for a secure and sound backup operational setup.

In the event of a natural or man-made disaster requiring temporary or permanent cessation of operations from VeriSign's primary facility, VeriSign's disaster recovery process is initiated by the VeriSign Emergency Response Team (hereinafter: VERT).

VeriSign has the capability to restore or recover essential operations within twenty four (24) hours following a disaster with, at a minimum, support for the following functions:

- Certificate issuance,
- Certificate revocation,
- Publication of revocation information, and
- Provision of key recovery information for Enterprise Customers using Managed PKI Key Manager.

VeriSign's disaster recovery database is synchronized regularly with the production database within the time limits set forth in the Security and Audit Requirements Guide. VeriSign's disaster recovery equipment is protected by physical security protections comparable to the physical security tiers specified in CPS § 5.1.2.

VeriSign's disaster recovery plan has been designed to provide full recovery within one week following disaster occurring at VeriSign's primary site. VeriSign tests its equipment at its primary site to support CA/RA functions following all but a major disaster that would render the entire facility inoperable. Results of such tests are reviewed and kept for audit and planning purposes. Where possible, operations are resumed at VeriSign's primary site as soon as possible following a major disaster.

VeriSign maintains redundant hardware and backups of its CA and infrastructure system software at its disaster recovery facility. In addition, CA private keys are backed up and maintained for disaster recovery purposes in accordance with CPS § 6.2.4.

VeriSign maintains offsite backups of important CA information for VeriSign CAs as well as the CAs of Service Centers, and Enterprise Customers, within VeriSign's Subdomain. Such information includes, but is not limited to: Certificate Application data, audit data (per Section 4.5), and database records for all Certificates issued.

5.7.4.2 ADACOM

ADACOM has implemented and tested a disaster recovery plan to mitigate the effects of any kind of natural or man-made disaster. This plan is regularly tested, verified, and updated to be operational in the event of a disaster.

Detailed disaster recovery plans are in place to address the restoration of information systems services and key business functions.

In the event of a natural or man-made disaster requiring temporary or permanent cessation of operations from ADACOM's primary facility, ADACOM's disaster recovery process is initiated by the ADACOM team in charge.

ADACOM has the capability to restore or recover operations, with top priority, the support for the functions of Certificate revocation and publication of revocation information.

ADACOM maintains backups of its CA and infrastructure system software at a secure offsite location. ADACOM also maintains offsite backups of important CA information for ADACOM CAs.

Additionally, CA private keys and secret shares are backed up for disaster recovery purposes in accordance with CPS § 6.2.4, the "ADACOM Disaster Recovery Plan for the Interim Offsite Storage of Cryptographic Materials", and the "ADACOM Disaster Recovery Plan", which will allow for business resumption at a later date.

5.8 CA or RA Termination

In the event that it is necessary for a KIBS CA, to cease operation, KIBS makes a commercially reasonable effort to notify Subscribers, Relying Parties, and other affected entities of such termination in advance of the CA termination. Where CA termination is required, KIBS will activate the documented "KIBS Termination Plan" to minimize disruption to Customers, Subscribers, and Relying Parties. This termination plan addresses the following, as applicable:

- Provision of notice to parties affected by the termination, such as Subscribers, Relying Parties, and Customers, informing them of the status of the CA,
- Handling the cost of such notice,
- The revocation of the Certificate issued to the CA
- The preservation of the CA's archives and records for the time periods required in this CPS,
- The continuation of Subscriber and customer support services,
- The continuation of revocation services, such as the issuance of CRLs or the maintenance of online status checking services,
- The revocation of unexpired unrevoked Certificates of end-user Subscribers and subordinate CAs, if necessary,
- Refunding (if necessary) Subscribers whose unexpired unrevoked Certificates are revoked under the termination plan or provision, or alternatively, the issuance of replacement Certificates by a successor CA,
- Disposition of the CA's private key and the hardware tokens containing such private key,
- Provisions needed for the transition of the CA's services to a successor CA, and
- Provision notice to the Macedonian Supervisory Authority.

In the event that it will be necessary for KIBS to cease all operations, KIBS will additionally follow all the necessary steps, provided in the relative Macedonian law. This includes, but not limited to, the submission of the KIBS CA's archives and records to another contracting Certification Service Provider for Qualified Certificates, for the time periods required by the law.

6. TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

CA key pair generation is performed by multiple pre-selected, trained and trusted individuals using Trustworthy Systems and processes that provide for the security and required cryptographic strength for the generated keys. For PCA and Issuing Root CAs, the cryptographic modules used or key generation meets the requirements of CC EAL 4+ and FIPS 140-1 level 3.

All CA key pairs are generated in pre-planned Key Generation Ceremonies in accordance with the requirements of the Key Ceremony Reference Guide, the CA Key Management Tool User's Guide, and the VeriSign Security and Audit Requirements Guide. The activities performed in each key generation ceremony are recorded, dated and signed by all individuals involved. These records are kept for audit and tracking purposes for a length of time deemed appropriate by ADACOM Management.

Generation of RA key pairs is generally performed by the RA using a CC EAL 4+ and FIPS 140-1 level 1 certified cryptographic module provided with their browser software.

Generation of end-user Subscriber key pairs is performed by the Subscriber.

6.1.2 Private Key Delivery to Subscriber

End-user Subscriber key pairs are generated by the end-user Subscriber, thus private key delivery to a Subscriber is not applicable.

6.1.3 Public Key Delivery to Certificate Issuer

End-user Subscribers and RAs submit their public key to KIBS for certification electronically through the use of a PKCS#10 Certificate Signing Request (CSR) or other digitally signed package in a session secured by Secure Sockets Layer (SSL).

6.1.4 CA Public Key Delivery to Relying Parties

KIBS makes the CA Certificates for VeriSign PCAs and its root CAs available to Subscribers and Relying Parties through their inclusion in web browser software. As new PCA and root CA Certificates are generated, VeriSign provides such new Certificates to the browser manufacturers for inclusion in new browser releases and updates.

KIBS generally provides its own full certificate chain (including the issuing CA and any CAs in the chain) to the end-user Subscriber upon Certificate issuance.

Users, during the certificate pick-up process, automatically download and install into their computer, the intermediate and issuing CA's public keys. This is a process controlled by the PKI application. In any case if a user needs to verify and/or download the public key of the CA, he can do so by accessing the KIBS's web-based repository: <https://ca.kibs.com.mk/repository/rpa>.

6.1.5 Key Sizes

Key pairs shall be of sufficient length to prevent others from determining the key pair's private key using cryptanalysis during the period of expected utilization of such key pairs. VeriSign's third generation (G3) PCAs have 2048 bit RSA key pairs. KIBS CAs for Qualified Certificates have 2048 bit RSA key pairs.

KIBS RAs use key pairs of 1024 bit or more. VeriSign and ADACOM recommend that end-user Subscribers generate 1024 bit RSA key pairs. KIBS may not approve certain end entity certificates generated with a key pair size of 512 bit or less.

6.1.6 Public Key Parameters Generation and Quality Checking

Not applicable.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

ADACOM has implemented a combination of physical, logical, and procedural controls to ensure the security of KIBS CA private keys. Subscribers are required by contract to take necessary precautions to prevent the loss, disclosure, modification, or unauthorized use of private keys.

