

Version: 1.0 (draft)

Appendix [TBC]

VWKI Certificate Policy

Contents

1	INTRODUCTION	11
1.1	Overview	11
1.2	Document Name and Identification	11
1.3	VWKI Participants	11
1.3.1	The VWKI Certification Authority	11
1.3.2	VWKI Registration Authority	11
1.3.3	VWKI Subscribers	11
1.3.4	VWKI Relying Parties	12
1.3.5	VWKI Policy Management Authority	12
1.3.6	VWKI Repository Provider	12
1.4	Usage of VWKI Certificates	12
1.4.1	Appropriate Certificate Uses	12
1.4.2	Prohibited Certificate Uses	13
1.5	Policy Administration	13
1.5.1	Organisation Administering the Document	13
1.5.2	Contact Person	13
1.5.3	Person determining Certification Practice Statement suitability for the Policy	13
1.5.4	CPS Approval Procedures	13
1.5.5	Registration Authority Policies and Procedures	13
2	PUBLICATION AND REPOSITORY RESPONSIBILITIES	13
2.1	Repositories	13
2.2	Publication of Certification Information	13
2.3	Time or Frequency of Publication	13
2.4	Access Control on Repositories	13
3	IDENTIFICATION AND AUTHENTICATION	13
3.1	Naming	13
3.1.1	Types of Names	13
3.1.2	Need for Names to be Meaningful	14
3.1.3	Anonymity or Pseudonymity of Subscribers	14
3.1.4	Rules for Interpreting Various Name Forms	14
3.1.5	Uniqueness of Names	14
3.1.6	Recognition, Authentication, and Role of Trademarks	14
3.2	Initial Identity Validation	14
3.2.1	Method to Prove Possession of Private Key	14
3.2.2	Authentication of Organisation Identity	14
3.2.3	Authentication of Individual Identity	14
3.2.4	Non-verified Subscriber Information	14
3.2.5	Validation of Authority	15
3.2.6	Criteria for Interoperation	15
3.3	Identification and Authentication for re-key Requests	15
3.2.7	Identification and Authentication for Routine Re-Key	15
3.2.8	Identification and Authentication for Re-Key after Revocation	15
3.4	Identification and Authentication for Revocation Requests	15

4	CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS.....	15
4.1	Certificate Applications	15
4.1.1	Submission of Certificate Applications	15
4.1.2	Enrolment Process for the Subscriber and its Representatives.....	15
4.1.3	Enrolment Process for the Registration Authority and its Representatives	15
4.2	Certificate Application Processing.....	16
4.2.1	Performing Identification and Authentication Functions	16
4.2.2	Approval or Rejection of Certificate Applications	16
4.2.3	Approval or Rejection of Certificate Applications	16
4.2.4	Time to Process Certificate Applications	16
4.3	VWKI Certificate Issuance.....	16
4.3.1	VWKICA actions during certificate Issuance	16
4.3.2	Notification to VWKI Eligible Subscriber by the VWKICA of Issuance of Certificate	17
4.4	Certificate Acceptance	17
4.4.1	Conduct Constituting Certificate Acceptance	17
4.4.2	Publication of Certificates by the VWKICA.....	17
4.4.3	Notification of Certificate Issuance by the VWKICA to Other Entities	17
4.5	Key Pair and Certificate Usage	17
4.5.1	VWKI Authorised Subscriber Private Key and Certificate Usage.....	17
4.5.2	VWKI Relying Party Public Key and Certificate Usage	17
4.6	Certificate Renewal	17
4.6.1	Circumstances of Certificate Renewal.....	17
4.6.2	Circumstances of Certificate Replacement.....	17
4.6.3	Who May Request a Replacement Certificate	18
4.6.4	Processing Replacement Certificate Requests.....	18
4.6.5	Notification of Replacement Certificate Issuance to a Subscriber	18
4.6.6	Conduct Constituting Acceptance of a Replacement Certificate.....	18
4.6.7	Publication of a Replacement Certificate by the VWKICA.....	18
4.6.8	Notification of Certificate Issuance by the VWKICA to Other Entities	18
4.7	Certificate Re-Key.....	18
4.7.1	Circumstances for Certificate Re-Key.....	18
4.7.2	Who may request Certificate re-key.....	18
4.7.3	Processing Certificate Re-Keying Requests	18
4.7.4	Notification of New Certificate Issuance to Subscriber	18
4.7.5	Conduct Constituting Acceptance of a Re-Keyed Certificate.....	18
4.7.6	Publication of the Re-Keyed Certificate by the VWKICA	18
4.7.7	Notification of Certificate Issuance by the VWKICA to Other Entities	18
4.8	Certificate Modification	18
4.8.1	Circumstances for Certificate Modification	18
4.8.2	Who may request Certificate Modification	18
4.8.3	Processing Certificate Modification Requests.....	18
4.8.4	Notification of New Certificate Issuance to Subscriber	18
4.8.5	Conduct Constituting Acceptance of Modified Certificate.....	19
4.8.6	Publication of the Modified Certificate by the VWKICA	19
4.8.7	Notification of Certificate Issuance by the VWKICA to Other Entities	19

4.9	Certificate Revocation and Suspension.....	19
4.10	Certificate Status Services	19
4.10.1	Operational Characteristics.....	19
4.10.2	Service Availability	19
4.10.3	Optional Features	19
4.11	End of Subscription	19
4.12	Key Escrow and Recovery	19
4.12.1	Key Escrow and Recovery Policies and Practices	19
4.12.2	Session Key Encapsulation and Recovery Policy and Practices.....	19
5	FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS	19
5.1	Physical Controls	19
5.1.1	Site location and construction.....	19
5.1.2	Physical access	20
5.1.3	Power and air conditioning	20
5.1.4	Water exposure.....	20
5.1.5	Fire prevention and protection.....	20
5.1.6	Media storage.....	20
5.1.7	Waste disposal.....	20
5.1.8	Off-site backup	20
5.2	Procedural controls	21
5.2.1	Trusted roles	21
5.2.2	Number of persons required per task	21
5.2.3	Identification and authentication for each role.....	21
5.2.4	Roles requiring separation of duties	21
5.3	Personnel controls	21
5.3.1	Qualification, experience and clearance requirements	21
5.3.2	Background check procedures	21
5.3.3	Training requirements.....	21
5.3.4	Retraining frequency and requirements.....	22
5.3.5	Job rotation frequency and sequence	22
5.3.6	Sanctions for unauthorised actions.....	22
5.3.7	Independent contractor requirements	22
5.3.8	Documentation supplied to personnel.....	22
5.4	Audit logging procedures	22
5.4.1	Types of events recorded	22
5.4.2	Frequency of processing log.....	22
5.4.3	Retention period for Audit Log.....	22
5.4.4	Protection of audit log	22
5.4.5	Audit Log backup procedures	23
5.4.6	Audit collection system (internal or external)	23
5.4.7	Notification to event-causing subject.....	23
5.4.8	Vulnerability assessments	23
5.5	Records archival.....	23
5.5.1	Types of records archived	23
5.5.2	Retention period for archive	23

5.5.3	Protection of archive	23
5.5.4	Archive backup procedures.....	24
5.5.5	Requirements for Time-Stamping of records	24
5.5.6	Archive collection system (internal or external)	24
5.5.7	Procedures to obtain and verify archive information	24
5.6	Key changeover.....	24
5.6.1	Issuing VWP CA key changeover	24
5.6.2	Issuing VWD CA key changeover	24
5.6.3	VWKI Root Key changeover	24
5.7	Compromise and disaster recovery	25
5.7.1	Incident and compromise handling procedures	25
5.7.2	Computing resources, software and/or data are corrupted	25
5.7.3	Entity private key compromise procedures	25
5.7.4	Business continuity capabilities after a disaster	25
5.7.5	VWKICA and VWKI Registration Authority termination	25
6	TECHNICAL SECURITY CONTROLS	25
6.1	Key pair generation and installation	25
6.1.1	Key pair generation.....	25
6.1.2	Private Key delivery to VWKI Subscriber.....	25
6.1.3	Public Key delivery to certificate issuer	26
6.1.4	VWKICA Public Key delivery to Relying Parties.....	26
6.1.5	Key sizes	26
6.1.6	Public Key parameters generation and quality checking	26
6.1.7	Key usage purposes (as per X.509 v3 key usage field)	26
6.2	Private Key Protection and Cryptographic Module Engineering Controls	26
6.2.1	Cryptographic module standards and controls	26
6.2.2	Private Key (key (m out of n) multi-person control	26
6.2.3	Private Key escrow.....	26
6.2.4	Private Key backup	26
6.2.5	Private Key archival	27
6.2.6	Private Key transfer into or from a Cryptographic Module	27
6.2.7	Private Key Storage on Cryptographic Module	27
6.2.8	Method of Activating Private Key.....	27
6.2.9	Method of deactivating Private Key.....	27
6.2.10	Method of destroying Private Key.....	27
6.2.11	Cryptographic module rating.....	27
6.3	Other aspects of Key Pair management.....	28
6.3.1	Public Key archival	28
6.3.2	Certificate operational periods and Key Pair usage periods	28
6.4	Activation Data.....	28
6.4.1	Activation data generation and installation.....	28
6.4.2	Activation data protection.....	28
6.5	Computer security controls	28
6.5.1	Specific computer security technical requirements	28
6.5.2	Computer security rating.....	28

6.6	Life cycle technical controls.....	28
6.6.1	System development controls.....	28
6.6.2	Security management controls	28
6.6.3	Life cycle security controls	28
6.7	Network security controls	29
6.7.1	Protection against attack.....	29
6.7.2	Health Check of VWKICA Systems.....	29
6.8	Time-stamping.....	29
6.8.1	Use of time-stamping.....	29
7	CERTIFICATE, CRL AND OCSP PROFILES.....	29
7.1	Certificate profile	29
7.1.1	Version number(s).....	29
7.1.2	Certificate extensions.....	29
7.1.3	Algorithm object identifiers.....	29
7.1.4	Name forms	29
7.1.5	Name constraints.....	29
7.1.6	Certificate policy object identifier	29
7.1.7	Usage of Policy Constraints extension	29
7.1.8	Policy qualifiers syntax and semantics	30
7.1.9	Processing semantics for the critical Certificate Policies extension	30
7.2	CRL profile	30
7.2.2	Version number(s).....	30
7.2.3	CRL and CRL entry extensions	30
7.1	OCSP profile	30
7.3.1	Version number(s).....	30
7.3.2	OCSP extensions	30
8	COMPLIANCE AUDIT AND OTHER ASSESSMENTS	30
8.1	Frequency or circumstances of assessment.....	Error! Bookmark not defined.
8.2	Identify/qualifications of assessor.....	Error! Bookmark not defined.
8.3	Assessor's relationship to assessed entity.....	Error! Bookmark not defined.
8.4	Topics covered by assessment.....	30
8.5	Actions taken as a result of deficiency	30
8.6	Communication of results.....	Error! Bookmark not defined.
9	OTHER BUSINESS AND LEGAL MATTERS.....	31
9.1	Fees	31
9.1.1	Certificate Issuance or renewal fees	31
9.1.2	Device certificate access fees.....	31
9.1.3	Revocation or status information access fees	31
9.1.4	Fees for other services.....	31
9.1.5	Refund policy	31
9.2	Financial responsibility.....	31
9.2.1	Insurance coverage.....	31
9.2.2	Other assets.....	31
9.2.3	Insurance or warranty coverage for subscribers and subjects	31
9.3	Confidentiality of business information	31

9.3.1	Scope of confidential information	31
9.3.2	Information not within the scope of confidential information	31
9.3.3	Responsibility to protect confidential information	31
9.4	Privacy of personal information	31
9.4.1	Privacy plan	31
9.4.2	Information treated as private	32
9.4.3	Information not deemed private	32
9.4.4	Responsibility to protect private information	32
9.4.5	Notice and consent to use private information	32
9.4.6	Disclosure pursuant to judicial or administrative process	32
9.4.7	Other information disclosure circumstances	32
9.5	Intellectual property rights	32
9.6	Representations and warranties	32
9.6.1	CA representations and warranties	32
9.6.2	RA representation and warranties	32
9.6.3	Subscriber representations and warranties	32
9.6.4	Relying party representations and warranties	32
9.7	Representations and warranties of other participants	32
9.8	Disclaimers of warranties	32
9.9	Limitations of liability	32
9.10	Indemnities	32
9.11	Term and termination	32
9.11.1	Term	32
9.11.2	Termination	32
9.11.3	Effect of termination and survival	32
9.12	Individual notices and communications with participants	33
9.13	Amendments	33
9.13.1	Procedure for amendment	33
9.13.2	Notification mechanism and period	33
9.13.3	Circumstances under which OID must be changed	33
9.14	Dispute resolution provisions	33
9.15	Governing law	33
9.16	Compliance with applicable law	33
9.17	Miscellaneous provisions	33
9.17.1	Entire agreement	33
9.17.2	Assignment	33
9.17.3	Severability	33
9.17.4	Enforcement (attorneys' fees and waiver of rights)	33
9.17.5	Force Majeure	33
9.18	Other provisions	33
ANNEX A		33
DEFINED TERMS		33
ANNEX B		38
VWKI CERTIFICATE PROFILES		38
End Entity Certificate Structure and Contents		38

Common Requirements applicable to all VWKI Certificates	38
Requirements applicable to VWP Certificates only	38
Requirements Applicable to VWD Certificates only	38
Requirements Applicable to Issuing VWP CA Certificates only	39
Requirements Applicable to Issuing VWD CA Certificates only	39
Requirements Applicable to Root VWKICA Certificates only	39
VWP Certificate Profile for the purposes of establishing TLS Communications	40
Interpretation	41
version	41
serialNumber	41
signature.....	41
issuer	41
Validity	41
notBefore	41
notAfter	42
subject.....	42
subjectPublicKeyInfo.....	42
Extensions.....	42
authorityKeyIdentifier	43
subjectKeyIdentifier.....	43
keyUsage.....	43
certificatePolicies	43
extendedKeyUsage	43
subjectAltName	43
VWD Certificate Profile for the purposes of establishing TLS communications	43
Interpretation	44
version	44
serialNumber	44
signature.....	44
issuer	45
validity	45
notBefore	45
notAfter	45
subject.....	45
subjectPublicKeyInfo.....	45
Extensions.....	46
authorityKeyIdentifier	46
subjectKeyIdentifier.....	46
keyUsage.....	46
certificatePolicies	46
extendedKeyUsage	46
Issuing VWP CA Certificate Profile	47
Interpretation	48
version	48
serialNumber	48

signature.....	48
issuer	48
Validity	48
notBefore	48
notAfter	49
subject.....	49
subjectPublicKeyInfo.....	49
Extensions.....	50
authorityKeyIdentifier	50
subjectKeyIdentifier.....	50
keyUsage.....	50
certificatePolicies	50
basicConstraints	50
Issuing VWD CA Certificate Profile.....	51
Interpretation	52
version	52
serialNumber	52
signature.....	52
Validity	52
notBefore	52
notAfter	53
subject.....	53
subjectPublicKeyInfo.....	53
Extensions.....	54
authorityKeyIdentifier	54
subjectKeyIdentifier.....	54
keyUsage.....	54
certificatePolicies	54
basicConstraints	54
Root VWKICA Certificate VWKI Certificate Profile.....	55
Interpretation	55
version	56
serialNumber	56
signature.....	56
issuer	56
Validity	56
notBefore	56
notAfter	56
subject.....	56
subjectPublicKeyInfo.....	56
Extensions.....	57
authorityKeyIdentifier	57
subjectKeyIdentifier.....	57
keyUsage.....	58
certificatePolicies	58

basicConstraints	58
-------------------------------	-----------

1 INTRODUCTION

- (a) The document comprising this Appendix [TBC] (together with its Annexes A and B):
 - (i) shall be known as the “VWKI Certificate Policy” (and in this document is referred to simply as the “Policy”); and
 - (ii) is a SEC Subsidiary Document related to Section L18.28 (The VWKI SEC Documents) of the Code.

