FRCS VMS PKI

CERTIFICATE POLICY/ CERTIFICATION PRACTICE STATEMENT

OIDs: 1.3.6.1.4.1.49952.3.2.4.1
1.3.6.1.4.1.49952.3.2.4.2

Effective Date: 27 Dec 2017

Version: 1.0

Important Note About this Document

This is the Certificate Policy/Certification Practice Statement (CP/CPS) of FRCS VMS Public Key Infrastructure (FRCS VMS PKI). It contains an overview of the practices and procedures that FRCS VMS PKI employs as a Certification Authority (CA). This document is not intended to create contractual relationships between FRCS and any other person. This document is intended for use only in connection with FRCS and its business. This version of the CP/CPS has been approved for use by the FRCS VMS Policy Management Authority (PMA) and is subject to amendment and change in accordance with the policies and guidelines adopted, from time to time, by the PMA and as otherwise set out herein. The date on which this version of the CP/CPS becomes effective is indicated on this CP/CPS. The most recent effective copy of this CP/CPS supersedes all previous versions. No provision is made for different versions of this CP/CPS to remain in effect at the same time.

Contact Information:

Revenue & Customs Services Complex

Lot 1 Corner of Queen Elizabeth Drive & Ratu Sukuna Road, Nasese,

Suva

https://www.frcs.org.fj/our-services/vat-monitoring-system-vms/

efdcompliance@frcs.org.fj

Version Control:

Author	Date	Version	Comment
FRCS VMS PMA	12/27/2017	1.0	Initial version

Table of Contents

1 INTRODUCTION

1.1 Overview

This FRCS VMS CP/CPS sets out the policies, processes and procedures followed in the generation, issue, use and management of Key Pairs and Digital Certificates. It also describes the roles, responsibilities and relationships of Participants within the FRCS VMS PKI.

FRCS VMS PKI is support process for FRCS Vat Monitoring System (VMS) and it usage is limited to FRCS VMS requirements regarding Digital Certificates usage. FRCS VMS PKI is managed by third party, company Data Tech International (DTI), but operated by FRCS VMS (outsourced services).

The structure of this CP/CPS is based on the RFC 3647 Certificate Policy and Certification Practices Framework but does not seek to adhere to or follow it exactly.

This CP/CPS undergoes a regular review process and is subject to amendment as prescribed by the FRCS VMS Policy Management Authority.

1.2 Document Name, Identification and Applicability

The Private Enterprise Object Identifier (OID) assigned by the Internet Assigned Numbers Authority to Data Tech International (DTI) is 1.3.6.1.4.1.**49952**.

Data Tech International (DTI) assigned 1.3.6.1.4.1.49952.**3.2** OID for FRCS VMS

1.3.6.1.4.1.49952.3.2	OID for FRCS VMS
1.3.6.1.4.1.49952.3.2.1	OID for FRCS VMS CP
1.3.6.1.4.1.49952.3.2.2	OID for FRCS VMS CPS
1.3.6.1.4.1.49952.3.2.3.1	OID for FRCS VMS Certificate Type Web Site Class1
1.3.6.1.4.1.49952.3.2.3.2	OID for FRCS VMS Certificate Type Client Authenticate Class1
1.3.6.1.4.1.49952.3.2.3.3	OID for FRCS VMS Certificate Type Invoice Signing Class2
1.3.6.1.4.1.49952.3.2.3.4	OID for FRCS VMS Certificate Type Client Authenticate Class2
1.3.6.1.4.1.49952.3.2.3.5	OID for FRCS VMS Certificate Type Invoice Signing Class1
1.3.6.1.4.1.49952.3.2.3.6	OID for FRCS VMS Certificate Type Encrypting Message Class1
1.3.6.1.4.1.49952.3.2.4.1	OID for FRCS VMS Issuing Policy Class1
1.3.6.1.4.1.49952.3.2.4.2	OID for FRCS VMS Issuing Policy Class2
1.3.6.1.4.1.49952.3.2.5	FRCS VMS service URL for E-SDC
1.3.6.1.4.1.49952.3.2.6	Taxpayer Identification Number (TIN)

1.3 Public Key Infrastructure Participants

FRCS VMS Issuing CA service holds

- FRCS VMS Root Certificate Authority
    - digitally creates, signs, issues, revoke Issuing CA Certificates using the Root Certificate
- FRCS VMS Issuing Certificate Authority
    - digitally creates, signs, issues, revoke (Certificates Holders) / (Applicant for a Digital Certificate) using the Issuing Certificate
- FRCS VMS Registration Authority
    - managing activities between Issuing CAs and an (Certificates Holders) / (Applicant for a Digital Certificate)

- perform due diligence on potential Certificate Holders and only successful applicants are approved and receive Digital Certificates
- For Digital Certificates that is issuing to Organization Authorization Person identification processes require applicants to present themselves for face-to-face verification

FRCS VMS Digital Certificates comply with Internet Standards (x509 v.3) as set out in RFC 5280.

FRCS VMS Digital Certificates may not be used, and no participation is permitted in the FRCS VMS PKI in:

1. circumstances that breach, contravene, or infringe the rights of others,
2. circumstances that offend, breach, or contravene any applicable law, statute, regulation, order, decree, or judgment of a court of competent jurisdiction or governmental order,
3. connection with fraud, pornography, obscenity, hate, defamation, harassment, or other activity that is contrary to public policy,
4. Man in the Middle (MITM) purposes for the interception of encrypted communications.

1.3.1 Certification Authorities

1.3.1.1 Root Certification Authority

The FRCS VMS PKI contains the following Root Certification Authority “VMS RCA” available on http://pki.vms.frcs.org.fj/pki/VMSRCA.cer

FRCS VMS Root Certification Authority is RSA4096SHA256

1.3.1.2 Issuing CAs and Their Obligations

The FRCS VMS PKI contains the following Issuing Certification Authority “VMS ICA1” available on http://pki.vms.frcs.org.fj/pki/VMSICA1.cer

FRCS VMS Root Certification Authority is RSA2048SHA256

Issuing CAs is authorized to issue and manage types of Digital Certificates supported by this CP/CPS.

Digital Certificate Management includes all aspects associated with the application, issue and revocation of Digital Certificates, including any required identification and authentication processes included in the Digital Certificate application process.

Issuing CAs chaining to a FRCS VMS Root must not be used for Man in the Middle (MITM) purposes for the interception of encrypted communications. Such Issuing CAs should also not be used for traffic management of domain names /IP addresses that the entity does not own or control. FRCS VMS will not issue a subordinate Issuing CA Certificate to be used for these purposes.

Issuing CAs are required to ensure that:

- Private Keys are used only in connection with the signature of Digital Certificates and Certificate Revocation Lists.
- All administrative procedures related to personnel and procedural requirements, as well as physical and technological security mechanisms, are maintained in accordance with this CP/CPS.
- They follow a privacy policy in accordance with this CP/CPS, see 9.4

1.3.2 Registration Authorities and Their Obligations

Perform the Identification and Authentication and Digital Certificate request and revocation functions defined by this CP/CPS.

