INDEPENDENT CERTIFIED PUBLIC ACCOUNTANT'S REPORT ON APPLYING AGREED-UPON PROCEDURES

January 30, 2017

Benjamin Wilson
VP Compliance
DigiCert, Inc.

Dear Mr. Wilson:

I have performed the procedures on the accompanying pages, which were agreed to by the management of DigiCert, Inc., with respect to examining the conformance of selected criteria of Vodafone Groups's Vodafone Corporate Domain 2009 Root CA and its Vodafone Corporate Services 2009 Issuing CA as of January 27, 2017.

This agreed-upon procedures engagement was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. The sufficiency of these procedures is solely the responsibility of DigiCert Inc. Consequently, I make no representation regarding the sufficiency of the procedures described below either for the purpose for which this report has been requested or for any other purpose.

I was not engaged to and did not conduct an audit, the objective of which would be the expression of an opinion on the sufficiency of these procedures. Accordingly, I do not express such an opinion. The scope of these procedures was limited to Certification Authorities mentioned above during the fieldwork period of January 25, 2017 through January 27, 2017. I did not extend my procedures normally associated with a full-scope WebTrust report. Had I performed additional procedures, other matters might have come to my attention that would have been reported to you.

This report is intended solely for the information and use of the management of DigiCert Inc, Vodafone, Microsoft, Google and Mozilla and is not intended to be and should not be used by anyone other than these specified parties.

Scott S. Perry CPA, PLLC

Scott S. Perry CPA, PLLC
Bellevue, Washington

Agreed-Upon Procedures Criteria	Procedures Performed	Procedure Notes	Procedure Results
The CA maintains controls to provide reasonable assurance that: • security is planned, managed and supported within the organization; • security risks are identified and managed; • the security of CA facilities, systems and information assets accessed by third parties is maintained; and • the security of subscriber and relying party information is maintained when the responsibility for CA sub-functions has been outsourced to another organization or entity.	Corroborated risk assessment and security organization with management. Toured data center.	The security organization is compartmentalized throughout the enterprise. There are risk assessment, security architecture, design and operation teams that are organized into separate groups that work independently. Security appears to be taken seriously and is an integral part of development and deployment of operational solutions including the PKI.	No exceptions noted
The CA maintains controls to provide reasonable assurance that: • physical access to CA facilities and equipment is limited to authorized individuals, protected through restricted security perimeters, and is operated under multiple person (at least dual custody) control; • CA facilities and equipment are protected from environmental hazards; • loss, damage or compromise of assets and interruption to business activities are prevented; and • compromise of information and information processing facilities is prevented.	Toured the data center housing the in-scope CAs and supporting HSM devices. Reviewed access and contents to safe containing key material and access cards for CA system.	Our visit purpose was highly scrutinized by surety guards at the data center entrance. Visitors have restricted escort privileges that limit access to physical zones with man traps that validate single occupancy. Environmental controls are addressed with redundant power and, chillers and facilities.	No exceptions noted.

Agreed-Upon Procedures Criteria	Procedures Performed	Procedure Notes	Procedure Results
The CA maintains controls to provide reasonable assurance that: the correct and secure operation of CA information processing facilities is ensured; the risk of CA systems failure is minimized; the integrity of CA systems and information is protected against viruses and malicious software; damage from security incidents and malfunctions is minimized through the use of incident reporting and response procedures; and media are securely handled to protect them from damage, theft and unauthorized access.	Reviewed network configuration and hardening standards used for all operational level servers. Corroborated use of systems monitoring tools that alert upon predetermined events.	Standards and processes appear commensurate with reliable production grade standards.	No exceptions noted.
The CA maintains controls to provide reasonable assurance that CA system access is limited to authorized individuals. Such controls provide reasonable assurance that: • operating system and database access is limited to authorized individuals with predetermined task privileges; • access to network segments housing CA systems is limited to authorized individuals, applications and services; and • CA application use is limited to authorized individuals.	Reviewed access rights to CA systems	Two people can manage the CA. This done remotely from Vodafone support operations in India. Four people can issue and manage certificates. Rights are adequately segregated to require two individuals to handle an issuance and revocation from beginning to end.	No exception noted.
The CA maintains controls to provide reasonable assurance that CA keys are used only for their intended functions in their predetermined locations.	Reviewed key part storage in locked safe. Toured data center and identified HSM model to NIST FIPS 140-2 website.	Backup keys are comingled with pins in the office safe potentially allowing staff to circumvent multi-person control of keys. Offline Root and Online Issuing CA HSMs are older nCipher models but compliant with FIPS 140-2.	Minor exception noted.

