Idently Subscriber Agreement - Version 1.0

PLEASE READ THIS AGREEMENT CAREFULLY BEFORE USING THE CERTIFICATE ISSUED TO YOU OR YOUR ORGANIZATION. BY APPLYING FOR A CERTIFICATE, YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, CANCEL YOUR ORDER WITHIN SEVEN (7) DAYS OF THE AVAILABILITY OF THE CERTIFICATE FOR A FULL REFUND. IF YOU HAVE PROBLEMS UNDERSTANDING THIS AGREEMENT, E-MAIL US AT legal@idently.com

This Idently Subscriber Agreement (the "Agreement") between Idently and the Applicant or Subscriber is effective as of the date of the application for the Certificate (the "Effective Date").

“Idently” is the entity with which the Subscriber places an order to procure the Certificate, specifically Idently Systems Limited (Kenya).
If you are a Procuring Party and are acting as the authorized representative of a Subscriber in applying for, or reselling, Certificate(s) or related hosted CA services, you represent and warrant to Idently and Relying Parties that you have obtained the authority of the Subscriber to enter into this Agreement on behalf of the Subscriber and that you shall comply with and procure Subscriber’s compliance with this Agreement.

If Subscriber procures or uses the Services through a Procuring Party, then Subscriber hereby represents and warrants that Subscriber has authorized such Procuring Party to act on Subscriber’s behalf for the Services. By authorizing a Procuring Party to provide or resell the Services to Subscriber, Subscriber hereby confirms its acceptance of this Agreement as it relates to Subscriber’s use of the Services. If Subscriber does not agree to the terms of this Agreement, then Subscriber may not purchase or use the applicable Services of Idently.

If the Subject and Subscriber are two separate entities and the Subject is a natural or legal person, Subscriber shall ensure that the Subject ratifies the requirements of this Agreement applicable to Subject.

1.0 Definitions and Incorporation by Reference

The following policies and associated guidelines are incorporated by reference into this Agreement:

- The Idently Certification Practice Statement (CPS);
- The Idently Warranty Policy; and
- The Idently Payment Terms;

The current versions of the above Idently documents are located at https://www.idently.com/repository and https://www.idently.com/corporate-policies.

The current versions of the CA/Browser Forum documents are located at https://cabforum.org/baselinerequirements-documents/.

The following definitions are used in this Agreement:

Affiliate: A corporation, partnership, joint venture or other entity controlling, controlled by, or under common control with another entity, or an agency, department, political subdivision, or any entity operating under the direct control of a Government Entity.

Applicant: The natural person or Legal Entity that applies for (or seeks renewal of) a Certificate. Once

the Certificate issues, the Legal Entity is referred to as the Subscriber. For Certificates issued to devices, the Applicant is the entity that controls or operates the device named in the Certificate, even if the device is sending the actual Certificate Request.

Application Software Supplier: A supplier of Internet browser software or other Relying Party application software that displays or uses Certificates and incorporates Root Certificates.

Authority Information Access: A Certificate extension that indicates how to access information and services for the issuer of the Certificate in which the extension appears.

CA/Browser Forum: An industry expert group of CA's and Application Software Suppliers. Details are available from www.cabforum.org.

Certificate: An electronic document that uses a Digital Signature to bind a Public Key and an identity.

Certificate Beneficiaries: The Subscriber that is a party to the Subscriber Agreement or Terms of Use for the Certificate, all Application Software Suppliers with whom Idently has entered into a contract for inclusion of its Root Certificate in software distributed by such Application Software Supplier, and all Relying Parties who reasonably rely on a Valid Certificate.

Certificate Custodian: A nominated individual responsible for the lifecycle of the Certificate. This may or may not be the same entity as the Subscriber.

Certificate Request: Communications described in Section 10.2 of the CA/Browser Forum Baseline Requirements for the Issuance of Publicly-Trusted Certificates ("Baseline Requirements"), CA/Browser Forum Guidelines For The Issuance And Management Of Extended Validation Certificates ("EV Guidelines"), CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates ("Code Signing Requirements"), requesting the issuance of a Certificate.