1.1 Overview

- (a) This Policy sets out the arrangements relating to:
 - (i) The Root VWKICA Certificate;
 - (ii) Issuing VWP CA Certificates; and
 - (iii) Issuing VWD CA Certificates;

together referred to as the “**VWKICA Certificates**” and

 - (iv) VWP Certificates; and
 - (v) VWD Certificates;

together with the VWKICA Certificates referred to as the “**VWKI Certificates**”.
- (b) This Policy is structured according to the guidelines provided by IETF RFC 3647, with appropriate extensions, modifications and deletions.

1.2 Document Name and Identification

- (a) This Policy has been registered with the Internet Address Naming Authority and assigned an OID of 1.2.826.0.1.8641679.1.2.1.5.

1.3 VWKI Participants

1.3.1 The VWKI Certification Authority

- (a) The definition of the VWKI Certification Authority is set out in Annex A.

1.3.2 VWKI Registration Authority

- (a) The definition of the VWKI Registration Authority is set out in Annex A.

1.3.3 VWKI Subscribers

- (a) In accordance with Section L18.2 and L18.34 to L18.38 of the Code (VWKI Authorised Subscribers), certain Parties may become VWKI Authorised Subscribers.
- (b) In accordance with Section L18.6 of the Code, a VWKI Authorised Subscriber shall be a VWKI Eligible Subscriber in relation to certain Certificates.
- (c) The VWKI RAPP sets out the procedure to be followed by Parties in order to become a VWKI Authorised Subscriber.
- (d) The VWKI RAPP sets out the procedure to be followed by an Eligible Subscriber in order to become a Subscriber for one or more Certificates
- (e) The DCC (acting in its capacity as the Root VWKICA, Issuing VWP CA, Issuing VWD CA or Virtual WAN Provider) shall be a VWKI Authorised Subscriber and:
 - (i) it (and only it) shall be a VWKI Eligible Subscriber in respect of VWKICA Certificates; and
 - (ii) (save for the purpose of replacement of the Root VWKICA), it shall be a VWKI Eligible Subscriber only in respect of a single Root VWKICA Certificate

- (iii) It (and only it) shall be a VWKI Eligible Subscriber in respect of VWP Certificates.
- (f) VWKI Eligible Subscribers and VWKI Subscribers are subject to the applicable requirements of this Policy, the VWKI RAPP and Sections L18.34 to L18.38 (The VWKI Subscriber Obligations) of the Code.
- (g) The definitions of the following terms are set out in Annex A of this document:
 - (i) VWKI Subscriber; and
 - (ii) VWKI Eligible Subscriber.
 - (iii) VWKI Authorised Subscriber

1.3.4 VWKI Relying Parties

- (a) The definition of a VWKI Relying Party is set out in Section A of the Code (Definitions and Interpretations).
- (b) VWKI Relying Parties shall be subject to the applicable requirements of Section L18.39 to L18.43 (The VWKI Relying Party Obligations) of the Code.

1.3.5 VWKI Policy Management Authority

- (a) The SMKI PMA shall fulfil the functions of the VWKI PMA in accordance with the provisions set out in Sections L1.1 to L1.17 (The VWKI PMA Functions) of the Code.

1.3.6 VWKI Repository Provider

- (a) Provision in relation to the VWKI Repository Service is made in Section L18.14 (The VWKI Repository Service) of the Code.

1.4 Usage of VWKI Certificates

1.4.1 Appropriate Certificate Uses

- (a) The VWKICA shall ensure that VWKICA Certificates are Issued only to:
 - (i) the Root VWKICA for use in its capacity as, and for the purposes of, exercising its functions as the Root VWKICA; and
 - (ii) the Issuing VWP CA and the Issuing VWD CA, in their capacity as, and for the purposes of exercising the functions of, issuing authorities.
- (b) Subject to 1.4.1 (e), the VWKICA shall ensure that VWP Certificates are Issued only:
 - (i) by the Issuing VWP CA, and only to DCC (acting in its capacity as the Virtual WAN Provider); and
 - (ii) for the purposes of:
 - (1) establishing TLS communications with the VWDs over an Internet connection; or
- (c) Subject to 1.4.1 (e), the VWKICA shall ensure that VWD Certificates are Issued only:
 - (i) by the Issuing VWD CA, and to VWD Manufacturers; and
 - (ii) for the purpose of establishing TLS communications by VWDs with the VWP over an Internet connection.
- (d) Further provision in relation to Parties obligations in respect of the use of VWKI Certificates is made in Sections L18.34 to L18.38 (The VWKI Subscriber Obligations) of the Code and Sections L18.39 to L18.43 (The VWKI Relying Party Obligations) of the Code.

1.4.2 Prohibited Certificate Uses

- (a) No Party shall use a VWKI Certificate other than for the purposes permitted in Part 1.4.1 of this Policy.

1.5 Policy Administration

1.5.1 Organisation Administering the Document

- (a) This Policy is a SEC Subsidiary Document and shall be maintained in accordance with the provisions of the Code.

1.5.2 Contact Person

- (a) Questions in relation to the content of this Policy should be addressed to the SMKI PMA or the Service Desk.

1.5.3 Person determining Certification Practice Statement suitability for the Policy

- (a) Provision is made in Section L18.29 (the VWKI Certification Practice Statement) of the Code in relation to the suitability of the VWKI CPS for the Policy.

1.5.4 CPS Approval Procedures

- (a) Provision is made in Section L18.30 of the Code for the procedure by which the SMKI PMA may approve the VWKI CPS.

1.5.5 Registration Authority Policies and Procedures

- (a) The VWKI Registration Authority Policies and Procedures are set out at Appendix [TBC] of the Code.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

- (a) Provision is made in Section L18.14 (the VWKI Repository Service) of the Code for the establishment, operation and maintenance of the VWKI Repository.

2.2 Publication of Certification Information

- (a) Section L18.15 (the VWKI Repository Service) of the Code makes provision for the lodging of documents and information in the VWKI Repository.

2.3 Time or Frequency of Publication

- (a) The VWKICA shall ensure that:
 - (i) The Root VWKICA Certificate is promptly lodged in the VWKI Repository; and
 - (ii) each Issuing VWP CA Certificate and Issuing VWD CA Certificate issued under this Policy is promptly lodged in the VWKI repository.

2.4 Access Control on Repositories

- (a) Provision in relation to access controls for the VWKI Repository is made in Section L18.19 (the VWKI Repository Service) of the Code and the VWKI Interface Design Specification and the VWKI Certification Practice Statement.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of Names

- (a) Provision is made in the VWKI RAPP to ensure that the name of the Subject of each VWKI Certificate is in accordance with the relevant VWKI Certificate Profile in Annex B to this document.

3.1.2 Need for Names to be Meaningful

- (a) Provision is made in the VWKI RAPP to ensure that the name of the Subject of each VWP Certificate and VWD Certificate is meaningful and consistent with the relevant VWKI Certificate Profile in Annex B to this document.

3.1.3 Anonymity or Pseudonymity of Subscribers

- (a) Provision is made in the VWKI RAPP section 17.3 to prohibit VWKI Eligible Subscribers from requesting the issue of a VWKI Certificate anonymously or by means of a pseudonym.

3.1.4 Rules for Interpreting Various Name Forms

- (a) Provision in relation to name forms is made in Annex B to this document.

3.1.5 Uniqueness of Names

- (a) Provision in relation to the uniqueness of names is made in Annex B to this document.

3.1.6 Recognition, Authentication, and Role of Trademarks

- (a) Provision in relation to the use of trademarks, trade names and other restricted information in VWKI Certificates is made in Section L18.35 of the Code.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

- (a) Provision is made in the VWKI RAPP in relation to:
 - (i) the procedure to be followed by a VWKI Eligible Subscriber in order to prove its possession of the Private Key that is associated with the Public Key to be contained in any VWP Certificate or VWD Certificate that is the subject of a VWKI Certificate Signing Request which has been submitted by that Eligible Subscriber; and
 - (ii) that the procedure established for this purpose is in accordance with the procedure in PKCS#10 or an equivalent cryptographic mechanism as agreed by the SMKI PMA.
- (b) Provision is made in the VWKI CPS in relation to:
 - (i) the procedure to be followed by the VWKICA in order to prove its possession of the Private Key that is associated with the Public Key to be contained in any VWKICA Certificate that is the subject of a VWKI Certificate Signing Request; and

3.2.2 Authentication of Organisation Identity

- (a) Provision is made in the VWKI RAPP section 6.2 in relation to:
 - (i) The procedure to be followed by a Party in order to become a VWKI Authorised Subscriber;
 - (ii) The criteria in accordance with which the VWKI Registration Authority shall determine whether a Party is entitled to become a VWKI Authorised Subscriber;
 - (iii) The requirement that the Party shall be Authenticated by the VWKICA for that purpose; and
 - (iv) The criteria in accordance with which the VWKICA shall determine whether a Party is Authenticated.

3.2.3 Authentication of Individual Identity

- (a) Provision is made in the VWKI RAPP section 3 in relation to the Authentication of individuals engaged by VWKI Authorised Subscribers to fulfil roles defined in this Policy.

3.2.4 Non-verified Subscriber Information

[not applicable]

3.2.5 Validation of Authority

See Part 3.2.2 of this Policy.

3.2.6 Criteria for Interoperation

[Not applicable]

3.3 Identification and Authentication for re-key Requests**3.2.7 Identification and Authentication for Routine Re-Key**

- (a) This Policy does not support Certificate Re-Key.
- (b) The VWKICA shall not provide a Certificate Re-Key service.

3.2.8 Identification and Authentication for Re-Key after Revocation

[Not applicable]

3.4 Identification and Authentication for Revocation Requests

[Not applicable]

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS**4.1 Certificate Applications****4.1.1 Submission of Certificate Applications**

- (a) Provision is made in the VWKI RAPP section 17 with respect to the circumstances in which an VWKI Eligible Subscriber may:
 - (i) submit a VWKI Certificate Signing Request in relation to a VWP Certificate;
 - (ii) submit a VWKI Certificate Signing Request in relation to a VWD Certificate; and
 - (iii) submit a VWKI Certificate Signing Request in relation to a VWKICA Certificate,
 and, in each case, the means by which that VWKI Eligible Subscriber may do so.

4.1.2 Enrolment Process for the Subscriber and its Representatives

- (a) Provision is made in the VWKI RAPP section 6 in relation to the:
 - (i) establishment of an enrolment process in relation to Parties in order to Authenticate them and verify that they are authorised to act as VWKI Authorised Subscribers;
 - (ii) establishment of an enrolment process in relation to individuals nominated to act on behalf of VWKI Authorised Subscribers as VWKI Senior Responsible Officers or VWKI Authorised Responsible Officers, in order to Authenticate them and verify that they are authorised to act on behalf of those VWKI Authorised Subscribers; and
 - (iii) maintenance by the SMKI RA of a list of Parties enrolled in accordance with those enrolment processes.

4.1.3 Enrolment Process for the Registration Authority and its Representatives

- (a) Provision is made in the VWKI RAPP section 2 in relation to the establishment of an enrolment process in respect of VWKICA Personnel and VWKICA Systems for the purpose of Authentication and to verify that they are authorised to act on behalf of the VWKICA in its capacity as the VWKI Registration Authority; including in particular, for that purpose, provision for:
 - (i) the Authentication of all VWKI Registration Authority Personnel by a VWKI Registration Authority Manager; and

- (ii) all VWKI Registration Authority Personnel to have their identity and authorisation verified prior to being provided these roles.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

- (a) Provision is made in the VWKI RAPP section 3 in relation to the Authentication by the VWKICA of a VWKI Eligible Subscriber which submits:
 - (i) a VWKI Certificate Signing Request in relation to a VWP Certificate; or
 - (ii) a VWKI Certificate Signing Request in relation to a VWD Certificate.

4.2.2 Approval or Rejection of Certificate Applications

- (a) Where any VWKI Certificate Signing Request made in relation to a VWP Certificate or a VWD Certificate fails to satisfy the requirements set out in the VWKI RAPP section 17.10, this Policy or any other provisions of the Code, the VWKICA:
 - (i) shall reject it and refuse to Issue the VWP Certificate or VWD Certificate which was the subject of that VWKI Certificate Signing Request, and
 - (ii) shall give notice to the person that made the VWKI Certificate Signing Request of the reasons for its rejection.
- (b) Where the failure results from a failure of Authentication of the VWKI Eligible Subscriber, then an Incident shall be raised by VWKICA Personnel.
- (c) Where any VWKI Certificate Signing Request satisfies the requirements set out in the VWKI RAPP, this Policy, and any other provision of the Code, the VWKICA shall Issue the VWKI Certificate that was the subject of that VWKI Certificate Signing Request.

