Vodafone Group CA Automated Code-Signing Certificate Policy

Publication Date: 05/05/09
Version: v.1.3

Table of Contents

Acknowledgments

This Vodafone Group CA CP endorses in whole or in part the following industry standards:

- RFC 3647: Internet X.509 Public Key Infrastructure – Certificate Policies and Certification Practices Framework.
- RFC 3280: Internet X.509 Public Key Infrastructure - Certificate and CRL Profile.
- RFC 2560: X.509 Internet Public Key Infrastructure - Online Certificate Status Protocol – OCSP.
- ISO 1-7799 standard on security and infrastructure.
- ETSI TS 101 042, Policy requirements for certification authorities issuing public key certificates.

1. INTRODUCTION

This Certificate Policy of the Certification Authority of the Vodafone Group (hereinafter, "Vodafone Group CA") applies to the services of the Vodafone Group CA associated with the issuance of digital certificates that carry out code signing. This Certificate Policy, formally titled the "Vodafone Group CA Automated Code-Signing Certificate Policy" (hereinafter, "CP") also includes the Table of Contents; it may be updated from time to time and can be found on the Vodafone Group CA repository at: http://ca.vodafone.com/repository.

This CP meets the formal requirements of Internet Engineering Task Force (IETF) RFC 3647, dated November 2003 with regard to content, layout and format. An RFC issued by IETF is an authoritative source of guidance with regard to standard practices in the area of electronic signatures and certificate management. While certain section titles are included in this CPS according to the structure of RFC 3647, the corresponding topic may not necessarily apply in the implementation under this CPS. These sections are appropriate indicated as "Section not applicable". Meeting the format requirements of RFC 3647 enhances and facilitates the mapping and interoperability of the Vodafone Group CA with other third party CAs and provides relying parties with advance notice on the practices and procedures of the Vodafone Group CA.

The CP explains in detail the technical, procedural and personnel policies and practices of the CA in all services and during the complete life cycle of certificates, issued by the Vodafone Group CA.

Information on the compliance of the Vodafone Group CA with accreditation schemes as well as any other inquiry associated with this CP can be obtained from the following address:

Vodafone Group CA
attn. Group Legal,
C/O VODAFONE GROUP SERVICES LIMITED,
VODAFONE HOUSE, THE CONNECTION,
NEWBURY,
BERKSHIRE RG14 2FN, UNITED KINGDOM.
Email: ca@vodafone.com
URL: ca.vodafone.com

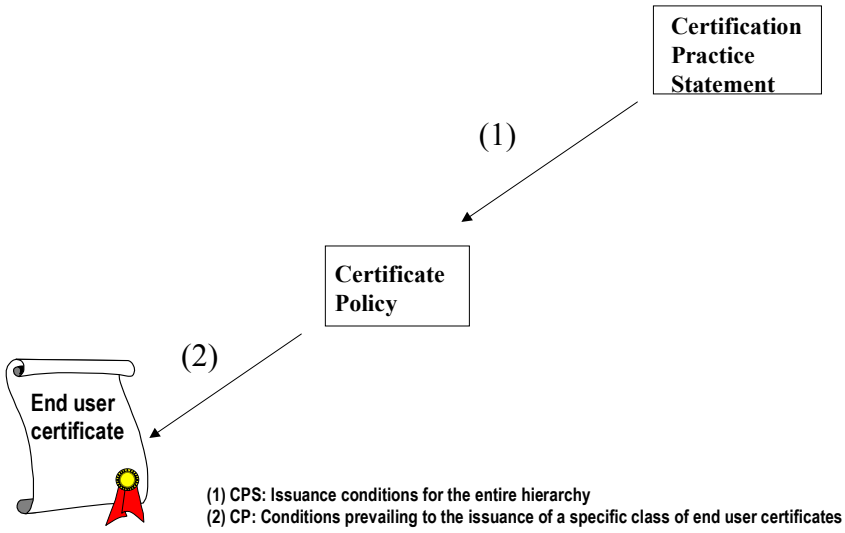
This CP becomes effective and binding between VODAFONE GROUP SERVICES LIMITED, a limited liability company incorporated under the laws of England and Wales, with registered office at VODAFONE HOUSE, THE CONNECTION, NEWBURY, BERKSHIRE RG14 2FN, UNITED KINGDOM, Company Register Number 03802001 (referred to in this CP as the "Vodafone Group CA" which is run as part of Vodafone Group Services Limited's activities) and the Subscriber and/or Relying Party, when the Subscriber enters into a Subscriber agreement within which this CP is incorporated by reference, or when the Relying Party attempts to validate a digital certificate issued subject to this CP, or otherwise relies upon any related VGCA information.

1.1 Overview

This CP applies to the general domain of the Vodafone Group CA services to the exclusion of any other. This CP aims at facilitating the Vodafone Group CA in delivering certification services for a CA issuing code signing certificates. The CA issuing these certificates is known as the Vodafone Executable Layer 2048 Bit CA (hereinafter, VELCA) and the certificates are known as Vodafone Automated Code-Signing End Entity certificates (hereinafter VACEE). This CP identifies the roles, responsibilities and practices of all entities involved in the life cycle, use, reliance upon and management of VACEE certificates. The provisions of this CP with regard to practices, level of services, responsibilities and liability are binding upon all parties involved including the Vodafone Group CA, Vodafone Group RAs, subscribers and relying parties. Certain provisions might also apply to other entities such as the certification service provider, application providers etc., as described below under section 1.3.7

This CP describes the policy requirements to issue, manage and use certificates within the scope of the Vodafone Group CA in issuing and managing VACEE certificates.

A Vodafone Group CA Certification Practice Statement (CPS) complements this CP. A Subscriber or Relying Party of a Vodafone Group CA certificate must refer to the Vodafone Group CA CPS in order to establish trust on a certificate issued by any Vodafone Root CA as well as for notices with regard to the prevailing practices thereof.

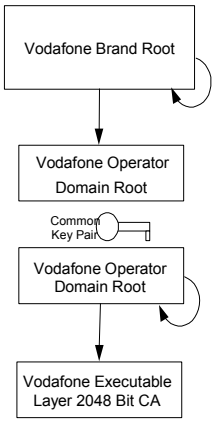


Subscribers and relying parties must consult the specific Vodafone Group CA CP to establish the trustworthiness of the Vodafone Group CA domain of their interest, e.g. the VELCA. It is also essential to establish the trustworthiness of the entire certificate chain of the Vodafone Group CA certificate hierarchy, including the Brand Root CA and/or other Roots, which can be established on the basis of the assertions featured in the CPS.

The exact name of the Vodafone Group CA that issues certificates in accordance with this CP is:

Vodafone Executable Layer 2048 Bit CA (hereinafter, VELCA)

The place of this CA certificate within the associated Vodafone trust hierarchy is shown in the figure below:



The hierarchy supports certificate chains of various lengths, terminated at either the Brand Root or a self-signed subordinate root. This gives Relying Parties a range of options for configuring software to accept only parts of the Vodafone hierarchy, including VACEE certificates. For example they can:

- Install the Vodafone Brand Root certificate, and accept only those Vodafone certificates marked with digital signature key-usage and code-signing extended key usage
- Install the Vodafone Brand Root certificate, and accept only those Vodafone certificates marked with a specific policy OID, or the policy OID range 1.2.826.0.1.1833679.1.1.3.1
- Install the offline Vodafone Operator Domain self-signed root certificate, and accept only those Vodafone certificates which present chains up to this subordinate root.

This CP is maintained by the Vodafone Group CA, which is the issuing authority. In a certificate management environment based on Public Key Infrastructure (PKI), an Issuing Authority is the entity that manages a Trust hierarchy from which all end user certificates inherit Trust.

This CP governs the issuance of Vodafone Group CA VACEE certificates during the application period of the VELCA. An application period is for example, the time during which a certain CA may issue Vodafone Group CA certificates. The application period is indicated in the certificate issued to the VELCA by a hierarchically superior CA within the Vodafone Group hierarchy.

This CP is made available on-line in the Repository of the issuing CA under http://ca.vodafone.com/repository.

The Vodafone Group CA accepts comments regarding this CP addressed to the address mentioned above in the Introduction of this document.

1.2 Document Name and Identification

The Vodafone Group CA may also use the following OID to identify this CP: 1.2.826.0.1.1833679.1.1.3.1.3.

1.3 PKI participants

The Vodafone Group CA aims at making its services available to selected Vodafone Group users. Example users include without limitation organisations that provide software needing to be

assessed, tested and validated for functionality and usability. Such software will be typically written in executable code, e.g. Java code that will be executed on mobile handsets.

A subject is an organisation submitting software for assessment and approval. Using a VACEE certificate, a subscriber will sign code for the purpose of authenticating the source and controlling the integrity of the piece of software before sending it to its intended recipients.

Examples of Vodafone services that users of Vodafone VACEE certificates might access include but are not limited to resources associated with the management of software code. Other applications or uses might become available at a later stage. The Vodafone Group reserves its right to make additional VACEE based services available.

The end user VACEE certificate is issued for the purpose of authentication of the source sending software, and for confirmation that the software has been through and passed the Vodafone approval process. The end user VACEE certificate, which is issued by the Vodafone Group CA and the end user's private key are factors in authenticating the source organisation when making software available to Vodafone Group recipients (especially mobile subscribers). Relying on code signatures constructed using VACEE certificates, Vodafone can conditionally accept the submitted software.

Vodafone envisages making available additional services to external (i.e. non Vodafone Group affiliated) parties that use VACEE certificates. The Vodafone Group CA acknowledges that its certification services will be made available to relying parties, which might not necessarily have any pre-existing contractual relationship with Vodafone.

Designated purposes for the Vodafone Group CA certificates include the following:

- Authenticating a source providing software to Vodafone Group recipients.
- Confirming that the software has been through and passed the Vodafone approval process.

1.3.1 Vodafone Group Certification Authority

A Certification Authority is an organisation that issues digital certificates that are used in the public domain, within a business framework, a transactions context etc. The Vodafone Group CA is a Certification Authority. Sometimes, a certification authority is also described by the term Issuing Authority to denote the purpose of issuing certificates at the request of an RA.

