KPMG

KPMG Inc
KPMG Crescent
85 Empire Road, Parktown, 2193,
Private Bag 9, Parkview, 2122, South Africa
Telephone +27 (0)11 647 7111
Fax   +27 (0)11 647 8000
Docex   472 Johannesburg
Web   http://www.kpmg.co.za

Management of TrustFactory TrustFactory (Pty) Ltd PO Box 802 Saxonwold	Your ref	PKI Assessment TrustFactory (Non-SSL)
	Our ref	TrustFactory_ CYBER19_O_Webtrust PKI Accreditation (Non-SSL)
	Contact	Duffield, Devon (+27832867588)

04 December 2019

Independent Assurance Report

To the Management of TrustFactory Certification Authority ("TrustFactory-CA")

Scope

We have undertaken a reasonable assurance engagement, to report on TrustFactory-CA Management's Assertion that for its Certification Authority (CA) operations at Rosebank Operations Centre (6th Floor, 16 Baker Street, Rosebank, Johannesburg, 2196 (Rosebank Office Park)) and the Bryanston Data Centre Vault (57 Sloane Str., Bryanston), throughout the period 08 October 2018 to 07 October 2019 for its CAs as enumerated in Appendix A, TrustFactory-CA has:

— Disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its :

  – TrustFactory CP, v1.5, dated 05 March 2019;

  – TrustFactory Client ROOT CA CPS, v1.5, dated 26 March 2019;

  – TrustFactory Client ISSUING CA CPS, v1.6, dated 20 March 2019;

  – TrustFactory SSL ROOT CA CPS, v1.5, dated 26 March 2019; and

  – TrustFactory SSL ISSUING CA CPS, v1.5, dated 21 November 2018.

— Maintained effective controls to provide reasonable assurance that:

- TrustFactory-CA's Certificate Practice Statement is consistent with its Certificate Policy

- TrustFactory-CA provides its services in accordance with its Certification Policy and Certification Practice Statements

— 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 TrustFactory-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 authorized and performed to maintain CA systems integrity

in accordance with the WebTrust Trust Service Principles and Criteria for Certification Authorities v2.1, and those provisions contained within Chapter 3 of the Accreditation Regulations of the Electronic Communications and Transaction Act of 2002.

TrustFactory does not escrow its CA keys, does not provide subscriber key generation services, and does not provide certificate suspension services. Accordingly, our procedures did not extend to controls that would address those criteria.

Certification authority's responsibilities

TrustFactory-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 Trust Service Principles and Criteria for Certification Authorities v2.1, and those provisions contained within Chapter 3 of the Accreditation Regulations of the Electronic Communications and Transaction Act of 2002.

Our independence and quality control

We have complied with the independence and other ethical requirements of Sections 290 and 291 of the Independent Regulatory Board for Auditors' *Code of Professional Conduct for Registered Auditors (Revised January 2018)* and parts 1 and 3 of the Independent Regulatory Board for Auditors' *Code of Professional Conduct for Registered Auditors (Revised November 2018)* (together the IRBA Codes), which are founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour. The IRBA Codes are consistent with the corresponding sections of the International Ethics Standards Board for Accountants' *Code of Ethics for Professional Accountants (including International Independence Standards*) respectively.

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.

Practitioner's responsibilities

Our responsibility is to express an opinion on Management's Assertion based on our procedures. We conducted our engagement in accordance with International Standard on Assurance Engagements 3000 (Revised), *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:

— obtaining an understanding of TrustFactory-CA'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;

— selectively testing transactions executed in accordance with disclosed key and certificate lifecycle management business practices;

— testing and evaluating the operating effectiveness of the controls; and

— performing such other procedures as we considered necessary in the circumstances.

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

Relative effectiveness of controls

The relative effectiveness and significance of specific controls at TrustFactory-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, TrustFactory-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 08 October 2018 to 07 October 2019, TrustFactory-CA Management's Assertion, as referred to above, is fairly stated, in all material respects, in accordance with the WebTrust Trust Service Principles and Criteria for Certification Authorities v2.1, and those provisions contained within Chapter 3 of the Accreditation Regulations of the Electronic Communications and Transaction Act of 2002.

