DigitalTrust Certificate Holder Agreement

IMPORTANT: READ CAREFULLY

THIS DIGITALTRUST CERTIFICATE HOLDER AGREEMENT ("AGREEMENT") IS ENTERED INTO BETWEEN:

- THE CERTIFICATE HOLDER;
  - THE ORGANISATION WITH WHICH DIGITALTRUST HAS CONTRACTED TO OPERATE THE ISSUANCE OF CERTIFICATES THROUGH A SUBORDINATE CA (SUBCA) UNDER DIGITALTRUST'S ROOT CHAIN;

  AND
- DIGITALTRUST L.L.C ("DigitalTrust").

THE CERTIFICATE HOLDER MUST FIRST READ THIS AGREEMENT AND AGREE, ACCEPT AND BE BOUND BY ITS TERMS. IF YOU DO NOT ACCEPT THE TERMS OF THIS AGREEMENT, YOU ARE NOT AUTHORIZED TO BE THE CERTIFICATE HOLDER OF A DIGITALTRUST SUBCA CERTIFICATE AND YOU MUST TERMINATE YOUR APPLICATION OR REQUEST REVOCATION OF SUCH CERTIFICATE. THIS AGREEMENT INCORPORATES BY REFERENCE ANY CERTIFICATE POLICIES CONTAINED IN THE DIGITALTRUST CERTIFICATE AND CONDITIONS OF THE APPLICABLE CERTIFICATE POLICY/CERTIFICATION PRACTICE STATEMENT ("CP/CPS") LOCATED AT
https://ca.digitaltrust.ae/CPS/

THE USE OF A DIGITAL CERTIFICATE SIGNIFIES ACCEPTANCE OF THAT DIGITAL CERTIFICATE. BY ACCEPTING A CERTIFICATE, THE CERTIFICATE HOLDER ACKNOWLEDGES THAT THEY AGREE TO THE TERMS AND CONDITIONS CONTAINED IN THIS CERTIFICATE HOLDER AGREEMENT AND THE CP/CPS. CAPITALIZED TERMS NOT DEFINED IN THIS AGREEMENT HAVE THE MEANING SPECIFIED IN THE CP/CPS.

DigitalTrust and the Certificate Holder, intending to be legally bound, agree as follows:

1. Issuance; Fees: Upon the Certificate Holder's submission of a completed Application and DigitalTrusts' acceptance of that Application, and after payment for the then-current published price for such SubCA Certificate by The Certificate Holder, DigitalTrust shall issue the number of SubCA Certificates applied for by the Certificate Holder.

2. Use, Purpose and Limitations: The Certificate Holder shall use the DigitalTrust Certificate in accordance with the terms and conditions of the CP/CPS.

3. Role and Obligations of DigitalTrust: DigitalTrust shall act as the Certification Authority for the Certificate Holder's SubCA Certificate and perform its obligations as specified in this Agreement and the CP/CPS. DigitalTrust will generate the SubCA key pair during a Key ceremony where the SubCA represenatives are present. DigitalTrust will store and protect the SubCA private key according to the CA operation procedures. DigitalTrust is not responsible or liable for the cryptographic methods used in connection with the Certificates issued by the Certificate Holder's SubCA. DigitalTrust represents and warrants that it has followed the requirements of the CP/CPS in issuing the SubCA Certificate and in verifying the accuracy of the information contained in the Certificate. Additional warranties, identified in the CP/CPS, apply to DigitalTrust SubCA Certificates.

4. Role and Obligations of the Certificate Holder: Before accepting and using a DigitalTrust Certificate, the Certificate Holder must: (i) submit an Application; and (iii) accept and agree to the terms of this Agreement.