Certificate Requester: Applicant's representative who has express authority to represent the Applicant, or a third party (such as an ISP or hosting company) that completes and submits Certificate Requests on behalf of the Applicant. Certificate Requesters can be pre-approved via the functionality of a Idently managed service such as MSSL or EPKI.

Certificate Revocation List ("CRL"): A regularly updated timestamped list of revoked Certificates that is created and Digitally Signed by the CA that issued the Certificates.

Certification Authority ("CA"): An organization that is responsible for the creation, issuance, revocation, and management of Certificates. The term applies equally to both Roots CAs and Subordinate CAs. Idently or an entity which is certified by Idently to issue the Certificate to the "Subject". Idently is Applicant's CA hereunder.

Digital Signature: To encode a message by using an asymmetric cryptosystem and a hash function such that a person having the initial message and the signer's Public Key can accurately determine whether the transformation was created using the Private Key that corresponds to the signer's Public Key and whether the initial message has been altered since the transformation was made. Digitally Signed shall refer to electronic data to which a Digital Signature has been appended.

Domain Name: The label assigned to a node in the Domain Name System.

Domain Name Registrant: Sometimes referred to as the “owner” of a Domain Name, but more properly the person(s) or entity(ies) registered with a Domain Name Registrar as having the right to control how a Domain Name is used, such as the natural person or Legal Entity that is listed as the “Registrant” by WHOIS or the Domain Name Registrar.

Domain Name Registrar: A person or entity that registers Domain Names under the auspices of or by agreement with: (i) the Internet Corporation for Assigned Names and Numbers (ICANN), (ii) a national Domain Name authority/registry, or (iii) a Network Information Center (including their affiliates, contractors, delegates, successors, or assigns).

Domain Name System: An Internet service that translates Domain Names into IP addresses.

Fully-Qualified Domain Name: A Domain Name that includes the labels of all superior nodes in the Internet Domain Name System.

Government Entity: A government-operated legal entity, agency, department, ministry, branch, or similar element of the government of a country, or political subdivision within such country (such as a state, province, city, county, etc.).

Key Compromise: A Private Key is said to be compromised if its value has been disclosed to an unauthorized person, an unauthorized person has had access to it, or there exists a practical technique by which an unauthorized person may discover its value.

Key Pair: The Private Key and its associated Public Key.

Legal Entity: An association, corporation, partnership, proprietorship, trust, government entity or other entity with legal standing in a country’s legal system.

Online Certificate Status Protocol ("OCSP"): An online Certificate-checking protocol that enables Relying Party application software to determine the status of an identified Certificate.

Private Key: The key of a Key Pair that is kept secret by the holder of the Key Pair, and that is used to create Digital Signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.

Procuring Party: A legal entity or business authorized by Idently to resell or provide the Services to Subscriber.

Public Key: The key of a Key Pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify Digital Signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.

Registration Authority (“RA”): Any Legal Entity that is responsible for identification and authentication of Subjects of Certificates, but is not a CA, and hence does not sign or issue Certificates. An RA may assist in the Certificate application process or revocation process or both. When “RA” is used as an adjective to describe a role or function, it does not necessarily imply a separate body, but can be part of the CA.

Relying Party: Any natural person or Legal Entity that relies on a Valid Certificate. An Application Software Supplier is not considered a Relying Party when software distributed by such supplier merely displays information relating to a Certificate.

Root Certificate: The self-signed Certificate issued by the Root CA to identify itself and to facilitate verification of Certificates issued to its Subordinate CAs.

Subject: The natural person, device, system, unit, or Legal Entity identified in a Certificate as the Subject.

If the Subject is a device or system, it must be under the control and operation of the Subscriber.

Subordinate CA: A Certification Authority whose Certificate is signed by the Root CA, or another Subordinate CA.

Subscriber: A natural person or Legal Entity to whom a Certificate is issued and who is legally bound by a Subscriber Agreement or Terms of Use.

Suspect Code: Code that contains malicious functionality or serious vulnerabilities, including spyware, malware and other code that installs without the user's consent and/or resists its own removal or detection, and code that can be exploited in ways not intended by its designers to compromise the trustworthiness of the platforms on which it executes.

