KPMG Advisory N.V.
P.O. Box 74500
1070 DB Amsterdam
The Netherlands

Laan van Langerhuize 1
1186 DS Amstelveen
The Netherlands
Telephone +31 (0)20 656 7890
www.kpmg.com/nl

To the Management of DIGITAL TRUST L.L.C.

Amstelveen, 30 December 2021

Subject: Independent Auditor's Report WebTrust for CAs Baseline Requirements

We have been engaged, in a reasonable assurance engagement, to report on DIGITAL TRUST L.L.C.'s (DigitalTrust) management's assertion that for its Certification Authority (CA) operations in the United Arabic Emirates, throughout the period 1 October 2020 through 30 September 2021 for its CAs as enumerated in Attachment A, DigitalTrust has:

- disclosed its SSL certificate lifecycle management business practices in its:
    - Certification Practice Statement, version 1.12, dated April 2021;
    - Certification Practice Statement, version 1.13, dated May 2021;
    - In accordance with its Certificate Policy, version 1.16, dated January 2021.

  including its commitment to provide SSL Certificates in conformity with the CA/Browser Forum Guidelines, as published on the DigitalTrust website, and provided such services in accordance with its disclosed practices
- maintained effective controls to provide reasonable assurance that:
    - the integrity of keys and SSL certificates it manages is established and protected throughout their lifecycles; and
    - SSL subscriber information is properly authenticated (for the registration activities performed by DigitalTrust)
- maintained effective controls to provide reasonable assurance that:
    - 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.

And, for its CAs as enumerated in Attachment A

- maintained effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum in accordance with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.5.

Certification Authority's responsibilities

DigitalTrust'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 v2.5.

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. Therefore, we are independent of DigitalTrust and complied with other ethical requirements in accordance with the Code of Ethics of NOREA (IT Auditors Association in The Netherlands) and the Code of Ethics for Professional Accountants (a regulation with respect to independence) of the NBA, Royal Netherlands Institute of Chartered Accountants.

We apply the International Standard on Quality Control 1, and accordingly maintain a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements. We also apply the Regulations for Quality management systems of the NBA and, accordingly, maintain 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 (ISAE) 3000, *Assurance Engagements Other than Audits or Reviews of Historical Financial Information,* issued by the International Auditing and Assurance Standards Board and the related Dutch Directive 3000A 'Attestation engagements', as issued by NOREA.

These standards require 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 DigitalTrust'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 DigitalTrust's network and certificate system security to meet the requirements set forth by the CA/Browser Forum;

2. selectively testing transactions executed in accordance with disclosed key and certificate lifecycle 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 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 DigitalTrust 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, DigitalTrust'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.

Opinion

In our opinion, throughout the period 1 October 2020 to 30 September 2021, DigitalTrust management's assertion as referred to above is fairly stated, in all material respects, based on the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.5.

This report does not include any representation as to the quality of DigitalTrust's services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.5, nor the suitability of any of DigitalTrust's services for any customer's intended purpose.

Subject: Independent Auditor Report WebTrust for CAs Baseline Requirements
Amstelveen, 30 December 2021

Use of the WebTrust seal

DigitalTrust's use of the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security 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.

On behalf of KPMG Advisory N.V.

Amstelveen, 30 December 2021

Original signed by

drs. ing. R.F. Koorn RE CISA
Partner

Subject: Independent Auditor Report WebTrust for CAs Baseline Requirements
Amstelveen, 30 December 2021

Attachment A: List of CAs in scope

The following CAs were in scope of the WebTrust for CAs Baseline Requirements Audit:

Common Name	SHA-256 Hash fingerprint	Type	Status
DigitalTrust Root CA G3	69062701346901A8E73BD846BFD1AE5752D389A857 68DFCB04D6DDEEDC1D6B54 CN=DigitalTrust Root CA G3,O=DigitalTrust L.L.C.,C=AE	Root	Active
DigitalTrust High Assurance CA G3	C1734233C45BCDD1F5EBE41278DF1AEC1C88AC22 C4D15125B8774D43E81EFAE3 CN=DigitalTrust High Assurance CA G3,O=DigitalTrust L.L.C.,C=AE	Intermediate	Active
DigitalTrust Root CA G4	1EEA09E623D764AF6F659141D3E41FBBE5158F9645 801180A1A86CE5DF538B82 CN=DigitalTrust Root CA G4,O=DigitalTrust L.L.C.,C=AE	Root	Active
DigitalTrust High Assurance CA G4	5718E3E84A286B0FA2A0B2DB14E955DF79A7655A1 EB5BE3A86120058196CC13E CN=DigitalTrust High Assurance CA G4,O=DigitalTrust L.L.C.,C=AE	Intermediate	Active
UAE Global Root CA G3	D2DBB1E65DE7FA8E13EF96B954C1E1FEE4349626 A822DE814F11A17C133D808B CN=UAE Global Root CA G3,O=UAE Government,C=AE	Root	Active
UAE High Assurance CA G3	B1941C7F78637CF5203A309CF91BC742A615AEEB8 EEDD91D389E6AD170880DC5 CN=UAE High Assurance CA G3,O=UAE Government,C=AE	Intermediate	Active
ICA Root CA G3	2DED99346FF9714C9117E7A9655385D5451DD15352 91F037F28C65CA2ABA89A3 CN=ICA Root CA G3,O=UAE Government,C=AE	Intermediate	Active
UAE Global Root CA G4	0791529BB8DED6D1CF7A48683275668F858B5A0110 1A335BC7722AE37B743F36 CN=UAE Root CA G4,O=UAE Government,C=AE	Root	Active
DTSigner CA G4	1879DE6EB4A196AE5121BEABA738E5C3546BB6032 F2313CD91009148AAC3CEDA CN=DTSigner CA G4,O=DigitalTrust L.L.C.,C=AE	Intermediate	Active

