Building a better
working world

Ernst & Young
Réviseurs d'Entreprises
Bedrijfsrevisoren
De Kleetlaan 2
B - 1831 Diegem

Tel: +32 (0)2 774 91 11
Fax: +32 (0)2 774 90 90
ey.com

INDEPENDENT ASSURANCE REPORT

To the management of Verizon Terremark NV ("Verizon Terremark"):

Scope

We have been engaged, in a reasonable assurance engagement, to report on Verizon Terremark management's assertion that for its Certification Authority services (Managed Identity and Access Management Services) at Culliganlaan 2E, Diegem (Belgium) on the Certificate Authorities as enumerated in Appendix A ("Subject Matter"). Verizon Terremark has designed and implemented controls as at September 13, 2019, in accordance with the WebTrust Principles and Criteria for Certification Authorities, Version 2.2 at Appendix B ("Criteria").

Certification authority's responsibilities

Verizon Terremark's management is responsible for its assertion, including the fairness of its presentation, and the provision of its described services in accordance with the WebTrust Principles and Criteria for Certification Authorities, Version 2.2 criteria at Appendix B.

Our independence and quality control

We have complied with the independence and other ethical requirements of the *Code of Ethics for Professional Accountants* issued by the International Ethics Standards Board for Accountants, which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

The firm applies International Standard on Quality Control 1, and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Auditor's responsibilities

Our responsibility is to express an opinion on management's assertion based on our procedures. We conducted our procedures in accordance with International Standard on Assurance Engagements 3000, *Assurance Engagements Other than Audits or Reviews of Historical Financial Information*, issued by the International Auditing and Assurance Standards Board. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, management's assertion is fairly stated, and, accordingly, included:

1. obtaining an understanding of Verizon Terremark's key and certificate lifecycle management business practices and its controls over key and certificate integrity, over the authenticity and confidentiality of subscriber and relying party information, over the continuity of key and certificate lifecycle management operations and over development, maintenance and operation of systems integrity;
2. evaluating the suitability of the design of the controls; and
3. performing such other procedures as we considered necessary in the circumstances.

We did not perform procedures to determine the operating effectiveness of controls for any period. Accordingly, we express no opinion on the operating effectiveness of any aspects of Verizon Terremark's controls, individually or in the aggregate.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

Suitability of controls

The suitability of the design of the controls at Verizon Terremark and their effect on assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls, and other factors present at individual subscriber and relying party locations. We have performed no procedures to evaluate the suitability of the design of the controls at individual subscriber and relying party locations.

Inherent limitations

Because of the nature and inherent limitations of controls, Verizon Terremark's ability to meet the aforementioned criteria may be affected. For example, controls may not prevent, or detect and correct, error, fraud, unauthorized access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

Restriction on use

This report is intended solely for the information and use of Verizon management, Digicert management, representatives of the browsers, and representatives of the trust stores, and should not be used by anyone other than these specified parties

Opinion

In our opinion, as at September 13, 2019, Verizon Terremark's management's assertion, as referred to above, is fairly stated, in all material respects, in accordance with the WebTrust Principles and Criteria for Certification Authorities, Version 2.2 criteria at Appendix B.

This report does not include any representation as to the quality of Verizon Terremark's services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities, Version 2.2 criteria at Appendix B, nor the suitability of any of Verizon Terremark's services for any customer's intended purpose.

Brussels, September 19, 2019

Ernst & Young Bedrijfsrevisoren cvba
Diegem, Belgium

Weymeersch

Christel Weymeersch*

Partner

* Acting on behalf of a bvba

verizon

Verizon Terremark's Management's Assertion - CA

Verizon Terremark NV ("Verizon Terremark") operates the Certification Authority (CA) services known as the CAs as disclosed in Appendix A and provides the following CA services:

- Subscriber registration
- Certificate renewal
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate validation

The management of Verizon Terremark is responsible for establishing and maintaining effective controls over its CA operations, including its CA business practices disclosure on its website, CA business practices management, CA environmental controls, CA key lifecycle management controls, subscriber key lifecycle management controls, certificate lifecycle management controls, and subordinate CA certificate lifecycle management controls. These controls contain monitoring mechanisms, and actions are taken to correct deficiencies identified.

There are inherent limitations in any controls, including the possibility of human error, and the circumvention or overriding of controls. Accordingly, even effective controls can only provide reasonable assurance with respect to Verizon Terremark's Certification Authority operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

Verizon Terremark management has assessed its disclosures of its certificate practices and controls over its Public Key Infrastructure providing Certification Authority (CA) services. Based on that assessment, in Verizon Terremark management's opinion, Verizon Terremark has designed and implemented controls supporting Certification Authority services (Managed Identity and Access Management Services) at Culliganlaan 2E, Diegem (Belgium) on the Certificate Authorities as enumerated in Appendix A ("Subject Matter") as at September 13, 2019, in accordance with the WebTrust Principles and Criteria for Certification Authorities, Version 2.2 at Appendix B ("Criteria"), including the following:

CA Environmental Controls

- Personnel Security
- Operations Management
- Business Continuity Management

CA Key Lifecycle Management Controls

- CA Key Destruction

Certificate Lifecycle Management Controls

- Certificate Issuance

Verizon Terremark
Culliganlaan 2E, Diegem (Belgium)

Signed by: Bruce R. Biesecker
Function: Director, Managed Security Services & Identity Management, Verizon Business Group

September 19, 2019

Appendix A – In-Scope CAs

OV SSL Issuing CAs		
#	Subject	SHA256 Hash

1	CN=Verizon Public SureServer CA G14-SHA2,
	OU=Cybertrust,
	O=Verizon Enterprise Solutions,
	L=Amsterdam,
	C=NL
		67:5c:1c:5d:bb:08:e9:fa:2c:81:7b:86:d5:fc:89:68:10:34:9a:2f:47:dd:64:93:8a:2b:ac:a6:49:97:c8:bb

Other CAs		
#	Subject	SHA

2	CN=Verizon Public SureCodeSign CA G14-SHA2,
	OU=Cybertrust,
	O=Verizon Enterprise Solutions,
	L=Amsterdam,
	C=NL
		fe:b9:15:62:8c:97:9e:06:f1:71:80:5d:6d:27:02:c0:27:04:20:bd:46:bf:60:11:d0:36:23:fc:93:24:54:fc

Appendix B – WebTrust Principles and Criteria for Certification Authorities, Version 2.2 Audit Criteria

Criterion	Controls
Criterion 3.3: The CA maintains controls to provide reasonable assurance that personnel and employment practices enhance and support the trustworthiness of the CA's operations.	3.3.4: The CA's policies and procedures specify the background checks and clearance procedures required for Trusted Roles and non-trusted roles. As a minimum, verification checks on permanent staff are performed at the time of job application and periodically for those individuals undertaking Trusted Roles. 3.3.9: Periodic reviews occur to verify the continued trustworthiness of personnel involved in the activities related to key management and certificate management.
Criterion 3.5: The CA maintains controls to provide reasonable assurance that: • the secure operation of CA information processing facilities is ensured; • the risk of CA systems failure is minimised; • the integrity of CA systems and information is protected against viruses and malicious • software; • damage from security incidents and malfunctions is minimised through the use of incident • reporting and response procedures; and • media are securely handled to protect them from damage, theft and unauthorised access.	3.5.3: Duties and areas of responsibility are segregated in order to reduce opportunities for unauthorised modification or misuse of information or services. 3.5.12: Procedures exist and are followed to assess that corrective action is taken for reported incidents.
Criterion 3.8: The CA maintains controls to provide reasonable assurance of continuity of operations in the event of a disaster or other type of business interruption. Such controls include, at a minimum: • the development and testing of a CA business continuity plan that includes a disaster recovery process for critical components of the CA system; • the storage of required cryptographic materials (i.e., secure cryptographic device and activation materials) at an alternate location; • creating backups of systems, data, and configuration information at regular intervals in accordance with the CA's disclosed business practices, and storage of these backups at an alternate location; and	3.8.8: Business continuity plans are tested regularly to ensure that they are up to date and effective

Criterion	Controls
- the availability of an alternate site, equipment and connectivity to enable recovery. The CA maintains controls to provide reasonable assurance that potential disruptions to Subscribers and Relying Parties are minimised as a result of the cessation or degradation of the CA's services.	
Criterion 4.6: The CA maintains controls to provide reasonable assurance that: - copies of CA keys that no longer serve a valid business purposes are destroyed in accordance with the CA's disclosed business practices; and - copies of CA keys are completely destroyed at the end of the key pair life cycle in accordance with the CA's disclosed business practices.	4.6.8: The CA follows a CA key destruction script for key destruction ceremonies that includes the following: a) definition and assignment of participant roles and responsibilities; b) management approval for conduct of the key destruction ceremony; c) specific cryptographic hardware, software and other materials including identifying information, e.g., serial numbers, that contain the CA key copies to be destroyed; d) specific steps performed during the key destruction ceremony, including; a. HSM and/or cryptographic hardware zeroization/initialization b. HSM and/or cryptographic hardware physical destruction c. Deletion of any encrypted files containing the CA key or fragments thereof e) physical security requirements for the ceremony location (e.g., barriers, access controls and logging controls); f) procedures for secure storage of cryptographic hardware and any associated activation materials following the key destruction ceremony pending their disposal or additional destruction g) sign-off on the script or in a log from participants and witnesses indicating whether the key destruction ceremony was performed in accordance with the detailed key destruction ceremony script; and h) notation of any deviations from the key destruction ceremony script (e.g., documentation of steps taken to address any technical issues).
Criterion 6.4: The CA maintains controls to provide reasonable assurance that certificates are generated and issued in accordance with the CA's disclosed business practices.	6.4.2: Validity periods are set in the CP and are formatted in accordance with ISO 9594/X.509 and ISO 15782-1 as disclosed within the CP.