Terms of Use: Provisions regarding the safekeeping and acceptable uses of a Certificate issued in accordance with the Idently CPS when the Applicant/Subscriber is an Affiliate of the CA.

Wildcard Certificate: A Certificate containing an asterisk (*) in the left-most position of any of the Subject Fully-Qualified Domain Names contained in the Certificate.

2.0 Authority to Use Certificates

2.1 Grant of Authority: From the Effective Date and for the term set forth within the validity period of any issued Certificate ("Valid from" date to "Valid to" date), Idently hereby grants to the Subscriber the authority to use the Certificate in conjunction with Private Key and/or Public Key operations.

2.2 Limitations on Authority: The Subscriber shall use the Certificate only in connection with properly licensed cryptographic software.

3.0 Services Provided by Idently

After acceptance of this Agreement and payment of applicable fees, in addition to the "Grant of Authority", Idently or a third-party provider designated by Idently shall provide the following services from the time of issuance of the Certificate.

3.1 Provision of Certificate Revocation Lists (CRL), Online Certificate Status Protocol (OCSP) Services and Certificate Issuing Authority Details: Idently shall use reasonable efforts to compile, aggregate and make electronically available for all Certificates signed and issued by Idently's CA:

- CRLs for any Certificate containing a CRL Certificate distribution point;
- OCSP responders for any Certificates containing an OCSP responder URL, and
- Issuing Certificate information from the Authority Information Access locations; provided, however that Idently shall not be in breach of its obligations hereunder as a result of any delay in or failure of performance on its part which arises out of any equipment failure or telecommunications breakdown beyond the reasonable control of Idently.

3.2 Revocation Services for Certificates:

Idently may revoke a certificate for the circumstances specified in the CPS or if Idently receives notice or otherwise becomes aware that the Subscriber violated any of its material obligations under this Subscriber Agreement.

3.3 Key Generation: If Key Pairs are generated by Idently on behalf of the Subscriber offered as Token or PKCS#12 options, Idently will endeavor to use trustworthy systems in order to generate such Key Pairs, in which case, the following terms also apply.

- Idently will generate Key Pairs using a platform recognized as being fit for such purpose and will ensure that Private Keys are encrypted if transported to the Subscriber,
- Idently will use a key length and algorithm which is recognized as being fit for the purpose of Digital Signature, and
- In the case of both Code Signing and EV Code Signing Certificates, Subscriber acknowledges that Idently will not sign Key Pairs that are smaller than 2048 bits and, in the case of EV Code Signing, will offer SHA2 as the only option for the signature algorithm.

Idently does not generate Key Pairs for publicly trusted SSL certificates.

3.4 Site Seal Services for SSL/TLS Certificates and OCSP/CRL Responses: Idently permits the Applicant to make use of Idently's site seal on the Applicant's web site with a maximum daily rate of five hundred thousand (500,000) impressions per day. Idently reserves the right to limit or stop the availability of the seal if this limit is exceeded.

Idently provides a 24x7 service to check the validity of an issued Certificate either through an OCSP responder or CRL. A maximum daily rate of five hundred thousand (500,000) validations per Certificate per day is set. Idently reserves the right to enforce OCSP stapling if this limit is exceeded.

3.5 Timestamping Services for Code Signing Certificate: Idently offers the ability to timestamp code signed with a Code Signing Certificate as a non-chargeable service provided the service is used reasonably. As a best practice, Idently recommends the Subscriber to timestamp the digital signature after signing his/her code, using the appropriate Idently Timestamp Authority. Idently establishes a limit of a reasonable number of timestamps for the validity period of the Code Signing Certificate and reserves the right to withdraw the service or charge additional fees for the service where the volume of timestamps is deemed excessive by Idently.

3.6 Timestamping Services for PDF Signing for Adobe CDS Certificate: Idently offers the ability to timestamp Portable Document Format (PDF) documents as a paid Idently service. The number of signatures per year allowed by this service is established during the application process. Idently reserves the right to withdraw the service or charge additional fees for the service where the volume of timestamps is in excess of the agreed limit.