Registration Authorities must perform following functions which include but are not limited to:

- Initiate Organization Authorized Person Digital Certificate application requests
- Process all Digital Certificate application requests initiated by Initiate Organization Authorized Person
- Maintain and process all supporting documentation related to Digital Certificate applications.
- Process all Digital Certificate Revocation requests.
- Follow a privacy policy in accordance with this CP/CPS, se 9.4

1.3.3 Certificate Holders

1.3.3.1 Obligations and Responsibilities

Certificate Holders are required to act in accordance with this CP/CPS. A Certificate Holder represents, warrants and covenants with and to FRCS VMS PKI processing their application for a Digital Certificate that:

- Both as an applicant for a Digital Certificate and as a Certificate Holder, submit complete and accurate information in connection with an application for a Digital Certificate and will promptly update such information and representations from time to time as necessary to maintain such completeness and accuracy.
- Comply fully with any and all information and procedures required in connection with the Identification and Authentication requirements relevant to the Digital Certificate issued. See Appendix A.
- Promptly review, verify and accept or reject the Digital Certificate that is issued and ensure that all the information set out therein is complete and accurate and to notify FRCS VMS PKI immediately in the event that the Digital Certificate contains any inaccuracies.
- Secure the Private Key and take all reasonable and necessary precautions to prevent the theft, unauthorized viewing, tampering, compromise, loss, damage, interference, disclosure, modification or unauthorized use of its Private Key (to include password, hardware token or other activation data used to control access to the Participant's Private Key).
- Exercise sole and complete control and use of the Private Key that corresponds to the Certificate Holder's Public Key.
- Immediately notify FRCS VMS PKI in the event that their Private Key is compromised, or if they have reason to believe or suspect or ought reasonably to suspect that their Private Key has been lost, damaged, modified or accessed by another person, or compromised in any other way whatsoever.

Following compromise, the use of the Certificate Holder's Private Key should be immediately and permanently discontinued.

- Take all reasonable measures to avoid the compromise of the security or integrity of the FRCS VMS PKI.
- Forthwith upon termination, revocation or expiry of the Digital Certificate (howsoever caused), cease use of the Digital Certificate absolutely.
- At all times utilize the Digital Certificate in accordance with all applicable laws and regulations.

- Use the signing Key Pairs for electronic signatures in accordance with the Digital Certificate profile and any other limitations known, or which ought to be known, to the Certificate Holder.
- Discontinue the use of the digital signature Key Pair in the event that FRCS VMS notifies the Certificate Holder that the FRCS VMS PKI has been compromised.

1.3.3.2 Accepted Limitation of Liability

Digital Certificates include a reference to the relevant CP/CPS, which contains statements detailing limitations of liability and disclaimers of warranty. In accepting a Digital Certificate, Certificate Holders acknowledge and agree to all such limitations and disclaimers documented in the CP/CPS.

1.3.4 Relying Parties

All certificate and their usage are part of FRCS VMS system.

Digital Certificates include a reference to the relevant CP/CPS, which contains statements detailing limitations of liability and disclaimers of warranty. In accepting a Digital Certificate, Relying Parties acknowledge and agree to all such limitations and disclaimers documented in the CP/CPS. A relying party shall make no assumptions about information that does not appear in a Digital Certificate.

Relying party cannot rely on a Digital Certificate issued by FRCS VMS current set as revoked Digital Certificates published by FRCS VMS. Certificates have pointers to URLs where FRCS VMS publishes status information, including Certificate Revocation Lists (CRLs), and Relying Parties are required to check the most recent CRL.

1.3.4.1 Authorization Relaying parties

Authorization Relying parties are involved in signed invoices creation and are required to act in accordance with this CP/CPS. Any device or software used to create signed invoice must be accredited by FRCS.

1.3.4.2 Relaying parties involved in signed invoices receives

Any party receiving a signed electronic invoice may use publicly available service to rely on that Digital Signature.

Every signed invoice from accredited device or software contains QR code which is used in verification process. Verification service URL is under https://vms.frcs.org.fj

1.3.5 Other Participants

Other Participants in the FRCS VMS PKI are required to act in accordance with this CP/CPS.

1.4 Certificate Usage

At all times, participants in the FRCS VMS PKI are required to utilize Digital Certificates in accordance with this FRCS VMS CP/CPS and all applicable laws and regulations.

1.4.1 Appropriate Certificate Usage

Digital Certificates may be used for identification, providing data confidentiality and data integrity, and for creating digital signatures as part of FRCS VMS system.

The use of Digital Certificates supported by this CP/CPS is restricted to parties of FRCS VMS system. Persons and entities other than those authorized may not use Digital Certificates for other purposes.

Reliance on signed invoice can be confirm using publicly available service from QR code on signed invoice.

Any person participating within the FRCS VMS PKI irrevocably agrees, as a condition to such participation, that the issuing of all products and services contemplated by this CP/CPS shall occur and shall be deemed to occur in Fiji and that the performance of FRCS VMS obligations hereunder shall be performed and be deemed to be performed in Fiji.

1.4.2 Prohibited Certificate Usage

Digital Certificates may not be used and no reliance may be placed other than FRCS VMS system Policy Administration

1.4.3 Organization Administering the CP/CPS

FRCS VMS operates the Policy Management Authority (PMA) that is responsible for setting policies and practices for the overall PKI.

1.4.4 Contact Person

This CP/CPS is administered by the FRCS VMS PMA. Enquiries or other communications about this CP/CPS should be addressed to FRCS.

PMA

Revenue & Customs Services Complex

Lot 1 Corner of Queen Elizabeth Drive & Ratu Sukuna Road, Nasese,

Suva

https://www.frcs.org.fj/our-services/vat-monitoring-system-vms/

Electronic mail: efdcompliance@frcs.org.fj

1.4.5 Person Determining the CP/CPS Suitability

The FRCS VMS PMA determines the suitability of this CP/CPS to the functions and uses of Participants in the FRCS VMS PKI.

1.4.6 CP/CPS Approval Procedures

This CP/CPS is regularly reviewed and approved by the FRCS VMS PMA. Notice of proposed changes are recorded in the change log at the beginning of this CP/CPS until they are approved, at which time the approved change will be recorded there permanently.

1.4.6.1 Publication of CP/CPS

This CP/CPS is published electronically in PDF format at http://pki.vms.frcs.org.fj/pki.

1.4.6.2 Frequency of Publication

Newly approved versions of this CP/CPS and other relevant documents are published in accordance with the amendment, notification and other relevant provisions contained within those documents. Information about amendments to this CP/CPS may be found in Section 9.12.

1.4.6.3 Access Control

FRCS VMS internal documents not published at http://pki.vms.frcs.org.fj/pki are available only to Participants in the FRCS VMS PKI where deemed necessary.

1.5 Definitions and Acronyms

See Appendix B

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

The FRCS VMS Repository (http://pki.vms.frcs.org.fj/pki) serves as the primary repository. However, copies may be published at such other locations as are required for the efficient operation of the FRCS VMS PKI.

2.2 Publication of Certificate Information

The FRCS VMS Root Certification Authority and chained Issuing CA publishes publicly available repository that lists all the Digital Certificates that have been revoked. Repository that lists all Digital Certificates issued is available only internally. The location of the repository is given in the individual Certificate Profiles more fully disclosed in Appendix A to this CP/CPS.

2.3 Time or Frequency of Publication

Digital Certificate information that have been revoked is published minimum once in 24 hours.

2.4 Access Controls on Repositories

Read-only access to Repositories is available to Relying Parties twenty-four hours a day, seven days a week, except for reasonable maintenance requirements, where access is deemed necessary. FRCS VMS is the only entity that has write access to Repositories.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

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

3.1.1 Types of Names

All Certificate Holders require a distinguished name that follows the X.500 standard for Distinguished Names.

