



**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

## Independent Auditor's Report

Amstelveen, 17 December 2019

To the management of Digital Trust LLC:

We have examined the assertion by the management of Digital Trust LLC (hereafter: DigitalTrust) that for its Certification Authority (CA) operations in the United Arab Emirates, throughout the period 1 October 2018 to 30 September 2019 for its infrastructure consisting of the following entities:

Common Name	SHA256 hash / DN
<b>DigitalTrust Root CA G3</b>	69062701346901A8E73BD846BFD1AE5752D389A85768DFCB04 D6DDEEDC1D6B54 CN=DigitalTrust Root CA G3, O=DigitalTrust L.L.C., C=AE
<b>DigitalTrust High Assurance CA G3</b>	C1734233C45BCDD1F5EBE41278DF1AEC1C88AC22C4D15125 B8774D43E81EFAE3 CN=DigitalTrust High Assurance CA G3, O=DigitalTrust L.L.C., C=AE
<b>DigitalTrust Root CA G4</b>	1EEA09E623D764AF6F659141D3E41FBBE5158F9645801180A1 A86CE5DF538B82 CN=DigitalTrust Root CA G4, O=DigitalTrust L.L.C., C=AE
<b>DigitalTrust High Assurance CA G4</b>	5718E3E84A286B0FA2A0B2DB14E955DF79A7655A1EB5BE3A8 6120058196CC13E CN=DigitalTrust High Assurance CA G4, O=DigitalTrust L.L.C., C=AE
<b>UAE Global Root CA G3</b>	D2DBB1E65DE7FA8E13EF96B954C1E1FEE4349626A822DE81 4F11A17C133D808B CN=UAE Global Root CA G3, O=UAE Government, C=AE
	0A9A4013AFC05650945CCA63B92A6B265857CF403403DEA52 E0E68CC4E1BF574 CN=UAE Global Root CA G3, O=UAE Government, C=AE
<b>UAE High Assurance CA G3</b>	B1941C7F78637CF5203A309CF91BC742A615AEEB8EEDD91D 389E6AD170880DC5 CN=UAE High Assurance CA G3, O=UAE Government, C=AE
<b>DigitalX1 High Assurance CA G3</b>	FDD7C3DB9D64509E008360402FCB1BE1C0CBE220D3D282AF 1F9B3D8E19B3E4A4 CN=DigitalX1 High Assurance CA G3, O=DarkMatter LLC, C=AE



**Digital Trust LLC**  
Independent Auditor's Report

Common Name	SHA256 hash / DN
<b>ICA Root CA G3</b>	2DED99346FF9714C9117E7A9655385D5451DD1535291F037F28C65CA2ABA89A3 CN=ICA Root CA G3, O=UAE Government, C=AE
	06AC79A8950254E62DA4668A4CA3D7770AD47AE665DE326E6C544BDCB40C6E9D CN=ICA Root CA G3, O=UAE Government, C=AE
	29245F81323631071E9C46BD0EC94F2623D8A5AABCC51DECF9EEC19C1A79DC3F CN=ICA Root CA G3, O=UAE Government, C=AE
<b>UAE Global Root CA G4</b>	0791529BB8DED6D1CF7A48683275668F858B5A01101A335BC7722AE37B743F36 CN=UAE Global Root CA G4, O=UAE Government, C=AE
	3E83A6C780B4C5B87538AD2E43A203708FF7FF29BEDC7B20626BF7C009199C0A CN=UAE Global Root CA G4, O=UAE Government, C=AE
<b>UAE High Assurance CA G4</b>	983F6BF8F365034A8F0714298F535A54F9FA2B4E0692A7ACDC5B83DF01F4058D CN=UAE High Assurance CA G4, O=UAE Government, C=AE
<b>DigitalX1 High Assurance CA G4</b>	F2B781704418CC6D4F200F74F542C845C91AC77C82F088912AA1A3D3B307F61F CN=DigitalX1 High Assurance CA G4, O=DarkMatter LLC, C=AE
<b>ICA Root CA G4</b>	5108E4F77552AF09C622443CA250F7DB96E00C09E9E88EF25F152C5A9017CCD8 CN=ICA Root CA G4, O=UAE Government, C=AE
	DCA38D15221B403B01A3838AC6A164143CEBDFD55F89A62F784886EAA3FD6D4D CN=ICA Root CA G4, O=UAE Government, C=AE
	13A49CD0109C45D95798831AD50DEFADB2AA5A836C181E11FB213391690A5499 CN=ICA Root CA G4, O=UAE Government, C=AE
<b>DarkMatter Root CA G3</b>	4B3F646CD878C2B0659A727E0EB8780E5010ECEC03E2EF5E679880E265D486A3 CN=DarkMatter Root CA G3, O=DarkMatter L.L.C., C=AE
	E68729013A50404DC1BAF7127B3D3C98A8FF392B735D0B1140858D5B91C3BE65 CN=DarkMatter Root CA G3, O=DarkMatter L.L.C., C=AE
<b>DM X1 High Assurance CA G3</b>	BB71A7881B6E7A2F2B81F57C5DC9C9B8C5F2C8899EEB820B55D675467CC01D8D CN=DM X1 High Assurance CA G3, O=DarkMatter LLC, C=AE