3.7 Timestamping Services for Adobe Authorized Trust List (AATL) Certificate: Idently may offer the ability to timestamp Portable Document Format (PDF) and Microsoft Office documents as a paid Idently service. The number of signatures per year allowed by this service is established during the application process. Idently reserves the right to withdraw the service or charge additional fees for the service where the volume of timestamps is in excess of the agreed limit.

4.0 Subscriber's Obligations and Warranties

Subscriber and/or Applicant warrants for the benefit of Idently and the Certificate Beneficiaries that:

4.1 Accuracy of Information: Subscriber will provide accurate, complete and truthful information at all times to Idently, both in the Certificate Request and as otherwise requested by Idently in connection with issuance of a Certificate, including but not limited to, the application name, information URL and application description in relation to Code Signing Certificates.

4.2 Protection of Private Key: Applicant (and if applicable, Subject) shall take all reasonable measures to maintain sole control of, keep confidential, and properly protect at all times the Private Key to be associated with the requested Certificate(s) and any associated activation data or device, e.g. password or token.

For Code Signing Certificates, the Applicant must maintain sole control of, keep confidential, and properly protect, at all times in accordance with Section 4.15 below the Private Key that corresponds to the Public Key to be included in the requested Certificate(s) (and any associated activation data or device, e.g. password or token). The Subscriber represents that it will generate and operate any device storing Private Keys in a secure manner, as described in a document of code signing best practices. The Subscriber must use passwords that are randomly generated with at least 16 characters containing uppercase letters, lowercase letters, numbers, and symbols to transport Private Keys.

4.3 Private Key Reuse: For Code Signing Certificates, the Applicant shall not apply for a Code Signing Certificate if the Public Key in the Certificate is or will be used with a non-Code Signing Certificate.

4.4 Prevention of Misuse: The Subscriber (and if applicable, Subject) will provide adequate network and other security controls to protect against unauthorized or misuse of the Private Key, and Idently will revoke the Certificate without requiring prior notification if there is unauthorized access to the Private Keys.

4.5 Acceptance of Certificate: Subscriber shall not use the Certificates until after Applicant, or an agent of Applicant, has reviewed and verified the Certificate contents for accuracy.

4.6 Use; Restrictions: Subscriber shall install the Certificate only on servers that are accessible at the subjectAltName(s) listed in the Certificate, and use the Certificate solely in compliance with all applicable laws and solely in accordance with the Subscriber Agreement or Terms of Use.

Under no circumstances must the Certificate be used for criminal activities such as phishing attacks, fraud, certifying or signing malware. Subscriber should not use a Certificate to knowingly sign software that contains Suspect Code or otherwise distribute content that has the effect of misleading, inconveniencing or annoying the recipient such as software that includes unwelcome features or programs not disclosed appropriately to the user prior to installation, or is recognized as unwelcome or suspicious by commercial anti-virus scanning applications.

Subscriber shall use the Certificate and associated Private Key only for authorized and legal purposes, including not using the Certificate to sign Suspect Code and to use the Certificate and Private Key solely in compliance with all applicable laws and solely in accordance with the Subscriber Agreement.

4.6.1 PDF Signing: In the event a Certificate is used to sign a PDF, the Subscriber shall maintain information that permits a determination of who approved the signature of a particular document.

4.6.2 EV Code Signing: Subscriber accepts these additional obligations and makes the following warranties when using EV Code Signing Certificates:

- Only to sign code that complies with the requirements set forth in the latest version of the CA/Browser Forum Baseline Requirements for the Issuance and Management of PubliclyTrusted Code Signing Certificates;
- Solely in compliance with all applicable laws;

- Solely for authorized company business; and
- Solely in accordance with this Agreement.

If Subscriber becomes aware (by whatever means) that it has signed code that contains malicious software or a serious vulnerability, the Subscriber must immediately inform Idently.

4.6.3 Microsoft Stipulation: Subscriber acknowledges that Microsoft may independently determine that a Certificate is malicious or there has been a Key Compromise, and Microsoft services and applications may have the ability to modify Microsoft customer experiences to reflect Microsoft's determination without notice and without regard to the revocation status of the Certificate.