The FRCS VMS Root Certification Authority approves naming conventions for the creation of distinguished names for Issuing CA applicants.

The Subject Name of all Digital Certificates issued to Individuals shall be the authenticated common name of the Certificate Holder. Each User must have a unique and readily identifiable Distinguished Name (DN) following RFC 5280. The Distinguished Name may include the following fields:

- Common Name (CN)
- Device Serial number (SERIALNUMBER)
- Given Name (G)
- Sur Name (SN)
- Organizational Unit (OU)
- Organization (O)
- Locality (L)
- State or Province (S)
- Country (C)

- Email Address (E)

Characters allowed in subject name is limited to

- Latin capital letters (A, B, … Z)
- Latin small letters (a, b, … z)
- Numbers (1, 2, … 9)
- Space
- Hyphen-minus (-)
- Full stop (.)

3.1.2 Need for Names to be Meaningful

Distinguished Names must be meaningful, unambiguous and unique. FRCS VMS supports the use of Digital Certificates as a form of identification in FRCS VMS system.

The contents of the Digital Certificate Subject Name fields must have a meaningful association with the name of the Organization Authorized Person or Organization. In the case of Organizations, the name shall meaningfully reflect the legal name of the Organization. In the case of Organization Authorized Person, the name should consist of the First name, Last name and Organizations data.

3.1.3 Pseudonymous Certificate Holders

Pseudonym Digital Certificates is not permitted.

3.1.4 Rules for Interpreting Various Name Forms

Fields contained in Digital Certificates are in compliance with this CP/CPS and the Digital Certificate Profiles detailed in section 7.1 and Appendix A. In general, the rules for interpreting name forms can be found in International Telecommunication (ITU) and Internet Engineering Task Force (IETF) Standards, such as the ITU-T X.500 series of standards and applicable IETF RFCs.

3.1.5 Uniqueness of Names

FRCS VMS PKI Registration Authorities propose and approve distinguished names for Applicants and as a minimum check that a proposed distinguished name is unique.

The Issuing CA insert additional numbers or letters to the Certificate Holder’s Subject Common Name, or other attribute, to distinguish between two Digital Certificates that would otherwise have the same Subject Name. This insertion is first 4 characters from SERIALNUMBER attribute.

3.1.6 Recognition, Authentication, and Role of Trademarks

Issuing CAs are not obligated to seek evidence of trademark usage by any Organization.

3.2 Initial Identity Validation

Identity Validation follows this CP/CPS and the Digital Certificate Profiles detailed in section 7.1 and Appendix A.

3.2.1 Method to Prove Possession of Private Key

Issuing CAs shall establish that each Applicant for a Digital Certificate is in possession and control of the Private Key corresponding to the Public Key contained in the request for a Digital Certificate. The Issuing CA shall do so in accordance with an appropriate secure protocol, such as the IETF PKIX Certificate Management Protocol, including PKCS#10.

3.2.2 Authentication of Organization Identity

The Identity of an Organization is required to be authenticated by FRCS VMS.

3.2.3 Authentication of Individual Identity

The Identity of an Organization authorized person is required to be authenticated by FRCS VMS.

3.2.4 Non-Verified Certificate Holder Information

An Issuing CA within the FRCS VMS PKI may accept the following Non-Verified Certificate Holder Information for other classes of Digital Certificate:

- Organizational Unit (OU)
- Other information that is permitted as Non-Verified according to the Certificate type or relevant industry standards

3.2.5 Validation of Authority

Information in first Digital Certificate containing Organization authorized person and Organizational Name are verified by FRCS.

All additional Digital Certificates that were requested by Organization authorized person will contain Organizational Name and submitted information of Location will not be verified additionally.

3.2.6 Criteria for Interoperation

N/A

3.3 Identification and Authentication for Renewal Requests

FRCS VMS does not support Certificate Renewal. Key Pairs must always expire at the same time as the associated Digital Certificate. Certificate Renewal requests are treated in the same manner as an initial Certificate Request and a new Digital Certificate and new Key Pair is issued. Application for a Digital Certificate following revocation is treated as an initial Certificate Request.

3.3.1 Identification and Authentication for Routine Re-Key

Identification and Authentication for routine Re-Key is based on the same requirements as issuing of new Certificates.

3.3.2 Identification and Authentication for Re-Key After Revocation

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

3.4 Identification and Authentication for Revocation Requests

A request to revoke Keys and Digital Certificates may be submitted by persons authorized to do so:

- FRCS VMS Security Officer
- Organization Authorized Person contacting FRCS VMS

3.4.1 Issuing Certification Authority

Only if request came from FRCS VMS system.

3.4.2 Registration Authority

A Registration Authority is part of FRCS VMS system and authorized FRCS personal request the revocation of Digital Certificates.

3.4.3 Certificate Holder

Organization Authorized Person contacting FRCS VMS for own organization Digital Certificate may request revocation by communicating with FRCS VMS system after appropriate identification.

4 CERTIFICATE LIFE-CYCLE OPERATION REQUIREMENTS

4.1 Certificate Application

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

4.1.1 Who Can Submit A Certificate Application

Initial certificate application for Organization authorized person is submitted by FRCS VMS.

Additional certificate application for Organization are submitted by Organization authorized person using initially received Digital Certificate and FRCS VMS system.

All applications are subject to review, approval, and acceptance by FRCS VMS PKI.

4.1.2 Enrolment Process and Responsibilities

4.1.2.1 Enrolment Process and Responsibilities for First Digital Certificate

1. Identification data preparation
    a. FRCS VMS Security officer is responsible to inform Organization authorized person to update identification data held by FRCS VMS system.
    b. Organization authorized person is responsible to update identification data.
2. Activation data and delivery method defining
    a. FRCS VMS Security officer is responsible to inform Organization authorized person to set Digital Certificate activation data – PIN.
    b. Organization authorized person is responsible to set Digital Certificate activation data – PIN and choose delivery process
3. Approving Digital Certificate issuing
    a. FRCS VMS Security officer is responsible to approve Digital Certificate issuing
    b. FRCS VMS Personalization officer is responsible to issue Digital Certificate on smart card
    c. FRCS VMS Personalization officer is responsible to deliver smart card by chosen Delivery method
    d. Officers at delivery address are responsible to identify Organization authorized person face-to-face and return cover letter signed by Organization authorized person
    e. FRCS VMS Security officer upon returned cover letter signed by Organization authorized person is responsible to enable Organization authorized person Digital Certificate in FRCS VMS system.

4.1.2.2 Enrolment Process and Responsibilities for other Digital Certificate

1. Identification data preparation
    a. Organization authorized person is responsible to add identification data for additional Locations and request addition digital certificates
2. Activation data and delivery method defining
    a. Organization authorized person is responsible to set Digital Certificate activation data – PIN and choose delivery process or set PKCS12 password and PKCS12 activation data for FRCS VMS system
3. Approving Digital Certificate issuing
    a. FRCS VMS Security officer is responsible to approve Digital Certificate issuing
    b. FRCS VMS system upon approval is responsible to automatically issue Digital Certificate in PKCS12

c. FRCS VMS Personalization officer is responsible to issue Digital Certificate on smart card
d. FRCS VMS Personalization officer is responsible to deliver smart card to chosen Delivery method
e. Officers at delivery address are responsible to identify Organization authorized person face-to-face and return cover letter signed by Organization authorized person
f. FRCS VMS Security officer is responsible to enable Organization authorized person Digital Certificate in FRCS VMS system.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

FRCS VMS internal process.