4.2.3 Approval or Rejection of Certificate Applications

- (a) Provision is made in the VWKI RAPP section 17.10 for the VWKICA to notify a VWKI Eligible Subscriber of the Issuance of a VWKI Certificate which was the subject of a VWKI Certificate Signing Request.

4.2.4 Time to Process Certificate Applications

- (a) Provision is made in the VWKI RAPP section 17.5 in relation to the agreed elapsed time for the processing of VWKI Certificate Signing Requests in accordance with this Policy.

4.3 VWKI Certificate Issuance

4.3.1 VWKICA actions during certificate Issuance

- (a) The Root VWKICA shall Issue a VWKICA Certificate only in accordance with the provisions of this Policy and the VWKI CPS.
- (b) The VWKICA shall Issue a VWP Certificate or a VWD Certificate only in accordance with the provisions of this Policy and the VWKI RAPP and:
 - (i) in the case of VWP Certificates or VWD Certificates, only in response to a VWKI Certificate Signing Request made by a VWKI Eligible Subscriber; and
- (c) The VWKICA shall ensure that each VWKI Certificate that is Issued by it contains information that:
 - (i) it has verified to be correct and complete; and
 - (ii) is consistent with the information in the VWKI Certificate Signing Request.

4.3.2 Notification to VWKI Eligible Subscriber by the VWKICA of Issuance of Certificate

- (a) Provision is made in the VWKI RAPP for the VWKICA to notify a VWKI Eligible Subscriber of the Issuance of a VWKI Certificate which was the subject of a VWKI Certificate Signing Request.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

- (a) Provision is made in the VWKI RAPP section 17.10 to:
 - (i) specify the means by which an VWKI Eligible Subscriber may clearly indicate to the VWKICA its rejection of a VWKI Certificate which has been Issued to it; and
 - (ii) specify the circumstances in which a VWKI Eligible Subscriber is treated as a VWKI Subscriber in relation to a VWKI Certificate.
- (b) Further provision in relation to subscribing for or rejecting VWKI Certificates is made in Section L18.36 (Subscribing for or Rejecting VWKI Certificates) of the Code.

4.4.2 Publication of Certificates by the VWKICA

- (a) Following Issuance, the VWKICA shall lodge a copy of each Root VWKICA Certificate, each Issuing VWP CA Certificate, each Issuing VWD CA certificate, VWP Certificate and each VWD Certificate in the VWKI Repository.
- (b) Further provision in relation to the publication of VWKI Certificates is made in Part 2 of this Policy and in Section - L18.14 to L18.18 (the VWKI Repository Service) of the Code.

4.4.3 Notification of Certificate Issuance by the VWKICA to Other Entities

- (a) The VWKICA shall give explicit notice of the Issue of a VWKI Certificate only to the VWKI Eligible Subscriber who submitted the VWKI Certificate Signing Request.

4.5 Key Pair and Certificate Usage

4.5.1 VWKI Authorised Subscriber Private Key and Certificate Usage

- (a) Provision for restrictions on the use by VWKI Authorised Subscribers of Private Keys in respect of VWKI Certificates is made in:
 - (i) Section G5.24 (the User Information Security Management System) of the Code;
 - (ii) Section - L18 (Virtual WAN Key Infrastructure) of the Code;
 - (iii) this Policy; and
 - (iv) the VWKI Certification Practice Statement.

4.5.2 VWKI Relying Party Public Key and Certificate Usage

- (a) Provision in relation to reliance that may be placed on a VWKI Certificate is made in Section - L18.39 to L18.43 (the VWKI Relying Party Obligations) of the Code.

4.6 Certificate Renewal

4.6.1 Circumstances of Certificate Renewal

- (a) This Policy does not support the renewal of VWKI Certificates.
- (b) The VWKICA may only replace, and shall not renew, any VWKI Certificate.

4.6.2 Circumstances of Certificate Replacement

- (a) A VWKI Certificate replacement may occur:
 - (i) where the request for VWKI Certificate replacement relates to normal business activity, in which case the process set out in the VWKI RAPP shall apply;
 - (ii) where suspicion of Compromise or Compromise is reported for a VWKI Certificate that has been issued; in which case the matter shall be managed through the Incident Management Policy and in accordance with the VWKI RAPP.

4.6.3 Who May Request a Replacement Certificate

See Part 4.1 of this Policy.

4.6.4 Processing Replacement Certificate Requests

See Part 4.2 of this Policy.

4.6.5 Notification of Replacement Certificate Issuance to a Subscriber

See Part 4.3 of this Policy.

4.6.6 Conduct Constituting Acceptance of a Replacement Certificate

See Part 4.4 of this Policy.

4.6.7 Publication of a Replacement Certificate by the VWKICA

See Part 4.4.2 of this Policy.

4.6.8 Notification of Certificate Issuance by the VWKICA to Other Entities

See Part 4.4.3 of this Policy.

4.7 Certificate Re-Key

- (a) This Policy does not support Certificate Re-Key.

4.7.1 Circumstances for Certificate Re-Key

[Not applicable]

4.7.2 Who may request Certificate re-key

[Not applicable]

4.7.3 Processing Certificate Re-Keying Requests

[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 by the VWKICA

[Not applicable]

4.7.7 Notification of Certificate Issuance by the VWKICA to Other Entities

[Not applicable]

4.8 Certificate Modification

- (a) This Policy does not support VWKI Certificate modification.

4.8.1 Circumstances 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 by the VWKICA

[Not applicable]

4.8.7 Notification of Certificate Issuance by the VWKICA to Other Entities

[Not applicable]

4.9 Certificate Revocation and Suspension

- (a) This certificate policy does not support certificate revocation or suspension.

4.10 Certificate Status Services**4.10.1 Operational Characteristics**

[Not applicable]

4.10.2 Service Availability

[Not applicable]

4.10.3 Optional Features

[Not applicable]

4.11 End of Subscription

[Not applicable]

4.12 Key Escrow and Recovery

- (a) This Policy does not support Key Escrow.
- (b) The VWKICA shall not provide a Key Escrow service.

4.12.1 Key Escrow and Recovery Policies and Practices

[Not applicable]

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

[Not applicable]

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS**5.1 Physical Controls****5.1.1 Site location and construction**

- (a) The VWKICA shall ensure that the VWKICA Systems are operated in a sufficiently secure environment which shall at least satisfy the requirements set out in Section G2 (System Security: Obligations on the DCC) and Section G5 (Information Security: Obligations on the DCC and Users) of the Code.
- (b) The VWKICA shall ensure that the VWKI CPS incorporates provisions in relation to physical controls including in particular provisions designed to ensure that:
 - (i) all of the physical locations in which the VWKICA Systems are situated, operated, routed or directly accessed are in the United Kingdom;
 - (ii) all bespoke Security Related Functionality is developed, specified, designed, built and tested only within the United Kingdom;
 - (iii) all Security Related Functionality is integrated, configured, tested in situ, implemented, operated and maintained only within the United Kingdom;
 - (iv) the VWKICA Systems cannot be indirectly accessed from any location outside the United Kingdom;
 - (v) the Root VWKICA shall operate as a secure offline entity that is Separate from the rest of the DCC Systems; and

- (vi) all Private Keys used to support the VWKICA are generated, stored and processed within the cryptographic envelope of a Cryptographic Module which meets the FIPS 140-2 Level 3 or equivalent cryptographic standard.
- (c) The functions of the VWKI Registration Authority shall securely interoperate with the other operational elements of the VWKICA, as detailed in the VWKI CPS.

5.1.2 Physical access

- (a) The VWKICA shall ensure that the VWKI CPS incorporates provisions in relation to access control including, in particular, provisions designed to:
 - (i) establish and maintain controls such that only appropriately authorised personnel may have unescorted physical access to VWKICA Systems;
 - (ii) ensure that any unauthorised personnel may have physical access to VWKICA Systems only if appropriately authorised and supervised;
 - (iii) ensure that site access procedures are audited as part of both internal audits and third-party audits carried out in accordance with ISO/IEC 27001;
 - (iv) ensure that all material in relation to cryptographic operation is securely managed; and
 - (v) ensure that removable media which contain sensitive data are kept in secure locations, managed through life and disposal, and accessible only to appropriately authorised individuals.

5.1.3 Power and air conditioning

- (a) The VWKICA shall ensure that the VWKI CPS incorporates provisions in relation to power and air conditioning at all physical locations in which the VWKICA Systems are situated.

5.1.4 Water exposure

- (a) The VWKICA shall ensure that the VWKI CPS incorporates provisions in relation to water exposure at all physical locations in which the VWKICA Systems are situated.

5.1.5 Fire prevention and protection

- (a) The VWKICA shall ensure that the VWKI CPS incorporates provisions in relation to fire prevention and protection at all physical locations in which the VWKICA Systems are situated.

5.1.6 Media storage

- (a) The VWKICA shall ensure that the VWKI CPS incorporates provisions in relation to media storage at all physical locations in which the VWKICA Systems are situated.

5.1.7 Waste disposal

- (a) The VWKICA shall ensure that all media used to store Data held by it for the purposes of carrying out its functions is securely disposed of in accordance with <https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media>.

5.1.8 Off-site backup

- (a) The VWKICA shall ensure that the VWKI CPS incorporates provisions in relation to off-site back up and data management of data held in the VWKICA Systems.
- (b) The VWKICA shall ensure that backups shall be made to support disaster recovery models as defined within the VWKI CPS.
- (c) The VWKICA shall ensure that:
 - (i) regular backups of critical VWKICA and VWKI Registration Authority operational data relating to the Issuing of VWKI Certificates are made;
 - (ii) appropriate backups of the Root VWKICA are made on a periodic basis;
 - (iii) backup of cryptographic material used in support of the Root VWKICA, Issuing VWP CA and the Issuing VWD CA shall be in line with manufacturer procedures and FIPS 140-2 Level 3 or an equivalent cryptographic standard; and
 - (iv) security of off-site storage shall be managed and implemented in alignment with security in place at the main locations.

5.2 Procedural controls

5.2.1 Trusted roles

- (a) The VWKICA shall ensure that the VWKI CPS incorporates provisions designed to ensure that:
 - (i) Persons with trusted roles are given only the access rights that are commensurate with their role and each has a clearly defined role and access level;
 - (ii) allocated roles are pertinent to the required task;
 - (iii) roles and responsibilities are documented;
 - (iv) no individual member of VWKICA Personnel is capable, by acting alone, of engaging in any action by means of which the VWKICA Systems may be compromised to a material extent;
 - (v) roles are implemented in line with best practice for a certification authority; and
 - (vi) multi-person controls are applied with respect to Root VWKICA Private Key management.

5.2.2 Number of persons required per task

- (a) The VWKICA shall ensure that the VWKI CPS incorporates provisions designed to establish:
 - (i) the appropriate separation of roles between the different members of VWKICA Personnel;
 - (ii) the application of controls to the actions of all members of VWKICA Personnel who are Privileged Persons, in particular:
 - (1) identifying any controls designed to ensure that the involvement of more than one individual is required for the performance of certain functions; and
 - (2) identifying the number of roles that an individual may hold.
 - (iii) the VWKICA shall apply such multi-person controls:
 - (1) in accordance with the operation and risk as identified with within the DCC Information Security Management System;
 - (2) in accordance with best practice in the case of management of cryptographic material; and
 - (3) with respect to Root VWKICA Private Key management.

5.2.3 Identification and authentication for each role

- (a) All VWKICA Personnel shall be required to authenticate via a strong at least two factor Authentication in accordance with the SMKI PMA Guidance on "Verifying Individual Identity" published on the Website before they can access any facilities.

5.2.4 Roles requiring separation of duties

- (a) The VWKICA shall identify roles that require separation of duties for VWKICA functions in line with industry best practice.
- (b) The VWKICA shall ensure that the VWKI CPS incorporates provisions that ensure separation of duties in roles requiring separation of duties.

5.3 Personnel controls

5.3.1 Qualification, experience and clearance requirements

- (a) The VWKICA shall ensure that all VWKICA Personnel must:
 - (i) be appointed to their roles in writing;
 - (ii) be bound by contract to the terms and conditions and non-disclosure agreements relevant to their roles;
 - (iii) have received appropriate training with respect to their duties; and
 - (iv) have, as a minimum, passed a Security Check level of vetting, before commencing their roles.

5.3.2 Background check procedures

- (a) The VWKICA shall ensure that all VWKICA Personnel with access to VWKICA operations shall undergo formal security checks, as set out within the VWKI CPS.

5.3.3 Training requirements

- (a) See Part 5.3.1 of this Policy.

5.3.4 Retraining frequency and requirements

- (a) The VWKICA shall ensure that the VWKI CPS incorporates appropriate provisions relating to the frequency and content of retraining and refresher training to be undertaken by VWKICA Personnel.

5.3.5 Job rotation frequency and sequence

- (a) The VWKICA shall ensure that the VWKI CPS incorporates appropriate provisions relating to the frequency and sequence of job rotations to be undertaken by VWKICA Personnel.

5.3.6 Sanctions for unauthorised actions

- (a) The VWKICA shall ensure that the VWKI CPS incorporates appropriate provisions relating to sanctions for unauthorised actions undertaken by VWKICA Personnel.

5.3.7 Independent contractor requirements

- (a) The VWKICA shall ensure that all contractors engaged by it adhere to requirements laid out in this Part 5.3.

5.3.8 Documentation supplied to personnel

- (a) The VWKICA shall ensure that all VWKICA Personnel are provided with access to all documents relevant to their roles or necessary for the performance of their duties, including in particular:
 - (i) this Policy;
 - (ii) the VWKI CPS; and
 - (iii) any supporting documentation, statutes, policies or contracts.

5.4 Audit logging procedures

5.4.1 Types of events recorded

- (a) The VWKICA shall ensure that:
 - (i) the VWKICA Systems record all relevant systems activity in Audit Logs;
 - (ii) the VWKI CPS incorporates a comprehensive list of all events that are to be recorded in an Audit Log in relation to the activities of VWKICA Personnel and the use of VWKICA equipment which shall include access, both authorised and violations; and
 - (iii) activities in relation to the VWKI Registration Authority, are logged in an appropriate manner by the VWKICA.

5.4.2 Frequency of processing log

- (a) VWKICA audit logging shall:
 - (i) operate at all times within the VWKICA Systems; and
 - (ii) ensure that audit monitoring of the VWKICA Systems is in compliance with the protective monitoring requirements of DCC Systems.
- (b) The VWKI CPS shall incorporate provisions which specify:
 - (i) how regularly information recorded in the Audit Log is to be reviewed; and
 - (ii) what actions are to be taken by the VWKICA in response to types of events recorded in the Audit Log.