The Vodafone Group CA drafts and implements the policy prevailing in issuing a certain type or class of digital certificates, such as VACEE certificates. The Vodafone Group CA is also a Policy Authority with regard to issuing Vodafone Group CA certificates.

The Vodafone Group CA ensures the availability of all services pertaining to the management of VACEE certificates, including issuance, revocation, and status verification, as they may become available or required in specific applications. The Vodafone Group CA also manages a core online registration system. This online registration system records the named representatives of the Certification Authority and Registration Authorities, their privileges, and the authentication mechanisms they use. The named individual responsible for the Vodafone Group CA is the *CA Owner.*

To provide notice or knowledge to relying parties of functions associated with the revoked and/or suspended certificates requires appropriate publication in an online directory containing, for example, a certificate revocation list. The Vodafone Group CA operates such a directory.

The Vodafone Group CA's domain of responsibility comprises of the overall management of the certificate life cycle including:

- Issuance
- Suspension
- Unsuspension
- Revocation

- Renewal
- Status validation
- Directory service.

To deliver CA services including the issuance, suspension, revocation, renewal and status validation of Vodafone Group CA certificates the Vodafone Group CA operates a secure facility.

Some of these tasks are delegated to Vodafone Group RAs.

1.3.2 Vodafone Group CA Registration Authorities

The Vodafone Group CA reaches its subscribers through designated Registration Authorities (RAs). Only a RA may request the issuance, suspension and revocation of a certificate under this CP, to the exclusion of any other party.

The RA submits the necessary data for the generation and revocation of the certificates to the CA.

The Vodafone Group RA interacts with the Subscriber to deliver public certificate management services to the end-user. The Vodafone Group RA:

- Accepts, evaluates, approves or rejects the registration of certificate applications.
- Registers subscribers to Vodafone Group CA certification services.
- Attends all stages of the identification of subscribers as assigned by the Vodafone Group CA according to the type of certificate they issue.
- May use official, notarised or otherwise authorised documents to evaluate a Subscriber application.
- Following approval of an application, notifies the Vodafone Group CA to issue a certificate.
- Initiates the process to suspend, or unsuspend or revoke a certificate and request a certificate revocation from the Vodafone Group CA.

The Distinguished name of the issuer is further specified in the section “Certificate Profile” of this CP.

Vodafone Group RAs act locally within their own context of geographical or business partnerships on approval and authorisation by the Vodafone Group CA. The Vodafone Group RAs act in accordance with the Vodafone Group CA’s approved practices and procedures.

To grant a VACEE certificate, the Vodafone Group CA uses an automated RA system. Applicants for VACEE certificates are required to present a Vodafone Transport Layer Client certificate. More information on the practices and warranties prevailing in the issuance of Vodafone Transport Layer Client certificates can be obtained from Vodafone at: http://ca.vodafone.com/repository.

The Vodafone Group RA will establish a whitelist of certain certificates issued under the Vodafone Transport Layer Client Root, as trusted for the purpose of requesting a VACEE certificate. An applicant is expected to obtain a Vodafone Transport Layer Client certificate prior to applying for a VACEE certificate. Requests for Vodafone Transport Layer Client certificates may be submitted to ca@vodafone.com.

After obtaining a Vodafone Transport Layer Client certificate the applicant sends the following information to the Vodafone Group RA, in order to request inclusion on the whitelist:

- A copy of the Vodafone Transport Layer Client public key certificate.
- The name of the applicant.
- Organisation name.
- Organisation address and contact information (telephone and fax numbers, email, URL etc.).
- Organisation trade registration and/or VAT registration numbers.

Subsequently, a Vodafone Group RA officer evaluates the request to add the Vodafone Transport Layer Client certificate to the whitelist, also taking into account additional context information that includes but is not limited to an agreement that has been executed between the Vodafone Group and the applying organisation.

If successful, the evaluation is followed by adding the Vodafone Transport Layer Client certificate to the whitelist, and informing the applicant.

The applicant can now request as many VACEE certificates as needed, by sending the following information to the Vodafone Group CA:

- A request for code objects to be signed with each VACEE certificate, identifying the precise application name and details, enclosed in a secure SSL/TLS session; this session signed with the Vodafone Transport Layer Client certificate.
- The name of the applicant (extracted from the Vodafone Transport Layer Client certificate).

The Vodafone RA will then evaluate each such request and submit it to an Authorising Manager for final authorisation. The Authorising Manager will confirm that the request is from an authorised source, using the applicant's supplied contact information, and further contextual information. This contextual information includes proof that the applicant has been appointed to submit particular software on behalf of the subject organisation.

If successful, the evaluation is followed by the issuance of the certificate to the applicant organisation.

1.3.2.1 Authorising Managers

Only the automated RA system can request the issuance of a certificate. An *Authorising Manager* is a natural person who gives final approval to the automated RA system to make certificate requests. The configuration of the automated system to recognise the appropriate Authorising Managers and Subscribers will be performed by natural persons who are logically part of the RA.

1.3.3 Subscribers

Subscribers of Vodafone Group CA services can be natural or legal persons that are not necessarily affiliated with Vodafone. Subscribers use electronic certificate services within the domain of the Vodafone Group. Subscribers are parties that:

- Set the framework of providing certification services with the Vodafone Group CA to the benefit of the subject mentioned in a certificate.
- Have operational control over the private key corresponding to the public key that is listed in the certificate.

Subscribers can be natural persons in their capacity as authorised to legally represent an organisation (e.g. Directors), professional end users (e.g. accountants) or system administrators.

Subscribers typically fulfil the requirements for holding a valid identification document, such as a passport or equivalent recognised in the United Kingdom.

Subscribers of VACEE certificates are representatives of organisations that need to have software signed before providing it for distribution to Vodafone recipients. The purpose of subscribers in signing such software when providing it to Vodafone is to indicate approval and compliance with pre-agreed software testing procedures, in particular for software that will subsequently be used in handsets.

For VACEE certificates, the Subscriber's control of the key-pair is automated. The subscriber specifies to the automated system what code objects the key is required to sign, but does not generate and manage the key-pair. The request for the corresponding certificate is also automated, as described in Section 1.3.2.1

Subscribers are expected to provide evidence of approval and testing of software code according to a designated procedure before sending it to Vodafone for automated signing. Subscribers request signing with a VACEE certificate from Vodafone subject to the conditions that the certificate will only be used to sign specified code agreed in advance with Vodafone and associated with the certificate's Subject, that the signing takes place only after the testing of the code is complete, and that the signing key is securely deleted immediately after the intended code has been signed. Subscribers are also required to obtain a Vodafone Transport Layer Client certificate prior to requesting signing with a VACEE certificate. An overview of the requirements to have a Vodafone Transport Layer Client certificate are described above under section 1.3.2.

Subscribers are expected to have an ongoing responsibility during the life-time of the VACEE certificate with respect to the quality of code that was signed. If the subscriber determines or is advised of material defects in the code which are only discovered after signing, but which would (for example) caused the code to fail the approval procedure if re-conducted, then the subscriber shall request from Vodafone the suspension or immediate revocation of the corresponding signing certificate, Full revocation shall be requested and conducted if Vodafone agrees that the defects are serious enough to prevent further circulation of the code. Failure by the Subscriber to comply with these provisions shall constitute a breach of the CP, and hence entitle the Vodafone Group CA to unilaterally revoke the VACEE certificate.

It is expected that a Subscriber organisation shall have a pre-existing agreement with Vodafone authorising it to supply software to Vodafone. Granting a VACEE certificate to a Subscriber organisation is only permitted pursuant to such an agreement between Vodafone and the subscribing organisation.

1.3.4 Subjects

Subjects of Vodafone Group CA certificate services are natural or legal persons that are not necessarily affiliated with Vodafone but instead are associated with the Subscriber. Subjects use services dependent upon electronic certificates within the domain of the Vodafone Group. Subjects are parties that:

- Appoint and approve a Subscriber to apply for a certificate.
- Are identified in a certificate.
- Have ultimate authority over the use of the private key corresponding to the public key that is listed in the certificate.

A subject enrols with the Service Provider that requires it to use a certificate within the designated service. A subject nominates a named Certificate Applicant, also called a Subscriber, to apply for a certificate. A certificate applicant can be any natural or legal person acting on behalf of the subject.

1.3.5 Certificate Applicants

A Certificate Applicant is a party wishing to become a Subscriber of a VACEE certificate. A certificate applicant is a party designated by the subject to act on the subject's behalf in:

- Applying for a certificate.
- Agreeing with and accepting the CA's Subscriber agreement.

The applicant may be, for example:

- The same as the subject itself, where this is a named individual.
- An individual employed by the subject.
- An individual employed by a contractor or sub-contractor.

1.3.6 Certificate Service Providers

A Certificate Service Provider makes available the resources for CA certificates life cycle management such as private keys and CRLs. It also makes available the operational infrastructure that the Certification Authority uses to manage the life cycle of end-user certificates. Its named representative is the *CA Manager*. Further details of infrastructure and life cycle duties assigned to the Vodafone Group CA, and in practice executed by a Certificate Service Provider, are described in Sections 4, 5 and 6.

1.3.7 Relying Parties

Relying parties are natural or legal persons that rely on a certificate and/or a digital signature verifiable with reference to a public key listed in a Subscriber's certificate. For example, the Vodafone Group operators that make use of certificate services are relying parties of the Vodafone Group CA certificates.

To verify the validity of a digital certificate, relying parties must always refer to Vodafone Group CA revocation information, such as a Certificate Revocation List (CRL), prior to relying on information featured in a certificate. The Relying Party may be advised of the Vodafone Group CA's Obligations to Relying Parties prior to accessing a validation service.

Typical relying parties of VACEE certificates include the ones mentioned below:

1.3.7.1 Service Provider

A service provider chooses the nature of a service that will use certificates, and the terms and conditions under which such service will be rendered. The Service Provider chooses or accepts Certificate Subjects and Service Users. It relies upon a Certification Authority such as the Vodafone Group CA to define and comply with a certificate policy for use in the designated service. It provides names of approved Certificate Subjects, and contact details for the corresponding Certificate Applicants, to the Registration Authority associated with that Certification Authority. Its named representative is the *Service Owner*.

