RICHTER

INDEPENDENT ASSURANCE REPORT

To the management of Carillon Information Security Certification Authority, Inc. ("CIS-CA"):

Scope

We have been engaged, in a reasonable assurance engagement, to report on CIS-CA management's assertion that for its Certification Authority (CA) operations at Vaudreuil-Dorion, Quebec, throughout the period February 10, 2020 to February 9, 2021 for its CAs as enumerated in Attachment A, CIS-CA has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its:
  - Certificate Practice Statement ("CPS") version 1.9 dated January 13, 2021
  - Sub CA Certificate Practice Statement ("CPS") version 1.4 dated January 17, 2021; and
  - [Certificate Policy ("CP") version 1.27 dated January 14, 2021](#)

- maintained effective controls to provide reasonable assurance that:
  - CIS-CA's Certification Practice Statements are consistent with its Certificate Policy
  - CIS-CA provides its services in accordance with its Certificate Policies and Certification Practice Statement

- maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and certificates it manages is established and protected throughout their lifecycles;
  - the integrity of subscriber keys and certificates it manages is established and protected throughout their lifecycles;
  - subscriber information is properly authenticated (for the registration activities performed by CIS-CA); and
  - subordinate CA certificate requests are accurate, authenticated, and approved

- maintained effective controls to provide reasonable assurance that:
  - logical and physical access to CA systems and data is restricted to authorised individuals;
  - the continuity of key and certificate management operations is maintained; and
  - CA systems development, maintenance, and operations are properly authorised and performed to maintain CA systems integrity

in accordance with the WebTrust Principles and Criteria for Certification Authorities v2.2.1.

CIS-CA does not escrow its CA keys and does not provide certificate suspension services. Accordingly, our audit did not extend to controls that would address those criteria.

Certification authority's responsibilities

CIS-CA'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 v2.2.1](#).

RICHTER

Our independence and quality control

We have complied with the relevant rules of professional conduct/code of ethics applicable to the practice of public accounting and related to assurance engagements, issued by various professional accounting bodies, which are founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

The firm applies Canadian 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 Canadian Standard on Assurance Engagements 3000, Attestation Engagements Other than Audits or Reviews of Historical Financial Information, set out in the CPA Canada Handbook – Assurance. 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 CIS-CA's key and certificate life cycle 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 life cycle management operations and over development, maintenance and operation of systems integrity;
(2) selectively testing transactions executed in accordance with disclosed key and certificate life cycle management business practices;
(3) testing and evaluating the operating effectiveness of the controls; and
(4) performing such other procedures as we considered necessary in the circumstances.

We believe that our audit provides a reasonable basis for our opinion.

Relative effectiveness of controls

The relative effectiveness and significance of specific controls at CIS-CA 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 effectiveness of controls at individual subscriber and relying party locations.

Inherent limitations

Because of the nature and inherent limitations of controls, CIS-CA's ability to meet the aforementioned criteria may be affected. For example, controls may not prevent, or detect and correct, error, fraud, unauthorised 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.

Opinion

In our opinion, throughout the period February 10, 2020 to February 9, 2021, CIS-CA 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 v2.2.1.

RICHTER

This report does not include any representation as to the quality of CIS-CA's services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities v2.2.1, nor the suitability of any of CIS-CA's services for any customer's intended purpose.

Use of the WebTrust seal

CIS-CA's use of the WebTrust for Certification Authorities Seal constitutes a symbolic representation of the contents of this report and it is not intended, nor should it be construed, to update this report or provide any additional assurance.

Richter LLP

Richter LLP
Toronto, Ontario, Canada
February 11, 2021

RICHTER

Attachment A: List of CAs In Scope

Root CAs

1. CISRCA1
2. Carillon PKI Services G2 Root CA 1

Signing CAs

3. Carillon PKI Services CA 1
4. Carillon PKI Services CA 2
5. Carillon PKI Services CA 3

RICHTER

CA Identifying Information

CA Name	Subject	Issuer	Serial	Key Algorithm	Key Size	Digest Algorithm	Not Before	Not After	SKI	SHA256 Fingerprint
CISRCA1	C=CA O=Carillon Information Security Inc. OU=Certification Authorities CN=CISRCA1	C=CA O=Carillon Information Security Inc. OU=Certification Authorities CN=CISRCA1	0b82dc943376	RSA	4096 Bits	sha256RSA	October 16, 2012 1:28:33 PM	October 16, 2032 1:28:33 PM	EA:95:15:DA:5C:39:00:E2:9A:DB:C4:BA:2D:67:FA:A1:F7:75:34:ED	A6:9E:03:36:C4:E5:90:23:FF:65:3C:71:F9:28:EB:73:F2:1C:00:F0
Carillon PKI Services G2 Root CA 1	C = CA O = Carillon Information Security Inc. OU = Certification Authorities CN = Carillon PKI Services G2 Root CA 1	C = CA O = Carillon Information Security Inc. OU = Certification Authorities CN = Carillon PKI Services G2 Root CA 1	4429d3b3c67d	RSA	4096 Bits	sha256RSA	January 20, 2020 2:42:45 PM	January 20, 2040 2:42:45 PM	3D:61:96:39:17:FB:10:80:FF:1A:68:58:65:FC:E9:03:19:56:1E:F9	EB:92:37:B7:20:76:F8:CC:8B:C1:3E:70:46:F2:FC:AB:C1:81:99:D3

