RCS Rich Business Messaging (RBM) Verification Authority (VA) Certificate Policy and Certificate Practices Statement (CP/CPS)

iconectiv

Version 1.1

Approved 30 April 2021

Abstract

This document defines the security controls and practices to support the issuance of certificates for the RBM VA ecosystem. It is based on GSMA RCC.07 and is consistent with the Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 (IETF PKIX) Certificate Policy and Certification Practices Framework.

Table of Contents

RCS RICH BUSINESS MESSAGING (RBM) I

VERIFICATION AUTHORITY (VA) I

CERTIFICATE POLICY AND CERTIFICATE PRACTICES STATEMENT (CP/CPS) I

ABSTRACT I

1 RBM VA CERTIFICATE POLICY 1

1.1 Overview 1
1.2 Document Name and Identification 1
1.3 PKI Participants 1
1.3.1 RBM VA Authority 1
1.3.2 Subscribers 2
1.3.3 Relying Parties 2
1.3.4 Other Participants 2
1.4 Certificate Usage 2
1.4.1 Appropriate Certificate Usage 2
1.4.2 Prohibited Certificate Uses 2
1.5 Policy Administration 2
1.5.1 Organization Administering the Document 2
1.5.2 Contact Person 2
1.5.3 Entity determining CPS suitability for the policy 3
1.5.4 CP/CPS approval procedures 3
1.6 References 3
1.7 Definitions and Acronyms 4
1.7.1 Definitions 4
1.7.2 Acronyms 5

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES 6

2.1 Repositories 6
2.1.1 Policy Repository 6
2.1.2 Certificate Repository 6
2.2 Publication of Certification Information 6
2.3 Time or Frequency of Publication 6
2.4 Access Controls on Repositories 6

3 IDENTIFICATION AND AUTHENTICATION 6

3.1 Naming 7

3.1.1 TYPES OF NAMES 7
3.1.2 NEED FOR NAMES TO BE MEANINGFUL 7
3.1.3 ANONYMITY OR PSEUDONYMITY OF SUBSCRIBERS 7
3.1.4 RULES FOR INTERPRETING VARIOUS NAME FORM 7
3.1.5 UNIQUENESS OF NAME 7
3.1.6 RECOGNITION, AUTHENTICATION, AND ROLE OF TRADEMARKS 7
3.2 INITIAL IDENTITY VALIDATION 7
3.2.1 METHOD TO PROVE POSSESSION OF PRIVATE KEY 7
3.2.2 AUTHENTICATION OF ORGANIZATION IDENTITY 7
3.2.3 AUTHENTICATION OF INDIVIDUAL IDENTITY 7
3.2.4 NON-VERIFIED SUBSCRIBER INFORMATION 7
3.2.5 VALIDATION OF AUTHORITY 7
3.2.6 CRITERIA FOR INTEROPERATION 8
3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS 8
3.3.1 IDENTIFICATION AND AUTHENTICATION FOR ROUTINE RE-KEY 8
3.3.2 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY AFTER REVOCATION 8
3.3.3 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUESTS 8

4 CERTIFICATE AND DIGITAL SIGNATURE LIFE-CYCLE OPERATIONAL REQUIREMENTS 8

4.1 DIGITAL SIGNATURE APPLICATION 8
4.1.1 WHO CAN SUBMIT A DIGITAL SIGNATURE APPLICATION 8
4.1.2 ENROLLMENT PROCESS AND RESPONSIBILITIES 8
4.2 APPLICATION PROCESSING 8
4.2.1 PERFORMING IDENTIFICATION AND AUTHENTICATION FUNCTIONS 8
4.2.2 APPROVAL OR REJECTION OF APPLICATIONS 9
4.2.3 TIME TO PROCESS APPLICATIONS 9
4.3 CERTIFICATE AND SIGNATURE ISSUANCE 9
4.3.1 CA ACTIONS DURING CERTIFICATE AND DIGITAL SIGNATURE ISSUANCE 9
4.3.2 NOTIFICATION TO SUBSCRIBER BY THE RBM VA OF ISSUANCE OF SIGNED JWT 9
4.4 CERTIFICATE AND DIGITAL SIGNATURE ACCEPTANCE 9
4.4.1 CONDUCT CONSTITUTING ACCEPTANCE 9
4.4.2 NOTIFICATION OF ISSUANCE OTHER ENTITIES 9
4.5 KEY PAIR, CERTIFICATE, AND SIGNED JWT USAGE 9
4.5.1 SUBSCRIBER PRIVATE KEY AND CERTIFICATE USAGE 9
4.5.2 RELYING PARTY PUBLIC KEY, CERTIFICATE AND SIGNED JWT USAGE 10
4.6 CERTIFICATE AND JWT SIGNATURE RENEWAL 10
4.6.1 CIRCUMSTANCE FOR RENEWAL 10
4.6.2 WHO MAY REQUEST RENEWAL 10
4.6.3 PROCESSING RENEWAL REQUESTS 10
4.6.4 NOTIFICATION OF ISSUANCE TO SUBSCRIBER 10
4.6.5 CONDUCT CONSTITUTING ACCEPTANCE OF A RENEWAL 10
4.6.6 PUBLICATION OF THE RENEWAL 10
4.6.7 NOTIFICATION OF ISSUANCE TO OTHER ENTITIES 10
4.7 CERTIFICATE RE-KEY 10
4.7.1 CIRCUMSTANCE FOR CERTIFICATE RE-KEY 10
4.7.2 WHO MAY REQUEST CERTIFICATION OF A NEW PUBLIC KEY 11
4.7.3 PROCESSING CERTIFICATE RE-KEYING REQUEST 11

4.7.4 NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER 11
4.7.5 CONDUCT CONSTITUTING ACCEPTANCE OF A RE-KEYED CERTIFICATE 11
4.7.6 PUBLICATION OF THE RE-KEYED CERTIFICATE 11
4.7.7 NOTIFICATION OF CERTIFICATE ISSUANCE TO OTHER ENTITIES 11
4.8 CERTIFICATE MODIFICATION 11
4.8.1 CIRCUMSTANCE FOR CERTIFICATE MODIFICATION 11
4.8.2 WHO MAY REQUEST CERTIFICATE MODIFICATION 11
4.8.3 PROCESSING CERTIFICATE MODIFICATION REQUESTS 11
4.8.4 NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER 11
4.8.5 CONDUCT CONSTITUTING ACCEPTANCE OF MODIFIED CERTIFICATE 11
4.8.6 PUBLICATION OF THE MODIFIED CERTIFICATE 11
4.8.7 NOTIFICATION OF CERTIFICATE ISSUANCE TO OTHER ENTITIES 11
4.9 CERTIFICATE REVOCATION AND SUSPENSION 11
4.9.1 CIRCUMSTANCES FOR REVOCATION 11
4.9.2 WHO CAN REQUEST REVOCATION 12
4.9.3 PROCEDURE FOR REVOCATION REQUEST 12
4.9.4 REVOCATION REQUEST GRACE PERIOD 12
4.9.5 TIME WITHIN WHICH RBM VA MUST PROCESS THE REVOCATION REQUEST 12
4.9.6 REVOCATION CHECKING REQUIREMENT FOR RELYING PARTIES 12
4.9.7 CRL ISSUANCE FREQUENCY (IF APPLICABLE) 12
4.9.8 MAXIMUM LATENCY FOR CRLS (IF APPLICABLE) 12
4.9.9 ON-LINE REVOCATION/STATUS CHECKING AVAILABILITY 12
4.9.10 ON-LINE REVOCATION CHECKING REQUIREMENTS 12
4.9.11 OTHER FORMS OF REVOCATION ADVERTISEMENTS AVAILABLE 13
4.9.12 SPECIAL REQUIREMENTS REGARDING KEY COMPROMISE 13
4.9.13 CIRCUMSTANCES FOR SUSPENSION 13
4.9.14 WHO CAN REQUEST SUSPENSION 13
4.9.15 PROCEDURE FOR SUSPENSION REQUEST 13
4.9.16 LIMITS ON SUSPENSION PERIOD 13
4.10 CERTIFICATE STATUS SERVICES 13
4.10.1 OPERATIONAL CHARACTERISTICS 13
4.10.2 SERVICE AVAILABILITY 13
4.10.3 OPTIONAL FEATURES 13
4.11 END OF SUBSCRIPTION 13
4.12 KEY ESCROW AND RECOVERY 14
4.12.1 KEY ESCROW AND RECOVERY POLICY AND PRACTICES 14
4.12.2 SESSION KEY ENCAPSULATION AND RECOVERY POLICY AND PRACTICES 14

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS 14

5.1 PHYSICAL SECURITY CONTROLS 14
5.1.1 SITE LOCATION AND CONSTRUCTION 14
5.1.2 PHYSICAL ACCESS 14
5.1.3 POWER AND AIR CONDITIONING 14
5.1.4 WATER EXPOSURES 14
5.1.5 FIRE PREVENTION AND PROTECTION 14
5.1.6 MEDIA STORAGE 14
5.1.7 WASTE DISPOSAL 14

5.1.8 OFF-SITE BACKUP 15
5.2 PROCEDURAL CONTROLS 15
5.2.1 TRUSTED ROLES 15
5.2.2 NUMBER OF PERSONS REQUIRED PER TASK 15
5.2.3 IDENTIFICATION AND AUTHENTICATION FOR EACH ROLE 15
5.2.4 ROLES REQUIRING SEPARATION OF DUTIES 16
5.3 PERSONNEL SECURITY CONTROLS 16
5.3.1 QUALIFICATIONS, EXPERIENCE, AND CLEARANCE REQUIREMENTS 16
5.3.2 BACKGROUND CHECK PROCEDURES 16
5.3.3 TRAINING REQUIREMENTS 16
5.3.4 RETRAINING FREQUENCY AND REQUIREMENTS 17
5.3.5 JOB ROTATION FREQUENCY AND SEQUENCE 17
5.3.6 SANCTIONS FOR UNAUTHORIZED ACTIONS 17
5.3.7 INDEPENDENT CONTRACTOR REQUIREMENTS 17
5.3.8 DOCUMENTATION SUPPLIED TO PERSONNEL 17
5.4 AUDIT LOGGING PROCEDURES 17
5.4.1 TYPES OF EVENTS RECORDED 17
5.4.2 FREQUENCY OF PROCESSING LOG 18
5.4.3 RETENTION PERIOD FOR AUDIT LOG 18
5.4.4 PROTECTION OF AUDIT LOG 18
5.4.5 AUDIT LOG BACKUP PROCEDURES 18
5.4.6 AUDIT COLLECTION SYSTEM (INTERNAL VS. EXTERNAL) 18
5.4.7 NOTIFICATION TO EVENT-CAUSING SUBJECT 18
5.4.8 VULNERABILITY ASSESSMENTS 18
5.5 RECORDS ARCHIVAL 19
5.5.1 TYPES OF RECORDS ARCHIVED 19
5.5.2 RETENTION PERIOD FOR ARCHIVE 19
5.5.3 PROTECTION OF ARCHIVE 19
5.5.4 ARCHIVE BACKUP PROCEDURES 19
5.5.5 REQUIREMENTS FOR TIME-STAMPING OF RECORDS 20
5.5.6 ARCHIVE COLLECTION SYSTEM (INTERNAL OR EXTERNAL) 20
5.5.7 PROCEDURES TO OBTAIN AND VERIFY ARCHIVE INFORMATION 20
5.6 KEY CHANGEOVER 20
5.7 COMPROMISE AND DISASTER RECOVERY 20
5.7.1 INCIDENT AND COMPROMISE HANDLING PROCEDURES 20
5.7.2 COMPUTING RESOURCES, SOFTWARE, AND/OR DATA ARE CORRUPTED 20
5.7.3 PRIVATE KEY COMPROMISE PROCEDURES 21
5.7.4 BUSINESS CONTINUITY CAPABILITIES AFTER A DISASTER 21
5.8 RBM VA TERMINATION 21

