IdenTrust
part of HID Global

IGC
Basic Assurance Affiliated Certificate
Forms Packet

Copyright © 2021 IdenTrust Services, LLC. All rights reserved.

IdenTrust Services, LLC | 5225 W. Wiley Post Way, Suite 450 | Salt Lake City, UT 84116

www.IdenTrust.com

Instructions for the Applicant

Thank you for choosing IdenTrust Services, LLC ("IdenTrust"), a subsidiary of IdenTrust, Inc., to issue you an IGC Basic Assurance Affiliated certificate. These certificates are issued to individuals such as employees, officers, and agents authorized to act on behalf of business entities that have been validated by IdenTrust.

THE ONLINE APPLICATION:

Complete the application process online at: www.IdenTrust.com.

Apply with your legal first and last name, full organization name and address, and a valid email address.

PART 1 FORM:

Fill out all of the fields on the form, then take the Part 1 form to an officer in your Organization who can sign on behalf of the Organization, representing to IdenTrust that you are an authorized representative of the Organization.

Have the officer sign and date Part 1 - Sponsoring Organization Authorization Form and return it to you.

PART 2 FORM:

Take this form to a licensed notary or your organization's Trusted Agent to verify your identity credentials. You have two options for presenting your ID:

Option 1 – **ONE** Federal Government-issued photo ID
Option 2 – **TWO** State or local government-issued IDs, of which one must be a photo ID.

All forms of ID must be verifiable. Some examples of acceptable IDs are:

Option 1 – Federal IDs

- Valid Passport
- Federal Employee ID Card
- US Military Photo ID
- DoD CAC Card

Option 2 State/local government ID, 1 must be photo ID

- State-issued Driver's License
- State-issued ID Card
- State-school Student ID
- Birth Certificate
- Social Security Card
- Concealed Weapons Permit
- State-issued Professional License

COMPLETE THE REGISTRATION PROCESS

Please check your email for a verification email request sent from Processing@IdenTrust.com and follow the steps laid out.

Choose one of the following:

- **Send the original, 'wet-signature' (pen to paper) Part 1 and Part 2 forms to IdenTrust for processing.** It is advised you select a traceable ship method such as FedEx or UPS, but you may also submit the originals using US Mail.

  Registration Department
  IdenTrust Services
  5225 W. Wiley Post Way, Ste 450
  Salt Lake City, UT 84116-2898

- **Submit the Part 1 and Part 2 forms to IdenTrust via email.** Signatures on the forms must be handwritten and may not be a stamp or electronic signature. The signature of the Notary or Trusted Agent may be either a handwritten signature or a digital signature that can be traced to a certificate root. Electronic signatures are not accepted.

Email to Processing@IdenTrust.com

This email inbox is monitored for forms packets only.

Processing and approval of your application will begin once valid, accurate forms have been received.

IGC Basic Assurance Affiliated Certificate
Part 1 – Subscribing Organization Authorization Form

This Subscribing Organization Authorization Form (the "Authorization") is given by "Subscribing Organization" (as identified below on this page), to IdenTrust Services, LLC, a Delaware corporation with its principal place of business located at 5225 Wiley Post Way, Suite 450, Salt Lake City, Utah 84116-2898 U.S.A ("IdenTrust").

WHEREAS, Subscribing Organization desires to authorize the issuance by IdenTrust of an IGC Basic Assurance Affiliated Certificate (a "Certificate") to Subscriber (identified below on this page), that, if issued, will identify Subscriber as being an employee, contractor, or agent of Subscribing Organization and will certify Subscriber's Public Keys corresponding to such Certificate.

WHEREAS, IdenTrust desires to receive this authorization and, if the application of Subscriber corresponding to this Authorization is acceptable to IdenTrust, desires to issue a Certificate to Subscriber.

NOW, THEREFORE, Subscribing Organization and IdenTrust agree as set forth below.

1. Subscribing Organization represents and warrants that Subscriber is an employee, contractor, or agent of the Subscribing Organization and is hereby authorized by Subscribing Organization to apply for, be issued, and use a Certificate to transact business and make Digital Signatures on behalf of the Subscribing Organization, and Subscribing Organization hereby authorizes IdenTrust to issue such a Certificate to Subscriber. Subscribing Organization provides the information below in this Section to identify itself and Subscriber to IdenTrust. See Box 1.

2. The Subscribing Organization agrees to be bound by the terms and conditions of the IGC Basic Assurance Affiliated Certificate Subscriber Agreement (attached hereto; see Part 3 – IGC Basic Assurance Affiliated Certificate Subscriber Agreement), and the terms and conditions of the IGC Basic Assurance Affiliated Certificate Subscriber Agreement are incorporated herein by this reference.

3. In the event IdenTrust issues a Certificate to Subscriber, Subscribing Organization agrees that it shall immediately request that IdenTrust revoke the Certificate and require Subscriber to cease use of the Certificate, if: (i) Subscribing Organization suspects any loss, disclosure, or other compromise of the Subscriber's Private Key; (ii) information contained in the Certificate is no longer accurate or current (e.g., the Subscriber changes his or her name, the Subscriber's email address changes); (iii) Subscriber is no longer an employee, contractor, or agent of the Subscribing Organization; or (iv) is no longer authorized by Subscribing Organization to transact business or make Digital Signatures on behalf of Subscribing Organization.