Agreed-Upon Procedures Criteria	Procedures Performed	Procedure Notes	Procedure Results
The CA maintains controls to provide reasonable assurance that: For authenticated certificates • Subscribers are accurately identified in accordance with the CA's disclosed business practices; and • Subscriber's certificate requests are accurate, authorized and complete. For domain validated certificates • Subscribers' domain names are accurately validated in accordance with the CA's disclosed business practices; and • Subscriber's certificate requests are accurate and complete.	Walked through subscriber registration process and subscriber agreement form. Examined sample CSR.	Subscribers appear properly vetted as Vodafone employees or must have a designated system owner liaison. Controls enforce use of approvals for requests. RA system automatically interrogates CSR format for errors.	No exceptions noted.
The CA maintains controls to provide reasonable assurance that Root, Subordinate, and Subscriber certificates generated by the CA contain certificate serial numbers greater than zero (0) containing at least 64 bits of output from a CSPRNG.	Examined available certificate profiles	Noted that there is no available SSL certificate profile which would allow the generation of SSL certificates.	Not applicable
The CA maintains controls to provide reasonable assurance that the extensions, key sizes, and certificate policy identifiers (including Reserved Certificate Policy Identifiers) of Subscriber certificates generated after the Effective Date (1 July 2012) conform to the Baseline Requirements.	Examined available certificate profiles	Noted that there is no available SSL certificate profile which would allow the generation of SSL certificates.	Not applicable
The CA maintains controls to provide reasonable assurance that the validity period of Subscriber certificates issued after the Effective Date (1 July 2012) does not exceed the maximum as specified in the Baseline Requirements.	Examined available certificate profiles	Noted that there is no available SSL certificate profile which would allow the generation of SSL certificates.	Not applicable
The CA maintains controls to provide reasonable assurance that it does not issue any new Subscriber or Subordinate CA certificates using the SHA-1 hash algorithm.	Examined available certificate profiles	Noted that there is no available SSL certificate profile which would allow the generation of SSL certificates.	Not applicable
The CA maintains controls to provide reasonable assurance that for Subscriber certificates issued:	Examined available certificate profiles	Noted that there is no available SSL certificate	Not applicable

Agreed-Upon Procedures Criteria	Procedures Performed	Procedure Notes	Procedure Results
· The subjectAltName extension is present and contains at least one entry		profile which would allow the generation of SSL certificates.	
· Each entry MUST be either:			
o A dNSName containing the Fully-Qualified Domain Name (Wildcard FQDNs permitted); or			
o An iPAddress containing the IP address of a server.			
The CA maintains controls to provide reasonable assurance that it does not issue certificates containing a Reserved IP Address or Internal Name in the subjectAltName extension or subject:commonName field, and as of 1 October 2016, will revoke any certificate containing a Reserved IP Address or Internal Name.	Examined available certificate profiles	Noted that there is no available SSL certificate profile which would allow the generation of SSL certificates.	Not applicable
The CA maintains controls to provide reasonable assurance that Subject information of Certificates conforms to the Baseline Requirements, including:	Examined available certificate profiles	Noted that there is no available SSL certificate profile which would allow the generation of SSL certificates.	Not applicable
· subject:commonName			
· subject:organizationName (if applicable)			
· subject:countryName			
The CA maintains controls to provide reasonable assurance that it rejects a certificate request if the Public Key does not meet the requirements set forth in Sections 6.1.5, 6.1.6, or if it has a weak Private Key (such as a Debian weak key).	Walked through the certificate request and CSR generation process	Noted that keys and the CSR are generated together during the request process. System configuration standards control the format of appropriate key strengths.	No exception noted.