6 TECHNICAL SECURITY CONTROLS 21

6.1 KEY PAIR GENERATION AND INSTALLATION 21
6.1.1 KEY PAIR GENERATION 21
6.1.2 PRIVATE KEY DELIVERY TO SUBSCRIBER 22
6.1.3 PUBLIC KEY DELIVERY TO CERTIFICATE ISSUER 22
6.1.4 PUBLIC KEY DELIVERY TO RELYING PARTIES 22
6.1.5 KEY SIZES 22

6.1.6 Public Key Parameters Generation and Quality Checking 22
6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field) 22
6.2 Private Key Protection and Cryptographic Module Engineering Controls 22
6.2.1 Cryptographic Module Standards and Controls 22
6.2.2 Private Key Multi-person Control 22
6.2.3 Private Key Escrow 22
6.2.4 Private Key Backup 22
6.2.5 Private Key Archival 22
6.2.6 Private Key Transfer into or from a Cryptographic Module 23
6.2.7 Private Key Storage on Cryptographic Module 23
6.2.8 Method of Activating Private Key 23
6.2.9 Method of Deactivating Private Key 23
6.2.10 Method of Destroying Private Key 23
6.2.11 Cryptographic Module Rating 23
6.3 Other Aspects of Key Pair Management 23
6.3.1 Public Key Archival 23
6.3.2 Certificate Operational Periods and Key Pair Usage Periods 23
6.4 Activation Data 23
6.4.1 Activation Data Generation and Installation 23
6.4.2 Activation Data Protection 23
6.4.3 Other Aspects of Activation Data 24
6.5 Computer Security Controls 24
6.5.1 Specific Computer Security Technical Requirements 24
6.5.2 Computer Security Rating 25
6.6 Life Cycle Security Controls 25
6.6.1 System Development Controls 26
6.6.2 Security Management Controls 26
6.6.3 Life Cycle Security Controls 26
6.7 Network Security Controls 26
6.8 Time-Stamping 27

7 CERTIFICATE, CRL AND OCSP PROFILES 27

7.1 Certificate Profile 27
7.2 CRL Profile 27
7.2.1 Version Numbers 27
7.2.2 CRL and CRL Entry Extensions 27
7.3 OCSP Profile 27

8 COMPLIANCE AUDIT AND OTHER ASSESSMENT 27

8.1 Frequency or Circumstances of Assessment 28
8.2 Identity/Qualifications of Assessor 28
8.3 Assessor's Relationship to Assessed Entity 28
8.4 Topics Covered by Assessment 28
8.5 Actions Taken as a Result of Deficiency 28
8.6 Communication of Results 28

9 OTHER BUSINESS AND LEGAL MATTERS 28

9.1 FEES 28
9.1.1 CERTIFICATE ISSUANCE OR RENEWAL FEES 28
9.1.2 CERTIFICATE ACCESS FEES 28
9.1.3 REVOCATION ACCESS FEES 28
9.2 FINANCIAL RESPONSIBILITY 29
9.2.1 INSURANCE OR WARRANTY COVERAGE 29
NO STIPULATION 29
9.2.2 OTHER ASSETS 29
9.3 CONFIDENTIALITY OF BUSINESS INFORMATION 29
9.3.1 SCOPE OF CONFIDENTIAL INFORMATION 29
9.3.2 INFORMATION NOT WITHIN THE SCOPE OF CONFIDENTIAL INFORMATION 29
9.3.3 RESPONSIBILITY TO PROTECT CONFIDENTIAL INFORMATION 29
9.4 PRIVACY OF PERSONAL INFORMATION 29
9.4.1 PRIVACY PLAN 29
9.4.2 INFORMATION TREATED AS PRIVATE 29
9.4.3 RESPONSIBILITY TO PROTECT PRIVATE INFORMATION 29
9.4.4 DISCLOSURE PURSUANT TO JUDICIAL OR ADMINISTRATIVE PROCESS 29
9.5 INTELLECTUAL PROPERTY RIGHTS 29
9.6 REPRESENTATIONS AND WARRANTIES 30
9.6.1 VA REPRESENTATIONS AND WARRANTIES 30
9.6.2 RELYING PARTY REPRESENTATIONS AND WARRANTIES 30
9.6.3 SUBSCRIBER REPRESENTATIONS AND WARRANTIES 30
9.6.4 DISCLAIMERS OF WARRANTIES 30
9.7 LIMITATIONS OF LIABILITY 30
9.8 INDEMNITIES 30
9.8.1 INDEMNIFICATION 30
9.8.2 INDEMNIFICATION BY SUBSCRIBERS 30
9.8.3 INDEMNIFICATION BY RELYING PARTIES 30
9.9 TERM AND TERMINATION 30
9.9.1 TERM 30
9.9.2 TERMINATION 30
9.9.3 EFFECT OF TERMINATION AND SURVIVAL 30
9.10 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS 30
9.11 AMENDMENTS 31
9.11.1 PROCEDURE FOR AMENDMENT 31
9.11.2 NOTIFICATION MECHANISM AND PERIOD 31
9.11.3 CIRCUMSTANCES UNDER WHICH OID MUST BE CHANGED 31
9.12 DISPUTE RESOLUTION PROCEDURES 31
9.13 GOVERNING LAW 31
9.14 COMPLIANCE WITH APPLICABLE LAW 31
9.15 MISCELLANEOUS PROVISIONS 31
9.15.1 ENTIRE AGREEMENT 31
9.15.2 ASSIGNMENT 31
9.15.3 SEVERABILITY 31
9.15.4 FORCE MAJEURE 31

1 RBM VA Certificate Policy

1.1 Overview

This Certificate Policy and Certificate Practices Statement (CP/CPS) is the principal statement of requirements, policies, practices and procedures that RCS-based Rich Business Messaging (RBM) entities must adhere to regarding certificates and digitally signed tokens when operating within this iconectiv RBM Verification Authority (VA) Public Key Infrastructure (PKI). It sets forth the business, legal, and technical requirements for approving, issuing, managing, using, revoking, and renewing certificates and signed tokens, and providing associated trust services for all participants, as well as details of the practices and procedures that meet those requirements. These requirements and practices protect the security and integrity of the iconectiv RBM VA PKI and comprise a single set of rules that apply consistently to all subscribers, relying parties, Certificate Authorities (CAs), and other PKI entities that interoperate therein, so as to provide assurance of uniform trust throughout it. The RBM initiative and the sender verification aspects that rely upon a VA PKI are defined by the GSMA Rich Communications Services (RCS) standards.

iconectiv's certificate policies and practices are controlled by the iconectiv Policy Management Authority (PMA) that determines how this CP/CPS applies to the entities operating within this iconectiv RBM VA PKI. This CP/CPS conforms to the requirements specified in GSMA RCC.07 and the Certificate Policy and Certification Practices Framework of the Internet Engineering Task Force as defined in (IETF) RFC 3647. It also adopts the current version of the CA/Browser Forum requirements as set forth in the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates.

1.2 Document Name and Identification

This document is the iconectiv "RCS Rich Business Messaging Verification Authority Certificate Policy and Certificate Practices Statement".

- Version 1.1 was approved for publication on 30 April 2021.

This document has been assigned the following Object Identifier [OID]: 2.16.840.1.114569.3.1.1.1 for RBM VA CP/CPS Version 1.1

Subsequent revisions to this CP/CPS will contain new OID extensions corresponding to the RBM VA CP/CPS version or additional geographies in which the iconectiv RBM VA operates.

1.3 PKI Participants

The participants in the iconectiv RBM VA PKI model include CAs, RAs, Subscribers, and Relying Parties (collectively, "Participants"). The Root CA is operated as an offline CA. The root certificate is pre-loaded into the Relying Party platforms along with Subordinate CA certificates serving distinct communities. End-entities are issued certificates, and associated keys are used to sign specific chatbots or groups of chatbots and are conveyed in the signed chatbot JWT in the form of an X.509 URI (x5u) which identifies the location of the public certificate. In the context of the iconectiv RBM VA PKI, all certificates are issued by iconectiv.

1.3.1 RBM VA Authority

The iconectiv RBM VA implements multiple functions within its framework. These are:

- One Root CA, which provides the root certificate trust anchor for the PKI, and issues certificates for subordinate CAs.
- One or more Subordinate CAs, which issue certificates for End-Entities.
- One or more End-Entity applications, which received Subscriber requests and form and sign JSON Web Objects (JWTs) using the private keys associated with End-Entity certificates.
- A Registration Process (RP) for identification and authentication of applicants for a signed JSON Web Token (JWT).

The certificate validation process must traverse the entire certificate chain for a signed JWT and must end with the root certificate.

1.3.2 Subscribers

Subscribers use iconectiv’s RBM VA services to acquire a signed JWT in order to support communications within the RBM ecosystem as a verified and trusted sender. Subscribers under this CP/CPS are Business to Consumer (B2C) communications partners who apply for a signed JWT on behalf of businesses/brands, and the businesses/brands themselves. B2C partners may include, but are not limited to, messaging aggregators, cloud communications providers, contact centers, digital marketing firms, chatbot platform providers, or mobile network operators working directly with organizations/brands. Prior to issuance of a signed chatbot JWT, a Subscriber is an Applicant.

1.3.3 Relying Parties

The Service Provider(s) or mobile network operators, their consortium when applicable, their agent(s), RBM hosted platform providers, and the B2C partners managing chatbots for organizations/brands are all relying parties that use the public certificate associated with the JWT signature to confirm which chatbots were verified by the iconectiv RBM VA.

1.3.4 Other Participants

Mobile subscribers (i.e., end users) can view the certificate details for signed chatbots provided by the RBM messaging platform serving their mobile devices. In order to avoid confusion, this document will refer to these parties as end users or consumers rather than subscribers. These parties do not participate in the PKI directly.

1.4 Certificate Usage

The RBM VA issues not only X.509 certificates, but also signed JWTs. The certificates and signed JWTs issued within the RBM VA PKI trust model are used to confirm that chatbots are from Subscribers who are verified senders. This enables the business entity engaged in the communication with consumers to prove its identity has been verified. Such business senders with signed JWTs display a trust mark in the messaging inbox on the mobile device as well as branding in the form of a service icon or logo.

1.4.1 Appropriate Certificate Usage

The certificates and signed JWTs issued within the RBM VA PKI trust model are to be used solely to securely confirm the information regarding RBM VA participants, and chatbots that have been signed with a JWT signature.