1.3.7.2 Service User

A Service User makes use of the service offered by the Service Provider, under specific terms and conditions. Part of the service requires the use of certificates to identify and authenticate approved Certificate Subjects for that service e.g. to agree a shared secret with the Certificate Subject, or to verify signed data created by the Certificate Subject.

The Service User and Service Provider agree on the equipment to be used and, implicitly or explicitly, how it is to be configured (e.g. use of pre-installed roots, download and checking of CRLs). These terms and conditions may make reference to the Vodafone Group CA's Obligations to Relying Parties made available by the Certification Authority.

1.4 Certificate use

Certain limitations apply to the use of Vodafone Group CA certificates.

1.4.1 Appropriate certificate use

Vodafone Group CA VACEE certificates can be used for specific electronic transactions that include the signing of tested and approved software code prior to dispatch to a Vodafone Group recipient. The Vodafone Group CA will specifically designate any such uses when they become available to end-users and provide notice through its web site.

The purpose of Vodafone Group CA VACEE certificates is to authenticate the source of software and confirm that the software has been through and passed the Vodafone approval process.

1.4.2 Prohibited certificate use

Certain limitations to the use of Vodafone Group CA certificates are stated below in this Vodafone Group CA CP.

End entity certificate use is restricted using certificate extensions (key usage and extended key usage). Any use of the certificate that is inconsistent with these extensions is prohibited.

1.5 Policy Administration

The Policy Managing Authority of the Vodafone Group CA manages this CP. The Vodafone Group CA is responsible for the registration, maintenance, and interpretation of this CP. The Vodafone Group CA reserves its right to periodically produce updates and changes to this policy as it sees fit. The Vodafone Group CA shall make best efforts to inform subscribers and relying parties thereof through its document repository http://ca.vodafone.com/repository.

It is intended that subscribers and relying parties will use this CP to establish the relationship between and trustworthiness of the Vodafone Group CA and other CAs. To establish the trustworthiness of Vodafone Group CA certification services subscribers and relying parties are hereby prompted to review to the Vodafone Group CA CPS available under http://ca.vodafone.com/repository.

1.6 Definitions and acronyms

A list of definitions can be found at the end of this CP.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

The Vodafone Group CA publishes information about the digital certificates it issues in (an) online publicly accessible repository(ies). The Vodafone Group CA reserves its rights to publish certificate status information on third party repositories together or independently of any eventual publications that it may carry out itself.

The Vodafone Group CA retains an online repository of documents where it makes certain disclosures about its practices, procedures and the content of certain of its policies including this CP while it reserves its rights to make available and publish information on its policies by any means it sees fit.

All parties associated with the issuance, use or management of the Vodafone Group CA certificates are hereby notified that the Vodafone Group CA may publish any submitted certificate status information on publicly accessible directories in association with the provision of electronic certificate status information.

The Vodafone Group CA refrains from making publicly available certain elements of documents including security controls, procedures, internal security polices etc.

2.1 Access control on repositories

While the Vodafone Group CA strives to keep access to its public repository and access to its policy information (e.g. CP, CPS etc.) free of charge, it might charge for services such as the publication of status information on third party databases, private directories, etc. In such case, notification will be provided through the Vodafone Group CA web site.

3. IDENTIFICATION AND AUTHENTICATION

The Vodafone Group CA operates RAs that authenticates the identity and/or other attributes of an end-user certificate applicant, in particular their authorisation (where applicable) to act on a Subject's behalf. Prior to requesting issuing a certificate a Vodafone Group RA verifies the identity of an applicant of a certificate to the Vodafone Group CA.

The RA maintains appropriate procedures to address naming practices, including the recognition of trademark rights in certain names.

The Vodafone Group RA authenticates the requests of parties wishing the revocation of certificates under this CP.

3.1 Naming

To identify a subject the Vodafone Group CA follows certain naming and identification rules that include types of names assigned to the subject, such as X.500 distinguished names, RFC-822 names or X.400 names. The Vodafone Group CA issues certificates to applicants submitting a documented application containing a verifiable name.

Names assigned to subjectss of a certificate are unique within the domain of the Vodafone Group CA as they are always used together with a unique sequential number.

3.2 Initial Identity Validation

For the identification and authentication procedures of the initial Subscriber registration for each subject type (CA, RA, VACEE Subscriber, Subject, or other participant) the Vodafone Group CA takes the following steps:

The entity identified in the subject field must demonstrate possession of the private key corresponding to the public key presented to the Vodafone Group CA. This demonstration must be performed by the subject itself, or by a designated applicant.

The Vodafone Group RA relies on such resources as third party databases to identify and authenticate natural persons or organisations applying for a Vodafone Group CA certificate. In addition, for VACEE certificates, the Vodafone Group RA relies on a Vodafone Transport Layer Client certificate that the applicant presents to it. More information on Vodafone Transport Layer Client certificates can be found under ca.vodafone.com/repository.

For the identification and authentication of individual subscribers applying for a Vodafone Group CA certificate a Vodafone Group RA may take steps that include but are not limited to:

- Controlling documents such as identity cards, passport, driver's licence.
- Authenticating the identity of the applicant based on other documentation or credentials provided.
- Requesting an applicant to physically appear before an RA before a digital certificate is issued.
- Relying on additional credentials, such as third party databases, digital certificates, e.g. a Vodafone Transport Layer Client certificate etc.
- Requesting from the service provider, subject or applicant, proof of the applicant's authorisation to act on the subject's behalf.

For VACEE certificates, a Vodafone Group RA will endeavour to provide the applicant with sufficient credentials (a whitelisted Vodafone Transport Layer Client certificate) such that the

enrolment process can then proceed online. The online process will be verified by the Vodafone Group RA, using an independent channel to contact the applicant, for example phone-call, SMS.

A Vodafone Group RA may refuse to issue a certificate to an applicant unless sufficient evidence is produced with regard to the applicant's identity and authorisation.

3.3 Identification and Authentication for Re-key Requests

Section not applicable.

3.4 Identification and Authentication for Revocation Requests

For the identification and authentication procedures for revocation requests for its subject types (CA, RA, VACEE Subject, and other participants) the Vodafone Group CA requires to use an online authentication mechanism from a Vodafone Group RA (e.g. digital certificate authentication, PIN etc.) and a request addressed to the Vodafone Group CA or an RA.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

All entities within the Vodafone Group CA domain including the RAs and subscribers or other participants have a continuous duty to inform the Vodafone Group CA of all changes in the information featured in a certificate during the operational period of such certificate and until it expires or gets revoked.

The Vodafone Group CA issues, revokes or suspends certificates following an authenticated and duly signed request issued by a Vodafone Group RA.

To carry out its tasks the Vodafone Group CA may use third party agents. The Vodafone Group CA assumes full responsibility and accountability for all acts or omissions of all third party agents it may use to deliver services associated with CA operations within the Vodafone Group CA.

4.1 Certificate Application

A Vodafone Group RA has the duty to provide the Vodafone Group CA with accurate information on the certificate requests it lodges on behalf of the end user applicants.

The Vodafone Group CA acts upon request of an RA that has the authority to make a request to issue a certificate.

Subscribers undergo an enrolment process that requires:

i. Filling out an application form.
ii. Generating a key pair, directly or through an agent.
iii. Delivering the generated public key corresponding to a private key to Vodafone Group CA.
iv. Accepting the Subscriber agreement.

In case that an individual subject enters into a Subscriber application then the above listed functions i-iv shall be carried out by the subject; otherwise, they are carried out by the subject's designated applicant. The Subscriber will be required to accept the issuance terms by a Subscriber agreement that will be executed with the Vodafone Group CA.

In general, an online enrolment process will be used, based on credentials already transmitted by the Vodafone Group RA to the applicant. However, where such remote verification of the applicant's identity was infeasible, further credentials may be requested, as appropriate, in a way that the exact identity of the applicant can reasonably be established. This may include a manually signed copy of the Subscriber agreement, and a copy of identity card, or physical appearance before the RA.

4.2 Certificate Application Processing

A Vodafone Group RA acts upon a certificate application to validate an applicant's identity. Subsequently, an RA either approves or rejects a certificate application. Such approval or rejection does not necessarily have to be justified to the applicant or any other party.

4.3 Certificate Issuance

The Vodafone Group RA subsequently sends a certificate issuance request to the Vodafone Group CA.

Requests from the RA are granted approval provided they are validly made and they contain valid Subscriber data, formatted according to the Vodafone Group CA specifications.

The Vodafone Group CA verifies the identity of the Vodafone Group RA on the basis of credentials presented (a special RA administrator certificate). The Vodafone Group CA retains its right to reject the application, or any applicant for RA certificates.

Following issuance of the certificate, the Vodafone Group CA delivers the issued certificate to the Subscriber directly or through an agent.

4.4 Certificate Acceptance

An issued Vodafone Group CA certificate is deemed accepted by the Subscriber when the RA confirms the acceptance of a certificate the Vodafone Group CA issues. In the absence of explicit acceptance a certificate is deemed accepted after lapse of 5 calendar days from issuance.

Any objection to accepting an issued certificate must explicitly be notified to the Vodafone Group CA. The reasoning for rejection including any fields in the certificate that contain erroneous information must also be submitted.

The Vodafone Group CA posts the issued but not accepted certificate on a repository (X.500 or LDAP). It also reserves its right to notify the certificate issuance by the Vodafone Group CA to other entities.