Subject: Independent Auditor Report WebTrust for CAs Baseline Requirements
Amstelveen, 30 December 2021

Common Name	SHA-256 Hash fingerprint	Type	Status
UAE High Assurance CA G4	983F6BF8F365034A8F0714298F535A54F9FA2B4E0692A7ACDC5B83DF01F4058D CN=UAE High Assurance CA G4,O=UAE Government,C=AE	Intermediate	Active
ICA Root CA G4	5108E4F77552AF09C622443CA250F7DB96E00C09E9E88EF25F152C5A9017CCD8 CN=ICA Root CA G4,O=UAE Government,C=AE	Intermediate	Active
ICA Mobile CA G4	6EBCA8499B2CF2D57380A72F204CAB8D2BB4C942ECC8F75A7900E9105A069619 CN=ICA Mobile CA G4,O=UAE Government,C=AE	Intermediate	Active
DarkMatter Root CA G3	4B3F646CD878C2B0659A727E0EB8780E5010ECEC03E2EF5E679880E265D486A3 CN=DarkMatter Root CA G3,O=DarkMatter L.L.C.,C=AE	Root	Retired (October 2020)
	E68729013A50404DC1BAF7127B3D3C98A8FF392B735D0B1140858D5B91C3BE65	Root	Retired (October 2020)
DM X1 High Assurance CA G3	BB71A7881B6E7A2F2B81F57C5DC9C9B8C5F2C8899EEB820B55D675467CC01D8D CN=DM X1 High Assurance CA G3,O=DarkMatter LLC,C=AE	Intermediate	Retired (December 2020)
DarkMatter Root CA G4	319A7F79258C33992B6BA277005AD3EA1802D899A99E42CD541750A4B4CC7CCD CN=DarkMatter Root CA G4,O=DarkMatter L.L.C.,C=AE	Root	Retired (October 2020)
	515869A435D6D47D3EB8F38D6F9198EC83F2A56AD31CC1AEDE4F7B89DA69E4BF	Root	Retired (October 2020)
DM X1 High Assurance CA G4	AB73ACF37C85B6F737D99E054863C29C0A583B06AF3656D21CA6E3B318D48CF7 CN=DM X1 High Assurance CA G4,O=DarkMatter LLC,C=AE	Intermediate	Retired (December 2020)

DIGITALTRUST

Level 12 Aldar HQ, P.O.Box 113979
Abu Dhabi, United Arab Emirates

+971-2-417-1483
www.digitaltrust.ae

DigitalTrust MANAGEMENT'S ASSERTION as to its Disclosure of its Business Practices and its Controls over its Certification Authority Operations during the period from 1 October 2020 to 30 September 2021

30 December 2021

Digital Trust LLC, a company under the United Arabic Emirates law, (hereafter: DigitalTrust), provides its SSL Certification Authority (CA) services through its public PKI infrastructure consisting of:

Common Name	SHA-256 Hash fingerprint	Type	Status
DigitalTrust Root CA G3	69062701346901A8E73BD846BFD1AE5752D389A85768D FCB04D6DDEEDC1D6B54 CN=DigitalTrust Root CA G3,O=DigitalTrust L.L.C.,C=AE	Root	Active
DigitalTrust High Assurance CA G3	C1734233C45BCDD1F5EBE41278DF1AEC1C88AC22C4D 15125B8774D43E81EFAE3 CN=DigitalTrust High Assurance CA G3,O=DigitalTrust L.L.C.,C=AE	Intermediate	Active
DigitalTrust Root CA G4	1EEA09E623D764AF6F659141D3E41FBBE5158F9645801 180A1A86CE5DF538B82 CN=DigitalTrust Root CA G4,O=DigitalTrust L.L.C.,C=AE	Root	Active
DigitalTrust High Assurance CA G4	5718E3E84A286B0FA2A0B2DB14E955DF79A7655A1EB5 BE3A86120058196CC13E CN=DigitalTrust High Assurance CA G4,O=DigitalTrust L.L.C.,C=AE	Intermediate	Active
UAE Global Root CA G3	D2DBB1E65DE7FA8E13EF96B954C1E1FEE4349626A822 DE814F11A17C133D808B CN=UAE Global Root CA G3,O=UAE Government,C=AE	Root	Active
UAE High Assurance CA G3	B1941C7F78637CF5203A309CF91BC742A615AEEB8EED D91D389E6AD170880DC5 CN=UAE High Assurance CA G3,O=UAE Government,C=AE	Intermediate	Active
ICA Root CA G3	2DED99346FF9714C9117E7A9655385D5451DD1535291F0 37F28C65CA2ABA89A3 CN=ICA Root CA G3,O=UAE Government,C=AE	Intermediate	Active
UAE Global Root CA G4	0791529BB8DED6D1CF7A48683275668F858B5A01101A3 35BC7722AE37B743F36 CN=UAE Root CA G4,O=UAE Government,C=AE	Root	Active