6.2.1 Cryptographic Module Standards and Controls

For PCA and Issuing Root CA key pair generation and CA private key storage, VeriSign uses hardware cryptographic modules that are certified at or meet the requirements of CC EAL 4+ and FIPS 140-1 Level 3. For the rest KIBS CAs, hardware cryptographic modules that are certified at or meet the requirements stated in section § 6.1.1. of this CPS.

In addition to the provision set forth in this CPS, KIBS distributes SSCDs to DL2 end-user Subscribers that meet the following requirements.

First, SSCDs, by appropriate technical and procedural means, ensure that at least:

- The private key within the SSCD can practically occur only once, and that its secrecy is reasonably assured,
- Such private key cannot, with reasonable assurance, be derived and the signature is protected against forgery using currently-available technology, and
- Such private key can reliably be protected by the Subscriber against use by others.

Second, SSCDs do not alter the data to be signed or/and prevent such data from being presented to the signatory prior to the signature process.

Specifically, the SSCD used by KIBS are certified and meet the requirements of CC EAL 4+.

6.2.2 Private Key (m out of n) Multi-Person Control

KIBS uses technical and procedural mechanisms implemented by ADACOM that require the participation of multiple trusted individuals to perform sensitive CA cryptographic operations. ADACOM uses "Secret Sharing" to split the activation data needed to make use of a CA private key into separate parts called "Secret Shares" which are held by trained and trusted individuals called "Shareholders." A threshold number of Secret Shares (m) out of the total number of Secret Shares created and distributed for a particular hardware cryptographic module (n) is required to activate a CA private key stored on the module.

The threshold number of shares needed to sign a CA certificate is three (3). Secret Shares are protected in accordance with this CPS.

6.2.3 Private Key Escrow

KIBS CA and end user's private keys are not escrowed.

6.2.4 Private Key Backup

ADACOM creates backup copies of KIBS CA private keys for routine recovery and disaster recovery purposes. Such keys are stored in encrypted form within hardware cryptographic modules and associated key storage devices. Cryptographic modules used for CA private key storage meet the requirements of this CPS. CA private keys are copied to backup hardware cryptographic modules in accordance with this CPS.

Modules containing onsite backup copies of CA private keys are subject to the requirements of CPS. Modules containing disaster recovery copies of CA private keys are subject to the requirements of this CPS.

ADACOM does not store copies of RA private keys. For the backup of end-user Subscriber private keys, see Section 6.2.3 and Section 4.12.

6.2.5 Private Key Archival

Upon expiration of a KIBS CA Certificate, the key pair associated with the certificate is securely retained for a period of at least 5 years using hardware cryptographic modules that meet the requirements of this and ADACOM's CPS. These CA key pairs are not be used for any signing events after their expiration date, unless the CA Certificate has been renewed in terms of this CPS.

KIBS does not archive copies of Subscriber private keys.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

ADACOM generates KIBS CA key pairs on the hardware cryptographic modules in which the keys will be used. In addition, ADACOM makes copies of such CA key pairs for routine recovery and disaster recovery purposes. Where CA key pairs are backed up to another hardware cryptographic module, such key pairs are transported between modules in encrypted form.

6.2.7 Private Key Storage on Cryptographic Module

CA or RA private keys held on hardware cryptographic modules are stored in encrypted form.

6.2.8 Method of Activating Private Key

All KIBS Subdomain Participants shall protect the activation data for their private keys against loss, theft, modification, unauthorized disclosure, or unauthorized use.

6.2.8.1 Qualified Certificates' Private Keys

The VTN Standards for private key protection is for Subscribers to take commercially reasonable measures for the physical protection of the Subscriber's workstation to prevent use of the workstation and its associated private key without the Subscriber's authorization. In addition, KIBS recommends that Subscribers use a password in accordance with Section 6.4.1 or security of equivalent strength to authenticate the Subscriber before the activation of the private key, which includes, for instance, a password to operate the private key, a Windows logon or screen saver password, or a network logon password.

In addition to the above:

- For DL1 Certificates

Subscribers of DL1 Certificates have no requirement to use an SSCD in connection with the use and activation of their private keys,

- For DL2 Certificates

Subscribers of DL2 Certificates shall use an SSCD in connection with the use and activation of their private keys.

6.2.8.2 Administrators' Private Keys

The Standard for Administrators' private key protection requires them to:

- Use a smart card, biometric access device, password in accordance with Section 6.4.1, or security of equivalent strength to authenticate the Administrator before the activation of the private key, which includes, for instance, a password to operate the private key, a Windows logon or screen saver password, or a network logon password; and
- Take commercially reasonable measures for the physical protection of the Administrator's workstation to prevent use of the workstation and its associated private key without the Administrator's authorization.

KIBS recommends that Administrators use a smart card, biometric access device, or security of equivalent strength along with the use of a password in accordance with Section 6.4.1 to authenticate the Administrator before the activation of the private key.

When deactivated, private keys are being kept in encrypted form only.

6.2.8.3 Private Keys Held by Processing Centers

An online CA's private key shall be activated by a threshold number of Shareholders, as defined in Section 6.2.2, supplying their activation data (stored on secure media). Once the private key is activated, the private key may be active for an indefinite period until it is deactivated when the CA goes offline. Similarly, a threshold number of Shareholders shall be required to supply their activation data in order to activate an offline CA's private key. Once the private key is activated, it shall be active only for one time.

6.2.9 Method of Deactivating Private Key

KIBS CA private keys are deactivated upon removal from the token reader. KIBS RA private keys (used for authentication to the RA application) are deactivated upon system log off. KIBS RAs are required to log off their workstations when leaving their work area.

Client Administrators, RA, and end-user Subscriber private keys may be deactivated after each operation, upon logging off their system, or upon removal of a smart card from the smart card reader depending upon the authentication mechanism employed by the user. In all cases, end-user Subscribers has an obligation to adequately protect their private key(s) in accordance with this CPS.

6.2.10 Method of Destroying Private Key

At the conclusion of a KIBS CA's operational lifetime, one or more copies of the CA private key are archived in accordance with CPS § 6.2.5. Remaining copies of the CA private key are securely destroyed. In addition, archived CA private keys are securely destroyed at the conclusion of their archive periods. CA key destruction activities require the participation of multiple trusted individuals.

Where required, ADACOM destroys KIBS CA private keys in a manner that reasonably ensures that there are no residuals remains of the key that could lead to the reconstruction of the key. This destruction takes place only when the minimum required archiving period for the CAs, in accordance with section 5.5.5., passes, after the revocation of the CA certificate. ADACOM utilizes the zeroization function of its hardware cryptographic modules and other appropriate

means to ensure the complete destruction of CA private keys. When performed, CA key destruction activities are logged.

6.2.11 Cryptographic Module Rating

See Section 6.2.1.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

KIBS CA, RA and end-user Subscriber Certificates are backed up and archived as part of KIBS 's routine backup procedures.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The Operational Period of a Certificate ends upon its expiration or revocation. The Operational Period for key pairs is the same as the Operational Period for the associated Certificates, except that they may continue to be used for decryption and signature verification. The maximum Operational Periods for KIBS Certificates for Certificates issued on or after the effective date of this CPS are set forth in Table 6 below.

In addition, KIBS CAs stops issuing new Certificates at an appropriate date prior to the expiration of the CA's Certificate such that no Certificate issued by a Subordinate CA expires after the expiration of any Superior CA Certificates.