4.5 Key Pair and Certificate Usage

The responsibilities relating to the use of keys and certificates include the ones addressed below:

4.5.1 Subscriber

The obligations of the Subscriber include the following ones:

4.5.1.1 Subscriber duties

Unless otherwise stated in this CP, the duties of the subscribers include the following:

1. Having knowledge and, if necessary, seeking training on using digital certificates and PKI.
2. Generating securely their private-public key pair, using a trustworthy system.
3. Providing correct and accurate information in their communications with the Vodafone Group CA.
4. Ensuring that the public key submitted to the Vodafone Group CA correctly corresponds to the private key used.
5. Accepting all terms and conditions in the Vodafone Group CA CPS and associated policies published in the Vodafone Group CA Repository.
6. Refraining from tampering with a Vodafone Group CA certificate.
7. Using Vodafone Group CA certificates for legal and authorised purposes in accordance with this Vodafone Group CPS.
8. Notifying the Vodafone Group CA or a Vodafone Group RA of any changes in the information submitted.
9. Ceasing to use a Vodafone Group CA certificate if any featured information becomes invalid.
10. Ceasing to use a Vodafone Group CA certificate when it becomes invalid.
11. Removing a Vodafone Group CA certificate when invalid from any applications and/or devices they have been installed on.
12. Using a Vodafone Group CA certificate, as it may be reasonable under the circumstances.
13. Preventing the compromise, loss, disclosure, modification, or otherwise unauthorised use of their private key (“loss” does not include controlled destruction of the key as defined below).

14. Using secure devices and products that provide appropriate protection to their keys.
15. For any acts and omissions of partners and agents subscribers use to generate, retain, escrow, or destroy any private keys.
16. Refraining from submitting to Vodafone Group CA or any Vodafone Group CA directory any material that contains statements that violate any law or the rights of any party.
17. Requesting the suspension or revocation of a certificate in case of an occurrence that materially affects the integrity of a Vodafone Group CA certificate.
18. Notifying the appropriate RA immediately, if a Subscriber becomes aware of or suspects the compromise of a private key.
19. Destroying the private key in a controlled fashion after it has fulfilled its intended purpose to sign designated Code.

The Subscriber has all the above stated duties towards the CA at all times. When the Subscriber applies on behalf of a different named Subject certain duties can be mitigated to the Subject, which in return shall have to inform the Subscriber of any eventualities affecting the life cycle of a certificate. In such case of mitigation, duties 6-14 and 17-18 above could apply to the Subject and not to the Subscriber.

4.5.1.2 Subscriber Duty Towards Relying Parties

Without limiting other Subscriber obligations stated elsewhere in this CP, subscribers have a duty to refrain from any misrepresentations they make in certificates to third parties that rely in good faith on the representations contained therein.

4.5.2 Relying Party

The duties of a Relying Party are as follows:

4.5.2.1 Relying Party duties

A party relying on a Vodafone Group CA certificate promises to:

- Have the technical capability to use digital certificates and PKI.
- Receive notice of the Vodafone Group CA and associated conditions for relying parties.
- Validate a Vodafone Group CA certificate by using the correct Vodafone root certificate and any suitable certificate status information (e.g. a CRL) published by the Vodafone Group CA, in accordance with the proper certificate path validation procedure.
- Trust a Vodafone Group CA certificate only if all information featured on such a certificate can be verified via such a validation procedure as being correct and up to date.
- Rely on a Vodafone Group CA certificate, only as may be reasonable under the circumstances.
- Notify the appropriate RA immediately, if the Relying Party becomes aware of or suspects that a private key has been compromised.

4.5.2.2 Vodafone Group CA Repository and Web site Conditions

Parties, including subscribers and relying parties, accessing the Vodafone Group CA Repository and web site agree with the provisions of this CP and any other conditions of usage that the Vodafone Group CA may make available. Parties demonstrate acceptance of the conditions of usage of the CP by submitting a query with regard to the status of a digital certificate or by anyway using or relying upon any such information or services provided. Here, “using” such Vodafone Group CA information or services is defined as:

- Obtaining information as a result of the search for a digital certificate.
- Verifying the status of digital signatures created with a private key corresponding to a public key included in a certificate.

- Verifying the status of a digital certificate prior to encrypting data using the public key included in a certificate.
- Providing information published on the Vodafone Group CA web site.
- Any other services that Vodafone Group CA might advertise for or provide through its web site.

4.5.2.3 Reliance at Own Risk

It is the sole responsibility of the parties accessing information featured in the Vodafone Group CA Repositories and web site to assess and rely on information featured therein. Parties acknowledge that they have received adequate information to decide whether to rely upon any information provided in a certificate. The Vodafone Group CA takes all steps necessary to update its records and directories concerning the status of the certificates and to issue relevant warnings. Failure to comply with the conditions of usage of the Vodafone Group CA Repositories and web site may result in terminating the relationship between the Vodafone Group CA and the party.

4.6 Certificate Renewal

Section not applicable.

4.7 Certificate Re-key

Section not applicable.

4.8 Certificate Modification

Section not applicable.

4.9 Certificate Revocation and Suspension

Upon request from an RA, the Vodafone Group CA suspends or revokes a digital certificate if:

- There has been a loss, theft, modification, unauthorised disclosure, or other compromise of the private key used by the certificate's Subject or Subscriber.
- There has been a change in the relationship between the Subject and the Subscriber, such that the Subscriber is no longer able or authorised to use the private key and certificate to the benefit of the Subject.
- The certificate's Subject or their appointed Subscriber has breached a material obligation under this CP.
- The performance of a person's obligations under this CP is delayed or prevented by a natural disaster, computer or communications failure, or other cause beyond the person's reasonable control, and as a result, another person's information is materially threatened or compromised.
- There has been a modification of the information, contained in the certificate, relating to the certificate's Subject.
- The Subscriber has requested revocation under the terms of the Subscriber agreement.
- The Subscriber agreement has been terminated for any reason prior to certificate expiry.

The Vodafone Group RA requests the suspension or revocation of a certificate promptly upon verifying the identity of the requesting party and confirming that the request has been issued in accordance with the procedures required by this CP. Verification of the identity can be done through information elements featured in the identification data the Subscriber has submitted to the Vodafone Group RA. Upon request by a Vodafone Group RA, the Vodafone Group CA takes prompt action to revoke the certificate.

4.9.1 Term and Termination of Suspension and Revocation

Suspension may last for a maximum of one week to establish the conditions that caused the request of suspension.

The Vodafone Group CA publishes notices of suspended or revoked certificates in the Vodafone Group CA repository. The Vodafone Group CA may publish its suspended or revoked certificates in its CRL and additionally, by any other means as it sees fit.

4.10 Certificate Status Services

The Vodafone Group CA makes available certificate status checking services including CRLs, OCSP where applicable, and appropriate Web interfaces.

CRL
A CRL lists all revoked and suspended certificates during the application period. CRLs are available from http://crl.vodafone-pki.com/crl.v.

A CRL is issued each 3 hours with a publication margin of plus or minus 1 hour.

OCSP
An OCSP responder provides a real-time status check for individual certificates during the application period, and is available within this CP. OCSP responses are available from http://ocsp.vodafone-pki.com.

4.11 End of Subscription

Subscriber subscription ends when a certificate is revoked, expired or the service is terminated.

4.12 Key Escrow and Recovery

Section not applicable.

5. MANAGEMENT, OPERATIONAL, AND PHYSICAL CONTROLS

This section describes non-technical security controls used by the Vodafone Group CA to perform the functions of key generation, subject authentication, certificate issuance, certificate revocation, audit, and archival.

5.1 Physical Security Controls

The Vodafone Group CA implements physical controls on its own premises. The Vodafone Group CA physical controls include the following:

The infrastructure of the Vodafone Group CA used for all CA services made available by the Vodafone Group CA, is logically separated from any other PKI infrastructure, used for any other purposes.

The Vodafone Group CA secure premises are located in an area appropriate for high-security operations.

Physical access is restricted by implementing mechanisms to control access from one area of the facility to another or access into high-security zones, such as locating CA operations in a secure computer room physically monitored and supported by security alarms and requiring movement from zone to zone to be accomplished using a token and access control lists.

The Vodafone Group CA implements prevention and protection as well as measures against fire exposures.

Media are stored securely. Backup media are also stored in a separate location that is physically secure and protected from fire and water damages.

The Vodafone Group CA implements a partial off-site backup facility.

The sites of the Vodafone Group CA host the infrastructure to provide the Vodafone Group CA services. The Vodafone Group CA sites implement proper security controls, including access control, intrusion detection and monitoring. Access to the sites is limited to authorized personnel listed on an access list, which is subject to audit.

5.2 Procedural Controls

The Vodafone Group CA follows personnel and management practices that provide reasonable assurance of the trustworthiness and competence of the members of the staff and of the satisfactory performance of their duties in the fields of the electronic signature-related technologies.

The Vodafone Group CA obtains a signed statement from each member of the staff on not having conflicting interests, maintaining confidentiality and protecting personal data.

All members of the staff operating the key management operations administrators, security officers, and system auditors or any other operations that materially affect such operations are considered as serving in a trusted position.

The Vodafone Group CA conducts an initial investigation of all members of staff who are candidates to serve in trusted roles to make a reasonable attempt to determine their trustworthiness and competence.

Where dual control is required at least two trusted members of the Vodafone Group CA staff need to bring their respective and split knowledge in order to be able to proceed with the ongoing operation.

The Vodafone Group CA ensures that all actions with respect to the Vodafone Group CA can be attributed to the system and the person of the CA that has performed the action.

The Vodafone Group CA implements dual control for critical CA functions.

5.3 Personnel Security Controls

5.3.1 Qualifications, Experience, Clearances

The Vodafone Group CA Partners perform checks to establish the background, qualifications, and experience needed to perform within the competence context of the specific job. Such background checks are specifically directed towards:

- Misrepresentations by the candidate.
- Any other as it might be deemed necessary.

5.3.2 Background Checks and Clearance Procedures

The Vodafone Group CA makes the relevant checks of prospective employees by means of status reports issued by a competent authority, third-party statements or self-declarations.

5.3.3 Training Requirements and Procedures

The Vodafone Group CA makes available training for its personnel to carry out CA and RA functions.

5.3.4 Retraining Period and Retraining Procedures

Periodic training updates might also be performed to establish continuity and updates in the knowledge of the personnel and procedures.

5.3.5 Job Rotation

Section not applicable.

5.3.6 Sanctions Against Personnel

The Vodafone Group CA sanctions personnel for unauthorized actions, unauthorized use of authority, and unauthorized use of systems for the purpose of imposing accountability on a participant's personnel, as it might be appropriate under the circumstances.

5.3.7 Controls of independent contractors

Independent contractors and their personnel are subject to the same privacy protection and confidentiality conditions as Vodafone Group CA personnel.