5.4.3 Retention period for Audit Log

- (a) The VWKICA shall retain an Audit Log that incorporates, on any given date, a record of all VWKICA System events occurring during a period of at least twelve months prior to that date.
- (b) A copy of the Audit Log incorporating a record of all system events occurring prior to the beginning of that period shall be archived in accordance with the requirements of Part 5.5 of this Policy.
- (c) The VWKICA shall ensure that the VWKI CPS makes provision for the specification of the Audit Log record.

5.4.4 Protection of audit log

- (a) The VWKICA shall ensure that the VWKI CPS incorporates provisions in relation to access to the Audit Log, providing, in particular, that:

- (i) access to those VWKICA Audit Log Data (other than those relating to protective monitoring) must be limited to those members of VWKICA Personnel who are specifically responsible for performing a system audit role in accordance with the VWKI CPS;
- (ii) to the extent to which the Audit Log is retained electronically, the VWKICA Event Log Data stored in it cannot be accessed other than on a read-only basis, and are protected from unauthorised viewing, modification and deletion in accordance with British Standard BS 10008:2014 (Evidential weight and legal admissibility of electronic information) or an equivalent standard; and
- (iii) to the extent which the Audit Log is retained in non-electronic form, the Data stored in it are appropriately protected from unauthorised viewing, modification and destruction in order to ensure that their integrity is maintained for evidential purposes.

5.4.5 Audit Log backup procedures

- (a) The VWKICA shall ensure that the Data contained in the Audit Log is backed up on a daily basis or, if activity has taken place on the VWKICA Systems only infrequently, such as in relation to the Root VWKICA, in accordance with the schedule for the regular backup of the Data held on those VWKICA Systems.
- (b) The VWKICA shall ensure that all VWKI Data contained in the Audit Logs that are backed up are, during backup, held in accordance with the DCC Information Security Management System and protected to the same standard of protection as the primary copy of the Audit Log in accordance with Part 5.4.4 of this Policy.

5.4.6 Audit collection system (internal or external)

- (a) The VWKICA shall ensure that the VWKI CPS incorporates provisions in relation to its system for collecting Data for the purpose of populating the Audit Log.

5.4.7 Notification to event-causing subject

- (a) The VWKICA shall ensure that the VWKI CPS incorporates provisions in relation to its notification of any person who is (or is responsible for any VWKICA System which is) the direct cause of an event recorded in the Audit Log.

5.4.8 Vulnerability assessments

- (a) The VWKICA shall carry out periodic vulnerability assessments covering the VWKICA Systems with recorded corrective action.

5.5 Records archival

5.5.1 Types of records archived

- (a) The VWKICA shall ensure that it archives:
 - (i) relevant Audit Data in accordance with Part 5.4 of this Policy;
 - (ii) records of all Data submitted to it by VWKI Eligible Subscribers for the purposes of VWKI Certificate Signing Requests; and
 - (iii) any other data specified in this Policy as requiring to be archived in accordance with this Part 5.5 of this Policy.
- (b) The VWKICA shall ensure that all VWKICA audit data are recorded in a standard format that is compliant with British Standard BS 10008:2014 (Evidential Weight and Legal Admissibility of Electronic Information) or an equivalent standard.
- (c) The VWKICA shall ensure that provision is made in the VWKI CPS in relation to the specification of data to be archived.

5.5.2 Retention period for archive

- (a) The VWKICA shall ensure that all Data, excluding audit data, which are Archived are retained for a period of at least seven years from the date on which they were Archived.

5.5.3 Protection of archive

- (a) The VWKICA shall ensure that Data held in its Archive is protected against any unauthorised access, adequately protected against environmental threats such as temperature, humidity and magnetism and incapable of being modified or deleted.

5.5.4 Archive backup procedures

- (a) The VWKICA shall ensure that the VWKI CPS incorporates provisions in relation to its procedures for the backup of its Archive.

5.5.5 Requirements for Time-Stamping of records

- (a) Provision in relation to Time-Stamping is made in Part 6.8 of this Policy.

5.5.6 Archive collection system (internal or external)

- (a) The VWKICA shall ensure that the VWKI CPS incorporates provisions in relation to maintaining internal and external archives.

5.5.7 Procedures to obtain and verify archive information

- (a) The VWKICA shall ensure that Data held in the Archive are stored in a readable format during their retention period and that the Data remain accessible at all times during the retention period.
- (b) The VWKICA shall ensure that the VWKI CPS incorporates provisions in relation to the periodic verification by the VWKICA of the Data held in the Archive.

5.6 Key changeover**5.6.1 Issuing VWP CA key changeover**

- (a) Where the VWKICA ceases to use an Issuing VWP CA Private Key after the expiry of the Validity Period of an Issuing VWP CA Certificate, it shall:
 - (i) generate a new Key Pair following key generation procedures, generate a VWKI Certificate Signing Request in relation to the Issuing VWP CA Certificate and submit to the Root VWKICA for signing and Issuance;
 - (ii) in its role as the VWKICA:
 - (1) Issue a new relevant Issuing VWP CA Certificate;
 - (2) confirm acceptance of the Issuing VWP CA Certificate once Issued; and
 - (iii) ensure that any relevant VWP Certificate subsequently Issued by the Issuing VWP CA is Issued using the Issuing VWP CA Private Key from the newly generated Key Pair until the expiry of the Validity Period of the newly Issued Issuing VWP CA Certificate; and
 - (iv) verifiably destroy the Private Key Material relating to the previous Issuing VWP CA Private Key; or retain such Private Key Material in such a manner that it is adequately protected against being put back into use.

5.6.2 Issuing VWD CA key changeover

- (a) Where the VWKICA ceases to use an Issuing VWD CA Private Key after the expiry of the Validity Period of an Issuing VWD CA Certificate, it shall:
 - (i) generate a new Key Pair following key generation procedures, generate a VWKI Certificate Signing Request in relation to the Issuing VWD CA Certificate and submit to the Root VWKICA for signing and Issuance;
 - (ii) in its role as the VWKICA:
 - (1) Issue a new relevant Issuing VWD CA Certificate;
 - (2) confirm acceptance of the Issuing VWD CA Certificate once Issued; and
 - (iii) ensure that any relevant VWD Certificate subsequently Issued by the Issuing VWP CA is Issued using the Issuing VWD CA Private Key from the newly generated Key Pair until the expiry of the Validity Period of the newly Issued Issuing VWD CA Certificate; and
 - (iv) verifiably destroy the Private Key Material relating to the previous Issuing VWD CA Private Key; or retain such Private Key Material in such a manner that it is adequately protected against being put back into use.

5.6.3 VWKI Root Key changeover

- (a) Where the Root VWKICA ceases to use a Root VWKICA Private Key after the expiry of the Validity Period of a Root VWKICA Certificate, it shall:
 - (i) generate a VWKI Certificate Signing Request for the new Root VWKICA Certificate and submit it for signing and Issuance;

- (ii) issue to itself a new relevant Root VWKICA Certificate;
- (iii) ensure that any relevant Issuing VWP CA Certificate or Issuing VWD CA Certificate subsequently Issued by the Root VWKICA is Issued using the Root VWKICA Private Key from the newly-generated Key Pair until the expiry of the Validity Period of the newly Issued Root VWKICA Certificate; and
- (iv) verifiably destroy the Private Key Material relating to the previous Root VWKICA Private Key; or retain such Private Key Material in such a manner that it is adequately protected against being put back into use.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

- (a) The VWKICA shall ensure that the VWKI CPS incorporates Business Continuity and Disaster Recovery Procedures which shall be designed to ensure the continuity or (where there has been unavoidable discontinuity) the recovery of the provision of the VWKI Services in the event of any Compromise of the VWKICA Systems or major failure in the VWKI processes.
- (b) In the event of an Incident involving Compromise of the VWKICA Systems, the VWKICA shall:
 - (i) ensure that the Incident Management Policy is invoked;
 - (ii) follow procedures defined in the VWKI CPS; and
 - (iii) treat the event as a Major Security Incident.
- (c) The VWKICA shall ensure that the VWKI CPS incorporates provisions setting out the approach to be taken by it in circumstances in which it suspects (or has reason to suspect) that any Issuing VWP CA Private Key or any Issuing VWD CA Private Key or any part of the VWKICA Systems is Compromised.

5.7.2 Computing resources, software and/or data are corrupted

- (a) The VWKICA shall ensure that the VWKI CPS incorporates provisions in relation to the steps to take to manage computing resources and software, and to deal with corrupted data.

5.7.3 Entity private key compromise procedures

- (a) See Part 5.7.1 of this Policy.

5.7.4 Business continuity capabilities after a disaster

- (a) The VWKICA shall ensure that Business Continuity and Disaster Recovery Procedures are invoked in accordance with Part 5.7 of this Policy and the VWKI CPS.

5.7.5 VWKICA and VWKI Registration Authority termination

- (a) DCC shall at all times fulfil the functions of the VWKICA and VWKI Registration Authority.

6 TECHNICAL SECURITY CONTROLS

- (a) The VWKICA shall ensure that the VWKI CPS incorporates detailed provision in relation to technical security controls so that such technical security controls are defined, documented and managed for the purpose of exercising its functions as Root VWKICA, Issuing VWP CA, Issuing VWD CA and VWKI Registration Authority.

6.1 Key pair generation and installation

6.1.1 Key pair generation

- (a) The VWKICA shall ensure that all VWKICA Key Pairs are generated:
 - (i) in a protected environment to be compliant with FIPS 140-2 Level 3 or an equivalent cryptographic standard;
 - (ii) using multi-person control, such that no single person is capable of generating any VWKICA Private Key; and
 - (iii) in accordance with the VWKI CPS, with records from the event to be held as archive.
- (b) The VWKICA shall not generate any Key Pairs other than a Key Pair associated with a VWKICA Certificate.

6.1.2 Private Key delivery to VWKI Subscriber

- (a) In accordance with Part 6.1.1(B), the Issuing VWP CA or Issuing VWD CA shall not generate any Private Key for delivery to a VWKI Eligible Subscriber.

6.1.3 Public Key delivery to certificate issuer

- (a) The VWKICA shall ensure that the VWKI CPS incorporates provisions in relation to the mechanism by which Public Keys of VWKI Eligible Subscribers are delivered to or generated by, the VWKICA for the purpose of the exercise of its functions as the Root VWKICA, Issuing VWP CA and Issuing VWD CA.

6.1.4 VWKICA Public Key delivery to Relying Parties

- (a) The VWKICA shall ensure that the VWKI RAPP section 17.14 incorporates provisions in relation to how Root VWKICA Public Keys, Issuing VWP CA Public keys and Issuing VWD CA Public Keys shall be delivered to Relying Parties.

6.1.5 Key sizes

- (a) The VWKI CA and every Subscriber shall ensure that all the Private Keys and Public Keys which each of them may use for the purposes of this Policy are of the following size and characteristics
 - (i) Keys shall be generated using the NIST P-256 elliptic curve (secp256r1) as specified in FIPS 186-5 and NIST SP 800-186 Appendix G, G.1.2, with an effective key size of 256 bits;
 - (ii) Digital signatures must utilise the Elliptic Curve Digital Signature Algorithm (ECDSA) with keys derived from the NIST P-256 curve with SHA-256 as the hash function.

6.1.6 Public Key parameters generation and quality checking

- (a) The VWKICA shall ensure that any Public Key used for the purposes of this Policy shall:
 - (i) be generated using the required key parameters, as defined in the VWKI Certificate Profiles in Annex B to this policy, which are in accordance with FIPS 186-5 or an equivalent cryptographic standard; and
 - (ii) ensure that the quality of the generated key parameters is verified in accordance with FIPS 186-5 or an equivalent cryptographic standard.

6.1.7 Key usage purposes (as per X.509 v3 key usage field)

- (a) The VWKICA shall ensure that each VWKI Certificate that is Issued by it shall include key usage extension fields that specify the intended use of that VWKI Certificate and technically limit the certificate's functionality in X.509v3 compliant software.
- (b) The VWKICA shall set key usage bits or assert extended key usage OIDs for each VWKI Certificate type in accordance with the relevant VWKI Certificate Profile defined in Annex B to this Policy.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

- (a) The VWKICA shall ensure that all VWKICA Private Keys are protected within the cryptographic boundary of a Cryptographic Module configured to be compliant with FIPS 140-2 Level 3 or an equivalent cryptographic standard at all times.
- (b) The VWKICA shall ensure that the key encryption key used to protect the VWKICA Private Keys is only stored within the cryptographic boundary of a Cryptographic Module configured to be compliant with FIPS 140-2 Level 3 or an equivalent cryptographic standard.

6.2.2 Private Key (key (m out of n) multi-person control

- (a) The VWKICA shall ensure that multi-person controls are applied for the generation and management of VWKICA Private Keys.
- (b) VWKI Authorised Subscribers shall implement multi-person control, where applicable, in accordance with their Information Security Management System.

6.2.3 Private Key escrow

- (a) Key Escrow shall not be used for the VWKICA.

6.2.4 Private Key backup

- (a) The VWKICA shall back up the VWKICA Private Keys using multi-person control and shall protect all copies in the same manner as the originals, and in accordance with provisions set out within the VWKI CPS.

- (b) The backup shall be available for use during disaster recovery as described within the VWKI CPS.

6.2.5 Private Key archival

- (a) Private Key archival shall not be implemented for the VWKICA.

6.2.6 Private Key transfer into or from a Cryptographic Module

- (a) The VWKICA shall ensure that no VWKICA Private Key is transferred or copied other than:
 - (i) for the purposes of:
 - (1) backup;
 - (2) restoration; or
 - (3) addition of new hardware, software, or firmware to a Cryptographic Module; and
 - (ii) in any event, in accordance a level of protection that is compliant with FIPS 140-2 Level 3 or an equivalent cryptographic standard.

6.2.7 Private Key Storage on Cryptographic Module

- (a) The VWKICA shall ensure that VWKICA Private Keys are stored within the cryptographic boundary of a Cryptographic Module configured to be complaint with FIPS 140-2 Level 3 or an equivalent cryptographic standard.