1.4.2 Prohibited Certificate Uses

Any use other than described in Section 1.4.1, are prohibited by this CP.

1.5 Policy Administration

1.5.1 Organization Administering the Document

The CP/CPS is administered by the iconectiv RBM VA Policy Management Authority, who can be contacted at:

iconectiv RBM VA Policy Management Authority

100 Somerset Corporate Blvd, Bridgewater, NJ 08807

rcsva@iconectiv.com

1.5.2 Contact Person

Administrative support personnel handling revocation, reporting and other operational matters can be contacted at:

RBM VA Support iconectiv

100 Somerset Corporate Blvd Bridgewater, NJ 08807

Email: rcsva@iconectiv.com

Phone:888-856-0265

1.5.3 Entity determining CPS suitability for the policy

The iconectiv PMA determines the suitability and applicability of this CP/CPS and the conformance of procedures established by the iconectiv PMA Director. The suitability and applicability criteria include the results and recommendations received from an independent auditor (see Section 8). The RBM VA is also responsible for evaluating and acting upon the results of any internal or external compliance audits.

1.5.4 CP/CPS approval procedures

Approvals of this CP/CPS and any amendments thereof are made by the PMA. Amendments shall be made by publishing a new version of this CP/CPS. Amendments may be based on, but are not limited to, changes to industry regulations, standards, business changes, or technical changes to the RBM VA infrastructure or application capabilities. A new version of the CP/CPS will become effective fifteen (15) days after such posting and will supersede all previous versions and will be binding on all Participants in the RBM VA from that point forward.

1.6 References

At the time of publication, the editions indicated below were valid. All standards are subject to revision, and parties to agreements based on this document are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below.

FIPS 186-4*, Digital Signature Standard*

GSMA RCC.07, *Rich Communication Suite – Advanced Communications Services and Client Specification v11.0*

GSMA RCC.59, *North America RCS Common Implementation Guidelines Version 4.0*

ISO/IEC 27001:2013*, Information technology – Security techniques – Information security management systems – Requirements*

NIST Cyber Security Framework*, Version 1.1*

RFC 3647, *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.*

RFC 4949, *Internet Security Glossary, Version 2.2*.

RFC 5217, *Memorandum for Multi-Domain Public Key Infrastructure Interoperability.*

RFC 5280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.*

RFC 5905, *Network Time Protocol Version 4 (NTPv4).*

RFC 7159, *The JavaScript Object Notation (JSON).*

RFC 7231, *Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content.*

RFC 7515, *JSON Web Signatures (JWS).*2 RFC 7516, *JSON Web Algorithms (JWA).*2 RFC 7517, *JSON Web Key (JWK).*

RFC 7518, *JSON Web Algorithm (JWA).*

RFC 7519, *JSON Web Token (JWT).*

RFC 8224, *Authenticated Identity Management in the Session Initiation Protocol*.

X.501, *ITU-T Recommendation X.501 (2005)* | *ISO/IEC 9594-2:2005, Information technology - Open Systems Interconnection The Directory: Models.*

1.7 Definitions and Acronyms

1.7.1 Definitions

The following provides some key definitions used in this document. Refer to IETF RFC 4949 for a complete Internet Security Glossary for many of these terms.

(Digital) Certificate: Binds a public key to a Subject (e.g., the end-entity). A certificate document in the form of a digital data object (a data object used by a computer) to which is appended a computed digital signature value that depends on the data object. [RFC 4949].

Certificate Chain: See Certification Path.

Certification Path: A linked sequence of one or more public-key certificates that enables a certificate user to verify the signature on the last certificate in the path, and thus enables the user to obtain (from that last certificate) a certified public key, or certified attributes, of the system entity that is the subject of that last certificate. Synonym for Certificate Chain. [RFC 4949].

Certificate Policy (CP): A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. [RFC 3647].

Certification Practice Statement (CPS): A statement of the practices that a certification authority employs in issuing, managing, revoking, and renewing or re-keying certificates. [RFC 3647].

Certificate Revocation List (CRL): A data structure that enumerates digital certificates that have been invalidated by their issuer prior to when they were scheduled to expire. [RFC 4949].

CPS Summary (or CPS Abstract) - A subset of the provisions of a complete CPS that is made public by a CA. [RFC 3647].

Certificate Signing Request (CSR): A CSR is sent to a CA to get enrolled. A CSR contains a Public Key of the end-entity that is requesting the certificate.

Certificate Validation: An act or process by which a certificate user established that the assertions made by a certificate can be trusted. [RFC 4949].

Chain of Trust: Deprecated term referring to the chain of certificates to a Trust Anchor. Synonym for Certification Path or Certificate Chain. [RFC 4949].

End-Entity: An entity that participates in the Public Key Infrastructure (PKI). Usually a Server, Service, Router, or a Person.

Fingerprint: A hash result ("key fingerprint") used to authenticate a public key or other data [RFC 4949].

Identity: Unless otherwise qualified, an identifier that unambiguously distinguishes an entity for authentication and other security and policy application purposes. In this CP, an organization or brand is an example of the identity of one kind of participant in the certificate management process.

Issuing CA: A Certification Authority that issues certificates to an End-Entity.

Online Certificate Status Protocol (OCSP): An Internet protocol used by a client to obtain the revocation status of a certificate from a server.

Policy Management Authority (PMA): A person, role, or organization within a PKI that is responsible for (a) creating or approving the content of the certificate policies and CPSs that are used in the PKI; (b) ensuring the administration of those policies; and (c) approving any cross-certification or interoperability agreements with CAs external to the PKI and any related policy mappings. The PMA may also be the accreditor for the PKI as a whole or for some of its components or applications.

Private Key: The key of a Key Pair that is kept secret by the holder of the Key Pair, and that is used to create digital signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key. [RFC 4949].

Public Key: The publicly disclosable component of a pair of cryptographic keys used for asymmetric cryptography by a Relying Party to verify digital signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key [RFC 4949].

Public Key Infrastructure (PKI): The set of hardware, software, personnel, policy, and procedures used by a CA to issue and manage certificates. [RFC 4949].

Relying party: The entities that use the public certificate associated with the JWT signature to confirm the verification status of chatbots. [RFC 5217].

Root CA: A CA that is directly trusted by an end-entity. The certificate path to a Root may include subordinate certificates and End-Entity certificates.

Signature: Created by signing digital object using the Private Key. It ensures the identity of the message sender and the integrity of related chatbot attributes. [RFC 4949].

Trust Anchor: An established point of trust (usually based on the authority of some person, office, or organization) from which a certificate user begins the validation of a certification path. The combination of a trusted public key and the name of the entity to which the corresponding Private Key belongs. [RFC 4949].

Trusted CA: A CA upon which a certificate user relies for issuing valid certificates; especially a CA that is used as a trust anchor CA. [RFC 4949].

Trust List: A set of one or more trust anchors used by a relying party to explicitly trust one or more PKIs. [RFC 5217].

Trust Model: Describes how trust is distributed from Trust Anchors.

Verification Authority (VA): An entity acting as the Certification Authority that issues digital certificates (especially X.509 certificates) and vouches for the binding between the data items in a certificate and any digital signatures issued thereunder. [RFC 4949].

1.7.2 Acronyms

CA	Certification Authority
CN	Common Name
CRL	Certificate Revocation List
CP	Certificate Policy
CPS	Certification Practice Statement
CR	Certificate Repository
CSR	Certificate Signing Request
DN	Distinguished Name
HTTPS	Hypertext Transfer Protocol, Secure
IETF	Internet Engineering Task Force
JSON	JavaScript Object Notation
JWT	JSON Web Token
OCSP	On-line Certificate Status Protocol
PKI	Public Key Infrastructure
PMA	Policy Management Authority
RBM	Rich Business Messaging

RCS	Rich Communications Services (a GSMA standard)
URI VA	Uniform Resource Identifier Verification Authority

2 Publication and Repository Responsibilities

2.1 Repositories

The RBM VA shall make policy, certificate, and revocation information available in accordance with this CP/CPS. The RBM VA shall ensure that its issued certificates and signed JWTs and their revocation data are regularly available through an online repository.

2.1.1 Policy Repository

The CP/CPS is available at:

https://intel.iconectiv.com/legal-intel

2.1.2 Certificate Repository

End-Entity Certificates locations are made available at the address encoded in the JWT Protected Header X5U. Root and Subordinate certificates are provided via out-of-band means.

2.2 Publication of Certification Information

The RBM VA publicly discloses its CP/CPS through an appropriate and readily accessible online means that is available on a 24x7 basis (see 2.1.1). The RBM VA publicly discloses its business practices to the extent required by the RBM VA's selected audit scheme (see Section 8).

The RBM VA, through this document, publicly gives effect to these requirements and practices and represents that it will adhere to the latest published version.

2.3 Time or Frequency of Publication

Updates to this CP/CPS are established in Section 1.5.4. The RBM VA updates and publishes the CP/CPS, and any associated Subscriber or Relying Party agreements, as necessary.

2.4 Access Controls on Repositories

Through the use of online repositories and mechanisms as detailed in this document, the RBM VA ensures access to this CP/CPS, Certificates, CRLs and Certificate Status information to all Relying Parties. The RBM VA implements access controls to prevent unauthorized adding, modifying or deleting repository entries.

3 Identification and Authentication

3.1 Naming

3.1.1 Types of Names

No stipulation.

3.1.2 Need for Names to be Meaningful

No stipulation.

3.1.3 Anonymity or Pseudonymity of Subscribers

No stipulation.

3.1.4 Rules for Interpreting Various Name Form

No stipulation.

3.1.5 Uniqueness of Name

The RBM VA certifies that subject names uniquely identify certificate issuers, and that the JWT signatures encode attributes that uniquely identify a chatbot.

3.1.6 Recognition, Authentication, and Role of Trademarks

RBM chatbots include a service icon which could be trademarked or, alternately, a Brand default logo. This is encoded in the chatbot signature if provided. The RBM VA verifies an Applicant's right to use a trademark and may reject any application or require revocation by Relying Parties of any chatbot signature that is part of a trademark dispute. The trademark status is verified by checking that the logo serial number is in the Issued and Active status.

3.2 Initial Identity Validation

The RBM VA may use any legal means of communication or investigation to ascertain the identity of an organizational or individual Applicant.

3.2.1 Method to Prove Possession of Private Key

Not applicable

3.2.2 Authentication of Organization Identity

Certificates contain the 'countryName' field and other Subject Identity Information.

With respect to JWT signature, the RBM VA verifies that an Applicant is a licensed/legitimate entity in the stated jurisdiction in the country associated with the Applicant. If the Applicant Identity Information is to include the name or address of an organization, the RBM VA verifies the identity and address of the organization and that the address is the Applicant's address of existence or operation The RBM VA may use the same documentation or communication methods to verify both the Applicant's identity and address. The verification is achieved using reliable third-party data sources.

3.2.3 Authentication of Individual Identity

The RBM VA employs procedures to identify at least one individual as a representative of each Subscriber. When Business to Consumer (B2C) communications partners apply for a signed JWT on behalf of businesses/brands, the partners must employ procedures to identify at least one individual as a representative of each business/brand.