Certificate Issued By:	Validity Period
PCA self-signed (1024 bit)	30 years
PCA to Offline intermediate CA	15 years
Offline intermediate CA to online CA	10 years
Online CA to End-user Individual Subscriber	Normally up to 2 years, but under the conditions described below, up to 5 years ³

Table 5 – Certificate Operational Periods

KIBS Subdomain Participants shall cease all use of their key pairs after their usage periods have expired.

Certificates issued by CAs to end-user Subscribers may have Operational Periods longer than two years, up to five years, if the following requirements are met:

- The Certificates are individual Certificates,
- Subscribers' key pairs reside on a Secure Signature Creation Devices, such as a smart card,
- Subscribers are required to undergo re-authentication at least every 25 months under Section 3.2.2,
- Subscribers shall prove possession of the private key corresponding to the public key within the Certificate at least every 25 months under Section 3.2.2,

³ If 5-year end-user subscriber certificates are issued, the online CA certificate's operational period will be 10 years with no option to renew. Re-key will be required after 5 years.

- If a Subscriber is unable to complete re-authentication procedures successfully or is unable to prove possession of such private key when required by the foregoing, the CA shall revoke the Subscriber's Certificate.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

Activation data (Secret Shares) used to protect tokens containing KIBS CA private keys is generated in accordance with the requirements of CPS § 6.2.2 and the Key Ceremony Reference Guide. The creation and distribution of Secret Shares is logged.

KIBS RAs are required to select strong passwords to protect their private keys. KIBS's password selection guidelines require that passwords:

- be generated by the user;
- have at least eight characters;
- have at least one alphabetic and one numeric character;
- have at least one lower-case letter;
- not contain many occurrences of the same character;
- not be the same as the operator's profile name; and
- not contain a long substring of the user's profile name.

KIBS RA uses, and KIBS strongly recommends end-user Subscribers choose, passwords that meet the same requirements. KIBS also recommends the use of two factor authentication mechanisms (e.g., token and passphrase, biometric and token, or biometric and passphrase) for private key activation.

6.4.2 Activation Data Protection

KIBS Shareholders are required to safeguard their Secret Shares and sign an agreement acknowledging their Shareholder responsibilities.

KIBS RAs store their Administrator/RA private keys in encrypted form using password protection and their browser's "high security" option.

KIBS RA and its Client Administrators, store their private keys in encrypted form and protect their private keys through the use of a hardware token and/or strong passphrase uses, and KIBS strongly recommends that end-user Subscribers store their private keys in encrypted form and protect their private keys through the use of a hardware token and/or strong passphrase. The use of two factor authentication mechanisms (e.g., token and passphrase, biometric and token, or biometric and passphrase) is encouraged.

6.4.3 Other Aspects of Activation Data

6.4.3.1 Activation Data Transmission

To the extent activation data for private keys are transmitted, VTN Participants shall protect the transmission using methods that protect against the loss, theft, modification, unauthorized disclosure, or unauthorized use of such private keys. To the extent Windows or network logon

user name/password combination is used as activation data for an end-user Subscriber, the passwords transferred across a network shall be protected against access by unauthorized users.

6.4.3.2 Activation Data Destruction

Activation data for CA private keys are decommissioned using methods that protect against the loss, theft, modification, unauthorized disclosure, or unauthorized use of the private keys protected by such activation data. After the record retention periods in Section 5.5.2 lapse, KIBS recommits activation data by overwriting and/or physical destruction.

6.5 Computer Security Controls

ADACOM and KIBS performs all CA and RA functions using Trustworthy Systems that meet the requirements of VeriSign's Security and Audit Requirements Guide.

6.5.1 Specific Computer Security Technical Requirements

KIBS ensures that the systems maintaining CA software and data files are Trustworthy Systems secure from unauthorized access. In addition, KIBS limits access to production servers to those individuals with a valid business reason for such access. General application users do not have accounts on production servers.

KIBS's production network is logically separated from other components. This separation prevents network access except through defined application processes. KIBS uses firewalls to protect the production network from internal and external intrusion and limit the nature and source of network activities that may access production systems.

KIBS requires the use of passwords that have a minimum character length and a combination of alphanumeric and special characters. KIBS requires that passwords be changed on a periodic basis.

Direct access to KIBS databases supporting KIBS's CA Operations is limited to Trusted Persons in KIBS's Production Operations group having a valid business reason for such access.

6.5.2 Computer Security Rating

No stipulation.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

Applications are developed and implemented by KIBS in accordance with KIBS systems development and change management standards.

VeriSign developed software, when first loaded provides a method to verify that the software on the system originated from VeriSign, has not been modified prior to installation, and is the version intended for use.

6.6.2 Security Management Controls

KIBS has mechanisms and/or policies in place to control and monitor the configuration of its CA systems. VeriSign creates a hash of all software packages and VeriSign software updates. This hash is used to verify the integrity of such software manually. Upon installation and periodically thereafter, KIBS validates the integrity of its CA systems.

6.6.3 Life Cycle Security Controls

No stipulation.

6.7 Network Security Controls

KIBS performs all its CA and RA functions using networks secured in accordance with the VeriSign Security and Audit Requirements Guide to prevent unauthorized access and other malicious activity. KIBS protects its communications of sensitive information through the use of encryption and digital signatures.

6.8 Time-Stamping

Certificates, CRLs, and other revocation database entries contain time and date information. Such time information need not be cryptographic-based.

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate Profile

KIBS Certificates generally conform to (a) ITU-T Recommendation X.509 (1997): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, June 1997 and (b) RFC 5280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, April 2002 ("RFC 5280").

At a minimum, X.509 Certificates contain the basic fields and indicated prescribed values or value constraints in Table 6 below:

Field	Value or Value constraint
Serial Number	Unique value per Issuer DN
Signature Algorithm	Object identifier of the algorithm used to sign the certificate (See Section 7.1.3)
Issuer DN	See Section 7.1.4
Valid From	Universal Coordinate Time base. Encoded in accordance with RFC 5280.
Valid To	Universal Coordinate Time base. Encoded in accordance with RFC 5280.
Subject DN	See Section 7.1.4
Subject Public Key	Encoded in accordance with RFC 5280
Signature	Generated and encoded in accordance with RFC 5280

Table 6 – Certificate Profile Basic Fields

In addition, pursuant to the Qualified Certificate Profile, DL1 and DL2 Certificates also comply with RFC 3739 where it does not conflict with the Qualified Certificate Profile. Also, the basic fields within Certificates required under CP § 7.1 adhere to the requirements of the Directive to include within Certificates:

- An indication that the certificate is issued as a qualified certificate,
- The identification of the CA [Certification-Service-Provider] and the State in which it is established,
- The name of the signatory,
- Signature-verification data (subject public key),
- The beginning and end of their validity periods (valid from and valid to dates),
- The identity code of the Certificate (serial number),
- The Advanced Electronic Signature of the issuing KIBS CA.

7.1.1 Version Number(s)

VeriSign Root Certificate is X.509 Version 1 Certificate. KIBS intermediate and issuing CA certificates are X.509 Version 3 CA Certificates, as well as End-user Subscriber Certificates.

7.1.2 Certificate Extensions

KIBS populates X.509 Version 3 VTN Certificates with the extensions required by Section 7.1.2.1-7.1.2.8.