4.7 Reporting and Revocation: Subscriber (and if applicable, Subject) shall promptly cease using a

Certificate and its associated Private Key (except for key decipherment) and promptly request that Idently revoke the Certificate if the Subscriber believes that (a) any information in the Certificate is, or becomes, incorrect or inaccurate, (b) the Private Key associated with the Public Key contained in the Certificate was misused, lost, stolen, potentially compromised, compromised, control over the subject's private key has been lost due to compromise of activation data (e.g. PIN code) or other reasons, or (c) in the case of a Code Signing Certificate, there is evidence that the Certificate was used to sign Suspect Code.

4.8 Termination of Use of Certificate: Subscriber (and if applicable, Subject) shall promptly cease use of the Private Key associated with the Public Key in the Certificate upon expiration or revocation of the Certificate or if the Issuing CA is compromised.

4.9 Responsiveness: Subscriber (and if applicable, Subject) shall respond to Idently's instructions concerning Key Compromise or Certificate misuse within forty-eight (48) hours.

4.10 Acknowledgement and Acceptance: Subscriber has evaluated Idently's CPS. Subscriber acknowledges and accepts that Idently is entitled to revoke the Certificate immediately if the Applicant violates the terms of the Subscriber Agreement or if Idently discovers that the Certificate is being used to enable criminal activities such as phishing attacks, fraud, or the distribution of malware. With respect to EV Code Signing Certificates used in connection with Microsoft services and applications,

Subscriber further acknowledges that even though an EV Code Signing Certificate may not be revoked by Idently, Microsoft may independently determine that the Certificate is malicious or compromised and modify the Microsoft customer experience in the applicable Microsoft services and applications to reflect Microsoft's determination without notice and without regard to the revocation status of the Certificate.

4.11 Sharing of Information: With respect to Code Signing Certificates, Subscriber acknowledges and accepts that, if: (a) the Certificate or the Applicant is identified as a source of Suspect Code, (b) the authority to request the Certificate cannot be verified, or (c) the Certificate is revoked for reasons other than Subscriber request (e.g. as a result of Key Compromise, discovery of malware, etc.), then Idently is authorized to share information about the Applicant, signed application, Certificate, and surrounding circumstances with other CAs or industry groups, including the CA/Browser Forum.

4.12 Compliance with Industry Standards: Subscriber acknowledges and accepts that Idently may modify the Subscriber Agreement when necessary to comply with any changes in the CA/Browser

Forum Baseline Requirements for the Issuance of Publicly-Trusted Certificates (the "Baseline Requirements"), CA/Browser Forum Guidelines For The Issuance And Management Of Extended Validation Certificates ("EV Guidelines"), CA/Browser Forum Baseline Requirements for the Issuance and

Management of Publicly-Trusted Code Signing Certificates (“Code Signing Requirements”), Browsers’ root programs requirements or any other applicable requirements.

4.13 Domain Control for SSL/TLS Certificate: The Subscriber acknowledges and asserts that s/he has control of the domain(s) or IP Address listed in the SubjectAltName(s) for which s/he is applying for the SSL/TLS Certificate. Should control cease for any domain(s), the Subscriber acknowledges that s/he must promptly inform Idently in accordance with the obligations of the 'Reporting and Revocation' section 4.7.

4.14 Email Control for Personal/Professional Certificate: The Subscriber acknowledges and asserts that s/he have control of the e-mail address for which they are applying for a Personal/Professional Certificate. Should control cease for any e-mail address(s), the Subscriber acknowledges that s/he must promptly inform Idently in accordance with the obligations of the 'Reporting and Revocation' section 4.7.

4.15 Key Generation and Usage: Where Key Pairs are generated by the Subscriber or the Certificate Requester, trustworthy systems must be used to generate Key Pairs, in which case, the following terms also apply:

- Key Pairs must be generated using a platform recognized as being fit for such purpose. In the case of PDF Signing for Adobe CDS, AATL secure email and document signing, this must be FIPS 140-2 Level 2 compliant,
- A key length and algorithm must be used which is recognized as being fit for the purpose of Digital Signature,
- The Subscriber shall ensure that the Public Key submitted to Idently correctly corresponds to the Private Key used.