3.2.4 Non-verified Subscriber Information

Information that is not verified is identified in the RBM VA attribute repository for Subscribers and their chatbots.

3.2.5 Validation of Authority

The RBM VA employs procedures to verify that an entity or individual claiming to represent a Subscriber to which a digital signature is issued is authorized to represent that Subscriber in this context. These procedures may include the verification of the Subscriber's business identity through established repositories, identification systems and classification systems, as well as execution of a service agreement and collection and verification of billing information.

3.2.6 Criteria for Interoperation

This RBM VA is not intended to interoperate with any other PKI.

3.3 Identification and Authentication for Re-key Requests

Re-Keys are not supported in this PKI.

3.3.1 Identification and Authentication for Routine Re-key

NA

3.3.2 Identification and Authentication for Re-key after Revocation

NA

3.3.3 Identification and Authentication for Revocation Requests

The specific certificate to be revoked needs to be identified, published to Relying Parties, and the reason for revocation documented for audit purposes and review by the iconectiv PMA.

4 Certificate and Digital Signature Life-Cycle Operational Requirements

This component of the CP/CPS specifies requirements and practices imposed upon and carried out by the CAs within the RBM VA with respect to the life cycle of certificates and signed JWTs.

4.1 Digital Signature Application

4.1.1 Who can Submit a Digital Signature Application

Applications can be submitted by anyone who complies with the provisions specified in the registration form, CP/CPS and relevant End-User Agreements.

4.1.2 Enrollment Process and Responsibilities

Prior to the issuance of a signed JWT for a Subscriber, the RMB VA obtains at a minimum the following documentation from the Subscriber:

1. A chatbot enrollment request, which is electronic; and
2. An executed Subscriber Agreement or Terms of Use, which is electronic.

Prior to the issuance of a signed JWT, the RBM VA obtains from the Applicant an enrollment request in a form prescribed by the RBM VA. Multiple signed JWTs may be issued to the same Applicant, provided that each request is supported by a valid, current chatbot request signed by the appropriate Applicant Representative on behalf of the Applicant. The request is made, submitted and/or signed electronically. The request contains a request from, or on behalf of, the Applicant for the issuance of a chatbot signature, and a certification by, or on behalf of, the Applicant that all of the information contained therein is correct.

4.2 Application Processing

This Section describes the procedure for processing Subscriber applications for signed JWTs.

4.2.1 Performing Identification and Authentication Functions

The Applicant request includes all factual information about the Applicant to be included in the verification process, and such additional information as is necessary for the RBM VA to obtain from the Applicant in order to comply with this CP/ CPS. The RBM VA ensures that all communication between the RBM VA and a Subscriber regarding digital signature issuance or changes in the status of a signature are made using secure and auditable methods.

4.2.2 Approval or Rejection of Applications

The RBM VA has established programmatic procedures for application verification in accordance with Relying Party policies. In each case, the RBM VA identifies which information elements in the application verification process were not verifiable or were only partially verifiable. When an application cannot be verified, the RBM VA records a reason for rejecting an application.

4.2.3 Time to Process Applications

All parties involved in digital signature application processing shall use reasonable efforts to provide requisite information to ensure that applications may be processed in a timely manner. Once an application is received, the request for multi-factor information is communicated to the applicant within a maximum of one business day. Given the multi-factor authentication means involved in processing an application, there is no time stipulation to complete the processing of an application unless otherwise indicated in the relevant Subscriber Agreement, CP/CPS or other Agreement between the RBM VA participants.

4.3 Certificate and Signature Issuance

4.3.1 CA Actions During Certificate and Digital Signature Issuance

Subordinate Certificate issuance by the root CA requires an individual authorized by the root CA to deliberately issue a direct command in order to perform certificate signing operations for received CSRs. Multiple individuals in unique roles are required to sign, retrieve, and install Subordinate certificates.

Issuance by a Subordinate CA of End-Entity Certificates, and issuance of signed JWTs by the RBM VA, is automated and secured using access control and application permissions, as well as secure key stores for all end-entity secret keys.

4.3.2 Notification to Subscriber by the RBM VA of Issuance of Signed JWT

The RBM VA notifies the Subscriber within a reasonable time of signed JWT issuance and may use any reliable mechanism to deliver the signed JWT to the Subscriber and/or Relying Parties. The RBM VA uses a REST API (Notification API) to notify subscribed parties when the JWS has been issued/reissued. Alternatively, parties can also register for email notifications.

4.4 Certificate and Digital Signature Acceptance

4.4.1 Conduct Constituting Acceptance

The passage of time after delivery or notice of issuance of a signed JWT to the Subscriber or the actual use of a signed JWT constitutes the Subscriber’s acceptance of the object.

4.4.2 Notification of Issuance Other Entities

Notification will consist of Certificates and signed JWTs being published to the RMB VA’s repository. The certificate location associated with the JWS is explicitly indicated in the JWTs protected header x5u. Relying Parties may also be notified of the issuance of signed JWTs.

4.5 Key Pair, Certificate, and Signed JWT Usage

A summary of the RBM VA framework for the PKI is provided below.

4.5.1 Subscriber Private Key and Certificate Usage

Not Applicable.

4.5.2 Relying Party Public Key, Certificate and Signed JWT Usage

Relying parties must use certificates to validate signatures using the certificate chain up to the root CA, and check CRLs as specified. The RBM VA provides a mechanism for identifying signed JWTs whose certificates have been revoked and relying parties must use this mechanism to check the validity of signed JWTs. Relying parties use the JWS to confirm verified Chatbots, validating the JWS digital signature with the public key, which should be obtained from the end-entity certificate based on the x5u. The digital signature on the CRL must also be validated via the certificate.

4.6 Certificate and JWT Signature Renewal

The process for renewal follows that of certificate issuance per Sections 4.2 through 4.4.

4.6.1 Circumstance for Renewal

The RBM VA must process issuance of a new certificate for Subordinate CAs and End-Entities prior to the expiration date of the certificates currently in use. New certificates will be issued at least one week prior to expiration.

Processes for a certificate renewal may incorporate the same public key as the previous certificate, unless the private key has been reported as compromised.

The Subscriber must confirm issuance of a new signed JWT prior to the expiration date of the End-Entity certificate it is currently bound to otherwise their JWT can no longer be relied upon.

4.6.2 Who May Request Renewal

Only the Subscriber that is the holder of the expiring signed JWT, or their designated agent, can request a new signed JWT. Only the holder of the expiring subordinate or end-entity certificate, or their designated agent, can request a new certificate.

4.6.3 Processing Renewal Requests

The process for renewing a certificate or signed JWT follows the procedures for initial issuance per the previous Sections. The RBM VA may require reconfirmation or verification of the information being confirmed prior to renewal.

4.6.4 Notification of Issuance to Subscriber

The RBM VA will publish new certificates to Subscribers in the notification that a new signed JWT is available which is associated with that JWT's new end-entity certificate.

4.6.5 Conduct Constituting Acceptance of a Renewal

The acceptance of renewed certificates and signed JWTs follows the stipulations for initial acceptance per the previous section 4.4.1.

4.6.6 Publication of the Renewal

All renewed Certificates and signed JWTs are published in the RBM VA's repository.

4.6.7 Notification of Issuance to Other Entities

Per Section 4.4.3, Relying Parties may also be notified of issuance of renewed certificates and associated signed JWTs.

4.7 Certificate Re-key

Certificate re-key is the issuance of a new certificate to replace an old one for the reasons given in Section 4.7.1. Unlike certificate renewal, the public key and serial number must be changed. Certificate Re-Key is not supported in the RBM VA.

4.7.1 Circumstance for Certificate Re-key

Not Applicable

4.7.2 Who May Request Certification of a New Public Key

Not Applicable

4.7.3 Processing Certificate Re-keying Request

Not Applicable

4.7.4 Notification of New Certificate Issuance to Subscriber

Not Applicable

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

Not Applicable

4.7.6 Publication of the Re-keyed Certificate

Not Applicable

4.7.7 Notification of Certificate Issuance to other Entities

Not Applicable

4.8 Certificate Modification

Certificates will not be modified. If certificate information is not correct or compromised, then a new certificate will be created and all JWTs signed thereunder will be reissued.

4.8.1 Circumstance for Certificate Modification

Not Applicable

4.8.2 Who May Request Certificate Modification

Not Applicable

4.8.3 Processing Certificate Modification Requests

Not Applicable

4.8.4 Notification of New Certificate Issuance to Subscriber

Not Applicable

4.8.5 Conduct Constituting Acceptance of Modified Certificate

Not Applicable

4.8.6 Publication of the Modified Certificate

Not Applicable

4.8.7 Notification of Certificate Issuance to Other Entities

Not Applicable

4.9 Certificate Revocation and Suspension

Revocation of a CA Certificate, or the certificate associated with a signed JWT, permanently ends the operational period of the object prior to reaching the end of its stated validity period. Certificate or JWT certificate revocation will be made at the sole discretion of the RBM VA. The RBM VA will retain auditable evidence of revocations.

4.9.1 Circumstances for Revocation

The RBM VA may revoke a Certificate or the certificate associated with a signed JWT if one or more of the following occurs:

- The VA obtains evidence that the Private Key corresponding to the Public Key in the Certificate or any certificate supporting the JWT signature suffered a Key Compromise or no longer complies with the requirements;

- The VA obtains evidence that the Certificate or JWT was misused;
- The VA is made aware that the Certificate or JWT was not issued in accordance with these Requirements or the VA's Certificate Policy or Certification Practice Statement;
- The VA determines that any of the information appearing in the Certificate or JWT is inaccurate or
- misleading;
- The VA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;
- The technical content or format of the Certificate or JWT presents an unacceptable risk to Application Software Suppliers or Relying Parties

4.9.2 Who can Request Revocation

The RBM VA initiates the revocation. In addition, application software suppliers, and other third parties may submit Problem Reports informing the RBM VA of reasonable cause to revoke the certificate.

4.9.3 Procedure for Revocation Request

The RBM VA has established procedures for undertaking revocation, identifying the specific certificate, and establishing the reason for revocation.

4.9.4 Revocation Request Grace Period

There is no grace period for a revocation request. Once a Certificate or JWT has been identified for revocation, the certificate or JWT will be revoked immediately.

4.9.5 Time Within Which RBM VA Must Process the Revocation Request

Revocation timing allows reasonable times for investigation of the revocation request prior to determination by the RBM VA of whether to proceed with revocation.

4.9.6 Revocation Checking Requirement for Relying Parties

Prior to relying on the information listed in a Certificate or JWT, a Relying Party shall confirm the validity of each Certificate in the certificate path in accordance with IETF PKIX standards, including checks for certificate validity, issuer-to-subject name chaining, policy and key use constraints, and revocation status through CRLs identified in each Certificate in the chain.

Relying Parties will receive automatic notification from the RBM VA of a change to the CRL. A Relying Party shall acquire and check the CRL after such notification. Relying Parties must poll the VA repository once per day if not subscribed to the automated notifications.

Relying Parties must check for signed JWT validity using the mechanism provided by the RBM VA.