4. Also in the event IdenTrust issues a Certificate to Subscriber, Subscribing Organization may request revocation of the Certificate, if issued, at any time by: (i) sending an email to support@IdenTrust.com; (ii) calling the IdenTrust Support at 1-800-748-5360; or (iii) such other means as may be provided to Subscribing Organization by IdenTrust.

5. Subject to the provisions above in this Authorization, IdenTrust accepts the authorizations by Subscribing Organization herein above.

Subscribing Organization has caused this Authorization to be executed by its authorized representative, effective on the date printed below. The undersigned personally warrants and represents that he or she has authority to accept the terms and conditions of this Authorization on behalf of Subscribing Organization and to bind the Subscribing Organization by his or her signature.

Print Applicant's legal first and last name	Organization Officer Signature
Print Organization name	Print Organization Officer's name
Address line 1	Print Organization Officer's title
Address line 2	Organization Officer's telephone number
Address line 3	Organization Officer Email
City, State/Province, Country, Postal Code	Date Organization Officer signed

ALL FIELDS MUST BE COMPLETED

IGC Basic Assurance Affiliated Certificate
Part 2 - ID Form

Section 1: Terms and Conditions; Identity Credentials

The undersigned in this Section 1 warrants and represents that all facts and information provided in Part 1 – Subscribing Organization Authorization Form and this Part 2 – ID Form are, to the best of the undersigned's knowledge, accurate, current, and complete, and that he or she: (i) is authorized by his or her Subscribing Organization (as identified on the Part 1 – Subscribing Organization Authorization Form naming him or her as "Subscriber" in connection with the application made for a digital certificate in connection with this ID Form) to apply for, be issued, and use an IGC Basic Assurance Affiliated Certificate ("IGC Basic Assurance Affiliated Certificate" is defined in Part 3 – IGC Basic Assurance Affiliated Certificate Subscriber Agreement) issued by IdenTrust; (ii) has reviewed and accepts as identifying himself or herself the personal identifying information set forth below on this Part 2 – ID Form; (iii) is who he or she represents himself or herself to be; and (iv) has read, understands, and accepts the terms and conditions set forth in Part 3 – IGC Basic Assurance Affiliated Certificate Subscriber Agreement.

Sign only in the presence of a notary (or other Registrar; "Registrar" is defined in Part 3 – IGC Basic Assurance Affiliated Certificate Subscriber Agreement). If this Section 1 is signed within the United States, the signer makes the following declaration by doing so: I declare under penalty of perjury that the foregoing is true and correct. If this Section 1 is signed without (i.e. outside of) the United States, this signer makes the following declaration by doing so: I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Signed By: _____ (Subscriber to sign only in the presence of the Notary)

Print Legal Name: _____ Email Address: _____
First Name MI Last Name (Must match email address provided online)

One verifiable Photo ID issued by the Federal Government - or - **Two verifiable forms of ID issued by a state or local government At least one must be a photo ID**

PHOTO ID	PHOTO ID	2ND ID
Doc. Type/Title:	Doc. Type/Title:	Doc. Type/Title:
Doc. Issuer:	Doc. Issuer:	Doc. Issuer:
Serial/Unique #:	Serial/Unique #:	Serial/Unique #:
Full Name:	Full Name:	Full Name:
Issue Date:	Issue Date:	Issue Date:
Expire Date:	Expire Date:	Expire Date:

***Note**: If the name on your Photo ID is different from the name on your Second ID, please send a notarized copy of the document showing the name change (E.g. A notarized copy of your marriage license or notarized certificate of marriage).

Notarial Acknowledgement

I _____ (name of notary/officer), registered in the state of _____, county of _____ do hereby certify under PENALTY OF PERJURY under the laws of the State of _____ that the following information is true and correct:

1. On _____ (MM/DD/YY), before me personally appeared _____ (name of signer), who proved to me on the basis of satisfactory evidence to be the person whose name is subscribed to the within instrument and acknowledged to me that he/she executed the same in his/her authorized capacity, and that by his/her signature on the instrument the person, or the entity upon behalf of which the person acted, executed the instrument.

2. I have seen and verified the forms of identification for which information is written above and hereby assert that said forms of ID do not appear to be altered, forged or modified in any way.

WITNESS my hand and official seal

(Seal)

Signature _____

PART 3 – IGC BASIC ASSURANCE AFFILIATED CERTIFICATE SUBSCRIBER AGREEMENT

This IGC Basic Assurance Affiliated Certificate Subscriber Agreement (this "Agreement") is made by and among IdenTrust (defined below) on the one hand, and You (defined below) and Subscribing Organization (defined below) on the other. This Agreement sets the forth terms and conditions governing Your (defined below) application for a Certificate (defined below) and, if IdenTrust issues such Certificate to You, the terms and conditions applicable to the Certificate. Definitions of capitalized terms used herein are provided for in Section 35 below.