Where Key Pairs are generated in hardware (as required by the CPS):

- The Subscriber must maintain processes, including, without limitation, changing of activation data, that assure that each Private Key within a hardware security module (HSM) or token can be used only with the knowledge and explicit action of the “Certificate Custodian”,
- The Subscriber must ensure that the Certificate Custodian has received security training appropriate for purposes for which the Certificate is issued, and
- Certificate Custodians undertake to take all reasonable measures necessary to maintain sole control of, keep confidential, and properly protect at all times the Private Key that corresponds to the Public Key to be included in the requested Certificate, as well as any associated authentication mechanism to access the key (e.g., password to a token or HSM).

4.15.1 Code Signing: Subscriber represents that Subscriber will use one of the following methods to generate and protect their Code Signing Certificate Private Keys. Idently recommends Subscribers use method 1 or 2 over method 3:

1. A Trusted Platform Module (TPM) that generates and secures a key pair and that can document the Subscriber’s private key protection through a TPM key attestation.
2. A hardware crypto module with a unit design form factor certified as conforming to at least FIPS 140 Level 2, Common Criteria EAL 4+, or equivalent.
3. Another type of hardware storage token with a unit design form factor of SD Card or USB token (not necessarily certified as conformant with FIPS 140 Level 2 or Common Criteria EAL 4+). Subscriber also warrants that it will keep the token physically separate from the device that hosts the code signing function until a signing session is begun.

4.15.2 EV Code Signing: Subscriber must use one of the following methods to generate, store and use EV Code Signing Certificate Private Keys in a crypto module that meets or exceeds the requirements of FIPS 140-2 level 2.

- A hardware security module (HSM) certified as conforming to FIPS 140-2 Level 2 or higher.
- A hardware storage token with a unit design form factor of USB token FIPS 140-2 Level 2 or higher.

At any time during the application and life cycle of the Certificate, Subscriber must be able to, on request of Idently, present proof that the Key Pair associated with the Certificate (request) is stored on a cryptographic device that meets the requirements of FIPS 140-2 Level 2 (or equivalent). Failure to provide such evidence might result in revocation of the Certificate.

5.0 Fees

If the Certificate was purchased through a Idently Procuring Party, Subscriber shall pay the Procuring Party according to the payment terms agreed between Subscriber and the Procuring Party.

Subscriber acknowledges and agrees that (i) if Subscriber does not pay the applicable fees (for example where Subscriber has procured the Certificate through a Procuring Party and Subscriber does not pay the applicable fees to the Procuring Party), or (ii) if the Procuring Party does not pay Idently the applicable fees in accordance with Idently's agreement with Procuring Party, regardless if the Subscriber pays the applicable fees to the Procuring Party, then Subscriber may not use the Certificate and Idently may revoke the issued Certificates for which fees are outstanding.

6.0 Consent to Publish Information

By providing personal information when applying for a Certificate, Subscriber consents to Idently's disclosure of this information publicly by (i) embedding the information issued in the Certificate and (ii) publishing the Certificate in Certificate Transparency (CT) logs.

7.0 Test Certificates

Idently may provide or support issuing Certificates for testing and evaluation purposes, including but not limited to trial evaluation, interoperability testing and proof-of-concepts ("Test Certificate(s)"). Subscriber may only use a Test Certificate in an internal, non-production environment and as part of non-commercial evaluation.

The right to use a Test Certificate may be limited in time and further restricted in additional agreements between Subscriber and Idently, in which case Subscriber's right to use will be terminated after the end date specified. Idently may at its sole discretion terminate the right of use of any Test Certificate at any time. Subscriber shall cease the use of the Test Certificate upon such termination.

Warranty Disclaimer. SUBSCRIBER ACKNOWLEDGES THAT TEST CERTIFICATES ARE PROVIDED "AS IS" AND WITHOUT ANY WARRANTY WHATSOEVER. TO THE MAXIMUM EXTENT ALLOWED BY APPLICABLE LAW, IDENTLY EXPRESSLY DISCLAIMS ALL REPRESENTATIONS AND WARRANTIES OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT, RELATING TO ANY TEST CERTIFICATES, SUBSCRIBER'S USE OR ANY INABILITY TO USE A TEST CERTIFICATES, THE RESULTS OF ITS USE AND THIS AGREEMENT.