**Digital Trust LLC**  
Independent Auditor's Report

Common Name	SHA256 hash / DN
	89D3BF92914827AFEC6216DE9770AC437EE8C5F227B3B2982 0A9EF33551DBFC6 CN=DM X1 High Assurance CA G3, O=DarkMatter LLC, C=AE
	E6A41FF535AB87453D5FC4E7C818981479186595E00594B68A 08EFECBBCDB8EE CN=DM X1 High Assurance CA G3, O=DarkMatter LLC, C=AE
<b>DarkMatter Root CA G4</b>	319A7F79258C33992B6BA277005AD3EA1802D899A99E42CD5 41750A4B4CC7CCD CN=DarkMatter Root CA G4, O=DarkMatter L.L.C., C=AE
	515869A435D6D47D3EB8F38D6F9198EC83F2A56AD31CC1AE DE4F7B89DA69E4BF CN=DarkMatter Root CA G4, O=DarkMatter L.L.C., C=AE
<b>DM X1 High Assurance CA G4</b>	AB73ACF37C85B6F737D99E054863C29C0A583B06AF3656D21 CA6E3B318D48CF7 CN=DM X1 High Assurance CA G4, O=DarkMatter LLC, C=AE
	2744269BE81D480C51B21C1C26B7769A90564E6DA0AE44246 DD779CCAC70DA34 CN=DM X1 High Assurance CA G4, O=DarkMatter LLC, C=AE
	0B00D454B57F686976AD85CE6303C6A40FD5B80793CA7AC50 F811E55EAF68C83 CN=DM X1 High Assurance CA G4, O=DarkMatter LLC, C=AE
<b>DarkMatter Audit CA</b>	32BEADA3345287810EA32080D4F12834971C90E683FF289B2C ACDD55613DC35E CN=DarkMatter Audit CA, O=DarkMatter LLC, C=AE
<b>DarkMatter High Assurance CA</b>	3AE699D94E8FEBDACB86D4F90D40903333478E65E0655C432 451197E33FA07F2 CN=DarkMatter High Assurance CA, O=DarkMatter LLC, C=AE
	E0A670F4F1057E9179E9DB45E333CE37E3EE31C3499F1C584 A587BD9A5F53640 CN=DarkMatter High Assurance CA, O=DarkMatter LLC, C=AE
<b>DarkMatter Secure CA</b>	A25A19546819D048000EF9C6577C4BCD8D2155B1E4346A4599 D6C8B79799D4A1 CN=DarkMatter Secure CA, O=DarkMatter LLC, C=AE
	A019811E4369CA4C62AAA80A1549613E60F6C5CED383AF9D7 9DF8F8F193F1DFE CN=DarkMatter Secure CA, O=DarkMatter LLC, C=AE



**Digital Trust LLC**  
*Independent Auditor's Report*

DigitalTrust has:

- disclosed its SSL certificate lifecycle management business practices in its Certificate Practice Statement v1.11 of May 2019, in accordance with its Certificate Policy, version 1.3, dated December 2018, including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Guidelines on <https://ca.digitaltrust.ae/CPS/index.html>
- 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 – note that for this audit that meant we looked at the CAs whose Common Name starts with *DarkMatter* and those whose Common Name starts with *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
- 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

based on the [WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3](#).

The management of DigitalTrust is responsible for its assertion. Our responsibility is to express an opinion on management's assertion based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included:

- obtaining an understanding of DigitalTrust's SSL certificate life cycle management 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;
- selectively testing transactions executed in accordance with disclosed SSL certificate lifecycle management 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 our examination provides a reasonable basis for our opinion.

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.

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



**Digital Trust LLC**  
*Independent Auditor's Report*

findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

In our opinion, throughout the period 1 October 2018 to 30 September 2019, 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 (version 2.2).

This report does not include any representation as to the quality of DigitalTrust's services beyond those covered by the WebTrust for Certification Authorities – SSL Baseline with Network Security Criteria, or the suitability of any of DigitalTrust's services for any customer's intended purpose.

DigitalTrust's use of the WebTrust 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, 17 December 2019

*Originally signed by:*

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