6.2.8 Method of Activating Private Key

- (a) The VWKICA shall ensure that:
 - (i) the Cryptographic Module in which any VWKICA Private Key is stored may be accessed only by an authorised member of VWKICA Personnel; and
 - (ii) the requirements of the Cryptographic Module, including switching on and authenticating themselves to the Cryptographic Module shall be undertaken by the VWKICA Personnel.

6.2.9 Method of deactivating Private Key

- (a) The VWKICA shall ensure that any VWKICA Private Keys shall be capable of being deactivated by means of the VWKICA Systems, at least by:
 - (i) the actions of:
 - (1) turning off the power;
 - (2) logging off; or
 - (3) carrying out a system reset;
 - or;
 - (ii) following key changeover in accordance with procedures defined in Part 5.6 of this Policy.

6.2.10 Method of destroying Private Key

- (a) The VWKICA shall ensure that the VWKI CPS incorporates provisions for a set of procedures covering the destruction of VWKICA Private Keys. These shall be in accordance with the guidelines provided by the cryptographic manufacturer and compliant with UK Government publication 'IS4 - Management of Cryptographic Systems' or an equivalent cryptographic standard.
- (b) The VWKI CPS shall incorporate provisions for procedures for secure back up of cryptographic material.
- (c) Positive decisions on significant key management life cycle events shall be managed directly by the SMKI PMA.
- (d) VWKI Subscribers shall ensure that their User Information Security Management System includes procedures in relation to the secure management of all Secret Key Material provided to them by the VWKICA in relation to this Policy.

6.2.11 Cryptographic module rating

- (a) Any Cryptographic Module used in support of the VWKICA Systems shall meet the module rating specified within Parts 6.2.1 and 6.2.7 of this Policy.

6.3 Other aspects of Key Pair management

6.3.1 Public Key archival

- (a) Public Key archival shall be managed in accordance with Part 5.5 of this Policy and in line with VWKI Repository management requirements as detailed within the VWKI CPS.

6.3.2 Certificate operational periods and Key Pair usage periods

- (a) Annex B to this Policy specifies the detail for Key Pair usage, Validity Period and categories.
- (b) The VWKICA shall ensure that the Validity Period of each VWKI Certificate Issued by it shall be as follows:
 - (i) in the case of a Root VWKICA Certificate, until the notAfter date specified in Annex B;
 - (ii) in the case of an Issuing VWP CA Certificate, until the notAfter date specified in Annex B;
 - (iii) in the case of an Issuing VWD CA Certificate, until the notAfter date specified in Annex B;
 - (iv) in the case of a VWP Certificate or, until the notAfter date specified in Annex B; and
 - (v) in the case of a VWD Certificate or, until the notAfter date specified in Annex B.
- (c) The VWKICA shall ensure that no VWKICA Private Key can be used after the end of the Validity Period of the VWKICA Certificate containing the Public Key which is associated with that Private Key.

6.4 Activation Data

6.4.1 Activation data generation and installation

- (a) The VWKICA shall ensure that any Cryptographic Module within which a VWKICA Private Key is held has Activation Data that apply sufficient security protection to protect that VWKICA Private Key.
- (b) Activation Data pertaining to the VWKICA Private Key Material shall:
 - (i) have access controls applied as defined within the VWKI CPS;
 - (ii) have key management lifecycle procedures applied as defined within the VWKI CPS; and
 - (iii) have records generated, logged and archived on generation and each invocation.

6.4.2 Activation data protection

- (a) The VWKICA shall ensure that the VWKI CPS incorporates provisions in relation to the physical and logical controls to be employed to protect activation data.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

- (a) The DCC Information Security Management System shall define security technical requirements according to a risk assessment and risk treatment plan, or following corrective action that may result from an audit or IT health check service, which shall be undertaken by a CHECK approved service provider.

6.5.2 Computer security rating

- (a) This Policy makes no stipulation in relation to computer security rating.

6.6 Life cycle technical controls

6.6.1 System development controls

- (a) The VWKICA shall ensure that the VWKI CPS makes provision regarding controls in relation to development of the VWKICA Systems; and
- (b) any such development of the VWKICA Systems shall be made in accordance with DCC secure development policy as defined within the DCC Information Security Management System.

6.6.2 Security management controls

- (a) The VWKICA shall ensure that the VWKI CPS, incorporates provisions which are designed to ensure that the VWKICA Systems satisfy the requirements of Section G2 (System Security: Obligations on the DCC) and Section G5 (Information Security: Obligations on the DCC and Users) of the Code.

6.6.3 Life cycle security controls

- (a) See Part 6.6.2 of this Policy.

6.7 Network security controls

6.7.1 Protection against attack

- (a) The VWKICA shall ensure that the VWKICA systems are protected against attack in accordance with provisions made in the VWKI CPS and by at least the following means:
 - (i) continual protective monitoring shall be enforced; and
 - (ii) access to the systems shall be on a least privilege principle for access.
- (b) The VWKICA Systems shall be designed and operated so as to detect and prevent:
 - (i) Denial of Service Events; and
 - (ii) unauthorised attempts to connect to them.

6.7.2 Health Check of VWKICA Systems

- (a) The VWKICA shall ensure that the VWKI CPS incorporates provisions for periodically scheduled assessments of the VWKICA Systems by a CHECK approved service provider to form part of the input to the risk management process.

6.8 Time-stamping

6.8.1 Use of time-stamping

- (a) The VWKICA shall ensure Time-Stamping takes place in relation to all VWKI Certificates and other VWKI activities that require an accurate record of time.
- (b) The VWKICA shall ensure that the VWKI CPS incorporates provisions in relation to the time source and mechanisms used by any Time-Stamping Authority in relation to any Time-Stamping on behalf of the VWKICA.

7 CERTIFICATE, CRL AND OCSP PROFILES

7.1 Certificate profile

- (a) The VWKICA shall only issue certificates in accordance with the VWKI Certificate Profiles in Annex B of this Policy for Subscribers and the VWKI Certificate Profiles in Annex C of the VWKI CPS for Subscribers.

7.1.1 Version number(s)

- (a) The version field in the VWKI Certificates shall have a value of 2, indicating X.509v3 certificates.

7.1.2 Certificate extensions

- (a) In compliance with RFC 5280, the inclusion of the following certificate extensions shall be utilised:
 - (i) `authorityKeyIdentifier` NOT CRITICAL;
 - (ii) `basicConstraints` CRITICAL;
 - (iii) `extKeyUsage` NOT CRITICAL;
 - (iv) `keyUsage` CRITICAL;
 - (v) `certificatePolicies` NOT CRITICAL;
 - (vi) `subjectAltName` NOT CRITICAL;
 - (vii) `subjectKeyIdentifier` NOT CRITICAL.

7.1.3 Algorithm object identifiers

- (a) No stipulation.

7.1.4 Name forms

- (a) The VWKI CPS sets out the name forms utilised.

7.1.5 Name constraints

- (a) The VWKI CPS sets out the applicable Name Constraints.

7.1.6 Certificate policy object identifier

- (a) No stipulation.

7.1.7 Usage of Policy Constraints extension

- (a) [Not applicable].

7.1.8 Policy qualifiers syntax and semantics

- (a) [Not applicable].

7.1.9 Processing semantics for the critical Certificate Policies extension

- (a) [Not applicable].

7.2 CRL profile

- (a) [Not applicable].

7.2.2 Version number(s)

- (a) [Not applicable].

7.2.3 CRL and CRL entry extensions

- (a) [Not applicable].

7.1 OCSP profile

- (a) [Not applicable].

7.3.1 Version number(s)

- (a) [Not applicable].

7.3.2 OCSP extensions

- (a) [Not applicable].

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency or circumstances of assessment

- (a) The VWKICA shall be subject to assessment at least annually and otherwise as required by the SMKI PMA.
- (b) The scope of each assessment and the independence requirements and qualifications of the assessor shall be proposed by the DCC and be subject to the approval of the SMKI PMA.

8.2 Identify/qualifications of assessor

- (a) As approved by the SMKI PMA.

8.3 Assessor's relationship to assessed entity

- (a) As approved by the SMKI PMA.

8.4 Topics covered by assessment

- (a) The DCC Information Security Management System shall cover all aspects of the VWKI Service and the VWKI Repository Service, including but not limited to:
 - (i) the VWKI Repository;
 - (ii) the Root VWKICA;
 - (iii) the Issuing VWP CA;
 - (iv) the Issuing VWD CA;
 - (v) Cryptographic Modules relied upon in support of the service; and
 - (vi) this Policy and its supporting VWKI RAPP and VWKI CPS.

8.5 Actions taken as a result of deficiency

- (a) Any deficiencies identified through an assessment, internal audit or IT health check shall be raised by the DCC as non-conformances and be reported to the SMKI PMA, where appropriate accompanied by a risk assessment.

- (b) The DCC shall set out the remedial action it proposes to take in response to any deficiency and submit the proposal to the SMKI PMA for approval.

8.6 Communication of results

- (a) The results of any assessment shall be reported by the DCC to the SMKI PMA and be capable of being either approved, not approved or approved subject to the carrying out of remedial action by the DCC.
- (b) The DCC shall carry out any remedial action (including any remedial action referred to in 8.5(b) above) required by the SMKI PMA and the DCC shall provide progress reports on its implementation of any remedial action to the SMKI PMA.

9 OTHER BUSINESS AND LEGAL MATTERS

- (a) In so far as provision is made in relation to all the matters referred to in this Part, it is found in the DCC Licence and the provisions of the Code.

9.1 Fees

[Not applicable].

9.1.1 Certificate Issuance or renewal fees

[Not applicable].

9.1.2 Device certificate access fees

[Not applicable].

9.1.3 Revocation or status information access fees

[Not applicable].

9.1.4 Fees for other services

[Not applicable].

9.1.5 Refund policy

[Not applicable].

9.2 Financial responsibility

9.2.1 Insurance coverage

- (a) See the statement at the beginning of this Part.

9.2.2 Other assets

- (a) See the statement at the beginning of this Part.

9.2.3 Insurance or warranty coverage for subscribers and subjects

- (a) See the statement at the beginning of this Part.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

- (a) See the statement at the beginning of this Part.

9.3.2 Information not within the scope of confidential information

- (a) See the statement at the beginning of this Part.

9.3.3 Responsibility to protect confidential information

- (a) See the statement at the beginning of this Part.

9.4 Privacy of personal information

9.4.1 Privacy plan

- (a) See the statement at the beginning of this Part.

9.4.2 Information treated as private

- (a) See the statement at the beginning of this Part.

9.4.3 Information not deemed private

- (a) See the statement at the beginning of this Part.

9.4.4 Responsibility to protect private information

- (a) See the statement at the beginning of this Part.

9.4.5 Notice and consent to use private information

- (a) See the statement at the beginning of this Part.

9.4.6 Disclosure pursuant to judicial or administrative process

- (a) See the statement at the beginning of this Part.

9.4.7 Other information disclosure circumstances

- (a) See the statement at the beginning of this Part.

9.5 Intellectual property rights

- (a) See the statement at the beginning of this Part.

9.6 Representations and warranties

9.6.1 CA representations and warranties

- (a) See the statement at the beginning of this Part.

9.6.2 RA representation and warranties

- (a) See the statement at the beginning of this Part.

9.6.3 Subscriber representations and warranties

- (a) See the statement at the beginning of this Part.

9.6.4 Relying party representations and warranties

- (a) See the statement at the beginning of this Part.

9.7 Representations and warranties of other participants

- (a) See the statement at the beginning of this Part.

9.8 Disclaimers of warranties

- (a) See the statement at the beginning of this Part.

9.9 Limitations of liability

- (a) See the statement at the beginning of this Part.

9.10 Indemnities

- (a) See the statement at the beginning of this Part.

9.11 Term and termination

9.11.1 Term

- (a) See the statement at the beginning of this Part.

9.11.2 Termination

- (a) See the statement at the beginning of this Part.

9.11.3 Effect of termination and survival

- (a) See the statement at the beginning of this Part.

9.12 Individual notices and communications with participants

- (a) See the statement at the beginning of this Part.

9.13 Amendments**9.13.1 Procedure for amendment**

- (a) See the statement at the beginning of this Part.

9.13.2 Notification mechanism and period

- (a) See the statement at the beginning of this Part.

9.13.3 Circumstances under which OID must be changed

- (a) See the statement at the beginning of this Part.

9.14 Dispute resolution provisions

- (a) See the statement at the beginning of this Part.

9.15 Governing law

- (a) See the statement at the beginning of this Part.

9.16 Compliance with applicable law

- (a) See the statement at the beginning of this Part.

9.17 Miscellaneous provisions**9.17.1 Entire agreement**

- (a) See the statement at the beginning of this Part.

9.17.2 Assignment

- (a) See the statement at the beginning of this Part.

9.17.3 Severability

- (a) See the statement at the beginning of this Part.

9.17.4 Enforcement (attorneys' fees and waiver of rights)

- (a) See the statement at the beginning of this Part.

9.17.5 Force Majeure

[Not applicable].

9.18 Other provisions

- (a) See the statement at the beginning of this Part.

ANNEX A**DEFINED TERMS**

In this Policy, except where the context otherwise requires:

- expressions defined in Section A (Definitions and Interpretation) of the Code have the same meaning as is set out in that section;
- the expressions in the left-hand column below shall have the meanings given to them in the right-hand column below; and
- where any expression is defined in Section A (Definitions and Interpretation) of the Code and in this Annex, the definition in this Annex shall take precedence for the purposes of the Policy.

Definitions for this Policy

Administration User	has the meaning given to the term Administration User in Appendix AI of the Code (Self Service Interface Code of Connection)
Archive	means the archive of Data created in accordance with Part 5.5.1 of this Policy (and "Archives" and "Archived" shall be interpreted accordingly)
Audit Log	means the audit log created in accordance with Part 5.4.1 of this Policy
Authentication	means the process of establishing that an individual, VWKI Certificate, system or organisation is who or what they or it claims or is claimed to be (and "Authenticate" shall be interpreted accordingly)
Business Continuity and Disaster Recovery Procedure	means that part of the Incident Management Policy which describes the business continuity and disaster recovery procedures applicable to the VWKI Services.
Certificate Re-Key	means a change to the Public Key contained within a Certificate bearing a particular serial number.
Identity Provider Service	has the meaning given to that term in the Self Service Interface Code of Connection.
IRCA	International Register of Certificated Auditors, a professional body for management system auditors.
Issue	means the act of the VWKICA acting in accordance with this Policy, and in its capacity as the Root VWKICA, the Issuing VWP CA or the Issuing VWD CA as the context requires, of creating and signing a Certificate which contains the information set out in the relevant VWKI Certificate Profile in Annex B to this Policy (and "Issuance", "Issued" and "Issuing" shall be interpreted accordingly).
Issuing VWD CA	means the Issuing Authority for VWD Certificate, being a subordinate Issuing Authority for the VWKICA whose functions are carried out by the VWKICA.
Issuing VWP CA	means the Issuing Authority for VWP Certificate, being a subordinate Issuing Authority for the VWKICA whose functions are carried out by the VWKICA.
Key Escrow	means the storage of a Private Key by a person other than the Subscriber or Subject of the Certificate which contains the related Public Key.
Object Identifier (or OID)	means an object identifier assigned by the Internet Address Naming Authority.
Private Key Material	in relation to a Private Key, means that Private Key and the input parameters necessary to establish, use and maintain it.

