

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 CAs 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 - SSL Baseline with Network Security, Version 2.4.1](#) 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 - SSL Baseline with Network Security, Version 2.4.1](#) 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 SSL certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of SSL certificates, and obtaining an understanding of Verizon Terremark's network and certificate system security to meet the requirements set forth by the CA/Browser Forum;
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 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 - SSL Baseline with Network Security, Version 2.4.1](#) 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 - SSL Baseline with Network Security, Version 2.4.1](#) at [Appendix B](#), nor the suitability of any of Verizon Terremark's services for any customer's intended purpose.

September 19, 2019

Ernst & Young Bedrijfsrevisoren cvba

Diegem, Belgium



Christel Weymeersch

Partner*

* Acting on behalf of a bvba



Verizon Terremark's Management's Assertion - SSL

Verizon Terremark NV ("Verizon Terremark") operates the Certification Authority (CA) services known as the CAs as disclosed in [Appendix A](#) and provides SSL CA services.

The management of Verizon Terremark is responsible for establishing and maintaining effective controls over its SSL CA operations, including its network and certificate security system controls, its SSL CA business practices disclosure on its website, SSL key lifecycle management controls, and SSL 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 - SSL Baseline with Network Security, Version 2.4.1](#) at [Appendix B](#) ("Criteria").

Verizon Terremark
Culliganlaan 2E, Diegem (Belgium)

A handwritten signature in black ink, appearing to read "B-R-B" with a long horizontal stroke extending to the right.

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 - SSL Baseline with Network Security, Version 2.4.1 Audit Criteria

Principle	Criterion
<p>Principle 2: The Certification Authority (CA) maintains effective controls to provide reasonable assurance that:</p> <ul style="list-style-type: none"> Subscriber information was properly collected, authenticated (for the registration activities performed by the CA, Registration Authority (RA) and subcontractor) and verified; The integrity of keys and certificates it manages is established and protected throughout their life cycles. 	<p>Criterion 2.6.2: The CA maintains controls to provide reasonable assurance that:</p> <ul style="list-style-type: none"> the CA provides all personnel performing information verification duties (Validation Specialists) with skills-training that covers basic Public Key Infrastructure (PKI) knowledge, authentication and vetting policies and procedures (including the CA's Certificate Policy and/or Certification Practice Statement), common threats to the information verification process (including phishing and other social engineering tactics), and these Requirements. the CA maintains records of such training and ensures that personnel entrusted with Validation Specialist duties maintain a skill level that enables them to perform such duties satisfactorily. the CA documents each Validation Specialist possesses the skills required by a task before allowing the Validation Specialist to perform that task. the CA requires all Validation Specialists to pass an examination provided by the CA on the information verification requirements outlined in the Baseline Requirements. all personnel in Trusted Roles maintain skill levels consistent with the CA's training and performance programs.
<p>Principle 3: The Certification Authority (CA) maintains effective controls to provide reasonable assurance that:</p> <ul style="list-style-type: none"> Logical and physical access to CA systems and data is restricted to authorized individuals; The continuity of key and certificate management operations is maintained; and CA systems development, maintenance and operations are properly authorized and performed to maintain CA systems integrity. 	<p>Criterion 3.2 The CA maintains controls to provide reasonable assurance that it performs a risk assessment at least annually which:</p> <ul style="list-style-type: none"> Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate Data or Certificate Management Processes; Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes; and Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the CA has in place to counter such threats.

Principle	Criterion
<p>Principle 3: The Certification Authority (CA) maintains effective controls to provide reasonable assurance that:</p> <ul style="list-style-type: none"> • Logical and physical access to CA systems and data is restricted to authorized individuals; • The continuity of key and certificate management operations is maintained; • and CA systems development, maintenance and operations are properly authorized and performed to maintain CA systems integrity. 	<p>Criterion 3.4: The CA maintains controls to provide reasonable assurance that it develops, implements, and maintains a Business Continuity Plan that includes at a minimum:</p> <ul style="list-style-type: none"> • the conditions for activating the plan; • emergency procedures; • fall-back procedures; • resumption procedures; • a maintenance schedule for the plan; • awareness and education requirements; • the responsibilities of the individuals; • recovery time objective (RTO); • regular testing of contingency plans; • the CA's plan to maintain or restore the CA's business operations in a timely manner following interruption to or failure of critical business processes; • a requirement to store critical cryptographic materials (i.e., secure cryptographic device and activation materials) at an alternate location; • what constitutes an acceptable system outage and recovery time; • how frequently backup copies of essential business information and software are taken; • the distance of recovery facilities to the CA's main site; and • procedures for securing its facility to the extent possible during the period of time following a disaster and prior to restoring a secure environment either at the original or a remote site. <p>The Business Continuity Plan is tested at least annually, reviewed, and updated.</p>
<p>Principle 4: The Certification Authority (CA) maintains effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum.</p>	<p>Criterion 4.3.5: The CA maintains controls to provide reasonable assurance that a human review of application and system logs is performed at least monthly and includes:</p> <ul style="list-style-type: none"> • Validating the integrity of logging processes; and • Testing the monitoring, logging, alerting, and log-integrity-verification functions are operating properly.
<p>Principle 4: The Certification Authority (CA) maintains effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum.</p>	<p>Criterion 4.4.2: The CA maintains controls to provide reasonable assurance that a formal documented vulnerability correction process is followed and includes identification, review, response, and remediation of vulnerabilities.</p>

Principle	Criterion
<p>Principle 4: The Certification Authority (CA) maintains effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum.</p>	<p>Criterion 4.4.3: The CA maintains controls to provide reasonable assurance that a Vulnerability Scan is performed on public and private IP addresses identified by the CA or Delegated Third Party as the CA's or Delegated Third Party's Certificate Systems based on the following:</p> <ul style="list-style-type: none"> • Within one (1) week of receiving a request from the CA/Browser Forum; • After any system or network changes that the CA determines are significant; and • At least every three (3) months
<p>Principle 4: The Certification Authority (CA) maintains effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum.</p>	<p>Criterion 4.4.6: The CA maintains controls to provide reasonable assurance that it performs one of the following within ninety-six (96) hours of discovery of a Critical Vulnerability not previously addressed by the CA's vulnerability correction process:</p> <ul style="list-style-type: none"> • Remediate the Critical Vulnerability; • If remediation of the Critical Vulnerability within 96 hours is not possible, create and implement a plan to mitigate the Critical Vulnerability, giving priority to the following: <ul style="list-style-type: none"> ○ Vulnerabilities with high CVSS scores, starting with the vulnerabilities the CA determines are the most critical (such as those with a CVSS score of 10.0); and ○ Systems that lack sufficient compensating controls that, if the vulnerability were left unmitigated, would allow external system control, code execution, privilege escalation, or system compromise; OR • Document the factual basis for the CA's determination that the vulnerability does not require remediation because of one of the following: <ul style="list-style-type: none"> ○ The CA disagrees with the NVD rating; ○ The identification is a false positive; ○ The exploit of the vulnerability is prevented by compensating controls or an absence of threats; or ○ Other similar reasons.