1. Acceptance. By signing the ID Form or by clicking the checkbox next to "I have reviewed, and I hereby sign and accept the complete terms of the Subscriber Agreement" during the online application process, You agree to the terms and conditions of this Agreement. Subscribing Organization indicates its acceptance to the provisions hereof through the execution of the Subscribing Organization Authorization Form under which You are identified by the Subscribing Organization as affiliated therewith for purposes of the Certificate. If IdenTrust accepts the application and confirms the information submitted, IdenTrust will create the Certificate identifying You as the "Subscriber" (as provided for in the CPS) and Subscribing Organization as the organization which You are affiliated (i.e. the Subscribing Organization will be the "Subscribing Organization" within the meaning of the CPS), and will notify You how and where to retrieve the Certificate.

2. Integration; Amendment. The CP, CPS, ID Form, and the Subscribing Organization Authorization Form are incorporated by reference herein. The parties hereto agree that the CP and CPS can be amended from time to time by IdenTrust pursuant to the terms regarding amendment thereof set forth in the CP and CPS, respectively, and that any such amendments shall become effective as set forth in the CP and CPS, respectively. The terms of this Agreement may be amended upon renewal of the Certificate by the parties hereto with effect of such amendment at the time of such renewal, or at any time by IdenTrust with effect thirty (30) days after IdenTrust posts amended terms to the Repository. Use of the Certificate after the effective date of any such amendment shall constitute notice to IdenTrust of acceptance by Subscribing Organization and You of the amended terms; You may decline to accept any such amended terms by refraining from using the Certificate after the effective date of the applicable amendment. Subscribing Organization and You are responsible for periodically checking the Repository for the latest version of the CP, CPS, and this Agreement.

3. Application. You must complete both the online portion of the application process and provide to IdenTrust a completed and signed Subscribing Organization Authorization Form and ID Form. The identity credentials You presented and which were recorded on the ID Form must be the same identity credentials as those reported to IdenTrust during the online portion of the application process.

4. Verification of Identity. IdenTrust may seek to verify the identity of You and that of the Subscribing Organization by any reasonable means. IdenTrust is hereby authorized by You and Subscribing Organization, as applicable, to make inquiry with public or private databases or other sources, solely for the purpose of verifying any information that You or Subscribing Organization provide during the application process in order to determine whether to issue a Certificate to the You. IdenTrust may contact Subscribing Organization's human resources department to verify Your affiliation with Subscribing Organization. IdenTrust is hereby also authorized to retain and use any information generated during the application, identification, authentication, Certificate issuance, and Certificate management processes, provided that such retention and use shall be subject to the terms of this Agreement, including put not limited to Section 13.

5. Processing Payment. IdenTrust will begin processing the application for a Certificate made in connection herewith as soon as IdenTrust has received the following in connection herewith: (i) preauthorization to charge the credit card, purchase order, or voucher number provided by You; and (ii) a completed Subscribing Organization Authorization Form and the ID Form. You and Subscribing Organization, as may be applicable, hereby authorize IdenTrust to bill against such credit card, purchase order, or voucher number for the applicable Certificate issuance fee. In the event IdenTrust approves Your application for a Certificate in connection herewith, IdenTrust will process the credit card charge, purchase order, or voucher number. Once such processing occurs, unless otherwise required by law, no refunds will be provided by IdenTrust. If a Certificate is issued to You hereunder, IdenTrust will revoke the Certificate is IdenTrust does not actually receive payment for the Certificate within sixty (60) days of such issuance.

6. Approval of Application by IdenTrust.

IdenTrust, in its sole discretion and without incurring liability for any loss arising out of such denial or refusal, may deny the application for, or otherwise refuse to issue, an Certificate in connection herewith. IdenTrust shall have no liability for any delay experienced during the Certificate application and issuance process.

If IdenTrust approves the application for a Certificate made in connection herewith, notice thereof will be provided as describe in Section 7 and the certificate will be made available for issuance in keeping with the applicable provisions of Section 7 – 10, as applicable.

If IdenTrust does not approve Your application for a Certificate in connection herewith, IdenTrust will send notice of such non-approval to the email address listed for You on the ID Form and upon the sending of such a notice this Agreement terminates.

7. Certificate Issuance – Notice and Time to Download.

If IdenTrust approves the application for a Certificate made in connection herewith, IdenTrust will notify You that the Certificate is ready to be so issued. To so notify You, IdenTrust will email You at the email address for You as identified to IdenTrust on the ID Form. If IdenTrust sends You such notice, You must download the corresponding Certificate from the Web site specified by IdenTrust in the email within thirty (30) days of the completion date of the ID Form (i.e. the date provided on the ID Form with Your signature)

that was part of the approved application for such Certificate. If such download has not occurred within such thirty (30) day period, the ID Form becomes invalid and void for the purposes of applying for and issuing a Certificate, and the associated approval by IdenTrust will become void and this Agreement shall terminate without any refund of fees being payable by IdenTrust.

8. Certificate Issuance – Cryptomodule Requirement.

You must have and activate a Cryptomodule in order to download the Certificate. IdenTrust will provide You with instructions regarding such activation in connection with IdenTrust noticing You that issuance of the Certificate to You has been approved. Further, with respect to the Cryptomodule that You use in connection with the Certificate, You agree:

(i) to protect from disclosure to any other person Your password or other data used to activate the Cryptomodule;

(ii) not to leave the Cryptomodule unattended or open to unauthorized access while it is active; and

(iii) deactivate the Cryptomodule by manual logout or by use of an inactivity timeout function effecting automatic logout.