7.1.2.1 Key Usage

X.509 Version 3 Certificates are generally populated in accordance with RFC 5280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, April 2002. The KeyUsage extensions in X.509 Version 3 Certificates are configured so as to set and clear bits and the criticality field in accordance with Table 7 below. The criticality field of the KeyUsage extension is set to TRUE for ADACOM Intermediate and Issuing CA certificates and set to FALSE for end user's

		CAs	DL1 and DL2 End-User Subscribers
Criticality		TRUE	FALSE
0	digitalSignature	Clear	Set
1	nonRepudiation	Clear	Set
2	keyEncipherment	Clear	Set
3	dataEncipherment	Clear	Set
4	keyAgreement	Clear	Clear
5	keyCertSign	Set	Clear
6	CRLSign	Set	Clear
7	encipherOnly	Clear	Clear
8	decipherOnly	Clear	Clear

Table 7 – Settings for KeyUsage Extension

Note: The nonRepudiation bit⁴ is not required to be set in these Certificates because the PKI industry has not yet reached a consensus as to what the nonRepudiation bit means. Until such a consensus emerges, the nonRepudiation bit might not be meaningful for potential Relying Parties. Moreover, the most commonly used applications do not always respect the nonRepudiation bit. Therefore, setting the bit might not help Relying Parties make a trust decision. Any dispute relating to non-repudiation arising from the use of a digital certificate is a matter solely between the Subscriber and the Relying Party(s). VeriSign shall incur no liability in relation thereto.

7.1.2.2 Certificate Policies Extension

CertificatePolicies extension of X.509 Version 3 Certificates are populated with the object identifier for the VTN CP in accordance with CP and this CPS Section 7.1.6 and with policy qualifiers set forth in CP and this CPS Section 7.1.8. The criticality field of this extension is set to FALSE.

7.1.2.3 Private Certificate Extensions (QC Statement)

DL1 and DL2 Certificates contain a private extension containing an OID identifying the statement stating that the Certificate is issued in accordance with the Directive. Such extension conforms to the definition in section 4.2.1(2) of the Qualified Certificate Profile. This extension for KIBS DL1 and DL2 Certificates is marked as not critical.

7.1.2.4 Subject Alternative Names

The subjectAltName extension of X.509 Version 3 Certificates is populated in accordance with RFC 5280. The criticality field of this extension is set to FALSE.

⁴ The nonRepudiation bit may also be referred to as ContentCommitment in Digital Certificates in accordance with the X.509 standard.

7.1.2.5 Basic Constraints

KIBS X.509 Version 3 CA Certificates BasicConstraints extension have the CA field set to TRUE. End-user Subscriber Certificates BasicConstraints extension, are populated with a value of an empty sequence. The criticality field of this extension is set to TRUE for CA Certificates, but FALSE for end-user Subscriber Certificates.

KIBS X.509 Version 3 CA Certificates have a “pathLenConstraint” field of the BasicConstraints extension set to the maximum number of CA certificates that may follow this Certificate in a certification path.

7.1.2.6 Extended Key Usage

KIBS makes use of the ExtendedKeyUsage extension for the DL1 and DL2 certificates.

For these Certificates, KIBS populates the ExtendedKeyUsage extension in accordance with Table 8 below.

	DL1 and DL2 Certificates
Criticality	<i>FALSE</i>
ServerAuth	Clear
ClientAuth	Set
CodeSigning	Clear
EmailProtection	Set
ipsecEndSystem	Clear
ipsecTunnel	Clear
ipsecUser	Clear
TimeStamping	Clear
OCSP Signing	Clear

Table 8 – Settings for ExtendedKeyUsage Extension

7.1.2.7 CRL Distribution Points

KIBS end user Subscriber Certificates, Intermediate and Issuing CA Certificates include the cRLDistributionPoints extension containing the URL of the location where a Relying Party can obtain a CRL to check the CA Certificate’s status. The criticality field of this extension is set to FALSE.

7.1.2.8 Authority Key Identifier

DL1 and DL2 Certificates and the Issuing CA Certificate, include the Authority Key Identifier extension. The Authority Key Identifier is composed of the 160-bit SHA-1 hash of the public key of the CA issuing the Certificate. The criticality field of this extension is set to FALSE.

7.1.2.9 Subject Key Identifier

For DL1 and DL2 Certificates, the Intermediate and Issuing CAs, the Subject Key Identifier extension is included. The keyIdentifier based on the public key of the Subject of the Certificate is generated in accordance with one of the methods described in RFC 5280. The criticality field of this extension is set to FALSE.

7.1.3 Algorithm Object Identifiers

KIBS Certificates are signed with:

sha-1WithRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840)
rsadsi(113549) pkcs(1) pkcs-1(1) 5}

(OID: 1.2.840.113549.1.1.5))

Certificate signatures produced using these algorithms shall comply with RFC 3279.

7.1.4 Name Forms

KIBS populates Certificates with an Issuer and Subject Distinguished Name in accordance with Section 3.1.1.

In addition, KIBS includes within end-user Subscriber Certificates an additional Organizational Unit field that contains a notice stating that the terms of use of the Certificate are set forth in a URL which is a pointer to the applicable Relying Party Agreement.

7.1.5 Name Constraints

No stipulation.

7.1.6 Certificate Policy Object Identifier

VeriSign, acting as the policy-defining authority, has assigned an object identifier value extension for each Class of Certificate issued under the Verisign Trust Network (VTN).

Qualified Certificates (DL1 and DL2), contain two additional OIDs:

1. The OID for Class 2 Certificate Policy: VeriSign/pki/policies/vtn-cp/class2 (2.16.840.1.113733.1.7.23.2).⁵
2. The OID specified by the ETSI Policy Document (ETSI TS 101 456) for the Qualified Certificates:
 - o For DL1 certificates (0.4.0.1456.1.2)
 - o For DL2 certificates (0.4.0.1456.1.1)

7.1.7 Usage of Policy Constraints Extension

No stipulation.

7.1.8 Policy Qualifiers Syntax and Semantics

KIBS populates X.509 Version 3 VTN Certificates with a policy qualifier within the Certificate Policies extension. Such Certificates contain a CPS pointer qualifier that points to this CPS.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No stipulation.

⁵ Due to the fact, that Qualified Certificates are signed under the VeriSign Class 2 Root CA.

7.2 CRL Profile

CRLs contain the basic fields and contents specified in Table 9 below:

Field	Value or Value constraint
Version	See Section 7.2.1.
Signature Algorithm	Algorithm used to sign the CRL. For DL1 and DL2 algorithm used to sign the CRL is the sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5)
Issuer	Entity that has signed and issued the CRL.
Effective Date	Issue date of the CRL. CRLs are effective upon issuance.
Next Update	Date by which the next CRL will be issued. CRL issuance frequency is in accordance with the requirements of Section 4.4.7.
Revoked Certificates	Listing of revoked certificates, including the Serial Number of the revoked Certificate and the Revocation Date.

Table 9 – CRL Profile Basic Fields

7.2.1 Version Number(s)

KIBS issues Version 2 CRLs. For the KIBS Class 2 CA (Intermediate CA), VeriSign issues Version 1 CRLs.

The CRLs comply with the requirements of RFC 5280.

7.2.2 CRL and CRL Entry Extensions

No stipulation.

7.3 OCSP Profile

OCSP (Online Certificate Status Protocol) is a way to obtain timely information about the revocation status of a particular certificate. KIBS does not provide OCSP services for the DL1 and DL2 certificates.

7.3.1 Version Number(s)

Not applicable.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

An annual audit is performed for ADACOM's data center operations and key management operations supporting ADACOM's public Qualified CA services.