4.2.2 Approval or Rejection of Certificate Applications

FRCS VMS internal process.

4.2.3 Time to Process Certificate Applications

FRCS VMS internal process.

4.3 Certificate Issuing

4.3.1 Certification Authority Actions During Certificate Issuing

Digital Certificate issuing is governed by and should comply with the practices described in and any requirements imposed by the FRCS VMS CP/CPS.

4.3.1.1 FRCS VMS PKI

FRCS VMS PKI internal process.

4.3.1.2 Certificate Holder Certificates

See 4.1.2

4.3.2 Notification to Applicant Certificate Holder

See 4.1.2

4.4 Certificate Acceptance

See 4.1.2

4.4.1 Notice of Acceptance

See 4.1.2

4.4.2 Conduct Constituting Certificate Acceptance

See 4.1.2

4.4.3 Publication of The Certificate by The Certification Authority

All Digital Certificates issued within the FRCS VMS PKI are not made available in public repositories.

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

N/A

4.5 Key Pair and Certificate Usage

4.5.1 Certificate Holder Private Key and Certificate Usage

Within the FRCS VMS PKI, a Certificate Holder may only use the Private Key and corresponding Public Key in the Digital Certificate for their FRCS VMS intended use.

4.5.2 Relying Party Public Key and Certificate Usage

Any party receiving a signed electronic invoice may rely on that Digital Signature after verifying such invoice on verification service.

4.6 Certificate Renewal

Certificate Renewal means the issuing of a new Certificate without changing the Public Key or any other information in the Certificate.

The FRCS VMS PKI does not support Certificate Renewal

4.7 Certificate Re-Key

Certificate Re-Keyed when all the identifying information from a Digital Certificate is duplicated in a new Digital Certificate, but there is a different public key and a different validity period. Due diligence, Key Pair generation, delivery and management are performed in accordance with this CP/CPS.

The FRCS VMS PKI does support Certificate Re-Key but revokes previous digital certificate prior to issuing a new one.

4.7.1 Circumstance for Certificate Re-Key

Digital Certificates may be Re-Keyed upon request that old certificate is compromised.

4.7.2 Who May Request Re-Key

FRCS VMS Security officer initiate Re-Keying upon request described in 4.1.2.1

FRCS VMS Security officer approving Re-Keying upon request by Organization authorized person described in 4.1.2.2

4.7.3 Processing Certificate Re-Key Request

Digital Certificate Re-Key requests are processed in the same manner as requests for new Digital Certificates and in accordance with the provisions of this CP/CPS.

See 4.1.2

4.7.4 Notification of New Certificate Issuing to Certificate Holder

See 4.1.2

4.7.5 Conduct Constituting Acceptance of a Re-Key Certificate

See 4.1.2

4.7.6 Notification of Certificate Re-Key by The Certification Authority to Other Entities

N/A

4.8 Certificate Modification

Certificate Modification refers to the issuing of a new Digital Certificate due to changes in the information in an existing Digital Certificate (other than its associated Public Key). Digital Certificate

Modification requests are processed in the same manner as requests for new Digital Certificates and in accordance with the provisions of this CP/CPS.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

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

- FRCS VMS Certification Authority key compromise
- Certificate Holder profile creation error
- Key Compromise including unauthorized access or suspected unauthorized access to Private Keys, lost or suspected lost keys, stolen or suspected stolen keys, destroyed or suspected destroyed keys or superseded by replacement keys and a new Certificate.
- The Certificate Holder has failed to meet his, her or its obligations under this FRCS VMS CP/CPS or any other agreement, regulation, or law that may be in force with respect to that Digital Certificate;
- The Certificate was not issued in accordance with the terms and conditions of this CP/CPS or the Certificate Holder provided inaccurate, false or misleading information;
- The Private Key corresponding to the Certificate has been used to sign, publish or distribute spyware, Trojans, viruses, rootkits, browser hijackers, or other content, for phishing, or conduct that is harmful, malicious, hostile or to download malicious content onto a user's system without their consent;
- The Certificate Holder is a denied party or prohibited person on a government-issued blacklist, or is operating from a prohibited destination;
- Affiliation change
- Cessation of operation
- Incorrect information contained in Digital Certificate
- Certificate Holder bankruptcy
- Certificate Holder liquidation
- Certificate Holder death
- Certificate Holder request

4.9.2 Who Can Request Revocation

The following entities may request revocation of a Digital Certificate:

- FRCS VMS PKI may revoke any Digital Certificate issued within the FRCS VMS PKI and shall publish the list of revoked Digital Certificates in a publicly accessible Certificate Revocation List.
- Organization authorized person within the FRCS VMS may request revocation of their own Digital Certificates.

4.9.3 Procedure for Revocation Request

FRCS VMS will revoke a Digital Certificate upon receipt of a valid request. A revocation request should be promptly and directly communicated to the FRCS VMS that approved or acted in connection with the issue thereof. Organization authorized person may be required to submit the revocation request via the FRCS VMS Support Line or directly over an Internet connection.

FRCS VMS maintains a continuous 24/7 ability to internally respond to any high priority Certificate Problem Report and will take such action as deemed appropriate based on the nature of such a report. This may include, but not be limited to, the revocation of a Certificate that is the subject of such a complaint.

4.9.4 Revocation Request Grace Period

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

4.9.5 Time Within Which the Certification Authority Must Process the Revocation Request

N/A

4.9.6 Revocation Checking Requirement for Relying Parties

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

4.9.7 Certificate Revocation List Issuing Frequency

See 7.2

4.9.8 Maximum Latency for Certificate Revocation List

N/A

4.9.9 On-Line Revocation/Status Checking Availability

N/A

4.9.10 On-Line Revocation Checking Requirement

N/A

4.9.11 Other Forms of Revocation Advertisements Available

N/A

4.9.12 Special Requirements in Relation to Key Compromise

Should a Private Key become compromised, the related Certificate shall immediately be revoked. Should the private CA key become compromised, all Certificates issued by that CA shall be revoked.

4.9.13 Circumstances for Suspension

No suspension of Digital Certificates is permissible within the FRCS VMS PKI.

4.9.14 Who Can Request Suspension

No suspension of Digital Certificates is permissible within the FRCS VMS PKI.

4.9.15 Procedure for Suspension Request

No suspension of Digital Certificates is permissible within the FRCS VMS PKI.

4.9.16 Limits on Suspension Period

No suspension of Digital Certificates is permissible within the FRCS VMS PKI.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

The Status of Digital Certificates issued within the FRCS VMS PKI is published in a Certificate Revocation List se 7.1.2

4.10.2 Service Availability

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

4.11 End of Subscription

FRCS VMS requires all Organizations included in Fiscalization have valid certificates. If Digital Certificate is to expire or is revoked, new Digital Certificate must be issued.

4.12 Key Archival and Recovery

FRCS VMS provides Key Archive for Root CA and Issuing CA due Disaster recovery and Business Continuity. Key Archive for other Digital Certificate is not in place.

FRCS VMS CA Key Archival and Recovery Policy and Practices are part of internal documents.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical Controls

FRCS VMS PKI manages and implements appropriate physical security controls to restrict access to the hardware and software used in connection with CA operations wherever those operations physically occur.

5.1.1 Site Location and construction

FRCS VMS PKI performs its CA operations from a secure datacenter located in an office complex in Fiji.