4.9.7 CRL Issuance Frequency (If Applicable)

The CRL is updated whenever a Certificate is revoked. The CRL is updated and notices, where applicable, are automatically sent to Relying Parties within 24-hours of a Certificate revocation. Notification regarding the CRL being updated are supported via a Notification API or notification email to which a customer can subscribe.

4.9.8 Maximum Latency for CRLs (If Applicable)

CRLs are posted to the RBM VA Repository per section 4.9.7.

4.9.9 On-line Revocation/Status Checking Availability

The URL to the CRL maintained by the RBM VA is included in the 'cRLDistributionPointName' parameter in all issued certificates. The relying party accesses the list via an HTTPS interface. Online Certificate Status Protocol (OCSP) is not currently supported by the RBM VA.

4.9.10 On-line Revocation Checking Requirements

This URL is included in the 'cRLDistributionPointName' field in the end entity certificate so that during path validation, the relying party can check whether any certificates in the certification path have been revoked. The relying party must check the CRL once per day if polling or as soon as reasonably possible after receiving autonomous notification of an update to the CRL.

All digital signatures in JWTs are considered invalid if any certificate in the associated Certificate path has been revoked. An alternate and uncompromised Certificate must be used to revise all digital signatures associated with the revoked Certificate.

Revoked Certificates will be removed from the CRL after the end of the Certificate's validity period.

4.9.11 Other Forms of Revocation Advertisements Available

The RBM VA maintains an internal database of all previously revoked certificates and revoked, signed JWTs, as well as previously rejected Applicant signature requests due to suspected phishing or other fraudulent usage or concerns. The RBM VA uses this information to identify subsequent suspicious requests. Signed JWTs may be purged from the database after signature expiration.

4.9.12 Special Requirements Regarding Key Compromise

The RBM VA will use commercially reasonable efforts to notify potential Relying Parties if it discovers or suspects that any of its Private Keys have been compromised. The revocation reason code will be set to "key compromise". If a Certificate is revoked because of compromise or suspected compromise, the CRL will be updated within 18 hours after receiving notice of the compromise or suspected compromise.

4.9.13 Circumstances for Suspension

Not applicable.

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

As stated in Section 4.9.10, the URL to the CRL is provided in the 'cRLDistributionPointName' in the end entity certificate associated with the digital signature.

4.10.1 Operational Characteristics

Not applicable.

4.10.2 Service Availability

The CRL is available 24x7 and supports a response time of ten seconds or less under normal operating conditions.

4.10.3 Optional Features

No stipulation.

4.11 End of Subscription

The subscription ends when the end-entity certificate is revoked or expires and a revised JWT digital signature is not requested.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

The RBM VA private keys shall never be escrowed. If a private key is lost, then new certificates with a new key pair will be generated for use in all subsequent digital signatures.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Not applicable.

5 Facility, Management, and Operational Controls

This Section describes the technical and administrative security controls used by the RBM VA for key generation, certificate issuance, signing, certificate revocation, auditing, and archiving.

5.1 Physical Security Controls

For directly operated physical systems under iconectiv's control, the RBM VA maintains security controls for its facilities hosting the operation. For physical or virtual systems that are not under the direct control of the VA, an equivalent description of security guarantees and/or highly available, geo-redundant operation is maintained and made available by the system provider.

5.1.1 Site Location and Construction

The location and construction of the facility housing equipment, as well as sites housing remote workstations used to administer the RBM VA components, is consistent with facilities used to house sensitive information. The sites whether directly operated or operated by an external party, provide protection against unauthorized access to equipment and records.

5.1.2 Physical Access

Physical access to equipment hosting the RBM VA is limited to authorized personnel. The security mechanisms are commensurate with the level of threat in the equipment environment. The security mechanisms in place to prohibit unauthorized access to equipment hosting the RBM VA include guard stations, visitor sign in, badged access control, security guards, closed-circuit monitored cameras, 24x7 operations center facilities monitoring.

5.1.3 Power and Air Conditioning

For directly operated physical systems, RBM VA equipment has backup power capability sufficient to lock out input, finish any pending actions, and record the state of the equipment automatically before lack of power or air conditioning causes a shutdown.

5.1.4 Water Exposures

For directly operated physical systems, the RBM VA equipment is installed such that it is not in danger of exposure to water (e.g., on tables or elevated floors). Potential water damage from fire prevention and protection measures (i.e., sprinkler systems) are excluded from this requirement.

5.1.5 Fire Prevention and Protection

For directly operated physical systems, the physical systems hosting the RBM VA comply with local commercial building codes for fire prevention and protection.

5.1.6 Media Storage

For directly operated physical systems, media is stored so as to protect it from accidental damage (water, fire, electromagnetic) and unauthorized physical access.

5.1.7 Waste Disposal

For directly operated physical systems, RBM VA and Operations Staff remove and destroy normal office waste in accordance with local policy. Media used to collect or transmit privacy information is destroyed using a secure waste disposal service. Waste bins for paper and media are placed through the facilities. Sensitive media and paper are destroyed in a manner that renders the information printed on it unrecoverable by any means. Destruction of media and documentation containing sensitive information employs methods commensurate with those in SP 800-88.

5.1.8 Off-site Backup

RBM VA operational system backups are made on daily basis, with full copies done once per week. Backups are stored offsite at a disaster recover data center. The backup site employs physical and procedural controls commensurate to that of the operational RBM VA system.

The data backup media is stored in a manner appropriate for storage of information of the same value of the information that will be protected by the certificates and associated private keys issued or managed using the equipment with a minimum requirement of transferring, handling, packaging, and storage of the information in a manner compliant with requirements for sensitive material identified in Section 6.5.1.2.4.

5.2 Procedural Controls

Trusted roles (e.g., system administrator have the responsibilities, and the identification and authentication requirements, as defined below. The roles include separation of duties and the number of individuals required to perform a task.

5.2.1 Trusted Roles

A trusted role--if performed by a person versus a secure, autonomous computer program or process--is one in which the person acting in that role performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. The only trusted roles defined by this policy are RBM VA Administrators, RBM VA Operations Staff, and Security Auditors. Trusted role operations include:

- The validation, authentication, and handling of information in Certificate and Applicant Applications;
- The acceptance, rejection, or other processing of Certificate and JWT-signature issuance, revocations, or renewals;
- The issuance, or revocation of Certificates and signed JWTs, including personnel having access to restricted portions of its repository;
- Access to safe combinations and/or keys to security containers that contain materials supporting production services;
- Installation, configuration, and maintenance of the RBM VA;
- Access to restricted portions of the certificate repository; or
- The ability to grant physical and/or logical access to the RBM VA equipment.

The RBM VA maintain lists, including names, organizations, contact information, and organizational affiliation for those who act in trusted roles, and shall make them available during compliance audits.

5.2.2 Number of Persons Required Per Task

For those processes not performed by a secure, autonomous computer program or process, and where multi-party control is required, all participants hold a trusted role. If not being performed by a secure, autonomous computer program or process, and physical access is required, the following tasks require two or more persons:

- Key signing ceremonies for root and subordinates;
- Generation, activation, and backup of all keys;
- Performance of RBM VA administration or maintenance tasks;
- Archiving or deleting RBM VA audit logs. At least one of the participants in this task serves in a Security Auditor role.
- Physical access to RBM VA equipment;
- Access to any copy of the cryptographic module.

5.2.3 Identification and Authentication for Each Role

Individuals holding trusted roles identify themselves and are authenticated by the RBM VA systems before being permitted to perform any actions set forth above for that role or identity. Operations Staff authenticate themselves and assume a role that is distinct from any role they use to perform non-trusted functions.

RBM VA equipment and systems implement strong authenticated access control for remote access using multi-factor authentication.

Individuals holding trusted roles are appointed to the trusted role by an appropriate operational authority with the approval of the PMA. These appointments are periodically reviewed for continued need and renewed as appropriate. The approval is recorded in a secure and auditable fashion using a ticketing and facilities support system. Individuals holding trusted roles accept the responsibilities of the trusted role.

Users requiring access to a sensitive resource authenticate themselves to all aspects of the network (servers, operating systems, applications, databases, processes, etc.) before they can access that resource. Remote users utilize the same level of authentication as local users, with the addition of VPN protection to access RBM VA systems.

5.2.4 Roles Requiring Separation of Duties

Individuals serving as Security Auditors do not perform or hold any other trusted role with respect to the RBM VA. Only an individual serving in a Security Auditor role performs internal auditing functions, with the exception of those security audit functions (e.g., configuring, archiving, deleting) that require multi-person control. An individual that who performs any trusted role has only one identity when accessing RBM VA equipment or systems.

5.3 Personnel Security Controls

The RBM VA maintains personnel security controls for its operation. The personnel controls employed for RBM VA operation are documented.

5.3.1 Qualifications, Experience, and Clearance Requirements

Personnel employed in Trusted Roles have the requisite background, qualifications and experience needed to perform their prospective job responsibilities competently and satisfactorily.

Individuals appointed to any trusted role meet the following:

- Be employees of or contractor/vendor of the RBM VA and bound by terms of employment or contract;
- Have demonstrated the ability to perform their duties;
- Have no other duties that would interfere or conflict with their responsibilities as defined in Section 5.2.1; and
- Have never been previously relieved of trusted role duties for reasons of negligence or non- performance of duties.

5.3.2 Background Check Procedures

All persons fulfilling Trusted Roles, whether or not they require direct access to information related to secrets (i.e., private keys) that may compromise the integrity of the security of the RBM VA systems, pass a background check prior to commencement of employment. Such persons are subject to identity verification and background checks (in accordance with local privacy laws) which may include the following:

- Confirmation of previous employment;
- Checks of professional references;
- Confirmation of the highest or most relevant educational degree obtained;
- Search of criminal records (local, state or provincial, and national);
- Check of credit/financial records;
- Search of driver's license records;
- Identification verification via National Identity Check (e.g., Social Security Administration records), as applicable.

5.3.3 Training Requirements

Personnel performing duties with respect to the operation of the RBM VA receive training commensurate with their duties or possess demonstrated expertise in their field of operation. Training may be conducted in the following areas:

- PKI and RBM VA security principles and mechanisms;
- All RBM VA software versions in use on the system;
- All RBM VA duties they are expected to perform;

- Certificate lifecycle management;
- Subscriber vetting and identification and validation procedures;
- Disaster recovery and business continuity procedures;
- Stipulations of this policy.

Documentation is maintained identifying all personnel who received training and the level of training completed.

5.3.4 Retraining Frequency and Requirements

All individuals responsible for RBM VA Trusted Roles are made aware of changes in the RBM VA operation. Any significant change to the operations and the execution of such plan is documented. Examples of such changes are PKI software or hardware upgrades, changes in RBM VA operational procedures, changes in automated security systems, and relocation of equipment.

5.3.5 Job Rotation Frequency and Sequence

No Stipulation.

5.3.6 Sanctions for Unauthorized Actions

Appropriate administrative and disciplinary actions, as documented in organization policy, shall be taken against personnel who perform unauthorized actions (i.e., actions not permitted by this CP/CPS or other RBM VA security policies) involving the RBM VA systems, operational processes, security controls, the certificate status verification systems, and the certificate repository. Disciplinary actions may include measures up to and including termination and shall be commensurate with the frequency and severity of the unauthorized actions.