5.3.8 Documentation for initial training and retraining

The Vodafone Group CA, and RAs make available documentation to personnel, during initial training, retraining, or otherwise.

5.4 Audit Logging Procedures

Audit logging procedures include event logging and audit systems, implemented for the purpose of maintaining a secure environment. The Vodafone Group CA implements the following controls:

The Vodafone Group CA audit system records events that include but are not limited to:

- Issuance of a certificate.
- Revocation of a certificate.
- Suspension of a certificate.
- Publishing of a CRL.

Audit trail records contain:

- The identification of the operation.
- The date and time of the operation.
- The identification of the certificate, involved in the operation.
- The identification of the person that performed the operation.
- A reference to the request of the operation.

Documents that are required for audits include:

- Infrastructure plans and descriptions.
- Physical site plans and descriptions.
- Configuration of hardware and software.
- Personnel access lists.

The Vodafone Group CA ensures that designated personnel review log files at regular intervals and detect and report anomalous events.

Log files and audit trails are archived for inspection by the authorized personnel of the Vodafone Group CA, the RAs and designated auditors. The log files should be properly protected by an access control mechanism. Log files and audit trails are backed up.

Auditing events are not given log notice.

5.5 Records Archival

The Vodafone Group CA keeps internal records of the following items:

- All certificates for a period of a minimum of 10 years after the expiration of the certificate.
- Audit trails on the issuance of certificates for a period of a minimum of 10 years after issuance of a certificate.
- Audit trail of the revocation of a certificate for a period of a minimum of 10 years after revocation of a certificate.
- CRLs for a minimum of 10 years after publishing.

The Vodafone Group CA keeps archives in a retrievable format.

The Vodafone Group CA ensures the integrity of the physical storage media and implements proper copying mechanisms to prevent data loss.

Archives are accessible to authorized personnel of the Vodafone Group CA and the RAs as appropriate.

5.5.1 Types of records

The Vodafone Group CA retains in a trustworthy manner records of Vodafone Group CA digital certificates, audit data, certificate application information and documentation supporting certificate applications.

5.5.2 Retention period

The Vodafone Group CA retains in a trustworthy manner records of Vodafone Group CA digital certificates for a term as indicated in the Vodafone Group CA CPS.

5.5.3 Protection of archive

Conditions for the protection of archives include:

- Only the records administrator (member of staff assigned with the records retention duty) may view the archive.
- Protection against modification of archive, such as storing the data on a write once medium.
- Protection against deletion of archive.
- Protection against deterioration of the media on which the archive is stored, such as a requirement for data to be migrated periodically to fresh media.

5.5.4 Archive backup procedures

Section not applicable.

5.5.5 Requirements for Time-stamping of Records

Section not applicable.

5.5.6 Archive Collection

The Vodafone Group CA archive collection system is internal.

5.5.7 Procedures to obtain and verify archive information

To obtain and verify archive information the Vodafone Group CA maintains records under clear hierarchical control and a definite job description.

The Vodafone Group CA retains records in electronic or in paper-based format. The Vodafone Group CA may require RAs, subscribers, or their agents to submit documents appropriately in support of this requirement.

Filing terms begin on the date of expiration or revocation. Such records may be retained in electronic, in paper-based format or any other format that the Vodafone Group CA may see fit.

The Vodafone Group CA may revise record retention terms as might be required to comply with accreditation schemes.

5.6 Key Changeover

Section not applicable.

5.7 Compromise and Disaster Recovery

In a separate internal document, the Vodafone Group CA documents applicable incident, compromise reporting and handling procedures. The Vodafone Group CA documents the recovery procedures used if computing resources, software, and/or data are corrupted or suspected of being corrupted.

The Vodafone Group CA establishes the necessary measures to ensure full and automatic recovery of the service in case of a disaster, corrupted servers, software or data.

A business continuity plan has been implemented to ensure business continuity following a natural or other disaster.

5.8 CA or RA Termination

Before terminating its CA activities, the Vodafone Group CA will take steps to transfer to a designated organisation the following information at the Vodafone Group CA's own costs:

- All information, data, documents, repositories, archives and audit trails pertaining to the Vodafone Group CA.

6. TECHNICAL SECURITY CONTROLS

This section sets out the security measures taken by the Vodafone Group CA to protect its cryptographic keys and activation data (e.g., PINs, passwords, or manually-held key shares).

6.1 Key Pair Generation and Installation

The Vodafone Group CA protects its private key(s) in accordance with this CP. The Vodafone Group CA uses private signing keys only for signing certificates, CRLs, and OCSP responses in accordance with the intended use of each of these keys.

The Vodafone Group CA does not use its private keys for purposes not directly associated with the Vodafone Group CA domain.

6.1.1 Vodafone Group CA Private Key Generation Process

The Vodafone Group CA uses a trustworthy process for the generation of its root private key(s) according to a documented procedure. The Vodafone Group CA distributes the secret shares of its private key(s).

6.1.1.1 Vodafone Group CA Private Key Usage

The private keys of the Vodafone Group CA are used to sign Vodafone Group CA issued certificates, Vodafone Group CA certification revocation lists and OCSP responses. Other usages are restricted.

6.1.1.2 Vodafone Group CA Private Key Type

For the Brand Root key and offline Operator Domain Root key, the Vodafone Group CA makes use of the RSA algorithm with a key length of 2048 bits and an expiry date at the end of 2021.

For the operational VELCA key the Vodafone Group CA makes use of the RSA algorithm with a key length of 2048 bits and an expiry date at the end of 2021.

6.1.2 Vodafone Group CA Key Generation

The Vodafone Group CA securely generates and protects its own private keys, using a trustworthy system, and takes necessary precautions to prevent the compromise or unauthorised usage of them. The Vodafone Group CA implements and documents key generation procedures, in line with this CP.

6.2 Key Pair re-generation and re-installation

The Vodafone Group CA decommissions and destroys keys used in the past as well as the active tamper-resistant devices and all backup or escrowed copies of its private keys.

6.2.1 Vodafone Group CA Key Generation Devices

The generation of the private keys of the Vodafone Group CA occurs within a secure cryptographic device meeting appropriate requirements including ISO 15782-1, FIPS 140-1 level 3, ANSI X9.66.

6.2.1.1 Vodafone Group CA Key Generation Controls

The generation of the private keys of the Vodafone Group CA requires the control of more than one appropriately authorised member of staff serving in trustworthy positions. This action entails dual control.

6.2.2 Vodafone Group CA Private Key Storage

The Vodafone Group CA uses a secure cryptographic device to store its private keys meeting the appropriate ISO 15782-1/FIPS 140-1/ANSI X9.66 level 3 requirements.

6.2.2.1 Vodafone Group CA Key Storage Controls

The storage of the private keys of the Vodafone Group CA requires multiple controls by appropriately authorised members of staff serving in trustworthy positions. This action entails dual control.

6.2.2.2 Vodafone Group CA Key Back Up

The Vodafone Group CA's private keys are backed up, stored and recovered by multiple and appropriately authorised members of staff serving in trustworthy positions. This action entails dual control.

6.2.2.3 Secret Sharing

The Vodafone Group CA secret shares use multiple authorised holders, to safeguard and improve the trustworthiness of private keys and provide for key recovery. The Vodafone Group CA stores its own private keys in several tamper-resistant devices. This action entails dual control.

6.2.2.4 Acceptance of Secret Shares

Before secret shareholders accept a secret share they must personally have observed the creation, re-creation, and distribution of the share or its subsequent chain of custody.

A secret shareholder receives the secret share within a physical medium, such as a Vodafone Group CA approved hardware cryptographic module. The Vodafone Group CA keeps written records of secret share distribution.

6.2.3 Vodafone Group CA Private Key Distribution

The Vodafone Group CA documents its own private key distribution and has the ability to alter the distribution of tokens in case token custodians need to be replaced in their role of token custodians.

6.2.4 Vodafone Group CA Private Key Destruction

At the end of their lifetime the private keys of the Vodafone Group CA are destroyed in the presence of at least three trusted operatives in order to ensure that these private keys can never be retrieved and used again.

The key destruction process is documented and all associated records are archived.

6.3 Private Key Protection and Cryptographic Module Engineering Controls

The Vodafone Group CA uses appropriate cryptographic devices to perform CA key management tasks. Those cryptographic devices are known as Hardware Security Modules (HSMs).

Such devices meet formal requirements, which guarantee, amongst other things, that device tampering is immediately detected; and private keys cannot leave devices unencrypted

Hardware and software mechanisms that protect CA private keys are documented. The document demonstrates that CA key protection mechanisms are of at least equivalent strength to the CA keys they are protecting.

Each Vodafone Group CA private key remains under *m* out of *n* multi-person control.

Vodafone Group CA custodians are assigned with the task to activate and deactivate the private key. The key is then active for a defined time period.

The Vodafone Group CA private keys can be destroyed at the end of their lifetimes.

6.4 Other Aspects of Key Pair Management

The Vodafone Group CA archives its own public keys.

The Vodafone Group CA issues certificates to subscribing parties with usage periods as indicated on such certificates.

6.4.1 Computing resources, software, and/or data are corrupted

The Vodafone Group CA establishes the necessary measures to ensure full and automatic recovery of the service in case of a disaster, corrupted servers, software or data.

If resources or services are not under the control of the Vodafone Group CA, the CA ensures that any agreement with the resource owner or service provider is compliant with the requirements for disaster recovery.

6.4.2 CA public key revocation

If a Vodafone Group CA public key is revoked the Vodafone Group CA will immediately notify all CAs with which it is cross-certified.

6.4.3 CA private key is compromised

If a private key of the Vodafone Group CA is compromised, the corresponding certificate should immediately be revoked. Additional measures will be taken.

6.5 Activation Data

The Vodafone Group CA securely stores and archives activation data associated with its own private keys and operations.

6.6 Computer Security Controls

The Vodafone Group CA implements computer security controls.

6.7 Life Cycle Security Controls

The Vodafone Group CA performs periodic development controls and security management controls.