Agreed-Upon Procedures Criteria	Procedures Performed	Procedure Notes	Procedure Results
The CA maintains controls to provide reasonable assurance that as of the date the Certificate was issued, the CA obtains confirmation in accordance with the SSL Baseline Requirements Sections 3.2.2.4, 3.2.2.5, 3.2.2.6 and 4.2.2 related to the Fully-Qualified Domain Name(s) (including wildcard domains and new gTLDs (generic top-level domains)) and IP address(es) listed in the Certificate.	Examined available certificate profiles	Noted that there is no available SSL certificate profile which would allow the generation of SSL certificates.	Not applicable
The CA maintains controls to provide reasonable assurance that the following information provided by the Applicant is verified directly by performing the steps established by the SSL Baseline Requirements:	Examined available certificate profiles	Noted that there is no available SSL certificate profile which would allow the generation of SSL certificates.	Not applicable
· Identity (SSL Baseline Requirements Section 3.2.2.1)			
· DBA/Trade name (SSL Baseline Requirements Section 3.2.2.2)			
· Authenticity of Certificate Request (SSL Baseline Requirements Section 3.2.5)			
· Verification of Individual Applicant (SSL Baseline Requirements Section 3.2.3)			
· Verification of Country (SSL Baseline Requirements Section 3.2.2.3)			

Agreed-Upon Procedures Criteria	Procedures Performed	Procedure Notes	Procedure Results
The CA maintains controls to provide reasonable assurance that a process is available 24x7 that the CA is able to accept and respond to revocation requests and related inquiries, and that the CA provides a process for Subscribers to request revocation of their own certificates.	Walked through system management tools to maintain system uptime. Walked through revocation request process.	Vodafone uses tools such as Splunk, Remedy, Icinga, and Nagios to create alerts to administrators when incidents occur that threaten uptime. Corroborated with management that high availability has been maintained over the last few months. Revocation requests require approvals from Vodafone employees and are assigned to defined system owners to validate.	No exceptions noted.
The CA maintains controls to provide reasonable assurance that Subscriber Certificates are revoked within 24 hours if any of the following events occurs:	Walked through revocation reasons and subsequent processes	Revocations can be initiated by Subscribers or PKI administrators due to active monitoring of events. All revocation requests and subsequent actions are recorded on online databases which have been active since CA inception.	No exceptions found.
1. The Subscriber requests in writing that the CA revoke the Certificate;			
2. The Subscriber notifies the CA that the original certificate request was not authorized and does not retroactively grant authorization;			
3. The CA obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of SSL Baseline Requirements Sections 6.1.5 and 6.1.6;			
4. The CA obtains evidence that the Certificate was misused;			

Agreed-Upon Procedures Criteria	Procedures Performed	Procedure Notes	Procedure Results
5. The CA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use;			
6. The CA is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name or IP address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name);			
7. The CA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name;			
8. The CA is made aware of a material change in the information contained in the Certificate;			
9. The CA is made aware that the Certificate was not issued in accordance with these Requirements or the CA's Certificate Policy or Certification Practice Statement;			
10. The CA determines that any of the information appearing in the Certificate is inaccurate or misleading;			
11. The CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;			
12. The CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL/OCSP Repository;			
13. The CA is made aware of a possible compromise of the Private Key of the Subordinate CA used for issuing the Certificate;			

Agreed-Upon Procedures Criteria	Procedures Performed	Procedure Notes	Procedure Results
14. Revocation is required by the CA's Certificate Policy and/or Certification Practice Statement; or			
15. The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties (e.g. the CA/Browser Forum might determine that a deprecated cryptographic/signature algorithm or key size presents an unacceptable risk and that such Certificates should be revoked and replaced by CAs within a given period of time).			
The CA maintains controls to provide reasonable assurance that an online 24x7 Repository is provided that application software can use to automatically check the current status of all unexpired Certificates issued by the CA, and:	Examined format and availability of current CRL. Examined the serial number placement of a recently revoked certificate on CRL. Verified the use of OCSP.	There is a one day cycle for CRL issuance for Issuing CA. The root publishes its CRL annually. OCSP is updated in conjunction with the CRL issuance cycle.	No exceptions found.
· for the status of Subscriber Certificates:			
o If the CA publishes a CRL, then the CA shall update and reissue CRLs at least once every seven (7) days, and the value of the nextUpdate field must not be more than ten (10) days beyond the value of the thisUpdate field; and			
o The CA shall update information provided via an Online Certificate Status Protocol (OCSP) at least every four (4) days and OCSP responses must have a maximum expiration time of ten (10) days.			
· for the status of subordinate CA Certificates			
o The CA shall update and reissue CRLs at least (i) once every twelve (12) months and (ii) within 24 hours after revoking a Subordinate CA Certificate, and the value of the nextUpdate field must not be more than twelve months beyond the value of the thisUpdate field; and			