In addition to compliance audits, KIBS is entitled to perform other reviews and investigations under this CPS and ADACOM's CPS to ensure the trustworthiness of KIBS's Subdomain of the VTN, which include, but are not limited to:

- KIBS is entitled, within its sole and exclusive discretion, to perform at any time an "Exigent Audit/Investigation" on itself in the event KIBS has experienced an incident or compromise, or has acted or failed to act, such the way that poses an actual or potential threat to the security or integrity of the VTN.
- KIBS is entitled to perform "Supplemental Risk Management Reviews" on itself following incomplete or exceptional findings in a Compliance Audit or as part of the overall risk management process in the ordinary course of business.

KIBS is entitled to delegate the performance of these audits, reviews, and investigations to a third party audit firm. Entities that are subject to an audit, review, or investigation shall provide reasonable cooperation with KIBS and the personnel performing the audit, review, or investigation.

Additionally, a periodic compliance, with the law and this CPS, audit is performed, by the control bodies according to the law.

8.1 Frequency and Circumstances of Assessment

KIBS Compliance Audits are conducted at least annually. KIBS customer audits are conducted at the sole expense of the audited entity.

8.2 Identity/Qualifications of Assessor

ADACOM's CA compliance audits are performed by:

- ADACOM internally, by Qualified IT Auditors, and
- The control bodies according to the law, or
- An accounting firm that demonstrates proficiency in public key infrastructure technology, information security tools and techniques and security auditing.

8.3 Topics Covered by Assessment

The scope of ADACOM's annual audit includes CA environmental controls, key management operations and Infrastructure/Administrative CA controls, certificate life cycle management and CA business practices disclosure.

8.4 Actions Taken as a Result of Deficiency

With respect to compliance audits of ADACOM's operations, significant exceptions or deficiencies identified during the Compliance Audit will result in a determination of actions to be taken. This determination is made by ADACOM management with input from the auditor. ADACOM management is responsible for developing and implementing a corrective action plan. If ADACOM determines that such exceptions or deficiencies pose an immediate threat to the security or integrity of the VTN, a corrective action plan will be developed within 30 days and

implemented within a reasonable period of time. For less serious exceptions or deficiencies, ADACOM management will evaluate the significance of such issues and determine the appropriate course of action.

8.5 *Communications of Results*

Results of the compliance audit of ADACOM's operations may be released at the discretion of ADACOM Management.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

KIBS charges end-user Subscribers for the issuance, management, and renewal of Certificates.

9.1.2 Certificate Access Fees

KIBS does not charge a fee as a condition of making a Certificate available in a repository or otherwise making Certificates available to Relying Parties.

9.1.3 Revocation or Status Information Access Fees

KIBS does not charge a fee as a condition of making the CRLs required by this CP available in a repository or otherwise available to Relying Parties. KIBS does not permit access to revocation information, Certificate status information, or time stamping in their repositories by third parties that provide products or services that utilize such Certificate status information without KIBS 's prior express written consent.

9.1.4 Fees for Other Services

KIBS does not charge a fee for access to this CPS. Any use made for purposes other than simply viewing the document, such as reproduction, redistribution, modification, or creation of derivative works, shall be subject to a license agreement with KIBS.

9.1.5 Refund Policy

No Stipulation.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

KIBS maintains a commercially reasonable level of insurance coverage for errors and omissions according to insurance Policy published on: <http://ca.kibs.com.mk/repository>.

9.2.2 Other Assets

KIBS has sufficient financial resources to maintain its operations and perform its duties, and is reasonably able to bear the risk of liability to Subscribers and Relying Parties. Proofs of financial resources are not made publicly available.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

The following records of Subscribers shall, subject to Section 9.3.2, be kept confidential and private ("Confidential Information"):

- CA application records, whether approved or disapproved,

- Certificate Application records,
- Transactional records (both full records and the audit trail of transactions),
- Audit trail records created or retained by KIBS or a Customer,
- Audit reports created by KIBS or other auditors (whether internal or public),
- and
- Security measures controlling the operations of KIBS hardware and software and the administration of Certificate services and designated enrollment services.

9.3.2 Information Not Within the Scope of Confidential Information

Certificates, Certificate revocation and other status information, KIBS repositories and information contained within them are not considered Confidential Information. Information not expressly deemed Confidential Information under Section 9.3.1 is not considered confidential. This section is subject to applicable privacy laws.

9.3.3 Responsibility to Protect Confidential Information

KIBS secures confidential information from compromise and disclosure to third parties.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

KIBS has implemented a Privacy Policy, which is located at: <http://ca.kibs.com.mk/repository> in compliance with CP § 2.8 and the law.

9.4.2 Information Treated as Private

Any information about Subscribers that is not publicly available through the content of the issued certificate, certificate directory and online CRLs is treated as private.

9.4.3 Information Not Deemed Private

All information made public in a certificate is deemed not private.

9.4.4 Responsibility to Protect Private Information

KIBS and all its Subdomain Participants receiving private information shall secure it from compromise and disclosure to third parties and shall comply with all privacy laws in their jurisdiction.

9.4.5 Notice and Consent to Use Private Information

Unless where otherwise stated in this CPS, the applicable Privacy Policy or by agreement, private information are not used without the consent of the party to whom that information applies, in accordance with applicable privacy law.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

KIBS shall be entitled to disclose Confidential Information if, in good faith, KIBS believes that:

- disclosure is necessary in response to subpoenas and search warrants.
- disclosure is necessary in response to judicial, administrative, or other legal process during the discovery process in a civil or administrative action, such as subpoenas, interrogatories, requests for admission, and requests for production of documents.

This section is subject to applicable privacy laws.

9.4.7 Disclosure upon Owner's Request

KIBS's privacy policy contains provisions relating to the disclosure of private Information to the person disclosing it to KIBS.

9.4.8 Other Information Disclosure Circumstances

No stipulation.

9.5 Intellectual Property rights

The allocation of Intellectual Property Rights among KIBS Subdomain Participants other than Subscribers and Relying Parties is governed by the applicable agreements among such KIBS Subdomain Participants. The following subsections of Section 9.5 apply to the Intellectual Property Rights in relation to Subscribers and Relying Parties.

9.5.1 Property Rights in Certificates and Revocation Information

KIBS CAs retain all Intellectual Property Rights in and to the Certificates and revocation information that they issue. KIBS grants permission to reproduce and distribute Certificates on a nonexclusive royalty-free basis, provided that they are reproduced in full and that use of Certificates is subject to the Relying Party Agreement referenced in the Certificate. KIBS grants permission to use revocation information to perform Relying Party functions subject to the applicable Relying Party Agreement, or any other applicable agreements.

9.5.2 Property Rights in the CPS

KIBS Subscribers and Relying Parties acknowledge that KIBS retains all Intellectual Property Rights in and to this CPS.

9.5.3 Property Rights in Names

A Certificate Applicant retains all rights it has (if any) in any trademark, service mark, or trade name contained in any Certificate Application and distinguished name within any Certificate issued to such Certificate Applicant.