LIMITATION OF LIABILITY. IDENTLY SHALL NOT BE LIABLE TO SUBSCRIBER FOR ANY CLAIMS,

DEMANDS OR DAMAGES WHATSOEVER, INCLUDING, WITHOUT LIMITATION, DIRECT, INDIRECT, CONSEQUENTIAL OR SPECIAL DAMAGES, ARISING OUT OF THE USE OF ANY TEST CERTIFICATES AND THE USE OR FAILURE OF A TEST CERTIFICATE TO OPERATE FOR WHATEVER REASON, WHETHER SUCH ACTION IS BASED IN CONTRACT OR TORT OR OTHERWISE, INCLUDING, WITHOUT LIMITATION, NEGLIGENCE.

8.0 Idently Limited Warranty

EXCEPT TO THE EXTENT PROHIBITED BY LAW OR AS OTHERWISE PROVIDED HEREIN, IDENTLY DISCLAIMS ALL WARRANTIES INCLUDING ANY WARRANTY OF MERCHANTABILITY AND/OR FITNESS FOR A PARTICULAR PURPOSE.

TO THE EXTENT IDENTLY HAS ISSUED AND MANAGED THE CERTIFICATE IN ACCORDANCE WITH THE BASELINE REQUIREMENTS, EV GUIDELINES, CODE SIGNING REQUIREMENTS AND THE CPS, IDENTLY SHALL NOT BE LIABLE TO THE SUBSCRIBER, RELYING PARTY OR ANY THIRD PARTIES FOR ANY LOSSES SUFFERED AS A RESULT OF USE OR RELIANCE ON SUCH CERTIFICATE. OTHERWISE, IDENTLY'S LIABILITY TO THE SUBSCRIBER, RELYING PARTY OR ANY THIRD PARTIES FOR ANY SUCH LOSSES SHALL IN NO EVENT EXCEED ONE THOUSAND DOLLARS ($1,000) PER CERTIFICATE; PROVIDED HOWEVER THAT THE LIMITATION SHALL BE TWO THOUSAND DOLLARS ($2,000) PER CERTIFICATE FOR AN EV CERTIFICATE OR AN EV CODE SIGNING CERTIFICATE.
THIS LIABILITY CAP LIMITS DAMAGES RECOVERABLE OUTSIDE OF THE CONTEXT OF THE IDENTLY WARRANTY POLICY. AMOUNTS PAID UNDER THE WARRANTY POLICY ARE SUBJECT TO THEIR OWN LIABILITY CAPS.

IN NO EVENT SHALL IDENTLY SHALL BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES, OR FOR ANY LOSS OF PROFITS, LOSS OF DATA OR OTHER INDIRECT, INCIDENTAL, CONSEQUENTIAL DAMAGES ARISING FROM OR IN CONNECTION WITH THE USE, DELIVERY, RELIANCE UPON, LICENSE, PERFORMANCE OR NON PERFORMANCE OF CERTIFICATES, DIGITAL SIGNATURES OR ANY OTHER TRANSACTIONS OR SERVICES OFFERED OR CONTEMPLATED BY THIS SUBSCRIBER AGREEMENT.

THIS LIABILITY LIMITATION SHALL BE THE SAME REGARDLESS OF THE NUMBER OF DIGITAL SIGNATURES, TRANSACTIONS, OR CLAIMS RELATED TO SUCH CERTIFICATE.

9.0 Term and Termination

This Agreement shall terminate upon the earliest of:

- The expiration date of the Certificate issued to the Subscriber either directly, indirectly or through a MSSL or ePKI service that has not yet expired; or
- Failure by the Subscriber to perform any of its material obligations under this Agreement if such breach is not cured within five (5) days after receipt of notice thereof from Idently.

10.0 Effect of Termination

Upon termination of this Agreement for any reason, Idently may revoke the Subscriber's Certificate in accordance with Idently procedures. Upon revocation of the Subscriber's Certificate, all authority granted to the Subscriber pursuant to Section 2 shall terminate. Such termination shall not affect Sections 4, 5, 6, 7, 8 and 11 of this Agreement, which shall continue in full force and effect to the extent necessary to permit the complete fulfilment thereof.