Unless You have applied for a type of Certificate that includes “Hardware” in the title of the Certificate type relating thereto provided to You by IdenTrust, You (and not IdenTrust) are responsible for providing the Cryptomodule that You will use, for its ability to be used with the Certificate, and for its compliance with the applicable requirements of the CP and CPS. In the event You have applied for a type of Certificate that includes “Hardware” in the title of the Certificate type relating thereto provided to You by IdenTrust and IdenTrust approves the issuance of such Certificate to You, then in addition to the other provisions hereof, the provisions of Section 10 apply to You.

9. Certificate Issuance – Review of Certificate Contents, Downloading, and Acceptance of Certificate.

Prior to the Certificate being made available to You for downloading as described in Section 7, the contents of the Certificate shall be made available to You for review and You hereby agree that You shall review such contents. The contents of the Certificate will be based on information provided by You and the Subscribing Organization during the application process, including but not limited to information provided on the completed Subscribing Organization Authorization Form and ID Form. If upon Your review of the Certificate contents You determine that any portion of the content of the Certificate is not accurate or valid, You hereby agree that You shall not download the Certificate and You shall instead immediately inform IdenTrust of the inaccurate or invalid portion(s) by contacting the IdenTrust Support by phone at 1-800-748-5360 or by email at support@IdenTrust.com.

By downloading the Certificate after its contents are made available for Your review as described above, You accept the Certificate, warrant the accuracy and validity of its contents, and reaffirm Your acceptance of the terms of this Agreement (including but not limited to each of the representations and warranties You make under this Agreement). Without limiting the foregoing, Your failure to object to the Certificate or its contents by informing IdenTrust of such objection within 24 hours of downloading it constitutes acceptance of the Certificate by You and Subscribing Organization. Notwithstanding the foregoing provisions of this paragraph, any use by You of the Certificate constitutes acceptance of the Certificate by You and Subscribing Organization.

10. Certificate Issuance – Addition Provisions for Types of Certificates that include Hardware.

In the event You have applied for a type of Certificate that includes “Hardware” in the title of the Certificate type relating thereto provided to You by IdenTrust and IdenTrust approves the issuance of such Certificate to You, You will be provided with a Hardcryptomodule by IdenTrust along with instructions regarding how to activate such Hardcryptomodule.

When You activate the Hardcryptomodule as provided in Section 8 and are issued the corresponding Certificate, You will be required to use Your Certificate to digitally sign the then-current form of this Agreement and to acknowledge receipt of the Hardcryptomodule. In the event that You do not so sign and acknowledge, it is understood that IdenTrust will revoke the Certificate.

Also, when You activate the Hardcryptomodule, during the Key Pair generation and Certificate issuance that occurs as part of the activation process, the Private Key corresponding to the Encryption Certificate is securely escrowed by IdenTrust to allow for its recovery in case You lose the Private Key or in cases where an applicable law or policy requires key recovery. Procedures and requirements applicable to the recovery of such Private Key from IdenTrust by You or Subscribing Organization are available from IdenTrust upon request.

ANY HARDCRYPTOMODULE PROVIDED BY IDENTRUST UNDER THIS AGREEMENT ARE PROVIDED "AS IS". With respect to any Hardcryptomodule provided by IdenTrust under this Agreement, You and Subscribing Organization shall rely only on such representations and warranties as are provided by the applicable original equipment manufacturers. IdenTrust will use commercially reasonable efforts to facilitate any claims You may have with, and returns of any defective products to, the original equipment manufacturer. IdenTrust does not warrant that any Hardcryptomodule will meet the requirements of Subscribing Organization or You, or that use or operation of any Hardcryptomodule will be uninterrupted or error free.

11. Declaration of Identity. In the event that IdenTrust issues a Certificate to You in connection herewith, You agree that IdenTrust may require You to provide a declaration of Your identity information on a form provide by IdenTrust and require such declaration be digitally signed by You using such Certificate. In the event that You do not so sign such declaration when provided by IdenTrust, it is understood that IdenTrust will revoke the Certificate.

12. Legal Effect of Digital Signatures. All Digital Transmissions that are signed with a Digital Signature by You using a Private Key corresponding to the Certificate shall have the same legal effect, validity, and enforceability as if the Digital Transmissions had been in writing and manually signed by You. Neither You nor Subscribing Organization will challenge the legal effect, validity, or enforceability of a Digital Transmission on the basis of such Digital Transmission being in digital, rather than in written, form. You and Subscribing Organization shall be responsible for all Digital Transmissions that are Digitally Signed by You using a Private Key corresponding to the Certificate.

13. Privacy. IdenTrust agrees to use reasonable care to safeguard personally identifying information about You obtained by IdenTrust during the application, identification and authentication, and Certificate issuance processes. Use by IdenTrust of such personally identifying information shall be limited to use as provided for under this Agreement, the CPS, the IdenTrust Privacy Policy, or by You in writing. You hereby authorize IdenTrust to contact You and Subscribing Organization with information and offers from IdenTrust related to renewals of the Certificate. You also hereby authorize IdenTrust to disclose information about You to Subscribing Organization in connection with use and administration of the Certificate.