Root VWKICA	means the DCC exercising the function of Issuing the Root VWKI Certificate and other VWKI CA Certificates to the VWP CA and VWD CA, and storing and managing Private Keys associated with that function.
Root VWKICA Certificate	means a certificate of the form set out in the Root VWKI Certificate of VWKI Certificate Profile in accordance with Annex A of this Policy and self-signed, and Issued, by the Root VWKICA in accordance with this Policy.
Root VWKICA Private Key	means the Private Key which is stored and managed by the VWKICA acting in its capacity as the Root VWKICA.
Root VWKICA Public Key	means the Public Key of a Key Pair related to the Root VWKICA Certificate.
Security Related Functionality	means the functionality of the VWKICA Systems which is designed to detect, prevent or mitigate the adverse effect of any Compromise of those Systems.
Subject	means (a) in relation to a VWP Certificate or VWD Certificate as identified by the subject field of the relevant Certificate Profile in Annex B; (b) in relation to a VWKICA Certificate, the Root VWKICA , Issuing VWP CA or Issuing VWD CA as identified by the subject field of the relevant Certificate Profile in Annex B.
Time-Stamping	means the act that takes place when a Time-Stamping Authority, in relation to a VWKI Certificate, stamps a particular datum with an accurate indicator of the time (in hours, minutes and seconds) at which the activity of stamping takes place.
Time-Stamping Authority	means that part of the VWKICA that: a. where required, provides an appropriately precise timestamp in the format required by this Policy; and b. relies on a time source that is: i. accurate. ii. determined in a manner that is independent of any other part of the VWKICA Systems; and iii. such that the time of any timestamp can be verified to be that of the Independent Time Source at the time at which the timestamp was applied.
Transport Layer Security (or TLS)	means TLS in accordance with the relevant SMKI PMA and SSC Guidance (Standards, Procedures and Guidelines) published on the SEC website
Validity Period	means, in respect of a VWKI Certificate, the period of time for which that VWKI Certificate is intended to be valid.
Virtual WAN Provider (VWP)	the Virtual WAN Provider Service.

VWD Certificate	means a certificate in the form set out in the VWD Certificate Profile in accordance with Annex B to this Policy, and Issued by the Issuing VWD CA in accordance with this Policy.
VWD EUI64 ID	The EUI 64-bit identifier of the ZigBee radio interface installed in the Virtual WAN Device.
VWD Private Key	means a Private Key which is stored in a VWD.
VWD Public Key	means the Public Key of a Key Pair related to a VWD Certificate.
VWKI Authorised Responsible Officer (or VWKI ARO)	means an individual that has successfully completed the process for becoming (and remains) a VWKI ARO on behalf of a Party in accordance with the VWKI RAPP.
VWKI Authorised Subscriber	means (in relation to VWKICA Certificates and VWP Certificates), the DCC or (in relation to VWD Certificates), a Party that: i. has successfully completed the enrolment procedures to become a VWKI Authorised Subscriber as set out in the VWKI RAPP; ii. continues to have at least one (1) VWKI SRO currently appointed in accordance with the procedures set out in the VWKI RAPP; iii. continues to have at least one (1) VWKI ARO currently appointed in accordance with the procedures set out in the VWKI RAPP; iv. has not ceased to be a VWKI Authorised Subscriber in accordance with any other provision of the Code and in the case of the DCC only, subject to any alternative provisions in the VWKI CPS.
VWKI Certificate	has the meaning given to that expression in Part 1.1 of this Policy
VWKI Certificate Profile	means a table bearing that title in Annex B to this Policy and specifying the parameters to be contained within a VWKI Certificate
VWKI Certification Authority (or VWKICA)	means the Certification Authority for the VWKI, meaning the DCC, acting in this capacity and exercising the functions of a. the Root VWKICA; b. the Issuing VWP CA; c. the Issuing VWD CA; and d. the VWKI Registration Authority.
VWKI Eligible Subscriber	means, for the purposes of Section L18.6 (VWKI Eligible Subscribers) and this Certificate Policy: i. in relation to a VWKICA Certificate, the DCC acting in its capacity as the provider of the VWKI Service; ii. in relation to a VWP Certificate, the DCC acting in its capacity as the provider of the Virtual WAN Provider Service; and

	iii. in relation to a VWD Certificate, a VWD Manufacturer in relation to a Virtual WAN Device with a Device Model that is included on the list maintained by the Security Sub Committee pursuant to Section F2.40 of the Code.
VWKI Registration Authority	means the VWKI CA exercising the function of receiving and processing VWP Certificate Signing Requests and VWD Certificate Signing Requests made in accordance with the VWKI RAPP.
VWKI Registration Authority Manager	means any person who may be identified as such in accordance with the VWKI RAPP.
VWKI Registration Authority Personnel	means those persons who are engaged by the DCC, in so far as such persons carry out, or are authorised to carry out, any function of the VWKI Registration Authority.
VWKI Senior Responsible Officer (or VWKI SRO)	means an individual that has successfully completed the process for becoming (and remains) a VWKI SRO on behalf of a Party in accordance with the VWKI RAPP.
VWKI Subscriber	means, in relation to any VWKI Certificate, a Party which has been Issued with and accepted that Certificate, acting in its capacity as the holder of the Certificate.
VWKICA Certificate	means, as the context requires, either: (a) the Root VWKICA Certificate; (b) an Issuing VWP Certificate; or (c) an Issuing VWD Certificate.
VWKICA Personnel	means those persons who are engaged by the DCC, in so far as such persons carry out, or are authorised to carry out, any function of the VWKICA.
VWKICA Private Key	means a Private Key which is stored by the VWKICA acting in its capacity as either the Root VWKICA, the Issuing VWP CA or the Issuing VWD CA.
VWKICA Systems	means the Systems used by the VWKICA in relation to the VWKI Services.
VWP Certificate	means a certificate of the form set out in the VWP Certificate Profile in accordance with Annex B to this Policy, and Issued by the Issuing VWP CA in accordance with this Policy.
VWP Private Key	means a Private Key which is stored and managed by the VWKICA acting in its capacity as the Issuing VWP CA.
VWP Public Key	means the Public Key of a Key Pair related to a VWP Certificate.

ANNEX B

VWKI CERTIFICATE PROFILES**End Entity Certificate Structure and Contents**

This Annex B sets out requirements as to structure and content with which VWKICA Certificates, VWP Certificates, and VWD Certificates shall comply. All terms in this Annex shall, where not defined in the Code, this Policy have the meanings in and IETF RFC 5280.

Common Requirements applicable to all VWKI Certificates

All VWKI Certificates that are validly authorised within the VWKI shall:

- Be an X.509 v3 certificate;
- Have a `serialNumber` field of no more than 20 octets;
- have a valid `notBefore` field consisting of the time of issue, encoded as in section 4.1.2.5 of RFC 5280;
- have a fixed expiration date in the `notAfter` field, encoded as in section 4.1.2.5 of RFC 5280; and
- Contain a `subjectKeyIdentifier` extension to provide a means of identifying the certificate containing the corresponding public key. This extension shall be marked as non-critical.
- With the exception of the Root VWKICA Certificate, contain an `authorityKeyIdentifier` extension. This extension shall be marked as non-critical.
- Ensure the Distinguished Name of Subjects and Issuers is encoded as follows: the `countryName` attribute shall be a `PrintableString` of the two-letter ISO 3166-1 alpha-2 code; all other Name attributes (such as `commonName` and `organisationName`) shall be encoded as `UTF8String`.

Requirements applicable to VWP Certificates only

A VWKI VWP Certificate that is Issued by the Issuing VWP CA for the purposes of establishing Transport Layer Security (TLS) communications over the Internet shall:

- have a `keyUsage` extension (as per section 4.2.1.3 of RFC 5280) with a value of `digitalSignature`. This extension shall be marked as critical (as per section 4.2.1.3 of RFC 5280);
- have an `extendedKeyUsage` extension (as per section 4.2.1.12 of RFC 5280) with a value of `id-kp-serverAuth`. This extension shall be marked as non-critical;
- contain a single `policyIdentifier` in the `certificatePolicies` extension that refers to the OID for the VWKI Certificate Policy; and
- have a Validity Period of **3 years**.

Requirements Applicable to VWD Certificates only

A VWD Certificate that is Issued by the Issuing VWD CA for the purposes of establishing Transport Layer Security (TLS) communications over the Internet shall:

- have a `keyUsage` extension (as per section 4.2.1.3 of RFC 5280) with a value of `digitalSignature`. This extension shall be marked as critical (as per section 4.2.1.3 of RFC 5280);
- have an `extendedKeyUsage` extension (as per section 4.2.1.12 of RFC 5280) with a value of `id-kp-clientAuth`. This extension shall be marked as non-critical;
- contain a single `policyIdentifier` in the `certificatePolicies` extension that refers to the OID for the VWKI Certificate Policy; and
- have a Validity Period of 20 years.

Requirements Applicable to Issuing VWP CA Certificates only

An Issuing VWP CA Certificate issued by the Root VWKICA shall:

- have a `keyUsage` extension (as per section 4.2.1.3 of RFC 5280) with a value of `keyCertSign`. This extension shall be marked as critical (as per section 4.2.1.3 of RFC 5280);
- contain at least one `policyIdentifier` in the `certificatePolicies` extension that refers to the OID for the VWKI Certificate Policy;
- contain the `basicConstraints` extension, with values `cA=True`, and `pathLen=0`. This extension shall be marked as critical; and
- have a Validity Period of 10 years.

Requirements Applicable to Issuing VWD CA Certificates only

An Issuing VWD CA Certificate issued by the Root VWKICA shall:

- have a `keyUsage` extension (as per section 4.2.1.3 of RFC 5280) with a value of `keyCertSign`. This extension shall be marked as critical (as per section 4.2.1.3 of RFC 5280);
- contain at least one `policyIdentifier` in the `certificatePolicies` extension that refers to the OID for the VWKI Certificate Policy;
- contain the `basicConstraints` extension, with values `cA=True`, and `pathLen=0`. This extension shall be marked as critical; and
- have a Validity Period of 40 years.

Requirements Applicable to Root VWKICA Certificates only

Root VWKICA Certificates that are issued by the Root VWKICA shall:

- have a `keyUsage` extension (as per section 4.2.1.3 of RFC 5280) with a value of `keyCertSign`. This extension shall be marked as critical (as per section 4.2.1.3 of RFC 5280);
- contain a single `policyIdentifier` in the `certificatePolicies` extension that refers to the OID for `anyPolicy`;
- contain the `basicConstraints` extension, with values `cA=True`, and `pathLen` absent (unlimited). This extension shall be marked as critical; and
- have a Validity Period of 50 years.

VWP Certificate Profile for the purposes of establishing TLS Communications

Field Name	RFC 5759/5280 Type	Value	Reference
version	Version	v3	
serialNumber	INTEGER	Calculated by CA	
signature	AlgorithmIdentifier	ecdsa-with-SHA256	
issuer	Name	CN= Issuing VWP CA, O=DCC, C=GB	
validity	Validity	(see below)	
subject	Name	CN=<FQDN>, O= <Party Signifier>, C=GB	
subjectPublicKeyInfo	SubjectPublicKeyInfo	The subject's Public Key	
extensions	Extensions	(see below)	
Validity		The period from notBefore through notAfter, inclusive.	
notBefore	Time	Calculated by CA as time of issue	
notAfter	Time	Calculated by CA as not before + 3 years	
Extensions		Critical and non-critical extensions	
authorityKeyIdentifier	KeyIdentifier	Calculated by CA	
subjectKeyIdentifier	KeyIdentifier	Calculated by CA	
keyUsage	BIT STRING	digitalSignature	
certificatePolicies	SEQUENCE	1.2.826.0.1.8641679.1 .2.1.5	
extendedKeyUsage	SEQUENCE	id-kp-serverAuth	

subjectAltName		<Fully Qualified Domain Name> A single dNSName identical to the subject Common Name	
----------------	--	--	--

Interpretation

version

The version of the X.509 VWP Certificate. VWP Certificates shall identify themselves as version 3.

serialNumber

VWP Certificate serial number, a positive integer of no more than 20 octets. The Serial Number identifies the VWP Certificate, and shall be created by the Issuing VWP CA that signs the VWP Certificate. The Serial Number shall be unique in the scope of VWP Certificates signed by the Issuing VWP CA.

signature

The identity of the signature algorithm used to sign the VWP Certificate. This value is used in both the `signatureAlgorithm` field in the `Certificate` structure and the `signature` field in the `TBSCertificate` structure and indicates the Issuing VWP CA signature algorithm used to sign this Certificate.

The ECDSA signature method is defined in NIST FIPS 186-5. When implementing ECDSA, the SHA-256 message digest algorithm and the P-256 elliptic curve as defined in NIST SP 800-186 Appendix G, G.1.2, shall be used.

The signature algorithm shall be `ecdsa-with-SHA256` as specified in RFC 5759. The algorithm identifier is:

```
ecdsa-with-SHA256      OBJECT IDENTIFIER ::= { iso(1)
    member-body (2)    us(840)      ansi-X9-62(10045) signatures
(4) ecdsa-with-sha2(3) 2 }
```

The hash algorithm used shall be the SHA-256 secure hash algorithm as defined in NIST FIPS 180-4.

issuer

The name of the signer of the VWP Certificate. This will consist of the Country (C), Organisation Name (O) which will be DCC and a Common Name (CN) which will be Issuing VWP CA (as defined in the Issuing VWP CA Certificate profile).