5.1.2 Physical Access

FRCS VMS PKI permits entry to its secure operating area only to security-cleared and authorized personnel.

5.1.3 Power and Air-Conditioning

The FRCS VMS PKI secure operating area is connected to a standard power supply. All critical components are connected to uninterrupted power supply (UPS) units, to prevent abnormal shutdown in the event of a power failure.

5.1.4 Water Exposures

The FRCS VMS secure operating area provides protection against water. It is located on an upper floor with raised flooring.

5.1.5 Fire Prevention and Protection

The FRCS VMS secure operating area provides protection against fire with extinguishing system.

5.1.6 Media Storage

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

5.1.7 Waste Disposal

Paper documents and magnetic media containing trusted elements of FRCS VMS or confidential information are securely disposed of by:

- in the case of magnetic media:
    - physical damage to, or complete destruction of, the asset;

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

5.1.8 Off-Site Backup

N/A

5.2 Procedural Controls

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

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

5.2.1 Trusted Roles

Responsibilities are shared by multiple roles and individuals in order to ensure that one person acting alone cannot circumvent security safeguards:

- Root CA private Key Custodians protecting Root CA private key (cannot be Security Officer or Personalization Officer)
- Security Officer (cannot be Key Custodians or Personalization Officer)
    - initiates certificate request for Organization authorized person requesting him to set PIN and delivery method
    - approves issuing of certificate request
    - revokes certificate upon request
- Personalization Officer (cannot be Key Custodians or Security Officer)
    - Prints smart card
    - issues certificates on smart cards
    - prepares smart card for delivery
- Delivery service delivers smart cards to location specified by Organization authorized person
- Organization authorized person
    - Sets PIN and chooses delivery method
    - Requests additional Digital Certificate in form of PFX or Smart Card specifying activation parameters for certificates
    - Requests Digital Certificate revocation
- Audit Officer

5.2.2 Number of Persons Required Per Task

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

5.2.3 Identification and Authentication for Each Role

Persons filling trusted roles are part of FRCS VMS systems.

5.2.4 Roles Requiring Separation of Duties

Process of issuing Digital Certificate involves Security Officer, Personalization Officer and Organization authorized person. Security Officer cannot be Personalization Officer.

5.3 Personnel Controls

Persons filling trusted roles are part of FRCS VMS systems.

5.3.1 Qualifications, Experience, and Clearance Requirements

Persons filling trusted roles are provided by FRCS VMS systems training and clearance.

5.3.2 Background Check Procedures

Persons filling trusted roles are part of FRCS VMS systems and are subject to procedures of FRCS.

5.3.3 Training Requirements

FRCS VMS PKI provides its personnel with on-the-job and professional training.

5.3.4 Retraining Frequency and Requirements

FRCS VMS PKI provides its personnel with on-the-job and professional training.

5.3.5 Job Rotation Frequency and Sequence

N/A

5.3.6 Sanctions for Unauthorized Actions

Persons filling trusted roles are part of FRCS VMS systems and are subject to procedures of FRCS.

5.3.7 Independent Contractor Requirements

Persons filling trusted roles are part of FRCS VMS systems and are subject to procedures of FRCS.

5.3.8 Documentation Supplied to Personnel

FRCS MVS PKI provides personnel with all required training materials needed to perform their job function and their duties.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

Relevant events involved in the generation of the Certification Authority Key Pairs are recorded. This includes all configuration data used in the process.

Relevant events involved in the generation of the Certification Holder's Key Pairs are recorded. This includes all configuration data used in the process.

Activation data that Organization Authorized Person defined prior to Digital Certificate issuing are not part of event recording.

The types of data recorded by FRCS VMS PKI:

- all data involved in each individual Digital Certificate registration, issuing and distribution process except activation data will be recorded for future reference if needed,
- all data relevant to the publication of Digital Certificates and Certificate Revocation Lists will be recorded,
- all Digital Certificate revocation request details are recorded including reason for revocation,
- certificate and hardware security lifecycle management are recorded,
- all procedures involved in the backup process are recorded,

- all aspects of the installation of new or updated software,
- all aspects of equipment maintenance.

5.4.2 Frequency of Processing Log

Audit logs are verified and consolidated at least monthly.

5.4.3 Retention Period for Audit Log

N/A

5.4.4 Protection of Audit Log

The relevant audit data collected is regularly analyzed for any attempts to violate the integrity of any element of the FRCS VMS PKI.

Only Security Officers and auditors may view audit logs in whole.

5.4.5 Audit Log Backup Procedures

N/A

5.4.6 Audit Collection System

Security audit processes are invoked at system start up and cease only at system shutdown.

5.4.7 Notification to Event-Causing Subject

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

5.4.8 Vulnerability Assessment

Vulnerability assessment procedures intend to identify FRCS VMS PKI threats and vulnerabilities and determine a risk value based upon existing safeguards and control practices.

5.5 Records Archival

5.5.1 Types of Records Archived

N/A

5.5.2 Retention Period for Archive

N/A

5.5.3 Protection of Archive

N/A

5.5.4 Archive Backup Procedures

N/A

5.5.5 Requirements for Time-Stamping of Records

N/A

5.5.6 Archive Collection System

N/A

5.5.7 Procedures to Obtain and Verify Archive Information

N/A

5.6 Key Changeover

Key changeover for CA is not automatic, but procedures enable the smooth transition from expiring CA Certificates to new CA Certificates. 3 years before the end of the CA Private Key's lifetime, FRCS VMS PKI ceases using its CA Private Key to sign Certificates and uses only to sign CRLs. A new CA signing Key Pair is commissioned and all subsequently issued Certificates and CRLs are signed with the new private signing key. Both the old and the new Key Pairs may be concurrently active.

Key changeover for Certificate Holder's is not implemented. Prior to Digital Certificate expiration, process for new Digital Certificate is started.

5.7 Compromise and Disaster Recovery

5.7.1 Disaster Recovery plan

FRCS VMS PKI has Disaster & Recovery Plan as part of FRCS VMS system DR plan. This Plan allow Business Continuity of FRCS VMS system and FRCS VMS PKI as it supported process.

5.7.2 Key compromise plan

FRCS VMS PKI have in place an appropriate Key compromise plan detailing the activities taken in the event of a compromise of a FRCS VMS PKI Issuing CA Private Key. Such plans include procedures for:

- Revoking all Digital Certificates signed with that FRCS VMS PKI Issuing CA's Private Key,
- Notifying all participants
- Issuing new Issuing CA certificate and all Certificate Holder's certificates

5.8 Certification Authority and/or Registration Authority Termination

Same as 5.7.2

6 TECHNICAL SECURITY CONTROLS

FRCS VMS PKI Root Certification Authority Private Key is protected within a hardware security device. Access to the device is within the FRCS VMS PKI environment. These hardware security device and pass phrases are allocated among the FRCS VMS PKI management team. The hardware security devices are always stored in a physically secure environment and are subject to security controls throughout their lifecycle.

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

All Key Pairs will be generated in a manner that FRCS VMS PKI deems to be secure.

The Certificate Holder is required to provide all the necessary identification and authentication information when the Digital Certificate is being requested. Certificate Holder's Key Pair are generated within a secure environment. Certificate Holders cannot generate their own Private Key during Digital Certificate request. Key Generation methods and requirements differ according to the type of Digital Certificate requested.

CA Certificate signing keys are only used within physically secure environment of FRCS VMS PKI.