Notwithstanding the foregoing, information contained in the Certificate and information about the status of the Certificate is not private; treating such information as private would defeat the purpose of the Certificate, which is to establish Your identity. Accordingly, IdenTrust may disclose without limitation, save for any limitations on the disclosure of such information that may set forth in the CP or CPS. any information contained in any of the Certificate, CRLs, OCSP responses, or the LDAP directory, including but not limited to the Public Keys, email address, Subscribing Organization's name, the certificate serial number, Certificate expiration date, and Certificate status such as valid, invalid, revoked, or expired.

14. Term. Certificates will be valid for the Validity Period specified therein. The term of this Agreement shall correspond to the term of the Certificate's validity. Sections 13, 14, 17 (insofar as the provisions thereof requiring You to "cease using the Certificate"), 18 – 35 of this Agreement will survive the termination, expiration, or revocation of this Agreement or the Certificate.

15. Permitted Uses of the Certificate.

The Certificate may be used for authentication, for Access Control, to create Digital Signatures, to support verification of Digital Signatures, to achieve confidentiality through the use of encipherment of shared secret, provided such use is consistent with the use described in the "Key usage extension" and "extended Key usage extension" in the Certificate.

The Signing Certificate issued in connection herewith may be used in applications where: (i) the identity of communicating parties needs to be authenticated; (ii) a message or file needs to be bound to the identity of its originator by a signature (i.e. You); or (iii) the integrity of the message or file has to be assured.

The Encryption Certificate issued in connection herewith may be used in applications where a message or file needs to be protected against disclosure to anyone else except You and intended recipients.

16. Prohibited Uses of the Certificate. Notwithstanding any other provision hereof, the Certificate must not be used for: (i) any application requiring fail-safe performance such as the operation of nuclear power facilities, air traffic control systems, aircraft navigation systems, weapons control systems, or any other system whose failure could lead to injury, death or environmental damage; or (ii) transactions where applicable law prohibits the use of Certificates for such transactions or where otherwise prohibited by law.

17. Your General Obligations.

You agree:

(i) to accurately represent You in all communications with IdenTrust;
(ii) to protect the Private Keys corresponding the Certificate that You are issued in connection herewith, including by not limited to protecting them from access by third parties and in conformity with the applicable requirements of the CP and CPS;
(iii) that You and Subscribing Organization assume the risk of any use of Your Private Key(s) or Certificates in violation of this Agreement; and
(iv) to respond in a timely manner to IGC-related notices issued by IdenTrust.

You must request that the Certificate be revoked:

(i) within one hour of You first suspecting or discovering that a Private Key corresponding to a Public Key listed in the Certificate is compromised; or
(ii) within 24 hours of You becoming aware of any information in the Certificate relating to Your identity or Your affiliation with Subscribing Organization no longer being valid, accurate, current or complete, or becomes misleading.

You may request that the Certificate be revoked at any time for reasons other than those described above in this Section 17.

You must immediately cease using the Certificate in the following circumstances:

(i) when You suspect or discover that the Private Key corresponding to the Certificate is compromised;
(ii) when any information in the Certificate is no longer accurate, current, or complete, or such information becomes misleading;
(iii) upon the revocation or expiration of the Certificate; or
(iv) upon termination of this Agreement.

In the event You have applied for a type of Certificate that includes "Hardware" in the title of the Certificate type relating thereto provided to You by IdenTrust and IdenTrust approves the issuance of such Certificate to You, You agree:

(i) that You will protect all passwords and personal identification numbers used to access the Cryptomodule corresponding to the Certificate; and
(ii) that the Private Keys corresponding to the Certificate that corresponds to the Cryptomodule never exist in plain text outside the Cryptomodule.

18. Revocation Requests by You or Subscribing Organization. You or Subscribing Organization, as applicable, can request revocation of the Certificate by:

(i) sending an email that is signed by You using the Private Key corresponding to the Certificate that You are requesting be revoked to support@IdenTrust.com;

(ii) calling the IdenTrust Support at 1-800-748-5360;
(iii) online-request via IdenTrust's online certificate management interface systems, if such systems are made available to You and You have signed up for access to such IdenTrust online systems, which such availability and access, if any, are outside the scope of this agreement; or
(iv) such other means as may be provided to You or Subscribing Organization by IdenTrust.

19. Revocation of the Certificate by IdenTrust. IdenTrust may revoke the Certificate without notice to You for any reason provided under the CPS. Unless prohibited by law or government rule, regulation, or order, in the event IdenTrust revokes the Certificate under this Section 18, IdenTrust shall use commercially reasonable efforts to promptly notify You of the action taken. Additionally, upon receiving a request for revocation of the Certificate, IdenTrust will promptly revoke the Certificate after determining the request was made by a person authorized to do so or if IdenTrust otherwise determines the Certificate should be revoked. Once a Certificate has been revoked, it cannot be used or reinstated.