Validity

The time period over which the Issuing VWP CA expects the VWD Certificate to be valid. The validity period is the period of time from `notBefore` through `notAfter`, inclusive.

All times shall be stated in the Universal Coordinated Time (UTC) time zone. Time up to and including 23:59:59 December 31, 2049 UTC shall be encoded as `UTCTime` as `YYMMDDHHmmssZ`.

Times later than 23:59:59 December 31, 2049 UTC shall be encoded as `GeneralizedTime` as `YYYYMMDDHHmmssZ`.

notBefore

The earliest time a VWP Certificate may be used. This shall be the time the VWP Certificate is created.

notAfter

The latest time a VWP Certificate is expected to be used. The value in a `notAfter` field shall be treated as specified in RFC 5280.

subject

The formatting of this field shall contain a unique X.500 Distinguished Name (DN). This shall consist of the Country (C), the Organisation Name (O) which will be the Party Signifier of the VWKI Subscriber and a Common Name (CN) which will be the Fully Qualified Domain Name of the VWKI Subscriber.

subjectPublicKeyInfo

The `subjectPublicKeyInfo` field shall indicate the Public Key algorithm identifier and the Public Key in the specified algorithm format as specified in RFC 3279 and RFC 5480.

The algorithm field in the `subjectPublicKeyInfo` structure shall contain the following identifier:

```
id-ecPublicKey OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) ansi-X9-62(10045) keyType(2) 1 }
```

`id-ecPublicKey` indicates that the algorithms that can be used with the subject Public Key are unrestricted. The key is only restricted by the values indicated in the `keyUsage` extension (explained further under the next extensions heading below).

The parameter for `id-ecPublicKey` is as follows and shall always be present:

```
ECParameters ::= CHOICE {
    namedCurve      OBJECT IDENTIFIER
    -- implicitCurve  NULL
    -- specifiedCurve SpecifiedECDomain
}
```

Only the following field in `ECParameters` shall be used:

- `namedCurve` - identifies all the required values for a particular set of elliptic curve domain parameters to be represented by an OID.

The OID for the curve choice to be used in VWP Certificate is:

```
secp256r1 OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) ansi-X9-62(10045) curves(3) prime(1) 7 }
```

The `subjectPublicKey` from `SubjectPublicKeyInfo` is the ECC Public Key.

Implementations of Elliptic Curve Cryptography according to this document shall only support the uncompressed form.

The first octet of the `subjectPublicKey` indicates whether the key is compressed or uncompressed. The uncompressed form is indicated by 0x04 (the compressed form is indicated by either 0x02 or 0x03). The Public Key shall be rejected if any value other than 0x04 is in the first octet.

Extensions

VWP Certificates MUST contain the extensions described below. They should not contain any additional extensions:

- o `authorityKeyIdentifier`: non-critical
- o `subjectKeyIdentifier`: non-critical
- o `keyUsage`: critical

- o `certificatePolicies`: non-critical
- o `extendedKeyUsage`: non-critical
- o `subjectAltName`: non-critical

authorityKeyIdentifier

A key identifier calculated using method 2 of section 4.2.1.1 of RFC 5280.

subjectKeyIdentifier

Calculated using method 2 of section 4.2.1.2 of RFC 5280.

keyUsage

As per RFC 5280 section 4.2.1.3 with a value of `digitalSignature`.

certificatePolicies

Contain a single `policyIdentifier` in the `certificatePolicies` extension that refers to the OID for the VWKI Certificate Policy.

extendedKeyUsage

This shall be an `extendedKeyUsage` extension (as per section 4.2.1.12 of RFC 5280) with a value of `id-kp-serverAuth`. This extension shall be marked as non-critical.

subjectAltName

Subject Alternative Name (SAN) shall be populated with the Fully Qualified Domain Name (FQDN) of the VWKI Subscriber pertaining to the service for which the VWP Certificate will be used.

VWD Certificate Profile for the purposes of establishing TLS communications

Field Name	RFC 5759/5280 Type	Value	Reference
<code>version</code>	Version	v3	
<code>serialNumber</code>	INTEGER	Calculated by CA	
<code>signature</code>	AlgorithmIdentifier	<code>ecdsa-with-SHA256</code>	
<code>issuer</code>	Name	CN= Issuing VWD CA, O=DCC, C=GB	
<code>validity</code>	Validity	(see below)	
<code>subject</code>	Name	CN=<VWD EUI64 ID>, O= <Party Signifier>, C=GB	
<code>subjectPublicKeyInfo</code>	SubjectPublicKeyInfo	The subject's Public Key	
<code>extensions</code>	Extensions	(see below)	
Validity		The period from <code>notBefore</code> through <code>notAfter</code> , inclusive.	

notBefore	Time	Calculated by CA as time of issue	
notAfter	Time	Calculated by CA as not before + 20 years	
Extensions		Critical and non-critical extensions	
authorityKeyIdentifier	KeyIdentifier	Calculated by CA	
subjectKeyIdentifier	KeyIdentifier	Calculated by CA	
keyUsage		digitalSignature	
certificatePolicies		1.2.826.0.1.8641679.1 .2.1.5	
extendedKeyUsage		id-kp-clientAuth	

Interpretation

version

The version of the X.509 VWD Certificate. VWD Certificates shall identify themselves as version 3.

serialNumber

VWD Certificate serial number, a positive integer of no more than 20 octets. The Serial Number identifies the VWD Certificate, and shall be created by the Issuing VWD CA that signs the VWD Certificate. The Serial Number shall be unique in the scope of VWD Certificates signed by the Issuing VWD CA.

signature

The identity of the signature algorithm used to sign the VWD Certificate. This value is used in both the `signatureAlgorithm` field in the Certificate structure and the `signature` field in the `TBSCertificate` structure and indicates the Issuing VWD CA signature algorithm used to sign this Certificate.

The ECDSA signature method is defined in NIST FIPS 186-5. When implementing ECDSA, the SHA-256 message digest algorithm and the P-256 elliptic curve as defined in NIST SP 800-186 Appendix G, G.1.2, shall be used.

The signature algorithm shall be `ecdsa-with-SHA256` as specified in RFC 5759. The algorithm identifier is:

```
ecdsa-with-SHA256      OBJECT IDENTIFIER ::= { iso(1)
    member-body (2)    us(840)      ansi-X9-62(10045) signatures
(4) ecdsa-with-sha2(3) 2 }
```

The hash algorithm used shall be the SHA-256 secure hash algorithm as defined in NIST FIPS 180-4.

issuer

The name of the signer of the VWD Certificate. This will consist of the Country (C), Organisation Name (O) which will be DCC and a Common Name (CN) which will be Issuing VWD CA (as defined in the Issuing VWD CA Certificate profile).

validity

The time period over which the Issuing VWD CA expects the VWD Certificate to be valid. The validity period is the period of time from `notBefore` through `notAfter`, inclusive.

All times shall be stated in the Universal Coordinated Time (UTC) time zone. Time up to and including 23:59:59 December 31, 2049 UTC shall be encoded as `UTCTime` as `YYMMDDHHmmssZ`.

Times later than 23:59:59 December 31, 2049 UTC shall be encoded as `GeneralizedTime` as `YYYYMMDDHHmmssZ`.

notBefore

The earliest time a VWD Certificate may be used. This shall be the time the VWD Certificate is created.

notAfter

The latest time a VWD Certificate is expected to be used. The value in a `notAfter` field shall be treated as specified in RFC 5280.

subject

The formatting of this field shall contain a unique X.500 Distinguished Name (DN). This shall consist of the Country (C), the Organisation Name (O) which will be the Party Signifier of the VWKI Subscriber and a Common Name (CN) which will be the VWD EUI64 ID pertaining to the Device for which the VWD Certificate will be used. The EUI64 ID must be in lowercase and must not include any separators such as hyphens or colons.

subjectPublicKeyInfo

The `subjectPublicKeyInfo` field shall indicate the Public Key algorithm identifier and the Public Key in the specified algorithm format as specified in RFC 3279 and RFC 5480.

The algorithm field in the `subjectPublicKeyInfo` structure shall contain the following identifier:

```
id-ecPublicKey OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) ansi-X9-62(10045) keyType(2) 1 }
```

`id-ecPublicKey` indicates that the algorithms that can be used with the subject Public Key are unrestricted. The key is only restricted by the values indicated in the `keyUsage` extension (explained further under the next extensions heading below).

The parameter for `id-ecPublicKey` is as follows and shall always be present:

```
ECParameters ::= CHOICE {
    namedCurve      OBJECT IDENTIFIER
    -- implicitCurve  NULL
    -- specifiedCurve SpecifiedECDomain
```

```
}
```

Only the following field in `ECPParameters` shall be used:

- `namedCurve` - identifies all the required values for a particular set of elliptic curve domain parameters to be represented by an OID.

The OID for the curve choice to be used in VWP Certificate is:

```
secp256r1 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840)
ansi-X9-62(10045) curves(3) prime(1) 7 }
```

The `subjectPublicKey` from `SubjectPublicKeyInfo` is the ECC Public Key.

Implementations of Elliptic Curve Cryptography according to this document shall only support the uncompressed form.

The first octet of the `subjectPublicKey` indicates whether the key is compressed or uncompressed. The uncompressed form is indicated by 0x04 (the compressed form is indicated by either 0x02 or 0x03). The Public Key shall be rejected if any value other than 0x04 is in the first octet.

Extensions

VWD Certificates MUST contain the extensions described below. They should not contain any additional extensions:

- o `authorityKeyIdentifier`: non-critical
- o `subjectKeyIdentifier`: non-critical
- o `keyUsage`: critical
- o `certificatePolicies`: non-critical
- o `extendedKeyUsage`: non-critical

authorityKeyIdentifier

A key identifier calculated using method 2 of section 4.2.1.1 of RFC 5280.

subjectKeyIdentifier

Calculated using method 2 of section 4.2.1.2 of RFC 5280.

keyUsage

As per RFC 5280 section 4.2.1.3 with a value of `digitalSignature`.

certificatePolicies

Contain a single `policyIdentifier` in the `certificatePolicies` extension that refers to the OID for the VWKI Certificate Policy.

extendedKeyUsage

This shall be an `extendedKeyUsage` extension (as per section 4.2.1.12 of RFC 5280) with a value of `id-kp-serverAuth`. This extension shall be marked as non-critical.

Issuing VWP CA Certificate Profile

Field Name	RFC 5759/5280 Type	Value	Reference
version	Version	v3	
serialNumber	INTEGER	Calculated by CA	
signature	AlgorithmIdentifier	Calculated by CA	
issuer	Name	CN= Root VWKICA, O=DCC, C=GB	
validity	Validity	(see below)	
subject	Name	CN= Issuing VWP CA, O=DCC, C=GB	
subjectPublicKeyInfo	SubjectPublicKeyInfo	The subject's Public Key	
extensions	Extensions	(see below)	
Validity		The period from notBefore through notAfter, inclusive.	
notBefore	Time	Calculated by CA as time of issue	
notAfter	Time	Calculated by CA as not before + 10 years	
Extensions		Critical and non-critical extensions	
authorityKeyIdentifier	KeyIdentifier	Calculated by CA	
subjectKeyIdentifier	KeyIdentifier	Calculated by CA	
keyUsage		keyCertSign	
certificatePolicies		1.2.826.0.1.8641679.1.2.1.5;	
basicConstraints		CA=True, pathLen=0	

Interpretation**version**

The version of the X.509 Issuing VWP CA Certificate. Issuing VWP CA Certificates shall identify themselves as version 3.

serialNumber

Issuing VWP CA Certificate serial number, a positive integer of no more than 20 octets. The Serial Number identifies the Issuing VWP CA Certificate, and shall be created by the Root VWKICA that signs the Issuing VWP CA Certificate. The Serial Number shall be unique in the scope of VWKICA Certificates signed by the Root VWKICA.

signature

The identity of the signature used by the Root VWKICA to sign the Issuing VWP CA Certificate. This value is used in both the `signatureAlgorithm` field in the Certificate structure and the `signature` field in the `TBSCertificate` structure and indicates the Root VWKICA signature algorithm used to sign this Certificate.

The ECDSA signature method is defined in NIST FIPS 186-5. When implementing ECDSA, the SHA-256 message digest algorithm and the P-256 elliptic curve as defined in NIST SP 800-186 Appendix G, G.1.2, shall be used.

The signature algorithm shall be `ecdsa-with-SHA256` as specified in RFC 5759. The algorithm identifier is:

```
ecdsa-with-SHA256      OBJECT IDENTIFIER ::= { iso(1)
    member-body (2)    us(840)      ansi-X9-62(10045) signatures
(4) ecdsa-with-sha2(3) 2 }
```

The hash algorithm used shall be the SHA-256 secure hash algorithm as defined in NIST FIPS 180-4.

issuer

The name of the signer of the Issuing VWP CA Certificate. This will consist of the Country (C), Organisation Name (O) which will be DCC and a Common Name (CN) which will be Root VWKICA (as defined in the Root VWKICA Certificate profile).

Validity

The time period over which the Root VWKICA expects the Issuing VWP CA Certificate to be valid. The validity period is the period of time from `notBefore` through `notAfter`, inclusive.

All times shall be stated in the Universal Coordinated Time (UTC) time zone. Time up to and including 23:59:59 December 31, 2049 UTC shall be encoded as `UTCTime` as `YYMMDDHHmmssZ`.

Times later than 23:59:59 December 31, 2049 UTC shall be encoded as `GeneralizedTime` as `YYYYMMDDHHmmssZ`.

notBefore

The earliest time an Issuing VWP CA Certificate may be used. This shall be the time the Issuing VWP CA Certificate is created.

notAfter

The latest time an Issuing VWP CA Certificate is expected to be used. The value in a `notAfter` field shall be treated as specified in RFC 5280.

subject

The formatting of this field shall contain a unique X.500 Distinguished Name (DN). This shall consist of the Country (C), the Organisation Name (O) which will be DCC and a Common Name (CN) which will be Issuing VWP CA.

subjectPublicKeyInfo

The Certificate's `subjectPublicKeyInfo` field shall indicate the Public Key algorithm identifier and the Public Key in the specified algorithm format as specified in RFC 3279 and RFC 5480.