6.8 Network Security Controls

The Vodafone Group CA maintains a high-level network of systems security including firewalls. Network intrusions are detected. To be specific:

- The Vodafone Group CA encrypts connections to the RAs, using dedicated administrative certificates.
- The Vodafone Group CA web site provides certificate based Secure Socket Layer connections and anti-virus protection.
- The Vodafone Group CA network is protected by a managed firewall and intrusion detection system.
- Accessing Vodafone Group CA databases from outside the CA's network is prohibited.
- Internet sessions for request and delivery of information are encrypted.

6.9 Time-stamping

Section not applicable.

7. CERTIFICATE AND CRL PROFILES

This section specifies the certificate format, CRL and OCSP formats.

7.1 Certificate Profile

The Vodafone Group CA maintains a record of the certificate profiles it uses in an independent technical document. This will be made available at the discretion of the Vodafone Group CA, on request from parties explaining their interest.

7.2 CRL Profile

The Vodafone Group CA maintains a record of the CRL profiles it uses in an independent technical document. This will be made available at the discretion of the Vodafone Group CA, on request from parties explaining their interest.

7.3 OCSP Profile

The Vodafone Group CA maintains a record of the OCSP profiles it uses in an independent technical document. This will be made available at the discretion of the Vodafone Group CA, on request from parties explaining their interest.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENT

The Vodafone Group CA may accept under certain conditions the auditing of practices and procedures it does not publicly disclose, subject to approval with respect to the scope and content of such audits. The Vodafone Group CA will evaluate the results of such audits before possibly implementing them.

9. OTHER BUSINESS AND LEGAL MATTERS

Certain Legal conditions apply to the issuance of the Vodafone Group CA certificates under this CP as described in this section.

9.1 Fees

The Vodafone Group charges Subscriber fees for the use of Vodafone Group CA products and services. The Vodafone Group retains its right to effect changes to such fees.

Communication of fees is done through the web site of the Vodafone Group CA, to partners or by contract where applicable.

During the validity period, the Vodafone Group CA charges a yearly fee per certificate issued.

Vodafone might charge separately for the use of services or resources that it makes available to end users of VACEE certificates.

9.1.1 Refund policy

Section not applicable.

9.2 Financial Responsibility

The Vodafone Group CA maintains warranty coverage for its conditional liability, as it might be required.

The Vodafone Group accepts no further liability beyond coverage under that limit.

9.3 Confidentiality of Business Information

The Vodafone Group CA observes personal data privacy rules and confidentiality rules as described in this Vodafone Group CP. Confidential information includes:

- Any personal identifiable information on subscribers, other than that contained in a certificate.
- Reason for the revocation or suspension of a certificate, other than that contained in published certificate status information.
- Audit trails.
- Correspondence regarding CA services.
- CA Private key(s).

The following items are not confidential information:

- Certificates and their content.
- Status of a certificate.

The Vodafone Group CA does not release nor is it required to release any confidential information without an authenticated and justified request specifying either:

- The party to whom the Vodafone Group CA owes a duty to keep information confidential as the party requesting such information.
- A court order.

The Vodafone Group CA may charge an administrative fee to process such disclosures.

Parties requesting and receiving confidential information are granted permission on the assumption that they use it for the requested purposes, secure it from compromise, and refrain from using it or disclosing it to third parties.

9.3.1 Disclosure Conditions

Non-confidential information can be disclosed to any Subscriber or Relying Party under the conditions below:

- Only a single certificate is delivered per inquiry by Subscriber or Relying Party.
- The status of a single certificate is provided per inquiry by a Subscriber or Relying Party.
- Subscribers can consult the information the CA holds about them.

Confidential information may not be disclosed to subscribers nor relying parties. The Vodafone Group CA properly manages the disclosure of information to the CA personnel.

The Vodafone Group CA authenticates itself to any party requesting the disclosure of information by:

- Presenting an authentication certificate at the request of the Subscriber or Relying Party.
- Signing responses to OCSP requests and CRLs.

The Vodafone Group CA encrypts all communications of confidential information including:

- The communications link between the CA and the RAs.
- Sessions to deliver certificates and certificate status information.

9.4 Privacy of Personal Information

The Vodafone Group CA may make available a specific Privacy Policy for the protection of personal data of the applicant seeking a Vodafone Group CA certificate through its web site http://ca.vodafone.com and/or the CP.

The Vodafone Group CA operates within the boundaries of the Data Protection Act of 1998 as it applies in England and Wales.

The regulation on the protection of personal data in the United Kingdom implements the European Union Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

The Vodafone Group CA also acknowledges Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector. The Vodafone Group CA operates within the conditions for the protection of personal data asserted in this Certificate Policy.

9.5 Intellectual Property Rights

The Vodafone Group CA owns and reserves all intellectual property rights associated with its databases, web sites, Vodafone Group CA digital certificates and any other publication whatsoever originating from the Vodafone Group CA including this CP.

The names of all CAs of the Vodafone Group CA remain the sole property of Vodafone Group, which enforces these rights.

Certificates are and remain property of the Vodafone Group CA. The Vodafone Group CA permits the reproduction and distribution of certificates on a non-exclusive, royalty-free basis, provided that they are reproduced and distributed in full. Certificates are not published in any publicly accessible repository or directory without the express written permission of the Vodafone Group CA. The scope of this restriction is also intended to protect subscribers against the unauthorised re-publication of their personal data featured on a certificate.

The Vodafone Group CA owns and reserves all intellectual property rights associated with its own products and services that it has not explicitly transferred or released to another party.

9.6 Representations and Warranties

The Vodafone Group CA uses this CP and a CPS, a Subscriber agreement and a statement of Obligations to Relying Parties to convey legal conditions of usage of Vodafone Group CA certificates to subscribers and relying parties.

Participants that may make representations and warranties include the Vodafone Group CA, RAs, subscribers, relying parties, and any other participants as it might become necessary.

All parties of the Vodafone Group CA domain, including the Vodafone Group CA, RAs and subscribers warrant the integrity of their respective private key(s). If any such party suspects that a private key has been compromised they will immediately notify the appropriate RA.

9.6.1 Subscriber Obligations

Unless otherwise stated in this CP, subscribers are responsible for:

- Having knowledge and, if necessary, seeking training on using digital certificates and PKI.
- Generating securely their private-public key pair, using a trustworthy system.
- Providing correct and accurate information in their communications with the Vodafone Group CA.
- Ensuring that the public key submitted to the Vodafone Group CA correctly corresponds to the private key used.
- Accepting all terms and conditions in the Vodafone Group CA CPS and associated policies published in the Vodafone Group CA Repository.
- Refraining from tampering with a Vodafone Group CA certificate.
- Using Vodafone Group CA certificates for legal and authorised purposes in accordance with this Vodafone Group CP.
- Notifying the Vodafone Group CA or a Vodafone Group RA of any changes in the information submitted.
- Ceasing to use a Vodafone Group CA certificate if any featured information becomes invalid.
- Ceasing to use a Vodafone Group CA certificate when it becomes invalid.
- Removing a Vodafone Group CA certificate when invalid from any applications and/or devices they have been installed on.
- Using a Vodafone Group CA certificate, as it may be reasonable under the circumstances.
- Preventing the compromise, loss, disclosure, modification, or otherwise unauthorised use of their private key (“loss” does not include controlled destruction of the key as defined below).
- Using secure devices and products that provide appropriate protection to their keys.
- For any acts and omissions of partners and agents subscribers use to generate, retain, escrow, or destroy any private keys.
- Refraining from submitting to the Vodafone Group CA or any Vodafone Group CA directory any material that contains statements that violate any law or the rights of any party.
- Requesting the suspension or revocation of a certificate in case of an occurrence that materially affects the integrity of a Vodafone Group CA certificate.
- Notifying the appropriate RA immediately, if a Subscriber becomes aware of or suspects the compromise of a private key.
- Destroying the private key in a controlled fashion after it has fulfilled its intended purpose to sign designated Code.

9.6.2 Relying Party Obligations

A party relying on a Vodafone Group CA certificate promises to:

- Have the technical capability to use digital certificates and PKI.
- Receive notice of the Vodafone Group CA and associated conditions for relying parties.
- Validate a Vodafone Group CA certificate by using the correct Vodafone root certificate and any suitable certificate status information (e.g. a CRL) published by the Vodafone Group CA in accordance with the proper certificate path validation procedure.
- Trust a Vodafone Group CA certificate only if all information featured on such certificate can be verified via such a validation procedure as being correct and up to date.
- Rely on a Vodafone Group CA certificate, only as it may be reasonable under the circumstances.
- Notify the appropriate RA immediately, if the Relying Party becomes aware of or suspects that a private key has been compromised.

9.6.3 Subscriber Liability Towards Relying Parties

Without limiting other Subscriber obligations stated elsewhere in this CP, subscribers are liable for any misrepresentations they make in certificates to third parties that rely in good faith on the representations contained therein.

9.6.4 Vodafone Group CA Repository and Web site Conditions

The Parties (including subscribers and relying parties) accessing the Vodafone Group CA Repository and web site agree with the provisions of this CP and any other conditions of usage that Vodafone Group may make available. Parties demonstrate acceptance of the conditions of usage of the CP by submitting a query with regard to the status of a digital certificate or by anyway using or relying upon any such information or services provided. Here “using” such Vodafone Group CA information or services is defined as:

- Obtaining information provided as a result of the search for a digital certificate.
- Verifying the status of digital signatures created with a private key corresponding to a public key included in a certificate.
- Verifying the status of a digital certificate prior to encrypting data using the public key included in a certificate.
- Retrieving information published on the Vodafone Group CA web site.
- Any other services that Vodafone Group CA might advertise or provide through its web site.

If a Repository becomes aware of or suspects the compromise of a private key, it will immediately notify the appropriate RA. The party that operates a Repository has exclusive responsibility for all acts or omissions associated with it.

The Vodafone Group CA is responsible for maintaining a certificate repository during the application period and for a maximum of ten years thereafter. The repository will be made available to the RA for queries at any time, in order to verify the integrity of the complete repository.

The Vodafone Group CA repository is available to relying parties.