The Certificate Holder represents and warrants, so long as the SubCA Certificate is valid, that:

(a) The Certificate Holder has provided/will provide accurate and complete information, both in the Certificate Request and as otherwise requested by DigitalTrust. The Certificate Holder consents to DigitalTrust retaining such registration information in accordance with the DigitalTrust data retention policy;

(b) The Certificate Holder will ensure that key material and operations of the SubCA meet all requirements of the governing CP, including any policies mandated by the DigitalTrust Root CA that signs the SubCA;

(c) The Certificate Holder will not deploy and use the SubCA Certificate(s) until it has reviewed and verified the accuracy of the data in each Certificate;

(d) The Certificate Holder will promptly cease using a SubCA Certificate and its associated Private Key, and promptly begin an incident investigation, in the event that: (a) any information in the Certificate is or becomes incorrect or the DigitalTrust Certificate Holder Agreement becomes inaccurate, or (b) there is any actual or suspected misuse or compromise of the Certificate Holder's Private Key associated with the Public Key listed in the Certificate; or (c) any misissuing of certificates signed by the SubCA has occurred. Findings of the incident report shall be made to DigitalTrust within 5 working days, and daily status updates shall be provided. Operations remain paused until DigitalTrust authorizes re-instatement or the SubCA is revoked due to non-compliance;

(e) The Certificate Holder will promptly cease all use of the Private Key corresponding to the Public Key listed in a Certificate upon expiration or revocation of that Certificate. The Certificate Holder shall indemnify and hold harmless DigitalTrust from any and all damages and losses arising out of: (i) use of a DigitalTrust Certificate in a manner not authorized by DigitalTrust; (ii) tampering with a DigitalTrust Certificate; or (iii)

any misrepresentations made during the use of a DigitalTrust Certificate. In addition, the Certificate Holder shall indemnify and hold harmless DigitalTrust from and against any and all damages (including legal fees) for lawsuits, claims or actions by third-parties relying on or otherwise using a DigitalTrust Certificate relating to: (i) the Certificate Holder's breach of its obligations under this Agreement or the CP/CPS; or (ii) claims (including without limitation infringement claims) pertaining to content or other information or data supplied by the Certificate Holder.

5. Revocation: SubCA Certificates issued by DigitalTrust will be revoked on the occurrence of any of the following events:

(a) The Certificate Holder or Certificate Owner requests revocation of its SubCA Certificate;

(b) The Certificate Holder indicates that the original Certificate Request was not authorized and does not retroactively grant authorization;

(c) DigitalTrust obtains reasonable evidence that the Certificate Holder's Private Key (corresponding to the Public Key in the Certificate) has been compromised, or that the Certificate has otherwise been misused;

(d) DigitalTrust receives notice or otherwise become aware that a Certificate Holder violates any of its material obligations under the Certificate Holder Agreement;

(e) The Certificate Holder fails or refuses to comply, or to promptly correct inaccurate, false or misleading information after being made aware of such inaccuracy, misrepresentation or falsity;

(f) DigitalTrust becomes aware that a private key of a CA or Managed PKI was used in order to issue the certificate may have been compromised.

(g) DigitalTrust determines, in its sole discretion, that the Private Key corresponding to the Certificate was used to sign, publish or distribute spyware, Trojans, viruses, rootkits, browser hijackers, phishing, or other content, or that is harmful, malicious, hostile or downloaded onto a user's system without their consent;

(h) DigitalTrust receives notice or otherwise becomes aware of a material change in the information contained in the SubCA Certificate or if DigitalTrust determines that any of the information appearing in the Certificate is not accurate

(i) DigitalTrust's right to issue SubCA Certificates by law, regulation, or policy expires or is revoked or terminated;

(j) DigitalTrust's Private Key for that SubCA Certificate has been compromised;

(k) Such additional revocation events as DigitalTrust publishes in its CP/CPS or deems appropriate based on the circumstances of the event; or

(l) DigitalTrust receives notice or otherwise becomes aware that a Certificate Holder has been added as a denied party or prohibited person to a blacklist, or is operating from a prohibited destination under the laws of DigitalTrust's jurisdiction of operation.

6. DISCLAIMER OF WARRANTIES. EXCEPT AS EXPRESSLY PROVIDED IN THE CP/CPS, DIGITALTRUST MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS, IMPLIED OR OTHERWISE, RELATING TO ANY DIGITALTRUST CERTIFICATE OR ANY RELATED SERVICES PROVIDED BY DIGITALTRUST, INCLUDING WITHOUT LIMITATION ANY WARRANTY OF NONINFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

7. LIMITATION OF LIABILITY AND DAMAGES: DESPITE ANY CONTRARY PROVISION CONTAINED IN THIS AGREEMENT OR THE CP/CPS, THE MAXIMUM LIABILITY OF DIGITALTRUST FOR ANY DAMAGES ARISING UNDER THIS AGREEMENT WILL NOT EXCEED US$250,000.