6.1.2 Private Key Delivery to Certificate Holder

Certificate Holder define private key activation parameters prior to Digital Certificate issuing. Delivery of private key with Digital Certificate is conducted without activation parameters. During delivery Private Key is in protected data structure (PKCS#12 or Smart Card)

6.1.3 Public Key Delivery to Certificate Issuer

N/A

6.1.4 Certification Authority Public Key to Relying Parties

FRCS VMS PKI Public Keys are securely delivered to software providers to serve as trust anchors. They are specified in a Certificate validation path of issued Digital Certificates. Relying Parties may also obtain FRCS VMS PKI self-signed CA Certificates containing the Public Key from the FRCS VMS PKI web site.

6.1.5 Key Sizes

FRCS VMS PKI use:

- RSA 4096-bit for Root CA
- RSA 2048-bit for Issuing CA
- RSA 2048-bit for Digital Certificates issued by Issuing CA

6.1.6 Public Key Parameters Generation and Quality Checking

All key generation is conducted in physically secure environment of FRCS VMS PKI.

6.1.7 Key Usage Purposes (As Per X.509 V3 Key Usage Field)

Root CA and Issuing CA Private Keys may be only used for Digital Certificate signing and CRL.

Certificate Holder Keys may be used for the purposes and in the manner described in the FRCS VMS PKI CP/CPS – Digital Certificate Profiles.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

All Participants in the FRCS VMS PKI should take all appropriate and adequate steps to protect their Private Keys in accordance with the requirements of this FRCS VMS PKI CP/CPS.

All Participants in the FRCS VMS PKI must secure their Private Key and take all reasonable and necessary precautions to prevent the loss, damage, disclosure, modification, or unauthorized use of their Private Key including all activation data used to control access to the Private Key.

6.2.1 Cryptographic Module Standards and Controls

The generation and maintenance of the Root and Issuing CA Private Keys are facilitated using an advanced cryptographic device and appropriate procedures.

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

N/A

6.2.3 Private Key Escrow

N/A

6.2.4 Private Key Backup

Issuing CA Private Keys are stored in an encrypted state (using an encryption key to create a “cryptographic wrapper” around the key). They are backed up under further encryption and maintained on-site and in a secure off-site storage.

6.2.5 Private Key Archive

N/A

6.2.6 Private Key Transfer into or from a Cryptographic Module

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

6.2.7 Private Key Storage on Cryptographic Module

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

6.2.8 Method of Activating Private Key

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

6.2.9 Method of Deactivating Private Key

Cryptographic Modules that have been activated must not be left unattended or otherwise open to unauthorized access. They are deactivated after passive timeout. When not in use, hardware Cryptographic Modules should be removed and stored, unless they are within the Holder’s sole control.

Issuing CA Private Keys are not usually deactivated but are kept in locked computer cabinets with appropriate physical and logical security controls. Other cryptographic modules used by FRCS VMS PKI are deactivated through a manual logout procedure or a passive timeout.

6.2.10 Method of Destroying Private Key

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

All Certificate Holders have an obligation to protect their Private Keys from being compromised. Private Keys shall be destroyed in a way that prevents their loss, theft, modification, unauthorized disclosure or unauthorized use.

6.2.11 Cryptographic Module Rating

The cryptographic modules used by the FRCS VMS PKI do not need to be validated to FIPS 140-2 Level-3 or EAL 4 security standards.

The cryptographic modules are configured to protect access to Private Key by requesting submission of valid Personal Identification Number (PIN).

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

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

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

Usage periods for Public Keys and Private Keys shall match the usage periods for the Digital Certificate. Please see the variable Issuing Certificate Authority ‘Valid From’ and ‘Valid To’ fields in the Certificate Profiles outlined in Appendix A.

The maximum validity periods for Digital Certificates issued within the FRCS VMS PKI are:

- Root CA Certificate 20 years
- Issuing CA Certificates 10 years
- Digital Certificates 3 years

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

Two-factor authentication shall be used to protect access to a Private Key. One of these factors is a randomly and automatically generated key that protects the Private Key. A unique Personal Identification Number (PIN) must be generated by an Organization authorized person and is unknow to operator officers during issuing of Digital Certificates

FRCS VMS PKI Certification Authority Officers are also required to use strong passwords to further prevent unauthorized access to CA systems.

6.4.2 Activation Data Protection

Organization authorized person is responsible of generating and protecting activation data.

6.4.3 Other Aspects of Activation Data

Activation data used to reset or unblock PIN are randomized and not stored. In case PIN code is forgotten new Digital Certificate must be requested with a new key pair and a new PIN.

6.5 Computer Security Controls

FRCS VMS PKI does not have a formal Information Security Policy that documents the FRCS VMS PKI policies, standards and guidelines relating to information security. But FRCS VMS PKI implements best-practice relating to information security.

6.6 Life Cycle Technical Controls

All hardware and software procured for operating an Issuing CA within the FRCS VMS PKI must be purchased in a manner that will mitigate the risk that can compromise business continuity.

6.7 Network Security Controls

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

Unused network ports and services are turned off to ensure that Issuing CA equipment is protected against known network attacks. Any network software present on the Issuing CA equipment is software required for the functioning of the Issuing CA application.

All Root CA equipment is maintained and operated in stand-alone, off-line configurations.

6.8 Time-Stamping

N/A

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate Profile

All FRCS VMS PKI Digital Certificates conform to Digital Certificate and Certificate Revocation List profiles as described in RFC 5280 and utilize the ITU-T X.509 version 3 Digital Certificate standard.

The table below describes the basic fields that may be included in FRCS VMS PKI Digital Certificates. Refer to APPENDIX A for additional Certificate contents that are specific to the individual type of Digital Certificates.

7.1.1 Basic Certificate Contents

FIELDS	CONTENT	DEMARCATION
Version	FRCS VMS PKI certificates are Version 3	Fixed
Serial Number	Unique system generated number assigned to each certificate	Fixed
Signature Algorithm	The algorithm identifier for the algorithm used to sign the certificate	Fixed
Issuer	Issuer is the entity that has signed and issued the certificate	
Common Name (CN)	Issuing Certification Authority Common Name	Fixed
Organization (O)	Organization legal name	Fixed
Country (C)	Issuing CA Jurisdiction	Fixed
Valid From	The date and time on which the Certificate validity period begins	Fixed
Valid To	The date and time on which the Certificate validity period ends	Fixed
Subject	The Subject field identifies the entity associated with the Public Key stored in the subject Public Key field	
Common Name (CN)	Subject Common Name	Holder Variable
Serial Number	Subject Serial Number	Holder Variable
Given Name (G)	Subject First Name	Holder Variable
Surname (SN)	Subject Family Name	Holder Variable
Organizational Unit (OU)	Subject Organizational Unit	Holder Variable
Organization (O)	Subject Organization Name	Holder Variable
Street (STREET)	Subject Street address	Holder Variable
Locality (L)	Subject Locality	Holder Variable
State/Province (S)	Subject State/Province	Holder Variable
Country (C)	Subject Country	Holder Variable
Subject email address (E)	The e-mail address of the subject	Holder Variable
Subject Public Key	Information Contains the Public Key and identifies the algorithm with which the Key is used	Fixed

7.1.2 Certificate Extensions

FIELDS	CONTENT	DEMARCATION
Authority Key Identifier	This field contains the Subject Key Identifier of the issuer's Certificate	Fixed
Subject Key Identifier	This field contains the ID of the Certificate Holder's key	Fixed
Key Usage (Critical)	Possible Key Usages include: • digitalSignature • keyEncipherment	Fixed