9.5.4 Property Rights in Keys and Key Material

Key pairs corresponding to Certificates of CAs and end-user Subscribers are the property of the CAs and end-user Subscribers that are the respective Subjects of these Certificates, regardless of the physical medium within which they are stored and protected, and such persons retain all Intellectual Property Rights in and to these key pairs. Without limiting the generality of the foregoing, VeriSign's root public keys and the root Certificates containing them, including all PCA public keys and self-signed Certificates, are the property of VeriSign. VeriSign licenses software and hardware manufacturers to reproduce such root Certificates to place copies in trustworthy hardware devices or software. Finally, Secret Shares of a CA's private key are the property of the

CA, and the CA retains all Intellectual Property Right in and to such Secret Shares even though they cannot obtain physical possession of those shares or the CA from VeriSign or KIBS.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

KIBS CA warrants that:

- There are no material misrepresentations of fact in the Certificate known to or originating from the entities approving the Certificate Application or issuing the Certificate,
- There are no errors in the information in the Certificate that were introduced by the entities approving the Certificate Application or issuing the Certificate as a result of a failure to exercise reasonable care in managing the Certificate Application or creating the Certificate,
- Their Certificates meet all material requirements of this CPS, and
- Revocation services and use of a repository conform to the applicable CPS in all material aspects.

KIBS Subscriber Agreement may include additional representations and warranties.

9.6.2 RA Representations and Warranties

KIBS RAs warrant that:

- There are no material misrepresentations of fact in the Certificate known to or originating from the entities approving the Certificate Application or issuing the Certificate,
- There are no errors in the information in the Certificate that were introduced by the entities approving the Certificate Application as a result of a failure to exercise reasonable care in managing the Certificate Application,
- Their Certificates meet all material requirements of this CPS,
- Revocation services (when applicable) and use of a repository conform to the applicable CPS in all material aspects, and
- Meet the requirements of CPS.

KIBS Subscriber Agreement may include additional representations and warranties.

9.6.3 Subscriber Representations and Warranties

Subscribers warrant that:

- Each digital signature created using the private key corresponding to the public key listed in the Certificate is the digital signature of the Subscriber and the Certificate has been accepted and is operational (not expired or revoked) at the time the digital signature is created,
- Their private key is protected and that no unauthorized person has ever had access to the Subscriber's private key,
- All representations made by the Subscriber in the Certificate Application the Subscriber submitted are true,
- All information supplied by the Subscriber and contained in the Certificate is true,

- The Certificate is being used exclusively for authorized and legal purposes, consistent with this CPS, and
- The Subscriber is an end-user Subscriber and not a CA, and is not using the private key corresponding to any public key listed in the Certificate for purposes of digitally signing any Certificate (or any other format of certified public key) or CRL, as a CA or otherwise.

KIBS Subscriber Agreement may include additional representations and warranties.

9.6.4 Relying Party Representations and Warranties

KIBS Relying Party Agreement require Relying Parties to acknowledge that they have sufficient information to make an informed decision as to the extent to which they choose to rely on the information in a Certificate, that they are solely responsible for deciding whether or not to rely on such information, and that they shall bear the legal consequences of their failure to perform the Relying Party obligations in terms of this CPS.

KIBS Relying Party Agreement contains a warranty to Relying Party who reasonably relies on Qualified Certificate to verify a digital signature that:

- The Qualified Certificate contains all the details prescribed for a Qualified Certificate under the Directive,
- The Subscriber of such Qualified Certificate held the private key corresponding to the public key within such Qualified Certificate at the time the Qualified Certificate was issued, and
- The CA and the RA exercises reasonable care to provide notice of the revocation of Qualified Certificates in accordance with CP §§ 4.9.7, 4.9.9.

KIBS Relying Party Agreement may include additional representations and warranties. KIBS Subscriber Agreement also contains the foregoing warranties and applies to the extent Subscribers also act as Relying Parties.

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimers of Warranties

KIBS, Subscriber Agreement and Relying Party Agreement disclaim KIBS's possible warranties, including any warranty of merchantability or fitness for a particular purpose.

9.8 Obligations for CAs issuing Qualified Certificates

KIBS Qualified CA also meets the CA requirements set forth in the EDP.

KIBS Subscriber Agreement is in writing and in readily understandable language. Furthermore, KIBS Subscriber Agreement contain the following terms required by the Directive, the Law and the ETSI Policy Document:

- The applicable policy, whether DL1 or DL2, including a clear statement as to whether the use of an SSCD is required or not,
- An acknowledgement that the information contained in the Certificate is correct unless the Subscriber informs the applicable CA or RA otherwise,
- Applicable limitations on use, which at a minimum include the limitations in CPS § 9.9.,

- The obligations of Subscribers set forth in this section and assent to perform such obligations,
- Information on how to validate a Certificate, including a requirement to check the status of a Certificate, and the conditions upon which reliance on a Certificate is deemed “reasonable” which apply to situations where Subscribers also act as Relying Parties,
- Applicable limitations of liability,
- Consent to the publication of the Certificate issued to the Subscriber and its availability for retrieval by Relying Parties,
- Consent to the retention of records used in enrollment, the provision of an SSCD to the Subscriber, revocation information, and the transition of such information to third parties in the event of CA termination,
- The records retention period for Certificate Application information,
- The records retention period for CA event logs,
- Applicable dispute resolution procedures,
- Governing law, and
- Whether the CA has been certified to be conformant with the DL1 Certificate policies or with the DL2 Certificate policies.

KIBS Subscriber Agreement is communicated to Certificate Applicants before they submit enrollment information and with means that preserve the integrity of the Subscriber Agreement. Prior to the issuance of a new Certificate upon renewal or rekeying, any changes to Subscriber Agreement implemented since the time of the last enrollment or re-enrollment are communicated to the Subscriber with means that preserve the integrity of the Subscriber Agreement.

KIBS Relying Party Agreement is in writing and in readily understandable language. Furthermore, KIBS Relying Party Agreement contain the following terms required by the ETSI Policy Document:

- The applicable policy, whether DL1 or DL2, including a clear statement as to whether Subscribers are required to use an SSCD or not,
- Applicable limitations on use, which at a minimum include the limitations in CPS § 1.4.2,
- Information on how to validate a Certificate, including a requirement to check the status of a Certificate, and the conditions upon which reliance on a Certificate is deemed “reasonable”
- Applicable limitations of liability,
- The records retention period for Certificate Application information,
- The records retention period for CA event logs,
- Applicable dispute resolution procedures,
- Governing law, and
- Whether the CA has been certified to be conformant with the DL1 Certificate policies or with the DL2 Certificate policies.

9.9 Limitations of Liability

KIBS Subscriber Agreement and Relying Party Agreement limit KIBS’s liability. Limitations of liability include an exclusion of indirect, special, incidental, and consequential damages. They

also include the liability cap of the amount, as set forth in the applicable KIBS Insurance Policy) limiting KIBS's damages concerning a DL1 or DL2 Certificate.

The liability (and/or limitation thereof) of Subscribers is as set forth in the applicable Subscriber agreements.

The liability (and/or limitation thereof) of Relying Parties is as set forth in the applicable Relying Party Agreements.

9.10 Indemnities

9.10.1 Indemnification by Subscribers

Subscribers are required to indemnify KIBS for:

- Falsehood or misrepresentation of fact by the Subscriber on the Subscriber's Certificate Application,
- Failure by the Subscriber to disclose a material fact on the Certificate Application, if the misrepresentation or omission was made negligently or with intent to deceive any party,
- The Subscriber's failure to protect the Subscriber's private key, to use a Trustworthy System, or to otherwise take the precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorized use of the Subscriber's private key, or
- The Subscriber's use of a name (including without limitation within a common name, domain name, or e-mail address) that infringes upon the Intellectual Property Rights of a third party.

The Subscriber Agreement may include additional indemnity obligations.