Common Name	SHA-256 Hash fingerprint	Type	Status
DTSigner CA G4	1879DE6EB4A196AE5121BEABA738E5C3546BB6032F2313CD91009148AAC3CEDA CN=DTSigner CA G4,O=DigitalTrust L.L.C.,C=AE	Intermediate	Active
UAE High Assurance CA G4	983F6BF8F365034A8F0714298F535A54F9FA2B4E0692A7ACDC5B83DF01F4058D CN=UAE High Assurance CA G4,O=UAE Government,C=AE	Intermediate	Active
ICA Root CA G4	5108E4F77552AF09C622443CA250F7DB96E00C09E9E88EF25F152C5A9017CCD8 CN=ICA Root CA G4,O=UAE Government,C=AE	Intermediate	Active
ICA Mobile CA G4	6EBCA8499B2CF2D57380A72F204CAB8D2BB4C942ECC8F75A7900E9105A069619 CN=ICA Mobile CA G4,O=UAE Government,C=AE	Intermediate	Active
DarkMatter Root CA G3	4B3F646CD878C2B0659A727E0EB8780E5010ECEC03E2EF5E679880E265D486A3 CN=DarkMatter Root CA G3,O=DarkMatter L.L.C.,C=AE	Root	Retired (Oct 2020)
	E68729013A50404DC1BAF7127B3D3C98A8FF392B735D0B1140858D5B91C3BE65	Root	Retired (Oct 2020)
DM X1 High Assurance CA G3	BB71A7881B6E7A2F2B81F57C5DC9C9B8C5F2C8899EEB820B55D675467CC01D8D CN=DM X1 High Assurance CA G3,O=DarkMatter LLC,C=AE	Intermediate	Retired (Dec 2020)
DarkMatter Root CA G4	319A7F79258C33992B6BA277005AD3EA1802D899A99E42CD541750A4B4CC7CCD CN=DarkMatter Root CA G4,O=DarkMatter L.L.C.,C=AE	Root	Retired (Oct 2020)
	515869A435D6D47D3EB8F38D6F9198EC83F2A56AD31CC1AEDE4F7B89DA69E4BF	Root	Retired (Oct 2020)
DM X1 High Assurance CA G4	AB73ACF37C85B6F737D99E054863C29C0A583B06AF3656D21CA6E3B318D48CF7 CN=DM X1 High Assurance CA G4,O=DarkMatter LLC,C=AE	Intermediate	Retired (Dec 2020)

The management of DigitalTrust 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 provide only reasonable assurance with respect to DigitalTrust's CA operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

The management of DigitalTrust has assessed the design of controls over its SSL-CA Services as scoped above. Based on that assessment, in DigitalTrust management's opinion, in providing its SSL-CA services throughout the period 1 October 2020 to 30 September 2021, DigitalTrust has:

- Disclosed its Certificate practices and procedures in its Certification Practice Statement, version 1.12, dated April 2020 and Certification Practice Statement, version 1.13, dated May 2021, in accordance with its Certificate Policy, version 1.6, dated January 2021, including its commitment to provide SSL Certificates in conformity with the applicable CA/Browser Forum Guidelines on https://ca.digitaltrust.ae/CPS/index.html, and provided such services in accordance with its disclosed practices

- maintained effective controls to provide reasonable assurance that
    - the integrity of keys and SSL certificates it manages is established and protected throughout their life cycles; and
    - SSL subscriber information is properly collected, authenticated (for the registration activities performed by DigitalTrust) and verified.

- maintained effective controls to provide reasonable assurance that
    - 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.

- maintained effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum.

in accordance with the WebTrust® Principles and Criteria for Certification Authorities – SSL Baseline Requirements with Network Security – Version 2.5 - November 2020, including the following:

- **CA BUSINESS PRACTICES DISCLOSURE**
- **CA SERVICE INTEGRITY**
    - Key Generation Ceremony
    - Certificate Content And Profile
    - Certificate Request Requirements
    - Verification Practices
    - Certificate Revocation And Status Checking
    - Employee And Third Parties
    - Data Records
    - Audit
- **CA ENVIRONMENTAL SECURITY**

For approval:

Original signed by

Scott Rea
SVP – Public Key Infrastructure,
Digital Trust LLC

_____