11.0 Miscellaneous Provisions

11.1 Governing Law and Venue

The (i) laws that govern the interpretation, construction, and enforcement of this Agreement and all matters, claims or disputes related to it, including tort claims, and (ii) the courts that have exclusive jurisdiction over any of the matters, claims or disputes, are set forth in the table below.

Idently Entity on Order Summary	**Governing Law**	**Venue**
Idently Systems Limited	Kenya	Nairobi, Kenya

11.2 Binding Effect

Except as otherwise provided herein, this Agreement shall be binding upon, and inure to the benefit of, the successors, executors, heirs, representatives, administrators and assigns of the parties hereto. Neither this Agreement not the Subscriber's rights in the Certificate shall be assignable by the Subscriber. Any such purported assignment or delegation shall be void and of no effect and shall permit Idently to terminate this Agreement.

11.3 Entire Agreement

This Agreement, along with all documents referenced herein, any product or service agreement, and the reseller agreement (if you are a reseller) constitute the entire agreement between the parties and supersedes any prior oral or written agreements, commitments, understandings, or communications with respect to the subject matter of this Agreement.

11.4 Severability

If any provision of this Agreement, or the application thereof, shall for any reason and to any extent, be invalid or unenforceable, the remainder of this Agreement and application of such provision to other persons or circumstances shall be interpreted so as best to reasonably effect the intent of the parties hereto. IT IS EXPRESSLY UNDERSTOOD AND AGREED THAT EACH AND EVERY PROVISION OF THIS AGREEMENT WHICH PROVIDES FOR A LIMITATION OF LIABILITY, DISCLAIMER OF WARRANTIES OR EXCLUSION OF DAMAGES IS INTENDED BY THE PARTIES TO BE SEVERABLE AND INDEPENDENT OF ANY OTHER PROVISION AND TO BE ENFORCED AS SUCH.

11.5 Notices

Whenever Subscriber desires or is required to give any notice, demand, or request to Idently with respect to this Agreement, each such communication shall be in writing and shall be effective only if it is delivered by a courier service that confirms delivery in writing or mailed, certified or registered mail, postage prepaid, return receipt requested, addressed to Idently at one of our International offices as listed at https://www.idently.com/#contactus, Attention: Legal Department. Such communications shall be effective when they are received.

11.6 Privacy; Use of third-party databases

Idently shall follow its privacy policy on its website (which can be found at https://www.idently.com/repository) when receiving and using information from Subscriber. Idently may amend the privacy policy at any time by posting the amended privacy policy on its website.

After Subscriber provides personal information to Idently when applying for a Certificate, Idently may process, disclose and/or transfer this information on a global basis to its affiliates, agents and subcontractors as necessary to validate and issue a Certificate, including processing, disclosure and/or transfer to countries that may have data protection laws that are less protective than those in the country where Subscriber is located.

For natural persons, Idently may validate items such as name, address and other personal information supplied during the application process against appropriate third party databases. This is necessary in order for Idently to provide the services and in performing these checks, personal information provided by the Subscriber may be disclosed to registered credit reference agencies, which may keep a record of that information. Such check is done only to confirm identity, and as such, a credit check is not performed. The Subscriber's credit rating will not be affected by this process.

11.7 Trade Names, Logos

By reason of this Agreement or the performance hereof, Subscriber and Idently shall acquire no rights of any kind in any trademark, brand name, logo or product designation of the other party and shall not make any use of the same for any reason except as otherwise authorized in writing by the party which owns all rights to such trademarks, trade names, logos or product designation.

12.0 Customer Support

The Subscriber must notify Idently through our contact information listed on https://www.idently.com/#contactus immediately if there is an error in the Certificate. If Subscriber fails to do so within seven (7) days from receipt, the Certificate shall be deemed accepted.

If Subscriber is not completely satisfied with the issued certificate, the subscriber may request a refund within seven (7) days of the certificate being issued. Any refunds will be net of any fees incurred by Idently.

[V 1.0 28-Apr-2021]