9.10.2 Indemnification by Relying Parties

KIBS Relying Party Agreement requires Relying Parties to indemnify KIBS for:

- The Relying Party's failure to perform the obligations of a Relying Party,
- The Relying Party's reliance on a Certificate that is not reasonable under the circumstances, or
- The Relying Party's failure to check the status of such Certificate to determine if the Certificate is expired or revoked.

The Relying Party Agreement may include additional indemnity obligations.

9.11 Term and Termination

9.11.1 Term

The CPS becomes effective upon publication in the KIBS repository. Amendments to this CPS become effective upon publication in the KIBS repository.

9.11.2 Termination

This CPS as amended from time to time remains in force until it is replaced by a new version.

9.11.3 Effect of Termination and Survival

Upon termination of this CPS, KIBS Subdomain Participants are nevertheless bound by its terms for all certificates issued for the remainder of the validity periods of such certificates.

9.12 Individual Notices and Communications with Participants

Unless otherwise specified by agreement between the parties, KIBS Subdomain Participants shall use commercially reasonable methods to communicate with each other, taking into account the criticality and subject matter of the communication.

9.13 Amendments

9.13.1 Procedure for Amendment

Amendments to this CPS are made by the KIBS Practices Development Group (KPDG). Amendments are incorporated in new version of CPS published at <https://ca.kibs.com.mk/repository/cps>. New version of CPS supersedes any designated or conflicting provisions of the previous version of the CPS.

9.13.2 Notification Mechanism and Period

KIBS reserve the right to amend the CPS without notification.

9.13.2.1 Comment Period

Not applicable.

9.13.2.2 Mechanism to Handle Comments

No stipulation.

9.13.3 Circumstances under Which OID Must be Changed

If the KPDG, in cooperation with VeriSign, determines that a change is necessary in the object identifier corresponding to a Certificate policy, the amendment contains new object identifiers for the Certificate policies corresponding to each Class of Certificate. Otherwise, amendments are not requiring a change in Certificate policy object identifier.

9.14 Dispute Resolution Provisions

9.14.1 Disputes among VeriSign, Affiliates, and Customers

No stipulation.

9.14.2 Disputes with End-User Subscribers or Relying Parties

KIBS Subscriber Agreements and Relying Party Agreements contain a dispute resolution clause. Disputes involving KIBS require an initial negotiation period of sixty (60) days followed by litigation in the court of Skopje.

9.15 Governing Law

The Macedonian law governs the enforceability, construction, interpretation, and validity of this CPS, irrespective of contract or other choice of law.

This governing law provision applies only to this CPS. Agreements incorporating the CPS by reference may have their own governing law provisions, provided that this Section 9.14 governs the enforceability, construction, interpretation, and validity of the terms of the CPS separate and apart from the remaining provisions of any such agreements, subject to any limitations appearing in applicable law.

9.16 Compliance with Applicable Law

This CPS is subject to Macedonian laws.

9.17 Miscellaneous Provisions

9.17.1 Entire Agreement

Not applicable.

9.17.2 Assignment

Not applicable.

9.17.3 Severability

In the event that a clause or provision of this CPS is held to be unenforceable by a court of law or other tribunal having authority, the remainder of the CPS shall remain valid.

9.17.4 Enforcement (Attorney's Fees and Waiver of Rights)

Not applicable.

9.17.5 Force Majeure

KIBS Subscriber Agreement and Relying Party Agreement include a force majeure clause protecting KIBS.

9.18 Other Provisions

Not applicable.

Appendix A. Table of Acronyms and definitions

Table of Acronyms

Term	Definition
CA	Certification Authority.
CP	Certificate Policy.
CPS	Certification Practice Statement.
CRL	Certificate Revocation List.
EAL	Evaluation assurance level (pursuant to the Common Criteria).
FIPS	United State Federal Information Processing Standards.
KPDG	KIBS Practices Development Group
LSVA	Logical security vulnerability assessment.
OCSP	Online Certificate Status Protocol.
PCA	Primary Certification Authority.
PIN	Personal identification number.
PKCS	Public-Key Cryptography Standard.
PKI	Public Key Infrastructure.
PMA	Policy Management Authority.
RA	Registration Authority.
RFC	Request for comment.
S/MIME	Secure multipurpose Internet mail extensions.
SSL	Secure Sockets Layer.
VTN	VeriSign Trust Network.

Definitions

Term	Definition
Administrator	A Trusted Person within the organization of a Processing Center, Service Center or Managed PKI Customer, that performs validation and other CA or RA functions.
Administrator Certificate	A Certificate issued to an Administrator that may only be used to perform CA or RA functions.
Affiliate	A leading trusted third party, for example in the technology, telecommunications, or financial services industry, that has entered into an agreement with VeriSign to be a VTN distribution and services channel within a specific territory.
Certificate	A message that, at least, states a name or identifies the CA, identifies the Subscriber, contains the Subscriber's public key, identifies the Certificate's Operational Period, contains a Certificate serial number, and is digitally signed by the CA.
Certificate Applicant	An individual or organization that requests the issuance of a Certificate by a CA.
Certificate Application	A request from a Certificate Applicant (or authorized agent of the Certificate Applicant) to a CA for the issuance of a Certificate.
Certificate Chain	An ordered list of Certificates containing an end-user Subscriber Certificate and CA Certificates, which terminates in a root Certificate.
Certificate Policies (CP)	The document, which is entitled "VeriSign Trust Network Certificate Policies" and is the principal statement of policy governing the VTN.
Certificate Revocation List (CRL)	A periodically (or exigently) issued list, digitally signed by a CA, of identified Certificates that have been revoked prior to their expiration dates. The list generally indicates the CRL issuer's name, the date of issue, the date of the next scheduled CRL issue, the revoked Certificates' serial numbers, and the specific times and reasons for revocation.
Certificate Signing	A message conveying a request to have a Certificate issued.