This report does not include any representation as to the quality of TrustFactory-CA's services beyond those covered by the WebTrust Trust Service Principles and Criteria for Certification Authorities v2.1, and those provisions contained within Chapter 3 of the Accreditation Regulations of the Electronic Communications and Transaction Act of 2002, nor the suitability of any of TrustFactory-CA's services for any customer's intended purpose.

Restriction on use

As indicated, this report is for the purpose of providing information to the CPA Web Trust Certification Authorities in order to obtain Web Trust Certification and may not be suitable for any other purpose.

Use of the WebTrust seal

TrustFactory-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.

Yours faithfully

KPMG Inc.

Per Devon C Duffield
Chartered Accountant (SA)
Registered Auditor
Director

Appendix A – In Scope CAs

CA Distinguished Name	SHA256 Fingerprint	SHA1 Fingerprint
CN = TrustFactory Client Root Certificate Authority OU = TrustFactory PKI Operations O = TrustFactory(Pty)Ltd L = Johannesburg S = Gauteng C = ZA	92 C4 DB 06 C4 2A 13 0D 66 35 74 D7 74 1B 7F 93 C8 06 FD 67 14 DC E8 90 E8 4B 56 8F AE 86 E6 4C	f9 0c c7 52 1e ab 33 f2 28 ea a8 35 e4 e5 02 92 e3 1d 28 1e
CN = TrustFactory Client Issuing Certificate Authority OU = TrustFactory PKI Operations O = TrustFactory(Pty)Ltd L = Johannesburg S = Gauteng C = ZA	7D 9F A2 C0 85 90 81 F7 8A BD 73 5C 49 7E 79 5E 54 0C 58 98 D0 5E FA F1 5A BD 46 5E A7 D1 12 93	35 fc 04 61 2c 60 9d 14 c7 d8 ca 5e 89 55 f3 90 cf ba e7 42
CN = TrustFactory SSL Root Certificate Authority OU = TrustFactory PKI Operations O = TrustFactory(Pty)Ltd L = Johannesburg S = Gauteng C = ZA	60 81 42 DA 5C 67 5D D4 7C 1A A3 A2 6E E3 29 E2 4E 81 D5 FF 3B 94 01 7B C1 C1 A0 C3 7D B4 C1 A0	d1 14 78 e8 e5 fb 62 54 05 93 d2 2c 51 57 0d 01 4e ac 76 d8
CN = TrustFactory SSL Issuing Certificate Authority OU = TrustFactory PKI Operations O = TrustFactory(Pty)Ltd L = Johannesburg S = Gauteng C = ZA	55 3D D1 6E C1 C1 FE 49 96 89 FA FC 17 6A EB 88 19 ED CA 29 42 7D 60 8B 19 88 76 4D 12 D9 91 68	2c 6c aa 0f 78 6b 1a 35 15 1e 38 58 74 74 28 f4 7c 8c 15 5e

TRUSTFACTORY-CA MANAGEMENT'S ASSERTION

TrustFactory Certificate Authority ("TrustFactory-CA") operates the Certification Authority (CA) services known and enumerated in Appendix A, and provides the following CA services:
— Subscriber registration
— Certificate renewal
— Certificate rekey
— Certificate issuance
— Certificate distribution
— Certificate revocation
— Certificate validation
— Subordinate CA certification

The Management of TrustFactory-CA is responsible for establishing and maintaining effective controls over its CA operations, including its CA business practices disclosure on its website [https://www.trustfactory.net/repository/], 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 TrustFactory-CA's Certification Authority operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

TrustFactory-CA's Management has assessed its disclosures of its certificate practices and controls over its CA services. Based on that assessment, in TrustFactory-CA's Management's opinion, in providing its Certification Authority (CA) services at Rosebank Operations Centre (6th Floor, 16 Baker Street, Rosebank, Johannesburg, 2196 (Rosebank Office Park)) and the Bryanston Data Centre Vault (57 Sloane Str., Bryanston), throughout the period 08 October 2018 to 07 October 2019, has:

– disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its:

– TrustFactory CP, v1.5, dated 05 March 2019

– TrustFactory Client ROOT CA CPS, v1.5, dated 26 March 2019

– TrustFactory Client ISSUING CA CPS, v1.6, dated 20 March 2019

– TrustFactory SSL ROOT CA CPS, v1.5, dated 26 March 2019

– TrustFactory SSL ISSUING CA CPS, v1.5, dated 21 November 2018

– maintained effective controls to provide reasonable assurance that:

– TrustFactory-CA's Certificate Practice Statements are consistent with its Certificate Policy

T: +27 11 880 6103
F: +27 11 880 5443
www.trustfactory.net

P.O Box 802 Saxonwold, 2132
Gauteng, South Africa

6th Floor, Firestation Rosebank
16 Baker Street, Rosebank,
Johannesburg 2163

- TrustFactory-CA provides its services in accordance with its Certificate Policy and Certification Practice Statements
- 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 TrustFactory-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 Trust Service Principles and Criteria for Certification Authorities v2.1, and those provisions contained within Chapter 3 of the Accreditation Regulations of the Electronic Communications and Transaction Act of 2002, including the following:

CA Business Practices Disclosure
- Certification Practice Statement (CPS)
- Certificate Policy (CP)

CA Business Practices Management
- Certificate Policy Management
- Certification Practice Statement 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 and Maintenance
- 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 and Destruction
- CA Key Compromise
- CA Cryptographic Hardware Lifecycle Management

Subscriber Key Lifecycle Management Controls
- Requirements for Subscriber Key Management

Certificate Lifecycle Management Controls
- Subscriber Registration
- Certificate Renewal
- Certificate Rekey
- Certificate Issuance
- Certificate Distribution
- Certificate Revocation
- Certificate Validation

Subordinate CA Certificate Lifecycle Management Controls
- Subordinate CA Certificate Lifecycle Management

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

Jayesh Nana
Chief Executive Officer

04/12/2019

Appendix A – In Scope CAs

CA Distinguished Name	SHA256 Fingerprint	SHA1 Fingerprint
CN = TrustFactory Client Root Certificate Authority OU = TrustFactory PKI Operations O = TrustFactory(Pty)Ltd L = Johannesburg S = Gauteng C = ZA	92 C4 DB 06 C4 2A 13 0D 66 35 74 D7 74 1B 7F 93 C8 06 FD 67 14 DC E8 90 E8 4B 56 8F AE 86 E6 4C	f9 0c c7 52 1e ab 33 f2 28 ea a8 35 e4 e5 02 92 e3 1d 28 1e
CN = TrustFactory Client Issuing Certificate Authority OU = TrustFactory PKI Operations O = TrustFactory(Pty)Ltd L = Johannesburg S = Gauteng C = ZA	7D 9F A2 C0 85 90 81 F7 8A BD 73 5C 49 7E 79 5E 54 0C 58 98 D0 5E FA F1 5A BD 46 5E A7 D1 12 93	35 fc 04 61 2c 60 9d 14 c7 d8 ca 5e 89 55 f3 90 cf ba e7 42
CN = TrustFactory SSL Root Certificate Authority OU = TrustFactory PKI Operations O = TrustFactory(Pty)Ltd L = Johannesburg S = Gauteng C = ZA	60 81 42 DA 5C 67 5D D4 7C 1A A3 A2 6E E3 29 E2 4E 81 D5 FF 3B 94 01 7B C1 C1 A0 C3 7D B4 C1 A0	d1 14 78 e8 e5 fb 62 54 05 93 d2 2c 51 57 0d 01 4e ac 76 d8
CN = TrustFactory SSL Issuing Certificate Authority OU = TrustFactory PKI Operations O = TrustFactory(Pty)Ltd L = Johannesburg S = Gauteng C = ZA	55 3D D1 6E C1 C1 FE 49 96 89 FA FC 17 6A EB 88 19 ED CA 29 42 7D 60 8B 19 88 76 4D 12 D9 91 68	2c 6c aa 0f 78 6b 1a 35 15 1e 38 58 74 74 28 f4 7c 8c 15 5e