Subordinate CA Identifying Information

CA Name	Subject	Issuer	Serial	Key Algorithm	Key Size	Digest Algorithm	Not Before	Not After	SKI	SHA256 Fingerprint
Carillon PKI Services CA 1	C=CA O=Carillon Information Security Inc. OU=Certification Authorities CN= Carillon PKI Services CA 1	C=CA O=Carillon Information Security Inc. OU=Certification Authorities CN= CISRCA1	0dac490ea4f4	RSA	4096 Bits	sha256RSA	June 19, 2018 2:30:47 PM	October 23, 2027 2:30:47 PM	21:F8:19:47:44:C7:7C:18:91:BD:8E:0F:35:13:55:06:D4:E3:EF:A5	83:64:DC:64:CB:67:3A:FC:D3:40:CA:ED:10:84:B0:E6:D0:D9:D0:B4
Carillon PKI Services CA 2	C = CA O = Carillon Information Security Inc. OU = Certification Authorities CN = Carillon PKI Services CA 2	C = CA O = Carillon Information Security Inc. OU = Certification Authorities CN = Carillon PKI Services G2 Root CA 1	0dc6c1998f52	RSA	4096 Bits	sha256RSA	January 20, 2020 3:09:14 PM	January 20, 2033 3:09:14 PM	9D:3E:C7:6A:08:2A:51:C0:0B:B5:B2:FD:54:3D:F9:C2:DE:77:4F:94	36:B5:DE:A7:65:9C:62:36:7C:A0:47:ED:57:60:3A:C1:2C:9D:C5:81
Carillon PKI Services CA 3	C = CA O = Carillon Information Security Inc. OU = Certification Authorities CN = Carillon PKI Services CA 3	C = CA O = Carillon Information Security Inc. OU = Certification Authorities CN = Carillon PKI Services G2 Root CA 1	368333fa2dc9	RSA	4096 Bits	sha256RSA	January 20, 2020 3:17:29 PM	January 20, 2030 3:17:29 PM	C6:92:AB:AE:E1:D1:4D:AE:0D:26:0A:CF:0F:6C:A9:5C:8E:B1:CF:EA	A0:1D:5A:69:33:E0:68:E5:DE:EC:A2:ED:08:19:EC:ED:77:3D:DD:58

Carillon's Management Assertion

Carillon Information Security Certification Authority ("CIS-CA") operates the Certification Authority (CA) services known as Carillon Information Security Inc. ("CIS") Root CA, and provides the following CA services:

- Subscriber registration
- Certificate renewal
- Certificate rekey
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate validation
- Subscriber key generation and management
- Subordinate CA cross-certification

The management of CIS-CA 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 CIS-CA's Certification Authority operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

CIS-CA management has assessed its disclosures of its certificate practices and controls over its CA services. Based on that assessment, in CIS-CA management's opinion, in providing its Certification Authority (CA) services at Vaudreuil-Dorion, Quebec, throughout the period February 10, 2020 to February 9, 2021, CIS-CA has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its Root CA Certificate Practice Statement ("CPS") version 1.9 dated January 13, 2021, Sub CA Certificate Practice Statement ("CPS") version 1.4 dated January 17, 2021 and Certificate Policy ("CP") version 1.27 dated January 14, 2021

- maintained effective controls to provide reasonable assurance that:
    - CIS-CA's CPS is consistent with its CP
    - CIS-CA provides its services in accordance with its CP and CPS

- maintained effective controls to provide reasonable assurance that:
    - the integrity of keys and certificates it manages is established and protected throughout their lifecycles;
    - the integrity of subscriber keys and certificates it manages is established and protected throughout their lifecycles;
    - subscriber information is properly authenticated (for the registration activities performed by CIS-CA); and
    - subordinate CA certificate requests are accurate, authenticated, and approved

- maintained effective controls to provide reasonable assurance that:
    - logical and physical access to CA systems and data is restricted to authorised individuals;
    - the continuity of key and certificate management operations is maintained; and
    - CA systems development, maintenance, and operations are properly authorised and performed to maintain CA systems integrity

in accordance with the WebTrust Principles and Criteria for Certification Authorities v2.2.1, including the following:

CA Business Practices Disclosure

- Certification Practice Statement (CPS)
- Certificate Policy (CP)

CA Business Practices Management

- Certification Practice Statement (CPS) Management
- Certificate Policy (CP) Management
- CP and CPS Consistency

CA Environmental Controls

- Security Management
- Asset Classification and Management
- Personnel Security
- Physical & Environmental Security
- Operations Management
- System Access Management
- System Development, Maintenance, and Change Management
- Disaster Recovery, Backups, and Business Continuity Management
- Monitoring and Compliance
- Audit Logging

CA Key Lifecycle Management Controls

- CA Key Generation
- CA Key Storage, Backup, and Recovery
- CA Public Key Distribution
- CA Key Usage

- CA Key Archival
- CA Key Destruction
- CA Key Compromise
- CA Cryptographic Hardware Life Cycle Management
- CA Key Escrow
- CA Key Transportation
- CA Key Migration

Subscriber Key Lifecycle Management Controls

- CA-Provided Subscriber Key Generation Services
- CA-Provided Subscriber Key Storage and Recovery Services
- Integrated Circuit Card (ICC) Lifecycle Management
- Requirements for Subscriber Key Management

Certificate Lifecycle Management

- Subscriber Registration
- Certificate Renewal
- Certificate Rekey
- Certificate Issuance
- Certificate Distribution
- Certificate Revocation
- Certificate Suspension
- Certificate Validation

Subordinate CA and Cross Certificate Lifecycle Management Controls

- Subordinate CA Certificate and Cross Certificate Lifecycle Management

CIS-CA does not escrow its CA keys and does not provide certificate suspension services. Accordingly, our assertion does not extend to controls that would address those criteria.

Carillon Information Security Inc.
February 11, 2021