IN NO EVENT WILL DIGITALTRUST BE LIABLE TO THE CERTIFICATE HOLDER OR ANY THIRD- PARTY RELYING UPON OR OTHERWISE MAKING USE OF A DIGITALTRUST CERTIFICATE FOR ANY INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL OR CONSEQUENTIAL DAMAGES, EVEN IF DIGITALTRUST HAS BEEN ADVISED OF THE LIKELIHOOD OF THOSE DAMAGES IN ADVANCE.

THE CERTIFICATE HOLDER'S USE OF A DIGITALTRUST CERTIFICATE IN A TRANSACTION WHERE THE POTENTIAL LIABILITY EXPOSURE IS GREATER THAN THAT CERTIFICATE'S MAXIMUM LIABILITY LIMIT AS SPECIFIED IN THIS CLAUSE 7 IS AT THE CERTIFICATE HOLDER'S OWN RISK.

8. Third-Party Beneficiaries: All application software and operating system vendors with whom DigitalTrust has entered into a contract for inclusion of the DigitalTrust Root Certificate as a trusted root Certificate in their software and all relying parties who actually rely on such Certificate during the period when the Certificate is valid are intended third party beneficiaries of this Agreement.

9. Term & Termination: This Agreement is effective upon DigitalTrust acceptance of the Certificate Holder's Application, and will terminate, except for those provisions which by their nature survive termination, upon the earliest of: (i) the latest expiration DigitalTrust Certificate Holder Agreement date of the DigitalTrust Certificates issued to You under this Agreement; (ii) a breach of the Certificate Holder's obligations under this Agreement; (iii) the Certificate Holder's written request; or (iv) revocation of all DigitalTrust Certificates issued to You under this Agreement.

10. Governing Law: The Relationships between the Participants are dealt with under the system of laws applicable under the terms of the contracts entered into. In general these can be summarised as follows;

- Dispute between the Root CA and an Issuing CA is dealt with under UAE Law.
- Dispute between an Issuing CA and a Registration Authority is dealt with under the applicable law of the Issuing CA.
- Dispute between an Issuing CA and an Authorised Relying Party is dealt with under the applicable law of the Issuing CA.

11. Notices: All notices provided by the Certificate Holder are considered given when in writing and delivered in hand by independent courier, delivered by registered or certified mail-return receipt requested, or sent by facsimile with receipt confirmed by telephone or other verifiable means, to:
DigitalTrust L.L.C, P.O.Box 113979, Abu Dhabi, United Arab Emirates
Website: http://www.digitaltrust.ae; Electronic Mail: CA.compliance@digitaltrust.ae

YOU REPRESENT AND WARRANT THAT:
(A) THE INDIVIDUAL ACCEPTING THIS AGREEMENT IS DULY AUTHORIZED TO ACCEPT THIS AGREEMENT ON THE CERTIFICATE HOLDER'S BEHALF AND TO BIND THE CERTIFICATE HOLDER TO THE TERMS OF THIS AGREEMENT;
(B) CERTIFICATE HOLDER IS THE ENTITY, LEGAL OR NATURAL PERSON THAT IT CLAIMS TO BE IN THE DIGITAL TRUST CERTIFICATE APPLICATION;
(C) THE CERTIFICATE HOLDER HAS THE FULL POWER, CORPORATE OR OTHERWISE, TO ENTER INTO THIS AGREEMENT AND PERFORM ITS OBLIGATIONS UNDER THIS AGREEMENT; AND
(D) THIS AGREEMENT AND THE PERFORMANCE OF THE CERTIFICATE HOLDER'S OBLIGATIONS UNDER THIS AGREEMENT DO NOT VIOLATE ANY THIRD-PARTY AGREEMENT TO WHICH THE CERTIFICATE HOLDER IS A PARTY.

_____
Authorized Signatory
Name:
Title:
Date:

(* In the UAE, please provide Trade Registration, Power of Attorney for Authorized Signatory, and Company Stamp on Signature Page)