5.3.7 Independent Contractor Requirements

Contractor personnel filling trusted roles are subject to all requirements stipulated in this document. Independent contractors and consultants who have not completed or passed the background check procedures specified above may be permitted access to the RBM VA secure facilities only when they are escorted and directly supervised by people holding trusted roles at all times.

5.3.8 Documentation Supplied to Personnel

Personnel are provided with documentation sufficient to perform their duties, which includes this CP/CPS, as well as access to system and application documentation as required by their role.

5.4 Audit Logging Procedures

The RBM VA generates audit log files for all events relating to the security of the RBM VA operation. The log information is automatically collected. For the RBM VA systems, all transactions and events are automatically logged in a comprehensive Security Incident and Event Management (SIEM) system.

The PMA shall review the logs on a request basis.

5.4.1 Types of Events Recorded

Audit records are generated for the basic operations of the RBM VA computing equipment.

Audit records include the date, time, responsible user or process, success or failure indicators, and summary content data relating to the event.

Auditable events include but are not limited to:

- All security events;
- Access to computing equipment (e.g., logon, logout);
- Messages received requesting actions (e.g., certificate requests, signature requests, certificate revocation requests, compromise notifications);
- Subscriber identification information;
- Change in verification status or attributes
- Certificate creation, modification, re-key, revocation, or renewal actions;
- Posting of any material to a repository;
- Adding a revoked certificate to the CRL;

- Any attempts to change or delete audit data;
- Key generation;
- Generation of digital signatures;
- Notifications of CRL updates and digital signatures;
- Third party retrieval of CRL updates, digital signatures and public certificates;
- Third party retrieval of brand, partner or chatbot status and verification attributes;
- Software and/or configuration updates; or
- Clock adjustments.

5.4.2 Frequency of Processing Log

The audit log is reviewed using an automated system which monitors events in real time. Log events are collected using a SEIM, and actionable items are to 24x7 SOC personnel for investigation. Alerting will occur if log information is not being received. Actions taken are documented within the event management system and RBM VA support and ticketing systems.

5.4.3 Retention Period for Audit Log

Audit logs are retained online for at least one year, with 45 days of immediately queriable log data, in addition to being archived as described in Section 5.5. Currently, RBM VA audit logs are kept indefinitely, however, the purging of logs after the required retention periods have expired is not precluded. Any individual who manually removes audit logs from the RBM VA system serves in a different role from individuals who, in combination, command the RBM VA signature key.

5.4.4 Protection of Audit Log

The security audit data is not open for reading by any human, or by any automated process, other than those that perform security audit processing. The log is not writable except by the logging mechanism itself. Once written, the log is not modifiable by machine or human.

Electronic logs are protected to prevent alteration and detect tampering. RBM VA audit logs are protected from tampering using access controls which preclude their deletion

Security audit data is moved to a safe, secure storage location separate from the location where the data was generated. The RBM VA utilizes secure cloud storage and DR facilities for audit data.

RBM VA system configuration and procedures are implemented together to ensure that only authorized people archive or delete security audit data. Procedures are implemented to protect archived data from deletion or destruction before the end of the security audit data retention period (note that deletion requires modification access).

5.4.5 Audit Log Backup Procedures

Audit logs and audit summaries are backed up at least every thirty (30) days. The backup of the audit log is stored securely in an alternate location.

5.4.6 Audit Collection System (Internal vs. External)

The audit log collection system is external to the RMB VA system. Automated audit processes are invoked at system and application startup and cease only at system or application shutdown. Audit collection systems are configured such that security audit data is protected against loss (e.g., overwriting or overflow of automated log files). Should it become apparent that an automated audit system has failed; RMB VA certificate issuance and JWT signature processing shall be suspended until the security audit capability can be restored, except for revocation processing and in the situation where a certificate needed for real-time authentication has expired or is soon to expire.

5.4.7 Notification to Event-Causing Subject

No stipulation.

5.4.8 Vulnerability Assessments

The RBM VA personnel routinely test, at least annually, and assess the RBM VA systems to determine if they have any vulnerabilities. Continuous vulnerability assessments are performed on perimeter and hosted third party systems, and quarterly vulnerability assessments are performed for internal systems, including internal and external topology and access control evaluations. Each identified vulnerability is prioritized based on its risk level and a remediation plan is created. There is a patch management process to remediate critical and high rated vulnerabilities as soon as it is feasible or when a vendor patch is released.

5.5 Records Archival

5.5.1 Types of Records Archived

RBM VA archive records are sufficiently detailed to determine the proper operation of the RBM VA and the validity of any certificate (including those revoked or expired) or digital signature issued by the RBM VA. At a minimum, and on systems where applicable the following data is recorded for archive:

- CP/CPS
- Contractual obligations
- Other agreements concerning operations of the RBM VA
- System and equipment configuration
- Subscriber identity authentication data as per Section 3.2.3
- Documentation of receipt and acceptance of certificates (if applicable)
- Subscriber agreements
- Documentation of receipt of tokens
- All Certificate requests for which the authorization failed
- All Certificates issued
- All Certificates revoked, renewed, or modified
- All digital signatures issued or expired
- All changes in brand, partner or chatbot data
- All notifications sent to Subscribers or Relying Parties
- All Audit logs
- Other data or applications to verify archive contents
- Compliance Auditor reports
- Any changes to the Audit parameters, e.g., audit frequency, type of event audited
- Any attempt to delete or modify the Audit logs
- All access to any certificate subject private keys retained within the VA for key recovery purposes
- All changes to the trusted public keys, including additions and deletions
- Remedial action taken as a result of violations of physical security
- Violations of CP/CPS

5.5.2 Retention Period for Archive

Archive records are kept for a minimum of seven (7) years and six (6) months without any loss of data.

5.5.3 Protection of Archive

Archives are maintained indefinitely and protected using version control. No unauthorized user is permitted to write to, modify, or delete the archive.

The contents of the archive shall not be released. Records of individual transactions may be released upon request of any Subscribers or Relying Parties involved in the transaction or their legally recognized agents.

Archive media shall be stored in a safe, secure storage system at the DR center with physical and procedural security controls equivalent to or better than those of the RBM VA. The RBM VA ensures that all archived information can be obtained within a reasonable timeframe through recovery services.

5.5.4 Archive Backup Procedures

Archive records are backed up and managed through automated, programmatic methods.

5.5.5 Requirements for Time-Stamping of Records

The RBM VA archive records are automatically time-stamped as they are created.

5.5.6 Archive Collection System (Internal or External)

Archive data is collected in an expedient manner and on a regular basis.

5.5.7 Procedures to Obtain and Verify Archive Information

Procedures, detailing how to create, verify, package, transmit, and store the RBM VA archive information, is detailed in administrative documentation available in internal, online repositories.

5.6 Key Changeover

The RBM VA re-issues root and subordinate CA certificates prior to the end of the maximum key-usage periods defined in 6.3.2. THE RBM VA does not issue End-Entity certificates that extend beyond the expiration date of the root CA or their subordinate CA certificates. Each VA End-Entity certificate validity period extends one year past the last use of any issued signed JWT. When the private signing key changes, the RBM VA uses only the new key for certificate signing and digital signature generation.

The RBM VA retains its old Private Keys and makes the old Certificate available to verify signatures until all of the Certificates and digital signatures signed with the Private Key have expired.

End Entity Certificates re-issue is handled automatically by the application and there is no need for distribution of those since the location for those is passed in the JWS x5u header parameter.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

If compromise of a component of the RBM VA occurs, certificate and signature issuance shall be stopped immediately in the effected components and their subordinates. An, investigation shall be performed by security personnel in order to determine the nature and the degree of damage. The scope of potential damage shall be assessed in order to determine appropriate remediation procedures. If a private signing key is suspected of compromise, the procedures outlined in Section 5.7.3 shall be followed.

The RBM VA organization has an Incident Response Plan and a Disaster Recovery Plan. The RBM VA documents business continuity and disaster recovery procedures designed to notify and reasonably protect Application Software Suppliers, and Relying Parties in the event of a disaster, security compromise, or business failure. The VA is not required to publicly disclose its business continuity plans but shall make its business continuity plan and security plans available to the RBM VA auditors upon request. The RBM VA annually tests, reviews, and updates these procedures.

The RBM VA shall immediately notify the PMA if any of the following occur:

- Actual or detected compromise of any RBM VA system or subsystem;
- Physical or electronic penetration of any RBM VA system or subsystem;
- Successful denial of service attacks on any RBM VA system or subsystem.

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

When computing resources, software, and/or data are corrupted, the RBM VA shall respond as follows:

- Notify the PMA as soon as possible.
- Ensure that the system's integrity has been restored prior to returning to operation and determine the extent of loss of data since the last point of backup.
- Reestablish RBM VA operations.
- If the signing keys are destroyed, reestablish RBM VA operations as quickly as possible.
- If the integrity of the system cannot be restored, or if the risk is deemed substantial, reestablish system integrity before returning to operation.

5.7.3 Private Key Compromise Procedures

If the RBM VA suspects that a Private Key is compromised or lost then the RBM VA shall follow its Incident Response Plan and immediately assess the situation, determine the degree and scope of the incident, and take appropriate action in accordance with internal and external requirements as listed in section 1.1. RBM VA personnel shall report the results of the investigation. The report must detail the cause of the compromise or loss and the measures should be taken to prevent a reoccurrence.

Following revocation of a Certificate and implementation of the Incident Response Plan, the RBM VA shall generate a new Key Pair and sign a new Certificate in accordance with its CPS. The RBM VA shall distribute the new Certificate in accordance with Section 6.1.4.

5.7.4 Business Continuity Capabilities After a Disaster

The RBM VA maintains a Disaster Recovery Plan, which identifies what management and operations procedures are in place to mitigate risks to facilities, systems, networks, and application controls. The plan also identifies procedures for annual testing of processes to restore service, individuals on call for management, response and recovery activities, and the order of restoral of equipment and services.

In the case of a disaster in which the RBM VA equipment is damaged and inoperative, operations shall be re-established as quickly as possible, giving priority to the ability to revoke Certificates. If the RBM VA cannot re-establish revocation capabilities within eighteen (18) hours, then the inoperative status of the RBM VA shall be reported to the PMA. The PMA shall decide whether to declare the private signing key as compromised and the keys and certificates need to be reissued or allow additional time for reestablishment of the revocation capability.

In the case of a disaster in which an RBM VA installation is physically damaged and all copies of the signature keys are destroyed as a result, then all effected certificates will be revoked. The installation shall then be completely rebuilt by re-establishing the equipment and generating new private and public keys. Finally, all Subscribers and Relying Parties will be notified that digital signatures and their associated certificates need to be re-issued.