9.6.4.1 Reliance at Own Risk

It is the sole responsibility of the parties accessing information featured in the Vodafone Group CA Repositories and web site to assess and rely on information featured therein. Parties acknowledge that they have received adequate information to decide whether to rely upon any information provided in a certificate. The Vodafone Group CA takes all steps necessary to update its records and directories concerning the status of the certificates and to issue relevant warnings. Failure to comply with the conditions of usage of the Vodafone Group Repositories and web site may result in terminating the relationship between the Vodafone Group CA and the party.

9.6.4.2 Accuracy of Information

The Vodafone Group CA makes every effort to ensure that parties accessing its Repositories receive accurate, updated and correct information. The Vodafone Group CA, however, cannot accept any liability beyond the limits set in this CP and the Vodafone Group CA insurance policy.

9.6.5 Vodafone Group CA Obligations

To the extent specified in the relevant sections of the CP, the Vodafone Group CA promises to:

- Comply with this CP and its amendments as published under http://ca.vodafone.com/repository.
- Provide infrastructure and certification services, including the establishment and operation of the Vodafone Group CA Repository and web site for the operation of public PKI services.
- Provide Trust mechanisms, including a key generation mechanism, key protection, and secret sharing procedures regarding its own infrastructure.
- Provide prompt notice in case of compromise of its own private key(s).
- Provide and validate application procedures for the various types of certificates that it makes publicly available.
- Issue electronic certificates in accordance with this CP and fulfil its obligations presented herein.
- Revoke certificates issued according to this CP upon receipt of a valid and authenticated request to revoke a certificate from an RA.
- Publish accepted certificates in accordance with this CP.
- Provide support to subscribers and relying parties as described in this CP.
- Provide for the expiration and renewal of certificates according to this CP.
- Publish CRLs and/or OCSP responses of all suspended and revoked certificates on a regular basis in accordance with this CP.
- Provide appropriate service levels according to a service agreement.
- Notify relying parties of certificate revocation by publishing CRLs on the Vodafone Group CA repository.

The liability of the Vodafone Group CA under the above stated article for proven damages, directly caused by the occurrences listed above, is limited to one million GBP (£1 million) total for any individual VACEE certificate.

To the extent permitted by law the Vodafone Group CA cannot be held liable for:

- Any use of certificates, other than that specified in this CP or specified in the Laws of England and Wales.
- Improper use or configuration of equipment, not operated under the responsibility of the CA, used in a transaction involving certificates.
- Any use of certificates, other than reliance on the information contained in valid certificates.
- Any reliance on the information contained in invalid (revoked, suspended or expired) certificates, or in free, test or demo certificates.
- The use of public or private keys of cross-certified (non-subordinate) CA's and their relying parties.
- Acts of God.

The Vodafone Group CA acknowledges it has no further obligations under this CP.

9.6.6 Registration Authority Obligations

A Vodafone Group RA operating within the Vodafone Group CA VELCA network promises to:

- Generate securely an RA administrator key pair, using a trustworthy system directly or through an agent.
- Provide correct and accurate information in their communications with the Vodafone Group CA.

- Ensure that the public key submitted to the Vodafone Group CA is the correct one (if applicable).
- Generate a new, secure key pair to be used in association with a certificate that they request from Vodafone Group CA.
- Receive applications for Vodafone Group CA certificates in accordance with this Vodafone Group CA CP.
- Carry out all verification and authenticity actions prescribed by this Vodafone Group CA CP.
- Submit to the Vodafone Group CA the applicant's request in a signed message (certificate request).
- Record all actions in an event log.
- Receive, verify and relay to the Vodafone Group CA all requests for revocation of a Vodafone Group CA certificate in accordance with this Vodafone Group CA CP.
- Verify the accuracy and authenticity of the information provided by the subscriber at the time of renewal of a certificate according to this CP.

9.6.7 Information incorporated by reference into a digital certificate

The Vodafone Group CA incorporates by reference the following information in every digital certificate it issues:

- Terms and conditions of the corresponding CP (indicated by the policy identifier) as well as of the Vodafone Group CA CPS.
- Any other applicable certificate policy as may be stated on an issued Vodafone Group CA certificate.
- The mandatory elements of the standard X.509.
- Any non-mandatory but customised elements of the standard X.509.
- Content of extensions and enhanced naming that are not fully expressed within a certificate.
- Any other information that is indicated to be so in a field of a certificate.

9.6.8 Pointers to incorporate by reference

To incorporate information by reference the Vodafone Group CA uses computer-based and text-based pointers. The Vodafone Group CA may use URLs, OIDs etc.

9.7 Disclaimers of Warranties

This section includes disclaimers of express warranties.

9.7.1 Limitation for Other Warranties

The Vodafone Group CA does not warrant:

- The accuracy of any piece of information provided in conjunction with, but not contained in, certificates except as it may be stated in the relevant product description in this CP and in the Vodafone Group CA warranty policy, if available.
- The accuracy, authenticity, completeness or fitness of any information contained in invalid certificates (whether revoked, suspended or expired), or in free, test or demo certificates.

9.7.2 Exclusion of Certain Elements of Damages

In no event (except for fraud or wilful misconduct) is the Vodafone Group CA liable for:

- Any loss of profits.
- Any loss of data.
- Any indirect, consequential or punitive damages arising from or in connection with the use, delivery, license, and performance or non-performance of certificates or digital signatures.
- Any transactions or services offered outside the framework of this CP.
- Any damages caused by reliance on the information contained in invalid certificates (whether revoked, suspended or expired).

- Any other damages except for those directly caused by reliance on erroneous information in a valid certificate (not including information featured on, free, test or demo certificates).

9.8 Limitations of Liability

The total liability of the Vodafone Group CA is limited in accordance with the limits published by the Vodafone Group.

9.9 Indemnities

This section contains the applicable indemnities.

9.9.1 Indemnity

To the extent permitted by law the Subscriber agrees to indemnify and hold the Vodafone Group harmless from any acts or omissions resulting in liability, any loss or damage, and any suits and expenses of any kind, including reasonable attorneys' fees that the Vodafone Group may incur as a result of:

- **Any false or misrepresented data supplied by the Subscriber or its agent(s).**
- **Any failure of the Subscriber to disclose a material fact, if the misrepresentation or omission was made negligently or with intent to deceive the Vodafone Group or any person receiving or relying on the certificate.**
- **Failure to protect the Subscriber's private key, to use a trustworthy system as required, or to take precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorised use of the Subscriber's private key or to attend to the integrity of the Vodafone Group CA's Root certificate(s).**
- **Breaking any laws applicable in his/her country or territory including those related to intellectual property protection, viruses, accessing computer systems etc.**

9.10 Term and Termination

This CP remains in force until or unless otherwise notified by the Vodafone Group CA on its web site or repository.

Notified changes are appropriately marked by an indicated version. Following publications, changes become applicable 30 days thereafter.

9.11 Individual notices and communications with participants

The Vodafone Group CA accepts notices related to this CP by means of digitally signed messages or in paper form. Upon receipt of a valid, digitally signed acknowledgment of receipt from the Vodafone Group CA the sender of the notice deems its communication effective. The sender must receive such acknowledgment within five (5) days, or else written notice must then be sent in paper form through a courier service that confirms delivery or via certified or registered mail, postage prepaid, return receipt requested, addressed as follows. Individual communications made to the Vodafone Group CA must be addressed to: ca@vodafone.com or by post to the Vodafone Group CA at the address mentioned in the introduction of this document.

9.12 Amendments

Minor changes to this CP that do not materially affect the assurance level of this CP are indicated by a version number that contains a decimal number e.g. version 1.1 for a version with minor changes as opposed to version 2.0 that addresses major issues.

Minor changes to this Vodafone Group CA CP do not require a change in the CP OID or the CP pointer (URL) that might be communicated by the Vodafone Group CA. Major changes may materially change the acceptability of certificates for specific purposes, and these changes may require corresponding changes to the CP OID or CP pointer qualifier (URL).

The Vodafone Group CA Policy Management Authority decides on the numbering of versions.

9.13 Dispute Resolution Procedures

Section not applicable.

9.14 Governing Law

This CP is governed by the laws of England and Wales. This choice of law is made to ensure uniform interpretation of this CP, regardless of the place of residence or place of use of Vodafone Group CA digital certificates or other products and services. The laws of England and Wales apply also to all Vodafone Group commercial or contractual relationships in which this CP may apply or be quoted implicitly or explicitly in relation to Vodafone Group products and services where the Vodafone Group acts as a provider, supplier, beneficiary receiver or otherwise. Any claim or matter arising under or in connection with this CP.will be submitted to the exclusive jurisdiction of the English Courts.

9.15 Compliance with Applicable Law

The Vodafone Group CA complies with applicable laws of England and Wales. Export of certain types of software used in certain Vodafone Group CA public PKI products and services may require the approval of appropriate public or private authorities. Parties (including Vodafone Group CA partners, subscribers and relying parties) agree to conform to applicable export laws and regulations as pertaining in England and Wales.

9.16 Miscellaneous Provisions

The following additional provisions also apply.

9.16.1 Survival

The obligations and restrictions contained under the section “Other Business and Legal Matters” survive the termination of this CP.

9.16.2 Severability

If any provision of this CP, including limitation of liability clauses, is found to be invalid or unenforceable, the remainder of this CP shall be interpreted in such manner as to effect the original intention of the parties.