The algorithm field in the `subjectPublicKeyInfo` structure shall be use the following identifier:

```
id-ecPublicKey OBJECT IDENTIFIER ::= { iso(1) memberbody(2) us(840) ansi-
X9-62(10045) keyType(2) 1 }
```

`id-ecPublicKey` indicates that the algorithms that can be used with the subject Public Key are unrestricted. The key is only restricted by the values indicated in the `keyUsage` extension (explained further under the next extensions heading).

The parameter for `id-ecPublicKey` is as follows and shall always be present:

```
ECParameters ::= CHOICE {
    namedCurve          OBJECT IDENTIFIER
    -- implicitCurve      NULL
    -- specifiedCurve     SpecifiedECDomain
}
```

Only the following field in `ECParameters` shall be used:

- o `namedCurve` - identifies all the required values for a particular set of elliptic curve domain parameters to be represented by an OID.

The OID for the curve choice to be used in Certificates is:

```
secp256r1 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840)
ansi-X9-62(10045) curves(3) prime(1) 7 }
```

The `subjectPublicKey` from `SubjectPublicKeyInfo` is the ECC Public Key.

Implementations of Elliptic Curve Cryptography according to this document shall only support the uncompressed form.

The first octet of the `subjectPublicKey` indicates whether the key is compressed or uncompressed. The uncompressed form is indicated by 0x04 (the compressed form is indicated by either 0x02 or 0x03). The Public Key shall be rejected if any value other than 0x04 is in the first octet.

Extensions

Issuing VWP CA Certificates MUST contain the extensions described below. They should not contain any additional extensions:

- `authorityKeyIdentifier`: non-critical
- `subjectKeyIdentifier`: non-critical
- `keyUsage`: critical
- `certificatePolicies`: non-critical
- `basicConstraints`: critical

authorityKeyIdentifier

A key identifier calculated using method 2 of section 4.2.1.2 of RFC 5280.

subjectKeyIdentifier

Calculated using method 2 of section 4.2.1.2 of RFC 5280.

keyUsage

The Issuing VWP CA Certificate shall have a `keyUsage` extension (as per section 4.2.1.3 of RFC 5280) with a value of `keyCertSign`. This extension shall be marked as critical (as per RFC 5280 section 4.2.1.3).

certificatePolicies

The Issuing VWP CA Certificate shall contain at least one `policyIdentifier` in the `certificatePolicies` extension that refers to the OID for the VWKI Certificate Policy.

basicConstraints

The `basicConstraints` extension shall have the values `cA=True`, and `pathLen=0`. This extension shall be marked as critical.

Issuing VWD CA Certificate Profile

Field Name	RFC 5759/5280 Type	Value	Reference
version	Version	v3	
serialNumber	Integer	calculated by CA	
signature		ecdsa-with-SHA256	
issuer	Name	CN= Root VWKICA, O=DCC, C=GB	
validity	Validity	(see below)	
subject	Name	CN= Issuing VWD CA, O=DCC, C=GB	
subjectPublicKeyInfo		The subject's Public Key	
extensions	Extensions	(see below)	
Validity		The period from notBefore through notAfter, inclusive.	
notBefore	Time	Calculated by CA as time of issue	
notAfter	Time	Calculated by CA as not before + 40 years	
Extensions		Critical and non-critical extensions	
authorityKeyIdentifier	KeyIdentifier	Calculated by CA	
subjectKeyIdentifier	KeyIdentifier	Calculated by CA	
keyUsage		keyCertSign	
certificatePolicies		1.2.826.0.1.8641679.1.2.1.5;	
basicConstraints		CA=True, pathLen=0	

Interpretation**version**

The version of the X.509 Issuing VWD CA Certificate. Issuing VWD CA Certificates shall identify themselves as version 3.

serialNumber

Issuing VWD CA Certificate serial number, a positive integer of no more than 20 octets. The Serial Number identifies the Issuing VWD CA Certificate, and shall be created by the Root VWKICA that signs the Issuing VWD CA Certificate. The Serial Number shall be unique in the scope of VWKICA Certificates signed by the Root VWKICA.

signature

The identity of the signature used by the Root VWKICA to sign the Issuing VWD CA Certificate. This value is used in both the `signatureAlgorithm` field in the Certificate structure and the `signature` field in the `TBSCertificate` structure and indicates the Root VWKICA signature algorithm used to sign this Certificate.

The ECDSA signature method is defined in NIST FIPS 186-5. When implementing ECDSA, the SHA-256 message digest algorithm and the P-256 elliptic curve as defined in NIST SP 800-186 Appendix G, G.1.2, shall be used.

The signature algorithm shall be `ecdsa-with-SHA256` as specified in RFC 5759. The algorithm identifier is:

```
ecdsa-with-SHA256      OBJECT IDENTIFIER ::= { iso(1)
    member-body (2)    us(840)      ansi-X9-62(10045) signatures
(4) ecdsa-with-sha2(3) 2 }
```

The hash algorithm used shall be the SHA-256 secure hash algorithm as defined in NIST FIPS 180-4.

issuer

The name of the signer of the Issuing VWD CA Certificate. This will consist of the Country (C), Organisation Name (O) which will be DCC and a Common Name (CN) which will be Root VWKICA (as defined in the Root VWKICA Certificate profile).

Validity

The time period over which the Root VWKICA expects the Issuing VWD CA Certificate to be valid. The validity period is the period of time from `notBefore` through `notAfter`, inclusive.

All times shall be stated in the Universal Coordinated Time (UTC) time zone. Time up to and including 23:59:59 December 31, 2049 UTC shall be encoded as `UTCTime` as `YYMMDDHHmmssZ`.

Times later than 23:59:59 December 31, 2049 UTC shall be encoded as `GeneralizedTime` as `YYYYMMDDHHmmssZ`.

notBefore

The earliest time an Issuing VWD CA Certificate may be used. This shall be the time the Issuing VWD CA Certificate is created.

notAfter

The latest time an Issuing VWD CA Certificate is expected to be used. The value in a `notAfter` field shall be treated as specified in RFC 5280.

subject

The formatting of this field shall contain a unique X.500 Distinguished Name (DN). This shall consist of the Country (C), the Organisation Name (O) which will be DCC and a Common Name (CN) which will be Issuing VWD CA.

subjectPublicKeyInfo

The Certificate's `subjectPublicKeyInfo` field shall indicate the Public Key algorithm identifier and the Public Key in the specified algorithm format as specified in RFC 3279 and RFC 5480.

The algorithm field in the `subjectPublicKeyInfo` structure shall be use the following identifier:

```
id-ecPublicKey OBJECT IDENTIFIER ::= { iso(1) memberbody(2) us(840) ansi-
X9-62(10045) keyType(2) 1 }
```

`id-ecPublicKey` indicates that the algorithms that can be used with the subject Public Key are unrestricted. The key is only restricted by the values indicated in the `keyUsage` extension (explained further under the next extensions heading).

The parameter for `id-ecPublicKey` is as follows and shall always be present:

```
ECParameters ::= CHOICE {
    namedCurve          OBJECT IDENTIFIER
    -- implicitCurve      NULL
    -- specifiedCurve     SpecifiedECDomain
}
```

Only the following field in `ECParameters` shall be used:

- o `namedCurve` - identifies all the required values for a particular set of elliptic curve domain parameters to be represented by an OID.

The OID for the curve choice to be used in Certificates is:

```
secp256r1 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840)
ansi-X9-62(10045) curves(3) prime(1) 7 }
```

The `subjectPublicKey` from `SubjectPublicKeyInfo` is the ECC Public Key.

Implementations of Elliptic Curve Cryptography according to this document shall only support the uncompressed form.

The first octet of the `subjectPublicKey` indicates whether the key is compressed or uncompressed. The uncompressed form is indicated by 0x04 (the compressed form is indicated by either 0x02 or 0x03). The Public Key shall be rejected if any value other than 0x04 is in the first octet.

Extensions

Issuing VWD CA Certificates **MUST** contain the extensions described below. They should not contain any additional extensions:

- `authorityKeyIdentifier`: non-critical
- `subjectKeyIdentifier`: non-critical
- `keyUsage`: critical
- `certificatePolicies`: non-critical
- `basicConstraints`: critical

authorityKeyIdentifier

A key identifier calculated using method 2 of section 4.2.1.1 of RFC 5280.

subjectKeyIdentifier

Calculated using method 2 of section 4.2.1.2 of RFC 5280.

keyUsage

The Issuing VWD CA Certificate shall have a `keyUsage` extension (as per section 4.2.1.3 of RFC 5280) with a value of Certificate Signing. This extension shall be marked as critical (as per RFC 5280 section 4.2.1.3).

certificatePolicies

The Issuing VWD CA Certificate shall contain at least one `policyIdentifier` in the `certificatePolicies` extension that refers to the OID for the VWKI Certificate Policy.

basicConstraints

The `basicConstraints` extension shall have the values `cA=True`, and `pathLen=0`. This extension shall be marked as critical.

Root VWKICA Certificate VWKI Certificate Profile

Field Name	RFC 5759/5280 Type	Value	Reference
version	Version	v3	
serialNumber	Integer	calculated by CA	
signature	AlgorithmIdentifier	ecdsa-with-SHA256	
issuer	Name	CN= Root VWKICA, O=DCC, C=GB	
validity	Validity	(see below)	
subject	Name	CN=Root VWKICA, O=DCC, C=GB	
subjectPublicKeyInfo	SubjectPublicKeyInfo	The subject's Public Key	
extensions	Extensions	(see below)	
Validity		The period from notBefore through notAfter, inclusive.	
notBefore	Time	Calculated by CA as time of issue	
notAfter	Time	Calculated by CA as not before + 50 years	
Extensions		Critical and non-critical extensions	
authorityKeyIdentifier	KeyIdentifier	Calculated by CA	
subjectKeyIdentifier	KeyIdentifier	Calculated by CA	
keyUsage		keyCertSign	
certificatePolicies		anyPolicy	
basicConstraints		CA=True, pathLen= None	

Interpretation

These certificates are the root of trust for the VWKI.

version

The version of the X.509 Root VWKICA Certificate. Valid Root VWKICA Certificates shall identify themselves as version 3.

serialNumber

Root VWKICA Certificate serial number, a positive integer of no more than 20 octets. The Serial Number identifies the Root VWKICA Certificate, and shall be created by the Root VWKICA that signs the Root VWKICA Certificate (self-signed by the Root VWKICA). The Serial Number shall be unique in the scope of VWKICA Certificate signed by the Root VWKICA.

signature

The identity of the signature used by the Root VWKICA to self-sign the Root VWKICA Certificate. The field shall be ECDSA-with-SHA256 as defined in RFC 5480. This value is used in both the `signatureAlgorithm` field in the Certificate structure and the `signature` field in the `TBSCertificate` structure and indicates the Root VWKICA signature algorithm used to sign this Certificate.

issuer

The name of the signer of the Root VWKICA Certificate. This will consist of the Country (C), Organisation Name (O) which will be DCC and a Common Name (CN) which will be Root VWKICA which will be the same as the Subject Name as it is self-signed by the Root VWKICA.

Validity

The time period over which the Root VWKICA expects the Root VWKICA Certificate to be valid. The validity period is the period of time from `notBefore` through `notAfter`, inclusive.

All times shall be stated in the Universal Coordinated Time (UTC) time zone. Times up to and including 23:59:59 December 31, 2049 UTC shall be encoded as `UTCTime` as `YYMMDDHHmmssZ`.

Times later than 23:59:59 December 31, 2049 UTC shall be encoded as `GeneralizedTime` as `YYYYMMDDHHmmssZ`

notBefore

The earliest time a Root VWKICA Certificate may be used. This shall be the time the Root VWKICA Certificate is created.

notAfter

The latest time a Root VWKICA Certificate is expected to be used. The value in a `notAfter` field shall be treated as specified in RFC 5280.

subject

The formatting of this field shall contain a unique X.500 Distinguished Name (DN). This shall consist of the Country (C), the Organisation Name (O) which will be DCC and a Common Name (CN) which will be Root VWKICA.

subjectPublicKeyInfo

The Certificate's `subjectPublicKeyInfo` field shall indicate the Public Key algorithm identifier and the Public Key in the specified algorithm format as specified in RFC 3279 and RFC 5480.

The algorithm field in the `subjectPublicKeyInfo` structure shall be use the following identifier:

```
id-ecPublicKey OBJECT IDENTIFIER ::= { iso(1) memberbody(2) us(840) ansi-
X9-62(10045) keyType(2) 1 }
```

id-ecPublicKey indicates that the algorithms that can be used with the subject Public Key are unrestricted. The key is only restricted by the values indicated in the Key Usage Certificate extension (explained further under the next extensions heading).

The parameter for id-ecPublicKey is as follows and shall always be present:

```
ECParameters ::= CHOICE {
    namedCurve          OBJECT IDENTIFIER
    -- implicitCurve     NULL
    -- specifiedCurve     SpecifiedECDomain
}
```

Only the following field in ECParameters shall be used:

- namedCurve - identifies all the required values for a particular set of elliptic curve domain parameters to be represented by an OID.

The OID for the curve choice to be used in Certificates is:

```
secp256r1 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840)
ansi-X9-62(10045) curves(3) prime(1) 7 }
```

The subjectPublicKey from SubjectPublicKeyInfo is the ECC Public Key.

Implementations of Elliptic Curve Cryptography according to this document shall only support the uncompressed form.

The first octet of the subjectPublicKey indicates whether the key is compressed or uncompressed. The uncompressed form is indicated by 0x04 (the compressed form is indicated by either 0x02 or 0x03). The Public Key shall be rejected if any value other than 0x04 is in the first octet.

Extensions

Root VWKICA Certificate MUST contain the extensions described below. They should not contain any additional extensions:

- subjectKeyIdentifier non-critical
- keyUsage: critical
- certificatePolicies: non-critical
- basicConstraints: critical

authorityKeyIdentifier

A key identifier calculated using method 2 of section 4.2.1.1 of RFC 5280.

subjectKeyIdentifier

Calculated using method 2 of section 4.2.1.2 of RFC 5280.

keyUsage

The Root VWKICA Certificate shall have a `keyUsage` extension (as per RFC 5280 section 4.2.1.3) with a value of `keyCertSign`. This extension shall be marked as critical (as per RFC 5280 section 4.2.1.3).

certificatePolicies

The Root VWKICA Certificate shall contain only one `policyIdentifier` which shall be `anyPolicy`.

basicConstraints

The `basicConstraints` extension shall have the values `cA=True`, and `pathLen` absent (unlimited). This extension shall be marked as critical.