5.8 RBM VA Termination

If the RBM VA operations are terminated, the RBM VA shall provide notice to interested parties and may transfer its responsibilities and records to successor entities. The RBM VA may allow a successor to re-issue Certificates and digital signatures if the successor has all relevant permissions to do so and has operations that are at least as secure the RBM VA's.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

All keys are generated using a FIPS-approved method or equivalent international standard. Specifically, all cryptographic keying material is generated on a FIPS 140-2 level 3 validated cryptographic module using multiple individuals acting in trusted roles. When generating key material, the process creates auditable evidence to show that the VA enforced role separation and followed its key generation process. Root CA and Subordinate CA key pairs are generated in pre-planned Key Generation Ceremonies in accordance with the applicable documented procedures. 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 the RBM VA.

In all cases, the RBM VA :

- Generates the keys in a physically secured environment as described in this CP/CPS;
- generates the keys using personnel in Trusted Roles under the principles of multiple person control and split knowledge;
- generates the keys within cryptographic modules meeting requirements as disclosed in this CP/CPS;
- logs its key generation activities plus produce an auditable quality record; and
- maintains effective controls to provide reasonable assurance that the Private Key was generated and protected in conformance with documented procedures and script.

6.1.2 Private Key Delivery to Subscriber

Not applicable. The RBM VA is the only entity possessing private keys in this PKI

6.1.3 Public Key Delivery to Certificate Issuer

Not applicable. The RBM VA and the Certificate Issuer are one and the same.

6.1.4 Public Key Delivery to Relying Parties

Public Keys are provided to Subscribers and Relying Parties by publishing them in the location identified in the JWT x5u header as specified previously.

6.1.5 Key Sizes

Certificates and digital signatures generated under this policy use key sizes in accordance with NIST SP 800-57 and IETF RFC 7515 and 7518. ECDSA signatures on certificates use SHA-256. JWTs issued to Subscribers will include ECDSA signatures with SHA-256 as well as, optionally, one additional signature algorithm which shall be RSA2048, when required by Relying Parties. The preferred second signature algorithm is SHA256 with RSA encryption unless not supported by Relying Parties. Any other signature algorithm used will be arrived at by mutual agreement.

6.1.6 Public Key Parameters Generation and Quality Checking

Public key parameters shall always be generated and validated in accordance with FIPS 186-4.

6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field)

The use of a specific key is constrained by the key usage extension fields in the X.509 certificate.

Public keys that are bound into End-Entity Certificates include a key usage extension for digital signature.

Public keys that are bound into root and subordinate CA certificates are used only for verification of signatures on digital certificates, and do not include anyExtendedKeyUsage

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

Cryptographic modules are validated to FIPS 140-2 Level 3 (or higher).

6.2.2 Private Key Multi-person Control

The RBM VA employs both secure computer-based systems and multi-person controls to constrain access to their private keys. Use of root CA private keys is controlled by utilizing multiple roles to generate, sign, and process certificates. Use of subordinate and end-entity keys are protected using programmatic and access controls.

6.2.3 Private Key Escrow

Private keys shall never be escrowed.

6.2.4 Private Key Backup

The Certificates and CRL Private Keys shall be backed up under multi-person control and shall store at least one backup at a secure off-site location. The Issuer CA protects all copies of its CA and CRL Private Keys in the same manner as the originals.

6.2.5 Private Key Archival

Private keys shall not be archived.

6.2.6 Private Key Transfer into or from a Cryptographic Module

All private keys are generated by a cryptographic module. Private keys are exported from the cryptographic module only to perform key backup procedures as described in Section 6.2.4. At no time do private keys exist in plaintext outside the cryptographic module.

Transport keys used to encrypt private keys are handled in the same way as the private key.

6.2.7 Private Key Storage on Cryptographic Module

No stipulation beyond that specified in FIPS 140-2 Level 3. Private keys held on hardware cryptographic modules are stored in encrypted form.

6.2.8 Method of Activating Private Key

If private key activation is applicable to the use of a cryptographic module, personnel in trusted roles must be authenticated with a cryptographic token before the activation of the associated private key(s). Acceptable means of authentication to the cryptographic token include but are not limited to passphrases, PINs or biometrics. Entry of activation data shall be protected from disclosure (i.e., the data should not be displayed while it is entered).

6.2.9 Method of Deactivating Private Key

Private keys are deactivated and stored in secure cryptographic modules or in wrapped form when not in use.

6.2.10 Method of Destroying Private Key

Automated computer processes are used to destroy private keys when they are no longer needed or when the certificates to which they correspond expire or are revoked. Physical destruction of any hardware is not required.

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

The public key is archived as part of the certificate archival described in Section 5.5.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The RBM VA root certificate lifespan is 20 years consistent with best practice to provide strong stability to the PKI and all entities signed within its scope. The root CA is kept offline by the RBM VA and follows a detailed key generation script to generate new keys and root certificates when required for relying parties in the PKI. These procedures are documented.

The subordinate certificate lifespan is 10 years consistent with best practices for strong stability in the PKI. Subordinate CAs are kept online to support automated issuance of end-entity certificates. There will be additional subordinate certificates coexisting with the previous subordinate certificates after a number of years of operation. All new end-entity signing certificates will be created under the second subordinate no less than 2 years before the previous subordinate certificate expires. Additional subordinate certificates of similar lifespan may be created on a geographic or other basis.

End entity Certificates for digitally signing tokens for Subscriber chatbots have a lifespan of 2 years.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

Any activation data is generated with sufficient strength to protect its Private Keys to prevent the loss, theft, modification, unauthorized disclosure, or unauthorized use.

If the activation data must be transmitted, it shall be via an appropriately protected channel, and distinct in time and place from the associated cryptographic module.

6.4.2 Activation Data Protection

Data used to unlock private keys is protected from disclosure by a combination of cryptographic and physical access control mechanisms. Activation data may be

- memorized;
- biometric in nature; or
- recorded and secured at the level of assurance associated with the activation of the cryptographic module and shall not be stored with the cryptographic module.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

The RBM VA maintains documented technical controls covering all of the areas identified in this Section of the CP/CPS.

6.5.1.1 Access Control

Access to information such as sensitive details about customer accounts, passwords, and ultimately, private keys is carefully guarded, along with the systems housing such information.

6.5.1.1.1 Access Control Policy and Procedures

Roles and responsibilities are maintained for each trusted role employee job function. A mapping of these trusted roles and their associated responsibilities to specific employees and their accounts is maintained by IT.

6.5.1.1.2 Account Management

Information system account management features ensure that users access only that functionality permitted by their role or function. All account types with access to information systems are documented along with the conditions and procedures to follow in creating new accounts. Groups and roles have a documented relationship to the business or mission roles involved in operating the RBM VA.

All account administration activities are logged and made available for inspection by appropriate security personnel. Account administration activities that are audited include account creation, modification, enabling, disabling, group or role changes, and removal actions. See Section 5.4 for detailed requirements for these logs.

Guest/anonymous and defaults accounts for logon to RBM VA operations systems are prohibited. Accounts are assigned to a single user and are not shared.

6.5.1.1.3 Least Privilege

As per section 6.5.1.1.2. Furthermore, access to privileged commands and features of information systems are authorized only for specific, organization-defined compelling operational needs and documents the rationale for such access. Users of information systems with access to administrative privileges utilize non-privileged roles when accessing non-privileged functions (such as reading email).

6.5.1.1.4 Access Control Best Practices

The following best practices for access control are followed for RBM personnel access to RBM VA systems:

- Unique User IDs is associated with each individual user.
- All user activity shall be traceable to an individual.
- No shared or default accounts shall be used.
- There is a process to track the assignment and configurations of administrative privileges to RBM VA operations systems. The principle of least privilege shall be followed.
- There is an authorization process to approve users and their associated privileges.
- There is a process to establish, change, deactivate and remove User IDs and privileges.
- Passwords shall be at least 8 characters with associated complexity and usage rules.
- Passwords are never stored or transmitted in cleartext.
- There are defined session timeouts (15 minutes) during periods of user inactivity.
- There shall be a limit on failed login attempts (5). If there is a lockout, an administrator needs to reset the password.

- For remote access from external public networks, multi-factor authentication shall be used.
- There shall be logging of all failed login attempts and changes in administrative privileges.

6.5.1.1.5 Authentication: Passwords and Accounts

Strong passwords are employed when any authentication mechanism uses user selectable passwords. Additionally, the RBM VA enforces multi-factor authentication for access to all RBM VA systems by personnel.

6.5.1.1.6 Permitted Actions without Identification or Authentication

No Stipulation.

6.5.1.2 System Integrity

6.5.1.2.1 System Isolation and Partitioning

Systems are configured, operated, and maintained so as to ensure the continuous logical separation of operations processes and their assigned resources. This separation is enforced by:

- Physical and/or logical isolation mechanisms, such as dedicated systems or virtualization;
- Protecting an active process and any assigned resources from access by or interference from another process;
- Protecting an inactive process and any assigned resources from access by or interference from an active process; and
- Ensuring that any exception condition raised by one process will have no lasting detrimental effect on the operation or assigned resources of another process.

All trusted components are logically separated from each other and logically separated from any untrusted components of the system, as defined in the system documentation.

6.5.1.2.2 Malicious Code Protection

Where technically feasible, the RBM VA employs malicious code protection mechanisms to mitigate the risk of malicious code on system components. The RBM VA deploys multiple layers of defense against malicious code, including zero-day malware protection software, anti-virus software, web application firewalls, and ensures that all outbound traffic goes through firewall filtering.

6.5.1.2.3 Software and Firmware Integrity

Technical and procedural controls are employed to prevent and detect unauthorized changes to firmware and software on systems. Access control mechanisms and documented configuration management processes (see Sections 6.5.1.1 and 6.6.2) ensure that only authorized Administrators are capable of installing or modifying firmware and software on systems.

6.5.1.2.4 Information Protection

The confidentiality and integrity of sensitive information stored or processed on systems that could lead to abuse, compliance violations, or fraud is protected. Technical mechanisms are employed to prevent unauthorized changes or accesses to this information, including access control mechanisms that limit which users are authorized to view or modify files. Sensitive information stored on devices that are not physically protected from potential attackers is stored in an encrypted format.

6.5.2 Computer Security Rating

The RBM VA adheres to industry standards for information security, including ISO 27001 and the NIST Cyber Security Framework.

6.6 Life Cycle Security Controls

6.6.1 System Development Controls

The RBM VA system is implemented and tested in a non-production environment prior to implementation in a production environment. No changes are made to the production environment unless the change has gone through the documented change control process.

In order to prevent incorrect or improper changes to the system, the RBM VA system requires multi-party control for access to the CA systems when changes are made.

The RBM VA uses a defined software development methodology as well as implementation techniques intended to avoid common errors to reduce the number of vulnerabilities. Automated software assurance (e.g., static code analysis, dynamic code analysis) tools are used to catch common error conditions within developed code. Input validation is performed for all inputs into the system.

Hardware and software procured to operate the RBM VA are purchased from authorized vendors in a fashion to reduce the likelihood that any particular component was tampered with (e.g., by ensuring the vendor cannot identify the PKI component that will be installed on a particular device). Open-source software meets security requirements through software verification & validation and structured development/life-cycle management.

Hardware and software updates are purchased or developed in the same manner as original equipment and are installed by trusted and trained personnel in a defined manner. A formal configuration management methodology is employed for installation and ongoing maintenance of any component. Any modifications and upgrades to the Configuration Management System are documented and controlled in the RBM VA's ticketing system.