20. Representations, Warranties, and Covenants from You.

You represent and warrant to IdenTrust that:
(i) all information provided by You (and Subscribing Organization) that is included in the Certificate and all representations made by You in connection with Your application for the Certificate, are true and not misleading;
(ii) each Digital Signature created using the Private Key corresponding to the Public Key listed in the Encryption Certificate is a Digital Signature by You;
(iii) the Private Keys corresponding to the Public Keys listed in the Certificate have been protected continuously since You generated them during the issuance process of the Certificate and that no unauthorized person has had access to such Private Keys; and
(iv) the Certificate and the corresponding Key Pair will and are, as applicable, being used exclusively for purposes that are authorized by the Subscribing Organization and under the CP and CPS and that are legal.

Such representations and warranties shall survive the termination hereof, but shall only apply with respect to the Certificate as it stood during its Validity Period.

You covenant to IdenTrust that:
(i) You will accurately represent yourself in all communications with IdenTrust;
(ii) You will protect the Private Keys corresponding the Certificate that You are issued in connection herewith, including but not limited to protecting such Private Keys from access by third parties and in conformity with the applicable requirements of the CP and CPS; and
(iii) You will use the Private Keys corresponding to any Certificate that You are issued in connection herewith only as allowed herein, under the CP, and Section 1.4 of the CPS.

21. Indemnification by You.

You agree to indemnify and hold harmless each PKI Service Provider (including but not limited to IdenTrust), its affiliates, and their respective directors, officers and employees for any and all loss, cost, damage, or expense (including reasonable attorneys' fees and expenses) that arises from or relates to Your:
(i) improper use of the Certificate or Key Pairs;
(ii) failure to safeguard Private Keys;
(iii) failure to comply with the provisions of the CP, the CPS, or this Agreement,
(iv) breach of any representation or warranty made by You hereunder, or
(v) acts or omissions giving rise to a loss by any PKI Service Provider.

For purposes of the foregoing provisions of this Section, each PKI Service Provider other than IdenTrust, is a third-party beneficiary.

22. Representations, Warranties, and Covenants from Subscribing Organization.

Subscribing Organization:
(i) represents and warrants that it authorizes the affiliation of You with Subscribing Organization for the Certificate, as such affiliation is described under the CP and CPS;
(ii) represents and warrants that any information that it may provide in connection with the application process related to the Certificate, including but not limited to identity information, is accurate, current, and complete;
(iii) represents and warrants that it is duly-organized and validly-existing under the laws of its state of organization, to perform all duties and obligations of Obligation, and has full right and authority to use the Subscribing Organization's name set forth on the Subscribing Organization Authorization Form for purposes of identifying Subscribing Organization in the Certificate; and
(iv) covenants that it will immediately request revocation of the Certificate by IdenTrust if (a) information contained in the Certificate is no longer accurate or current (e.g., Your name changes, Your email address changes), or (b) You no longer an employee, contractor, or agent of the Subscribing Organization, or (c) You are no longer authorized by Subscribing Organization to transact business or make Digital Signatures on behalf of Subscribing Organization.

Such representations, warranties, and covenants shall survive the termination hereof, but shall only apply with respect to the Certificate as it stood during its Validity Period.

23. Indemnification by Subscribing Organization.

Subscribing Organization agrees to indemnify and hold harmless IdenTrust, its affiliates, and their respective directors, officers and employees from any and all loss, cost, damage, or expense (including reasonable attorneys' fees and expenses) arising from or related to:

(i) any misrepresentation or omission of material fact made by Subscribing Organization or You to IdenTrust;
(ii) any breach of this Agreement, the CP, or the CPS by Subscribing Organization or You; or
(iii) any misuse of the Certificate (other than by IdenTrust).

24. IdenTrust Representations and Warranties.

IdenTrust provides the representations and warranties set forth in Section 9.6.1 of the CPS to the extent such are applicable with respect to the Certificate that is the subject of this Agreement. Such representations and warranties shall survive the termination hereof, but shall only apply with respect to the Certificate as it stood during its Validity Period.

25. Disclaimer of Warranties; Limitations on Liability.

EXCEPT FOR THE REPRESENTATIONS AND WARRANTIES EXPRESSLY PROVIDED BY IDENTRUST ABOVE IN SECTION 24, IDENTRUST DISCLAIMS ANY AND ALL OTHER WARRANTIES OF ANY TYPE, WHETHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY IMPLIED WARRANTY OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE, WITH REGARD TO ANY SERVICES OF IDENTRUST PROVIDED IN CONNECTION HEREWITH OR THE CERTIFICATE.

IDENTRUST SHALL HAVE NO LIABILITY: (I) FOR LOSS DUE TO USE OF THE CERTIFICATE, UNLESS THE LOSS IS PROVEN TO BE A DIRECT RESULT OF A BREACH BY IDENTRUST OF THIS AGREEMENT OR THE CPS OR A PROXIMATE RESULT OF THE GROSS NEGLIGENCE, FRAUD OR WILLFUL MISCONDUCT OF IDENTRUST. IDENTRUST SHALL HAVE NO LIABILITY FOR CLAIMS ALLEGING ORDINARY NEGLIGENCE; OR (II) IF IDENTRUST IS PREVENTED, FORBIDDEN OR DELAYED FROM PERFORMING, OR OMITS TO PERFORM, ANY ACT OR REQUIREMENT BY REASON OF ANY PROVISION OF ANY APPLICABLE LAW, REGULATION, OR ORDER, THE FAILURE OF ANY ELECTRICAL, COMMUNICATION, OR OTHER SYSTEM OPERATED BY ANY PARTY OTHER THAN IDENTRUST OR ANY ACT OF GOD, EMERGENCY CONDITION OR WAR OR OTHER CIRCUMSTANCE BEYOND THE CONTROL OF IDENTRUST.