Agreed-Upon Procedures Criteria	Procedures Performed	Procedure Notes	Procedure Results
o The CA shall update information provided via an Online Certificate Status Protocol at least (i) every twelve (12) months and (ii) within 24 hours after revoking a Subordinate CA Certificate. · The CA makes revocation information available through an OCSP capability using the GET method for Certificates issued in accordance with the SSL Baseline Requirements.			
The CA maintains controls to provide reasonable assurance that the CA records details of the actions taken to process a certificate request and to issue a Certificate, including all information generated and documentation received in connection with the certificate request; the time and date; and the personnel involved.	Examined all supporting documentation of certificate requests	Relevant actions taken with certificate requests are recorded and stored on the self-developed Registration Authority database. Records go back to CA inception.	No exceptions noted.
The CA maintains controls to provide reasonable assurance that all documentation relating to certificate requests and the verification thereof, and all Certificates and revocation thereof, is retained for at least seven years after any Certificate based on that documentation ceases to be valid.	Examined all supporting documentation of certificate requests	Relevant actions taken with certificate requests are recorded and stored on the self-developed Registration Authority database. Records go back to CA inception.	No exceptions noted.
The CA maintains controls to provide reasonable assurance that: · it performs ongoing self-assessments on at least a quarterly basis against a randomly selected sample of at least three percent (3%) of the Certificates issued during the period commencing immediately after the previous self-assessment samples was taken,	Inquired of management of self-assessments of certificates	Management was not aware of this requirement and has not deployed any self-assessment of certificates. Noted that there is no available SSL certificate profile which would allow the generation of SSL certificates.	Exception noted.

Agreed-Upon Procedures Criteria	Procedures Performed	Procedure Notes	Procedure Results
The CA maintains controls to provide reasonable assurance that it enforces multi-factor authentication for all accounts capable of directly causing certificate issuance.	Walked through access controls over Root and Issuing CA certificate issuance. Examined multi-factor devices used in accessing offline Root CA	Cards and Pins are required for access to Root CA. Issuing CA requires hardware token inserted remotely.	No exceptions noted.
The CA maintains controls to provide reasonable assurance that certificate Systems are segmented into networks or zones based on their functional, logical, and physical (including location) relationship.	Examined network configuration of CA	CA infrastructure is segmented into a zone with other internal business applications and not in its own zone.	Minor exception noted.
The CA maintains controls to provide reasonable assurance that recommended security patches are applied to Certificate Systems within six months of the security patch's availability, unless the CA documents that the security patch would introduce additional vulnerabilities or instabilities that outweigh the benefits of applying the security patch.	Walked through patch management of CA operating system	Patch management is applied at an enterprise level without regard for the complexity and sensitivity of CA operations.	Minor exception noted.
The CA maintains controls to provide reasonable assurance that the responsibilities and tasks assigned to Trusted Roles are documented and "separation of duties" for such Trusted Roles based on the risk assessment of the functions to be performed is implemented.	Examined role position descriptions and job segregation scheme. Exaimed "MofN" security world scheme for access to CA private keys.	Job descriptions are documented in an operational manual. M of N is set to require 2 of three individuals to access CA private keys; however, all key parts and access codes are comingled in one safe allowing this segregation to be circumvented.	Minor exception noted.
The CA maintains controls to provide reasonable assurance that employees and contractors observe the principle of "least privilege" when accessing, or when configuring access privileges on, Certificate Systems.	Reviewed access rights to CA systems.	See previous notes	No exceptions noted

Agreed-Upon Procedures Criteria	Procedures Performed	Procedure Notes	Procedure Results
The CA maintains controls to provide reasonable assurance that it enforces multi-factor authentication for administrator access to Issuing Systems and Certificate Management Systems.	Examine use of multi-factor authentication for administrators.	System requires both Card and PIN for administration access to Issuing Systems and Certificate management Systems	No exceptions noted.
The CA maintains controls to provide reasonable assurance that a Penetration Test is performed on the CA's and each Delegated Third Party's Certificate Systems on at least an annual basis and after infrastructure or application upgrades or modifications that the CA determines are significant.	Examine latest system penetration test report	Latest report is from January 2014 which included PKI CA portal, and CA infrastructure.	Minor exception noted.