FIELDS	CONTENT	DEMARCATION
Certificate Policies	This extension contains Object Identifiers (OIDS) relates to the FRCS VMS PKI Certificate Class as well as a URL with a link to the FRCS VMS PKI Repository at http://pki.vms.frcs.org.fj/pki.	Fixed
Subject Alternative Name	Refer to Appendix A for the Subject Alternative Name specific to each type of FRCS VMS PKI Certificates.	Holder Variable
Extended Key Usage (EKU)	Possible Extended Key Usages include: • Client Authentication • Server Authentication • 1.3.6.1.4.1.49952.3.2.3.1 • 1.3.6.1.4.1.49952.3.2.3.2 • 1.3.6.1.4.1.49952.3.2.3.3 • 1.3.6.1.4.1.49952.3.2.3.4 • 1.3.6.1.4.1.49952.3.2.3.5 • 1.3.6.1.4.1.49952.3.2.3.6	Fixed
CRL Distribution Points	http://pki.vms.frcs.org.fj/pki/VMSRCA.crl or http://pki.vms.frcs.org.fj/pki/VMSICA1.crl	Fixed
Authority Information Access	http://pki.vms.frcs.org.fj/pki/VMSRCA.cer or http://pki.vms.frcs.org.fj/pki/VMSICA1.cer	Fixed
Basic Constraints (Critical)	Indicates whether the subject of the Digital Certificate is a CA and the maximum depth of valid certification paths that include this Certificate	Fixed
Thumbprint Algorithm	The algorithm used to hash the Certificate	Fixed
Thumbprint	The system generated hash of the Certificate	Fixed

7.1.3 Algorithm Object Identifiers

N/A

7.1.4 Name Forms

See 3.1.1

7.1.5 Name Constraints

See 3.1.1

7.1.6 CP/CPS Object Identifier

The Object Identifiers (OIDs) assigned to this CP/CPS are

- 1.3.6.1.4.1.49952.3.2.4.1
- 1.3.6.1.4.1.49952.3.2.4.2

7.1.7 Usage of Policy Constraints Extension

N/A

7.1.8 Policy Qualifiers Syntax and Semantics

Digital Certificates issued within the FRCS VMS PKI contain

- one of the Object Identifiers for this CP/CPS in Certificate Policy and
- an Object Identifier representing the FRCS VMS Certificate type in EKU.

7.1.9 Processing Semantics for The Critical Certificate Policies Extension

Key Usage has critical extension on all Digital Certificates limiting key par usage

- CA: for certificate signing and CRL signing
- Certificate Holders: Digital Signature and/or Key Encipherment depending on Certificate type

Basic Constraint has critical extension on all Digital Certificates limiting

- Root CA is CA type and can have only one level of Issuing CA
- Issuing CA is CA type and cannot issue certificate for CA
- Certificate Holders are end-entity certificates

7.2 Certificate Revocation List Profile

Certificate Revocation Lists are issued in the X.509 version 2 format in accordance with RFC 5280.

7.2.1 Root CA CRL

Root CA CRL is published every 6 months, and CRL overlap period is 2 weeks.

FIELDS	CONTENT	DEMARCATION
Version	Version 2	Fixed
Issuer	Issuer is the entity that has signed and issued the certificate	Fixed
Effective date	The date and time on which the CRL validity period begins	Fixed
Next update	The date and time on which the CRL validity period ends	Fixed
Signature Algorithm	The algorithm used to sign the CRL	Fixed
Signature HASH Algorithm	The algorithm used to hash the CRL	Fixed
Authority Key Identifier	This field contains the Subject Key Identifier of the issuer’s Certificate	Fixed
CA Version	This field contains the ID of the CA key	Fixed
CRL Number	This field contains the serial number of the CRL	Fixed
Next CRL publish	The date and time on which new CRL is published	Fixed
Revocation list	Revoked certificates include: • Certificate serial number • Revocation date • Revocation reason code	Fixed

7.2.2 Issuing CA CRL

Issuing CA Base CRL is published every 7 days, and CRL overlap period is 1 day.

Issuing CA delta CRL is published every day, and CRL overlap period is 6 hours.

7.2.2.1 Issuing CA Base CRL

FIELDS	CONTENT	DEMARCATION
Version	Version 2	Fixed

Issuer	Issuer is the entity that has signed and issued the certificate	Fixed
Effective date	The date and time on which the CRL validity period begins	Fixed
Next update	The date and time on which the CRL validity period ends	Fixed
Signature Algorithm	The algorithm used to sign the CRL	Fixed
Signature HASH Algorithm	The algorithm used to hash the CRL	Fixed
Authority Key Identifier	This field contains the Subject Key Identifier of the issuer's Certificate	Fixed
CA Version	This field contains the ID of the CA key	Fixed
CRL Number	This field contains the serial number of the CRL	Fixed
Next CRL publish	The date and time on which new CRL is published	Fixed
Freshest CRL	Delta CRL URL path	Fixed
Revocation list	Revoked certificates include: • Certificate serial number • Revocation date • Revocation reason code	Fixed

7.2.2.2 Issuing CA Delta CRL

FIELDS	CONTENT	DEMARCATION
Version	Version 2	Fixed
Issuer	Issuer is the entity that has signed and issued the certificate	Fixed
Effective date	The date and time on which the CRL validity period begins	Fixed
Next update	The date and time on which the CRL validity period ends	Fixed
Signature Algorithm	The algorithm used to sign the CRL	Fixed
Signature HASH Algorithm	The algorithm used to hash the CRL	Fixed
Authority Key Identifier	This field contains the Subject Key Identifier of the issuer's Certificate	Fixed
CA Version	This field contains the ID of the CA key	Fixed
CRL Number	This field contains the serial number of the CRL	Fixed
Next CRL publish	The date and time on which new CRL is published	Fixed
Delta CRL indicator	Base CRL Number	Fixed
Revocation list	Revoked certificates include: • Certificate serial number • Revocation date • Revocation reason code	Fixed

7.3 Online Certificate Status Protocol Profile

N/A

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency, Circumstance and Standards of Assessment

FRCS VMS PKI conduct internal audit and assessments minimum once a year.

8.2 Identity and Qualifications of Assessor

FRCS VMS PKI internal process.

8.3 Assessor’s Relationship to Assessed Entity

FRCS VMS PKI internal process.

8.4 Topics Covered by Assessment

FRCS VMS PKI internal process.

8.5 Actions Taken as A Result of Deficiency

FRCS VMS PKI internal process.

8.6 Publication of Audit Results

FRCS VMS PKI internal process.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

Fees may be payable with respect to the

- Issuing of Digital Certificates,
- re-issuing of Digital Certificates,
- revocation of Digital Certificates,

No fees for status information access.

No refund policy will be established.

9.2 Financial Responsibilities

No Insurance or Warranty Coverage for End-Entities.

9.3 Confidentiality of Business Information

Any personal or corporate information held by Issuing CAs related to a Certificate Holder’s application and the issuing of Digital Certificates is part of FRCS VMS system and will follow rules of FRCS VMS system.

9.4 Privacy of Personal Information

The content of Digital Certificates issued by FRCS VMS PKI is public information and deemed not private.

All information about Certificate Holders that is not publicly available through the content of issued Digital Certificates is part of FRCS VMS system and will follow rules of FRCS VMS system.