NOTWITHSTANDING ANY OTHER PROVISION HEREOF, NEITHER IDENTRUST NOR ANY PKI SERVICE PROVIDER SHALL HAVE ANY LIABILITY ARISING FROM IMPROPERLY USED OR IMPROPERLY RELIED UPON CERTIFICATES.

IN NO EVENT SHALL IDENTRUST'S TOTAL, AGGREGATE LIABILITY UNDER THIS AGREEMENT EXCEED AN AMOUNT EQUAL TO THE ACUTAL AMOUNT PAID TO IDENTRUST FOR ISSUANCE OF THE CERTIFICATE TO YOU HEREUNDER.

NOTWITHSTANDING ANY OTHER PROVISION HEREOF AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL IDENTRUST BE LIABLE FOR ANY EXEMPLARY, PUNITIVE, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, INCLUDING, WITHOUT LIMITATION, ANY LOSS OF PROFITS, LOSS OF DATA, OR COST OF PROCUREMENT OF SUBSTITUTE SERVICES, HOWEVER CAUSED, AND ON ANY THEORY OF LIABILITY, WHETHER FOR BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE AND STRICT LIABILITY), OR OTHERWISE. THE FOREGOING LIMITATIONS WILL APPLY WHETHER OR NOT IDENTRUST HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, WHETHER OR NOT IDENTRUST COULD HAVE FORESEEN SUCH DAMAGES, AND NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY.

EACH PARTY HERETO UNDERSTANDS THAT THE FOREGOING LIMITATION OF LIABILITY AND RECOURSE IS AN ESSENTIAL INDUCEMENT TO IDENTRUST TO ENTER INTO THIS AGREEMENT AND PROVIDE THE SERVICES.

26. Dispute Resolution.

In the event of any dispute or disagreement between the parties hereto ("Disputing Parties") arising out of or related to this Agreement or the Server Certificate, the Disputing Parties will use their best efforts to settle the dispute or disagreement through mediation or good faith negotiations following notice from one Disputing Party to the other. If the Disputing Parties cannot reach a mutually agreeable resolution of the dispute or disagreement within sixty (60) days following the date of such notice, then the Disputing Parties will submit the dispute to binding arbitration, as provided below.

Except for a controversy, claim, or dispute involving the federal government of the United States or a "Core Proceeding" under the United States Bankruptcy Code, the parties agree to submit any controversy, claim, or dispute, whether in tort, contract, or otherwise arising out of or related in any way to this Agreement, that cannot be resolved by mediation or negotiations between the parties, for resolution by binding arbitration by a single arbitrator, and judgment upon the award rendered by the arbitrator may be entered in any court having jurisdiction over the parties. The arbitrator will have no authority to impose penalties or award punitive damages. Binding arbitration will: (i) proceed in New York County, New York; (ii) be governed by the Federal Arbitration Act (Title 9 of the United States Code); and (iii) be conducted in accordance with the Commercial Arbitration rules of the American Arbitration Association ("AAA"). Each party will bear its costs for the arbitration; however, upon award of any judgment or conclusion of arbitration, the arbitrator will award the prevailing party the costs it expended in such arbitration. Unless the arbitrator otherwise directs, the parties, their representatives, other participants, and the arbitrator will hold the existence, content, and result of the arbitration in confidence. This arbitration requirement does not limit the right of any party to obtain provisional ancillary remedies such as injunctive relief or the appointment of a receiver, before, during, or after the pendency of any arbitration proceeding. This exclusion does not constitute a waiver of the right or obligation of any party to submit any dispute to arbitration.

27. Choice of Law; Conflicts. Subject to any limits appearing in applicable law, the laws of the state of New York, U.S.A., shall govern the enforceability, construction, interpretation, and validity of this CPS, irrespective of contract or other choice of law provisions. If any provision of this Agreement is found to be invalid or unenforceable, then this Agreement shall be deemed amended by modifying

such provision to the extent necessary to make it valid and enforceable while preserving its intent or, if that is not possible, by striking the provision and enforcing the remainder of this Agreement.

28. Assignment. Neither You nor Subscribing Organization will assign any of their rights or obligations under this Agreement without the written consent of IdenTrust. Any assignment in violation of the foregoing sentence shall be null and void.

29. Third Party Beneficiaries. Each Relying Party is an intended third-party beneficiary of each representation, warranty, and covenant made by any of Subscribing Organization or You hereunder.

30. Relationship of The Parties. Nothing in this Agreement shall be deemed to create a partnership or joint venture or fiduciary relationship between IdenTrust and any other party, nor make another party the agent, partner, employee, or representative of IdenTrust.

31. Headings and Titles. The headings and titles contained in this Agreement are included for convenience only, and will not limit or otherwise affect the terms of this Agreement.

32. Waiver. No waiver by either party of any default will operate as a waiver of any other default, or of a similar default on a future occasion. No waiver of any term or condition by any party will be effective unless in writing and signed by the party against whom enforcement of such waiver is sought.