All data input to RBM VA system components from users or other system components is validated prior to consumption by the receiving entity. Validating the syntax and semantics of system inputs (e.g., character set, length, numerical range, and acceptable values) verifies that inputs match the expected definitions for format and content.

6.6.2 Security Management Controls

A list of RBM VA system components is maintained and kept up to date within the configuration management system. Mechanisms and/or procedures in operation are designed to prevent the installation and execution of unauthorized software.

To reduce the available attack surface, only those ports, protocols, and services that are necessary to the system architecture are permitted to be installed or operating. The system maintains a list of ports, protocols, and services that are necessary for the correct function of each component within the system. There are automated mechanisms to monitor the running processes and open ports against the permitted list.

The RBM VA establishes and documents mandatory configuration settings for all information technology components, which comprise the system. All configuration settings capable of automated assessment are validated to be set according to the guidance contained within appropriate configuration documentation.

6.6.3 Life Cycle Security Controls

In accordance with Section 6.5.2.

6.7 Network Security Controls

The RBM VA utilizes numerous network security controls protecting computing systems, including the following key principles and controls:

- Documents and controls the configurations of systems, including any upgrades or modifications made.
- Implements a process and controls for detecting unauthorized modifications to hardware or software and for installing and maintaining systems.
- Utilizes defense-in-depth strategy to protect the network elements and externally facing perimeter, systems, applications and interfaces.
- Security devices that are being used include firewalls, web application firewalls, intrusion detection and prevention technology and denial-of-service protection, and others.
- Threat intelligence monitoring include procedures to update attack signatures in network security devices, and anomaly detection systems.

- Network segmentation to protect the operations systems from the enterprise systems and any third-party systems, and network data flow analysis and trending software.
- Security access controls for accessing network management tools and information.
- Network security monitoring and Security Incident and Event Management Tools (SIEM) from a 24x7 Security Operations Center (SOC).

6.8 Time-Stamping

All systems and logging facilities use synchronized time sources for timestamps. System clocks used for time-stamping are maintained in synchrony with an authoritative time standard (e.g., through the use of Network Time Protocol (NTP) [RFC 5905]).

7 Certificate, CRL and OCSP Profiles

7.1 Certificate Profile

Certificates adhere to the X.509 v3 certificate profile documented in RFC 5280.

The RBM VA documents the following withing its system design and implementation documentation, such as use cases, user stories, and CA instantiation scripts:

- Version number(s)
- Certificate extensions
- Algorithm object identifiers
- Name forms
- Name constraints
- Certificate policy object identifier
- Usage of Policy constraints extension
- Policy qualifiers syntax and semantics
- Processing semantics for the critical Certificate Policies extension

Certificates must contain the ExtendedKeyUsage extension but may not contain the anyEKU value.

7.2 CRL Profile

The CRL issued includes the crlExtensions CRLNumber as per RFC 5280. This extension is updated when the CRL is updated, or when the CRL expires and a new one is generated. The format required for entries in the CRL is described in the following Sections.

7.2.1 Version Numbers

CRL V2.

7.2.2 CRL and CRL Entry Extensions

Revoked certificates follow the procedures described in Section 4.9 CRL entries include the following:

- Certificate’s Serial Number;
- Revocation Date;
- Reason;
- Certificate Issuer.

7.3 OCSP Profile

Not applicable.

8 Compliance Audit and Other Assessment

This CP/CPS meets the requirements based on GSMA RCC.07, as well as generally accepted and published industry standards for ensuring RBM VA integrity. The VA ensures that audits are conducted for all RBM VA functions regardless of how or by whom the RBM VA components are managed and operated.

8.1 Frequency or Circumstances of Assessment

An independent properly trained internal auditor assesses the compliance with this CP/CPS on a periodic basis. This audit covers each system component that is specified in any certificate issued.   Assessments include, among others, an annual third-party penetration test, and an annual SOC2 audit.

8.2 Identity/Qualifications of Assessor

The auditor must demonstrate competence in the field of compliance audits and must be thoroughly familiar with this CP/CPS. The compliance auditor must perform such compliance audits as a regular ongoing business activity. In addition to the previous requirements, the auditor shall have appropriate professional certifications such as a Certified Information System Auditor (CISA) or IT security specialist or shall have demonstrated subject matter expertise and experience in conducting compliance audits and shall have available a PKI subject matter specialist who can offer input regarding acceptable risks, mitigation strategies, and industry best practices.

8.3 Assessor's Relationship to Assessed Entity

The auditor either shall be a private firm that is independent from the business operation being audited or shall be sufficiently organizationally separated from the business to provide an unbiased, independent evaluation. To ensure independence and objectivity, the lead auditor must not have contributed to developing or maintaining the entity’s facility or CP/CPS. The PMA shall determine whether an auditor meets this requirement.

8.4 Topics Covered by Assessment

The audit must conform to industry standards, cover compliance, and evaluate the integrity of the RBM VA operations. The audit must verify compliance with this CP/CPS and any other agreement between the RBM VA and any other entity.

8.5 Actions Taken as a Result of Deficiency

If an audit reports a material noncompliance with applicable law, this CP/CPS, or any other contractual obligations related to the services, then (1) the auditor shall document the discrepancy, (2) the auditor shall promptly notify the RBM VA and the PMA. The RBM VA shall develop a plan to rectify the noncompliance. The RBM VA shall submit the plan to the PMA for approval. The PMA may require additional action, if necessary, to rectify any significant issues created by the non-compliance, including requiring revocation of affected certificates.

8.6 Communication of Results

The Audit Compliance Report and identification of corrective measures shall be provided to the PMA within thirty (30) days of completion. The results shall also be communicated to any third-party entities entitled by law, regulation, or agreement to receive a copy of the audit results.

9 Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

No stipulation. Any fees for certificates or digital signatures will be identified in Agreements or Terms of Use applicable to Subscribers and/or Relying Parties.

9.1.2 Certificate Access Fees

No stipulation.

9.1.3 Revocation Access Fees

No stipulation.

9.2 *Financial Responsibility*

9.2.1 Insurance or warranty coverage

No stipulation

9.2.2 Other Assets

No stipulation

9.3 *Confidentiality of Business Information*

9.3.1 Scope of confidential information

The following shall constitute confidential information:

1. Subscriber application records, whether approved or disapproved;
2. Subscriber Agreements
3. Mobile Operator Service Agreements
4. SLA Reports
5. Transactional records
6. Contingency planning and disaster recovery plans; and
7. Security measures in place

9.3.2 Information not within the Scope of Confidential Information

No stipulation

9.3.3 Responsibility to Protect Confidential Information

Anyone with authorized access to confidential information shall be contractually obligated to protect such confidential information (including but not limited to employees, agents, and contractors).

9.4 *Privacy of Personal Information*

9.4.1 Privacy Plan

No stipulation

9.4.2 Information Treated as Private

No stipulation

9.4.3 Responsibility to Protect Private Information

No stipulation

9.4.4 Disclosure Pursuant to Judicial or Administrative Process

No stipulation

9.5 *Intellectual Property Rights*

The VA retains all intellectual property rights in and to the Certificates and revocation information that is issued. The RBM VA grants permission to reproduce and distribute Certificates, digital signatures and revocation information on a nonexclusive royalty-free basis, provided that they are reproduced in full and that use of such items is subject to any Relying Party Agreement associated with these Certificates.

Subscribers and Applicants retain all rights it has (if any) in any trademark, service mark, or trade name contained in any Certificate, token or digital signature issued to such Subscriber or Applicant.

9.6 Representations and Warranties

9.6.1 VA representations and Warranties

9.6.2 Relying Party Representations and Warranties

No stipulation

9.6.3 Subscriber Representations and Warranties

No stipulation

9.6.4 Disclaimers of Warranties

No stipulation

9.7 Limitations of Liability

To the extent iconectiv has issued and managed the Certificate(s) at issue in compliance with this CP/CPS, iconectiv shall have no liability to the Subscriber, any Relying Party, or any other third parties for any damages or losses suffered as a result of the use or reliance on such Certificate(s). To the extent permitted by applicable law, Subscriber Agreements and Relying Party Agreements shall limit iconectiv's liability outside the context of any extended warranty protection program. Limitations of liability shall include an exclusion of indirect, special, incidental, and consequential damages.

9.8 Indemnities

9.8.1 Indemnification

Indemnifications (and/or limitation thereof) of Subscribers shall be as set forth in the applicable Subscriber Agreements or Terms of Use. Similarly, indemnification (and/or limitation thereof) of Relying Parties shall be as set forth in the applicable Relying Party Agreements.

9.8.2 Indemnification by Subscribers

Any indemnification requirements for Subscribers will be identified in the Subscriber Agreements or Terms of Use.

9.8.3 Indemnification by Relying Parties

Any indemnification requirements for Relying Parties will be identified in Relying Party Agreements.

9.9 Term and Termination

9.9.1 Term

This CP/CPS and any amendments are effective when published online by the RBM VA and remain in effect until replaced with a newer version.

9.9.2 Termination

The CP/CPS and any amendments remain in effect until replaced by a newer version.

9.9.3 Effect of Termination and Survival

No stipulation

9.10 Individual Notices and Communications with Participants

The PMA accepts digitally signed or paper notices related to this CP/CPS that are addressed to the locations specified in Section 1.5 of this CP. Notices are deemed effective after the sender receives a valid and digitally signed acknowledgment of receipt from the PMA. If an acknowledgement of receipt is not received within five days, the sender must resend the notice in paper form to the street address specified in Section 1.5 using either a courier service that confirms delivery or via certified or registered mail with postage prepaid and return receipt requested.

The RBM VA shall notify the PMA at least two weeks prior to implementation of any planned change to the infrastructure that has the potential to affect the PKI operational environment, and all new artifacts, including CA root certificates, produced as a result of the change will be provided to the PMA within 24 hours following implementation.

The RBM VA shall notify the PMA one month in advance of any updates or changes with the potential to affect compliance with this CP, including:

1. Additions or changes of Root CAs
2. Additional CPs at the Root CA level
3. Changes in Certificate issuance procedures
4. Terminations or transition of ownership of Root CAs

9.11 Amendments

9.11.1 Procedure for Amendment

Changes to this CP/CPS may be made from time to time by the PMA. The PMA will review this CP/CPS annually and when any changes are made to the specifications from which requirements for this CP/CPS are derived.

9.11.2 Notification Mechanism and Period

The PMA will post notice on the website of any proposed significant revisions to this CP.

9.11.3 Circumstances Under which OID must be Changed

If the PMA determines that an amendment necessitates a change in an OID, then the revised version of this CP/CPS will identify that a new OID is required and will specify a revised OID.

9.12 Dispute Resolution Procedures

No stipulation.

9.13 Governing Law

No stipulation. Refer to Subscriber Agreements or Terms or Use and Relying Party Agreements.

9.14 Compliance with Applicable Law

No stipulation

9.15 Miscellaneous Provisions

9.15.1 Entire Agreement

No stipulation.

9.15.2 Assignment

No stipulation

9.15.3 Severability

No stipulation

9.15.4 Force Majeure

No stipulation.