Except for reason codes contained in a Certificate Revocation List, the detailed reason for a Digital Certificate being revoked, (if applicable) remains part of FRCS VMS system.

9.5 Intellectual Property Rights

FRCS VMS PKI OID starts with 1.3.6.1.4.1.49952.3.2.

9.6 Representations and Warranties

FRCS VMS PKI is support process of FRCS VMS system.

9.7 Disclaimers of Warranties

FRCS VMS PKI is support process of FRCS VMS system.

9.8 Liability and Limitations of Liability

FRCS VMS PKI is support process of FRCS VMS system.

9.9 Indemnities

FRCS VMS PKI is support process of FRCS VMS system.

9.10 Term and Termination

This CP/CPS becomes effective upon publication in the FRCS VMS PKI Repository. This CP/CPS shall remain in force until it is amended or replaced by a new version.

9.11 Individual Notices and Communications with Participants

FRCS VMS PKI is support process of FRCS VMS system.

9.12 Amendments

Amendments to this CP/CPS are made and approved by the FRCS VMS PKI Policy Management Authority. Frequency is not defined.

9.13 Dispute Resolution Provisions

N/A

9.14 Governing Law

N/A

9.15 Compliance with Applicable Law

N/A

9.16 Miscellaneous Provisions

N/A

9.17 Other Provisions

N/A

10 APPENDIX A

Within the FRCS VMS PKI an Issuing CA can only issue Digital Certificates with approved Digital Certificate types.

Certificate Type	**Description**	**Certificate type OID (EKU)**	**Certificate class OID (Certificate Policy)**	**token**
3.1	Intend for Web Site server authentication	1.3.6.1.4.1.49952.3.2.3.1	1.3.6.1.4.1.49952.3.2.4.1	No
3.2	Intend for Web site client authentication	1.3.6.1.4.1.49952.3.2.3.2	1.3.6.1.4.1.49952.3.2.4.1	No
3.3	Intend for Invoice Signing outside FRCS	1.3.6.1.4.1.49952.3.2.3.3	1.3.6.1.4.1.49952.3.2.4.2	Yes
3.4	Intend for Web site client authentication (paired with type 3.3)	1.3.6.1.4.1.49952.3.2.3.4	1.3.6.1.4.1.49952.3.2.4.2	Yes
3.5	Intend for Invoice Signing inside FRCS	1.3.6.1.4.1.49952.3.2.3.5	1.3.6.1.4.1.49952.3.2.4.1	No
3.6	Intend encrypting messages for FRCS	1.3.6.1.4.1.49952.3.2.3.6	1.3.6.1.4.1.49952.3.2.4.1	No

10.1 Digital Certificate Type 3.1

All web traffic except invoice verification service both external and internal is protected using https and client certificates. This type of certificate is intended for server’s authentication.

Web traffic for invoice verification service does not require authentication service and is https protected with public third-party certificates that is trusted by most used clients.

10.2 Digital Certificate Type 3.2

All internal services use this type of certificate to authenticate to web site services.

Organization authorized person can request this type of certificates for fiscalization solutions that use FRCS VMS online service for signing invoices. This certificate is distributed to Organization in form of PKCS#12 and protected with password defined by Organization authorized person.

10.3 Digital Certificate Type 3.3

For fiscalization solutions that do not use FRCS VMS online service, this is signing invoices certificate. This type of certificate is smart card (token) mandatory for protecting private key and PIN for activating data. Prior to issuing of certificate, PIN is defined by Organization authorized person.

10.4 Digital Certificate Type 3.4

Certificate type 3.3 is not for authenticating to FRCS VMS web site services. Type 3.4 fill in smart card usage for authenticating to FRCS VMS web site services.

10.5 Digital Certificate Type 3.5

FRCS VMS internal services use this type of certificate to sign invoices.

10.6 Digital Certificate Type 3.6

FRCS VMS use this certificate type for communication with smart card holding certificate type 3.3 for audit purpose.

11 APPENDIX B

11.1 Definitions and Acronyms

“Applicant” means an Organization or Organization authorized person prior to issuing of a Digital Certificate.

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

“Certification” means the process of creating a Digital Certificate for an entity and binding that entity’s identity to the Digital Certificate.

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

“Certification Authority Officer” means a responsible person, in a trusted role, who is involved in the day-to-day operations of a Certification Authority.

“CP/CPS” is a publicly available document that details the FRCS VMS PKI and describes the practices employed in issuing Digital Certificates.

“Certificate Holder” means a Holder of a Digital Certificate chained to the FRCS VMS PKI Root Certificate, including without limitation, organizations, individuals and/or hardware and/or software devices. A Certificate Holder is

- named in a Digital Certificate or responsible for the Device named in a Digital Certificate and
- holds a Private Key corresponding to the Public Key listed in that Digital Certificate.

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

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

“Certificate Renewal” is when all the identifying information and the Public Key from the old certificate are duplicated in the new certificate, but there is a different (longer) validity period.

“Certificate Re-issuing” is when a Certificate Holder registers for a new certificate, but there is an opportunity to change the identifying information (e.g. new email address, new last name, etc.) or other information (corrected certificate policies, modified key usage, etc.) from what was in the old certificate. The new certificate also has a different Public Key and a different validity period from the old certificate.

“Certificate Re-key” is when all the identifying information from the old certificate is duplicated in the new certificate, but there is a different Public Key and a different validity period.

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

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

“Cryptographic Module” means secure software, device or utility that

- generates Key Pairs
- stores cryptographic information and/or
- performs cryptographic functions.

“Digital Certificate” means a digital identifier within the FRCS VMS PKI that:

- identifies the Issuing CA
- identifies the Holder
- contains the Holder's Public and Private Keys
- specifies the Digital Certificate's Operational Term
- is digitally signed by the Issuing CA
- has prescribed Key Usages and Reliance Factor that governs its issuing and use whether expressly included or incorporated by reference to this CP/CPS.

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

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

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

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

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

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

“Identify” means a process to distinguish a subject or entity from other subjects or entities and means a set of attributes which together uniquely identify a natural person or entity

“Identification” means reliance on data to distinguish and Identify a natural person or entity.

“Individual” means a natural person.

“Issuing Certification Authority” (“Issuing CA”) means a Certification Authority duly authorized to operate by FRCS VMS PKI to issue Digital Certificates to Certificate Holders.

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

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

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

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

“Operational Term” means the term of validity of a Digital Certificate commencing on the date of its issue and terminating on the earlier of

- the date disclosed in that Digital Certificate or
- the date of that Digital Certificate’s Revocation.

“Organization” means an entity that is legally recognized by FRCS VMS as taxpayer.

“Participants” means participants within the FRCS VMS PKI and include

- Issuing CAs
- Certificate Holders, (including Certificate Applicants)

“PKCS” means Public-Key Cryptography Standard.

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

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

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

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

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

“Registration Authority” means a Registration Authority designated by an Issuing CA to operate within the FRCS VMS PKI responsible for identification and authentication of Certificate Holders.

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

“Relying Party” means a party that acts in reliance on a Digital Certificate. Any party receiving a signed electronic document may rely on that Digital Signature after using FRCS VMS verification service.

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

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

“Validation” means a check of the applicable Certificate Revocation List(s) of the validity of a Digital Certificate and the validity of any Digital Certificate in that Digital Certificate’s Certificate Chain for the purpose of confirming that the Digital Certificate is valid at the time of the check (i.e., it is not revoked or expired).