33. Severability. In case one or more of the provisions of this Agreement should be held invalid, illegal or unenforceable in any respect for any reason, the same will not affect any other provision in this Agreement, which will be construed to give maximum effect to the extent of the parties as evidenced by this original Agreement as originally drafted save to the extent of such invalid, illegal or unenforceable provision.

34. Entire Agreement. This Agreement represents the entire agreement of the parties, and supersedes all other agreements and discussions relating to the subject matter hereof. Except as expressly provided otherwise in this Agreement, this Agreement may not be amended except in writing signed by the parties.

35. Definitions. Unless otherwise defined below, capitalized terms used in this Agreement have the meaning given them in the CPS.

"Certificate" means a digital certificate of the "IGC Basic Software" assurance level as provided in for in the CPS and subject to the terms hereof, and which is applied for by You in connection with this Agreement. The "Certificate" is comprised of which is comprised of two digital certificates, one the Signing Certificate and the other the Encryption Certificate, which are to be construed hereunder as a single digital certificate unless indicated otherwise through the use of the term "Signing Certificate" or "Encryption Certificate". Also, when "Certificate" is used herein, such use is to be constructed to include an "if issued" condition.

"Compromised" means a given Private Key is in danger of being lost, disclosed, or subjected to unauthorized use in any way.

"CP" means the most recent version of the *IdenTrust Global Common Certificate Policy* posted by IdenTrust to the Repository, which may be amended from time to time by IdenTrust in its sole discretion.

"CPS" means the most recent version of the *Certificate Practice Statement for IdenTrust Global Common Certificate Policy* posted by IdenTrust to the Repository, which may be amended from time to time by IdenTrust in its sole discretion.

"Cryptomodule" means a hardware device (which includes any accompanying device reader hardware and any software embedded in the hardware device or reader) or software program that: (i) generates Key Pairs; (ii) stores cryptographic information (such as the Private Key); and (iii) performs cryptographic functions.

"Digital Signature" means the transformation of an electronic record by one person using a Private Key and Public Key Cryptography so that another person having the transformed record and the corresponding Public Key can accurately determine: (a) whether the transformation was created using the Private Key that corresponds to the Public Key; and (b) whether the record has been altered since the transformation was made.

"Encryption Certificate" means a Public Key Cryptography certificate that contains a Public Key that is intended to be used for encrypting data, rather than for verifying Digital Signatures or performing other cryptographic functions.

"Hardcryptomodule" means a hardware Cryptomodule, typically in the form of a USB token or other smartcard.

"ID Form" means the ID Form completed and signed in connection herewith.

"IdenTrust" means IdenTrust Services, LLC.

"IdenTrust Privacy Policy" means the then-current version of the Privacy Policy located at: identrust.com/privacy.html

"IGC Basic Assurance Affiliated Certificate" has the meaning given "Certificate" herein. An IGC Basic Assurance Affiliated Certificate can be issued with hardware or in software.

"Key Pair" means two mathematically related Keys (a Private Key and its corresponding Public Key), having the properties that: (a) one Key can be used to encrypt a communication that can only be decrypted using the other Key; and (b) even knowing one Key it is computationally infeasible to discover the other Key.

"Operational Period" means the Certificate's actual term of validity, beginning with the start of the Validity Period and ending on the earlier of: (i) the end of the Validity Period disclosed in the Certificate; or (ii) the revocation of the Certificate.

"PKI Service Provider" has the meaning provided such term in the CPS.

“Private Key” means the key of a Key Pair kept secret by its holder and that can be used by its holder to encrypt or decrypt messages or to create a Digital Signature.

“Public Key” means the key of a Key Pair publicly disclosed by the holder of the corresponding Private Key and that can be used to validate Digital Signatures created with the corresponding Private Key and to encrypt messages or files to be decrypted with the corresponding Private Key.

“Public Key Cryptography” means a form of cryptography (a process of creating and deciphering communications to keep them secure) in which two keys are used. One key encrypts a message, and the other key decrypts the message. One key, the Private Key, is kept secret, and the other, the Public Key, is made available to others. These keys are, in essence, large mathematically related numbers that form a unique pair. Either key may be used to encrypt a message, but only the other corresponding key may be used to decrypt the message.

“Registrar” has the meaning set forth in the CPS.

“Repository” means the information and data repository of IdenTrust located at the following address: https://www.identrust.com/support/documents/igc

“Signing Certificate” means a Public Key Cryptography certificate that provides authentication of the identity claimed by the certificate holder named in such certificate and create Digital Signatures.

"Subscribing Organization" shall mean the entity described as such in the Subscribing Organization Authorization Form completed and singed in connection herewith. Subscribing Organization is a “Subscribing Organization” for the purposes of the CP and CPS.

“Subscribing Organization Authorization Form” means the ID Form completed and signed in connection herewith.

“Validity Period” is the intended term of validity of a Certificate, beginning with the “notBefore” date asserted in the Certificate and ending with the “notAfter” date asserted in the Certificate.

“You” and “Your” refers to the person who is identified in the ID Form and who is identified as the “Subscriber” in the Subscribing Organization Authorization Form. You is a “Subscriber” for the purposes of the CP and CPS.