Term	Definition
Request	
Certification Authority (CA)	An entity authorized to issue, manage, revoke, and renew Certificates in the VTN.
Certification Practice Statement (CPS)	This document which states the practices that KIBS employs in approving or rejecting Certificate Applications and issuing, managing, and revoking Certificates, and requires its Customers to employ.
Challenge Phrase	A secret phrase chosen by a Certificate Applicant during enrollment for a Certificate. When issued a Certificate, the Certificate Applicant becomes a Subscriber and a CA or RA can use the Challenge Phrase to authenticate the Subscriber when the Subscriber seeks to revoke or renew the Subscriber's Certificate.
Class	A specified level of assurances as defined within the CP. See CP § 1.1.1.
Client Service Center	A Service Center that is ADACOM providing client Certificates either in the Consumer or Enterprise line of business.
Compliance Audit	A periodic audit that a Processing Center, Service Center or Managed PKI Customer undergoes to determine its conformance with VTN Standards that apply to it.
Compromise	A violation (or suspected violation) of a security policy, in which an unauthorized disclosure of, or loss of control over, sensitive information may have occurred. With respect to private keys, a Compromise is a loss, theft, disclosure, modification, unauthorized use, or other compromise of the security of such private key.
Confidential/Private Information	Information required to be kept confidential and private pursuant to CP § 2.8.1.
CRL Usage Agreement	An agreement setting forth the terms and conditions under which a CRL or the information in it can be used.
Enterprise, as in Enterprise Service Center	A line of business that ADACOM enters to provide Managed PKI services to Managed PKI Customers.
Exigent Audit/Investigation	An audit or investigation by VeriSign or ADACOM where ADACOM has reason to believe that an entity failure to meet VTN Standards, an incident or Compromise relating to the entity, or an actual or potential threat to the security of the VTN posed by the entity has occurred.
Intellectual Property Rights	Rights under one or more of the following: any copyright, patent, trade secret, trademark, and any other intellectual property rights.
Intermediate Certification Authority (Intermediate CA)	A Certification Authority whose Certificate is located within a Certificate Chain between the Certificate of the root CA and the Certificate of the Certification Authority that issued the end-user Subscriber's Certificate.
Key Generation Ceremony	A procedure whereby a CA's or RA's key pair is generated, its private key is transferred into a cryptographic module, its private key is backed up, and/or its public key is certified.
KIBS Practices Development Group	The group within KIBS responsible for promulgating this policy.
KIBS Repository	KIBS's database of Certificates and other relevant KIBS CA information accessible on-line.
Managed PKI	ADACOM's fully integrated managed PKI service that allows enterprise Customers of ADACOM to distribute Certificates to individuals, such as employees, partners, suppliers, and customers. Managed PKI permits enterprises to secure messaging, and e-commerce applications.
Manual Authentication	A procedure whereby Certificate Applications are reviewed and approved manually one-by-one by an Administrator using a web-based interface.
Nonverified Subscriber Information	Information submitted by a Certificate Applicant to a CA or RA, and included within a Certificate, that has not been confirmed by the CA or RA and for which the applicable CA and RA provide no assurances other than that the information was submitted by the Certificate Applicant.
Non-repudiation	An attribute of a communication that provides protection against a party to a

Term	Definition
	communication falsely denying its origin, denying that it was submitted, or denying its delivery. Denial of origin includes the denial that a communication originated from the same source as a sequence of one or more prior messages, even if the identity associated with the sender is unknown. Note: only an adjudication by a court, arbitration panel, or other tribunal can ultimately prevent repudiation. For example, a digital signature verified with reference to a VTN Certificate may provide proof in support of a determination of Non-repudiation by a tribunal, but does not by itself constitute Non-repudiation.
Offline CA	VeriSign PCAs Issuing Root CAs and other designated intermediate CAs that are maintained offline for security reasons in order to protect them from possible attacks by intruders by way of the network. These CAs do not directly sign end user Subscriber Certificates.
Online CA	CAs that sign end user Subscriber Certificates are maintained online so as to provide continuous signing services.
Online Certificate Status Protocol (OCSP)	A protocol for providing Relying Parties with real-time Certificate status information.
Operational Period	The period starting with the date and time a Certificate is issued (or on a later date and time certain if stated in the Certificate) and ending with the date and time on which the Certificate expires or is earlier revoked.
PKCS #10	Public-Key Cryptography Standard #10, developed by RSA Security Inc., which defines a structure for a Certificate Signing Request.
PKCS #12	Public-Key Cryptography Standard #12, developed by RSA Security Inc., which defines a secure means for the transfer of private keys.
Policy Management Authority (PMA)	The organization within VeriSign responsible for promulgating this policy throughout the VTN.
Primary Certification Authority (PCA)	A CA that acts as a root CA for a specific Class of Certificates, and issues Certificates to CAs subordinate to it.
Processing Center	The ADACOM site that creates a secure facility housing, among other things, the cryptographic modules used for the issuance of Certificates. In the Consumer and Web Site lines of business, Processing Centers act as CAs within the VTN and perform all Certificate lifecycle services of issuing, managing, revoking, and renewing Certificates. In the Enterprise line of business, Processing Centers provide lifecycle services on behalf of their Managed PKI Customers or the Managed PKI Customers of the Service Centers subordinate to them.
Public Key Infrastructure (PKI)	The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a Certificate-based public key cryptographic system. The VTN PKI consists of systems that collaborate to provide and implement the VTN.
Registration Authority (RA)	An entity approved by a CA to assist Certificate Applicants in applying for Certificates, and to approve or reject Certificate Applications, revoke Certificates, or renew Certificates.
Relying Party	An individual or organization that acts in reliance on a certificate and/or a digital signature.
Relying Party Agreement	An agreement used by a CA setting forth the terms and conditions under which an individual or organization acts as a Relying Party.
RSA	A public key cryptographic system invented by Rivest, Shamir, and Adelman.
Secret Share	A portion of a CA private key or a portion of the activation data needed to operate a CA private key under a Secret Sharing arrangement.
Secret Sharing	The practice of splitting a CA private key or the activation data to operate a CA private key in order to enforce multi-person control over CA private key operations under CP § 6.2.2.
Secure Server ID	A Class 3 organizational Certificate used to support SSL sessions between web browsers and web servers.
Secure Sockets Layer (SSL)	The industry-standard method for protecting Web communications developed by Netscape Communications Corporation. The SSL security protocol provides data encryption, server authentication, message integrity, and optional client authentication for a Transmission Control Protocol/Internet Protocol connection.

Term	Definition
Security and Audit Requirements Guide	A VeriSign document that sets forth the security and audit requirements and practices for Processing Centers and Service Centers.
Service Center	The ADACOM operation that does not house Certificate signing units for the issuance of Certificates for the purpose of issuing Certificates of a specific Class or type, but rather relies on a Processing Center to perform issuance, management, revocation, and renewal of such Certificates.
Subdomain	The portion of the VTN under control of an entity and all entities subordinate to it within the VTN hierarchy.
Subject	The holder of a private key corresponding to a public key. The term "Subject" can, in the case of an organizational Certificate, refer to the equipment or device that holds a private key. A Subject is assigned an unambiguous name, which is bound to the public key contained in the Subject's Certificate.
Subscriber	In the case of an individual Certificate, a person who is the Subject of, and has been issued, a Certificate. In the case of an organizational Certificate, an organization that owns the equipment or device that is the Subject of, and that has been issued, a Certificate. A Subscriber is capable of using, and is authorized to use, the private key that corresponds to the public key listed in the Certificate.
Subscriber Agreement	An agreement used by a CA or RA setting forth the terms and conditions under which an individual or organization acts as a Subscriber.
Superior Entity	An entity above a certain entity within a VTN hierarchy (the Class 1, or 3 hierarchy).
Trusted Person	An employee, contractor, or consultant of an entity within the VTN responsible for managing infrastructural trustworthiness of the entity, its products, its services, its facilities, and/or its practices as further defined in CP § 5.2.1.
Trusted Position	The positions within a VTN entity that must be held by a Trusted Person.
Trustworthy System	Computer hardware, software, and procedures that are reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable security policy. A trustworthy system is not necessarily a "trusted system" as recognized in classified government nomenclature.
VeriSign	Means, with respect to each pertinent portion of this CPS, VeriSign, Inc. and/or any wholly owned VeriSign subsidiary responsible for the specific operations at issue.
VeriSign Trust Network (VTN)	The Certificate-based Public Key Infrastructure governed by the VeriSign Trust Network Certificate Policies, which enables the worldwide deployment and use of Certificates by VeriSign and its Affiliates, and their respective Customers, Subscribers, and Relying Parties.
VTN Participant	An individual or organization that is one or more of the following within the VTN: VeriSign, ADACOM, a Customer, a Universal Service Center, a Reseller, a Subscriber, or a Relying Party.
VTN Standards	The business, legal, and technical requirements for issuing, managing, revoking, renewing, and using Certificates within the VTN.