10. LIST OF DEFINITIONS

ACCEPT (A CERTIFICATE)
To approve of a digital certificate by a certificate applicant within a transactional framework.
ACCREDITATION
A formal declaration by an approving authority that a certain function/entity meets specific formal requirements.
APPLICATION FOR A CERTIFICATE
A request sent by a certificate applicant to a CA to issue a digital certificate.
ARCHIVE
To store records for period of time for purposes such as security, backup, or audit.
ASSURANCES
A set of statements or conduct aiming at conveying a general intention.
AUDIT
Procedure used to validate compliance with formal criteria or controls.
AUTHENTICATED RECORD
A signed document containing assurances of authentication or a message with a digital signature verified by a valid Personalsign 2 certificate by a Relying Party.
AUTHENTICATION
A process used to confirm the identity of a person or to prove the integrity of specific information by placing them within the right context and verifying such relationship.
AUTHORISATION
Granting of rights.
AVAILABILITY
The rate of accessibility of information or resources.
BINDING
A statement by an RA of the relationship between a named entity and its public key.
CERTIFICATE
The public key of a subject and the associated information, digitally signed with the private key of the issuer of the certificate. Unless explicitly specified, the certificates described here are the Subscriber's ones.
CERTIFICATE REVOCATION LIST OR **CRL**
A list maintained by the CA of certificates that are revoked before their expiration time.
CERTIFICATION AUTHORITY OR **CA**
An entity that is trusted to associate a public key to the information on the subject, contained in the certificate. Unless explicitly specified, the CA described herein is the Vodafone Group CA.
CERTIFICATION PRACTICE STATEMENT OR **CPS**
A statement of the practices in the management of certificates during all life phases.
CERTIFICATE STATUS SERVICE OR **CSS**
A service, enabling relying parties and others to verify the status of certificates.
CONTRACT PERIOD
The duration of the Vodafone Group CA contract between the Subscriber or Relying Party and the CA organization.
CERTIFICATE CHAIN
A hierarchical list of certificates containing an end-user Subscriber certificate and CA certificates.
CERTIFICATE EXPIRATION
The end of the validity period of a digital certificate.
CERTIFICATE EXTENSION
A field in the digital certificate used to convey additional information on issues that include: the public key, the certified subject, the certificate issuer, and/or the certification process.
CERTIFICATE HIERARCHY
A level based sequence of certificates of one (root) CA and subordinate entities that include CAs and subscribers.
CERTIFICATE MANAGEMENT
Actions associated with certificate management include storage, dissemination, publication, revocation, and suspension of certificates.
CERTIFICATE REVOCATION LIST (CRL)
A list issued and digitally signed by a CA that includes revoked and suspended certificates. Such a list is to be consulted by relying parties at all times prior to relying on information featured in a certificate.
CERTIFICATE SERIAL NUMBER
A sequential number that uniquely identifies a certificate within the domain of a CA.
CERTIFICATE SIGNING REQUEST (CSR)
A machine-readable application form to request a digital certificate.
CERTIFICATION
The process to issue a digital certificate.
CERTIFICATION AUTHORITY (CA)
An authority, such as the Vodafone Group CA that issues, suspends, or revokes a digital certificate.
CERTIFICATE POLICY (CP)
A statement of the practices of a CA and the conditions of issuance, suspension, revocation etc. of a certificate. A CP is also used as guidance to establish the trustworthiness of a certification services infrastructure.

CERTIFICATE ISSUANCE
Delivery of X.509 v3 digital certificates for authentication and digital signature based on personal data and public keys provided by the RA and compliant with RFC 2527 and RFC 3039

CERTIFICATE SUSPENSION
Online service used to temporarily disable a digital certificate and to automatically revoke it if no request for re-activating it is submitted within a certain time period

CERTIFICATE REVOCATION
Online service used to permanently disable a digital certificate before its expiration date

CERTIFICATE REVOCATION LISTS
Online publication of complete and incremental digital certificates revocation lists compliant with RFC 3280.

COMMERCIAL REASONABLENESS
A legal term from Common Law. In electronic commerce it means the usage of technology that provide reasonable assurance of trustworthiness.

COMPROMISE
A violation of a security policy that results in loss of control over sensitive information.

CONFIDENTIALITY
The condition to disclose data to selected and authorised parties only.

CONFIRM A CERTIFICATE CHAIN
To validate a certificate chain in order to validate an end-user Subscriber certificate.

DIGITAL CERTIFICATE
A formatted piece of data that relates an identified subject with a public key the subject uses.

DIGITAL SIGNATURE
To encode a message by using an asymmetric cryptosystem and a hash function such that a person having the initial message and the signer's public key can accurately determine whether the transformation was created using the private key that corresponds to the signer's public key and whether the initial message has been altered since the transformation was made.

DISTINGUISHED NAME
A set of data that identifies a real-world entity, such as a person in a computer-based context.

DIRECTORY SERVICE
Online publication of certificates allowing the retrieval of a certificate based on its certificate identifier.

END-USER SUBSCRIBER
A Subscriber other than another CA.

ENHANCED NAMING
The usage of an extended organisation field (OU=) in an X.509 v.3.0 certificate.

EXTENSIONS
Extension fields in X.509 v.3.0 certificates.

GENERATE A KEY PAIR
A trustworthy process to create private keys during certificate application whose corresponding public key are submitted to the applicable CA during certificate application in a manner that demonstrates the applicant's capacity to use the private key.

HARDWARE MODULE
The complete system of the hardware module used to keep the certificates and securely generate a key pair.

HASH
An algorithm that maps or translates one set of bits into another (generally smaller) set in such a way that:

- A message yields the same result every time the algorithm is executed using the same message as input.
- It is computationally infeasible for a message to be derived or reconstituted from the result produced by the algorithm.
- It is computationally infeasible to find two different messages that produce the same hash result using the same algorithm.

IDENTIFICATION
The process to confirm the identity of an entity. Identification is facilitated in public key cryptography by means of certificates.

INCORPORATE BY REFERENCE
To make one document a part of another by identifying the document to be incorporated, with information that allows the recipient to access and obtain the incorporated message in its entirety, and by expressing the intention that it be part of the incorporating message. Such an incorporated message shall have the same effect as if it had been fully stated in the message.

KEY GENERATION PROCESS
The trustworthy process of creating a private/public key pair. The public key is supplied to a CA during the certificate application process.

KEY PAIR
A private key and its corresponding public key in asymmetric encryption.

NOTICE
The result of notification to parties involved in receiving CA services in accordance with this CP.

NOTIFY
To communicate specific information to another person as required by this CP and applicable law.

NOTARISED TIME STAMPING
Online service used to timestamp and securely archive a document; the document is re-timestamped on a regular basis with up-to-date technology.

ONLINE CERTIFICATE STATUS PROTOCOL (OCSP)
Online service used to provide information on a certificate's validity, defined by RFC 2560.

OBJECT IDENTIFIER (OID)
A sequence of integer components that can be assigned to a registered object and that has the property of being unique among all object identifiers within a specific domain.
PKI HIERARCHY
A set of CAs whose functions are organised according to the principle of delegation of authority and related to each other as subordinate and superior CA.
PRIVATE KEY
A mathematical key to create digital signatures and sometimes (depending upon the algorithm) to decrypt messages in combination with the corresponding public key.
PUBLIC KEY
A mathematical key that can be made publicly available that is used to verify signatures created with its corresponding private key. Depending on the algorithm, public keys can also be used to encrypt messages or files which can then be decrypted with the corresponding private key.
PUBLIC KEY CRYPTOGRAPHY
Cryptography that uses a key pair of mathematically related cryptographic keys.
PUBLIC KEY INFRASTRUCTURE (PKI)
The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a certificate-based public key cryptographic system.
REGISTRATION AUTHORITY OR **RA**:
An entity that has the responsibility to identify and authenticate subscribers. The RA does not issue certificates. It merely requests the issuance of a certificate on behalf of applicants whose identity it has verified.
RELATIVE DISTINGUISHED NAME (RDN)
A set of attributes that distinguishes the entity from others of the same type.
RELIANCE
To accept a digital signature and act in a way that shows trust in it.
RELYING PARTY
Any entity that relies on a certificate for carrying out any action.
REPOSITORY
A database and/or directory listing digital certificates and other relevant information accessible on-line.
REVOKE A CERTIFICATE
To permanently end the operational period of a certificate from a specified time forward.
SECRET SHARE
A portion of a cryptographic secret that has been divided among a number of physical tokens, such as smart cards etc.
SECRET SHARE HOLDER
An person that holds a secret share.
SHORT MESSAGE SERVICE (SMS)
A service for sending messages of up to 160 characters (224 characters if using a 5-bit mode) to mobile phones that use Global System for Mobile (GSM) communication.
SIGNATURE
A method that is used or adopted by a document originator to identify himself or herself, which is either accepted by the recipient or its use is customary under the circumstances.
SIGNER
A person who creates a digital signature for a message, or a signature for a document.
SMART CARD
A hardware token that contains a chip to implement among others cryptographic functions.
STATUS VERIFICATION
Online service based on the Online Certificate Status Protocol (RFC 2560) used to determine the current status of a digital certificate without requiring CRLs
SUBJECT OF A DIGITAL CERTIFICATE
The named party to which the public key in a certificate is attributable, as user of the private key corresponding to the public key.
SUBSCRIBER
The subject of a digital certificate, or a party designated by the subject to apply for the certificate.
SUBSCRIBER AGREEMENT
The agreement between a Subscriber and a CA for the provision of public certification services.
SUSPENDED CERTIFICATE
Temporarily discarded certificate, which nevertheless is kept on hold for one week until revocation or reactivation notice is given to the Vodafone Group CA by the RA.
TRUSTED POSITION
A role within a CA that includes access to or control over cryptographic operations that may allow for privileged access to the issuance, use, suspension, or revocation of certificates, including operations that restrict access to a repository.
TRUSTWORTHY SYSTEM
Computer hardware, software, and procedures that provide an acceptable level against security risks, provide a reasonable level of availability, reliability, and correct operation and enforce a security policy.
VODAFONE BRAND ROOT (VBR)
The top-level CA of the Vodafone Group CA.
VODAFONE GROUP CA REGISTRATION AUTHORITY:
An entity that verifies and provides all Subscriber data to the Vodafone Group CA.
VODAFONE GROUP CA PUBLIC CERTIFICATION SERVICES
A digital certification system made available by Vodafone Group CA as well as the entities that belong to the Vodafone Group CA domain as described in this CP.

VODAFONE GROUP CA PROCEDURES
A document describing the Vodafone Group CA's internal procedures with regard to registration of end users, security etc.
VODAFONE EXECUTABLE LAYER 2048 BIT CA (VELCA)
An operational CA of the Vodafone Group CA that issues code-signing certificates to end-user subscribers.
WEB -- WORLD WIDE WEB (WWW)
A graphics based medium for the document publication and retrieval of information on the Internet.
WRITING
Information accessible and usable for reference.
X.509
The standard of the ITU-T (International Telecommunications Union-T) for digital certificates.