

IGC
PIV-I Hardware Certificate and
PIV-I Card Authentication Certificate
Forms Packet

Copyright © 2020 IdenTrust Services, LLC. All rights reserved.



Instructions for the Applicant

Thank you for choosing IdenTrust Services, LLC (“IdenTrust”), a subsidiary of IdenTrust, Inc., to issue you an IGC PIV-I Hardware Certificate and IGC PIV-I Card Authentication Certificate..

THE ONLINE APPLICATION:

Complete the application process online at www.IdenTrust.com/Buy_IGC

PART 1 FORM:

Complete Part 1 – Subscribing Organization Authorization Form. Take Part 1 – Subscribing Organization Authorization Form to an officer in your Subscribing Organization (i.e. the entity named on in the “Subscribing Organization” field in Part 1 – Subscribing Organization Authorization Form) who can sign on behalf of your Subscribing Organization and bind your Subscribing Organization to the terms and conditions of Part 1 – Subscribing Organization Authorization Form. Have such officer sign Part 1 – Subscribing Organization Authorization Form and give you the signed (ink-on-paper) original document for you to send to IdenTrust. In the event your Subscribing Organization does not have an “officer”, then Part 1 – Subscribing Organization Authorization Form must be signed by an authorized representative of the Subscribing Organization with sufficient authority to bind the Subscribing Organization to the terms and conditions of Part 1 – Subscribing Organization Authorization Form.

PART 2 FORM:

Take this form to a licensed notary 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

- U.S. 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 Support@IdenTrust.com and follow the steps laid out.

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 Wiley Post Way, Ste 450
Salt Lake City, UT 84116-2898

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

IGC CERTIFICATE PROGRAM

**IGC PIV-I Hardware Certificate and IGC PIV-I Card Authentication 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 PIV-I Hardware Certificate and IGC PIV-I Card Authentication Certificate (together, 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 PIV-I Hardware Certificate and IGC PIV-I Card Authentication Certificate Subscriber Agreement (attached hereto; see Part 3 – IGC PIV-I Hardware Certificate and IGC PIV-I Card Authentication Certificate Subscriber Agreement), and the terms and conditions of the IGC PIV-I Hardware Certificate and IGC PIV-I Card Authentication 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 at any time by: (i) sending an email to Support@IdenTrust.com; (ii) calling 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 CERTIFICATE PROGRAM

IGC PIV-I Hardware Certificate and IGC PIV-I Card Authentication 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 the Certificate (“Certificate” is defined in Part 3 – IGC PIV-I Hardware Certificate and IGC PIV-I Card Authentication 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 PIV-I Hardware Certificate and IGC PIV-I Card Authentication Certificate Subscriber Agreement.

Sign only in the presence of a notary (or other Registrar; “Registrar” is defined in Part 3 – IGC PIV-I Hardware Certificate and IGC PIV-I Card Authentication 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	Two verifiable forms of ID issued by a state or local government At least one must be a photo ID	
PHOTO ID	PHOTO ID	2 ND 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).

Section 2: Notarial (or other eligible Registrar) Acknowledgement

I, _____ registered in (if notary) / resident of (if other Registrar than notary) in the state of _____, county of _____ do hereby certify under PENALTY OF PERJURY under the laws of such state that the following information is true and correct:

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

WITNESS my hand and, if this Section 2 is executed by a notary, official seal.

(Signature)

(Seal)

IGC CERTIFICATE PROGRAM

**PART 3 – IGC PIV-I HARDWARE CERTIFICATE AND
IGC PIV-I CARD AUTHENTICATION CERTIFICATE SUBSCRIBER AGREEMENT**

This IGC PIV-I Hardware Certificate Agreement Certificate and IGC-PIV-I Card Authentication 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 forth the 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 37 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 at any time by IdenTrust with effect thirty (30) days after IdenTrust posts amended terms to the Repository. The terms of this Agreement may also be amended upon renewal of the Certificate by the presentation of the then-current form of this Agreement to You during the renewal process and going into effect upon such renewal. 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 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 but 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 if 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, a Certificate in connection herewith. IdenTrust shall have no liability for any delay experienced during the Certificate application and issuance process.

IGC CERTIFICATE PROGRAM

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 Sections 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 notice You that the Certificate is ready to be issued. To so notice You, IdenTrust will email You at the email address for You 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). 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 and store the Certificate. 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.

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 and other data used to activate the Cryptomodule or access the Certificate after it is downloaded to 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.

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's contents You determine the 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 IdenTrust Support by phone at 1-888-248-4447 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 the Certificate's 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 the Certificate 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 – Cryptomodule Requirements.

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

Also, when You activate the Cryptomodule, 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 recovery of such Private Key in case You lose such Private Key or in cases where an applicable law or policy requires 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.

IGC CERTIFICATE PROGRAM

11. Declaration of Identity. In the event 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 provided by IdenTrust and require such declaration be digitally signed by You using such Certificate. In the event 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 Signing Certificate shall have the same legal effect, validity, and enforceability as if the Digital Transmissions had been in writing and manually signed by You, and neither You nor Subscribing Organization will challenge the legal effect, validity, or enforceability of such a Digital Transmission or Digital Signature on the basis of it 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 Signing 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 any of this Agreement, the CPS, or the IdenTrust Privacy Policy. In addition, without forming any limitation on the immediately preceding sentence, use by IdenTrust may include additional uses to those provided for in such sentence provided such additional uses are authorized 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, including but not limited to utility of the Certificate in establishing your identity to other entities and encrypting your communications with other entities. Accordingly, IdenTrust may publically publish and otherwise, subject to 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 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. The Certificate will be valid for the Validity Period specified therein. The term of this Agreement shall correspond to the term of the Certificate's validity, except where such Certificate is renewed as the result of a transaction between You and IdenTrust. In the event of such a renewal, the term of this Agreement shall be deemed to continue in effect with the terms of this Agreement amended as described in Section 2 as it relates to amendment in connection with renewal. Sections 13, 14, 17 (insofar as the provisions thereof requiring You to "cease using the Certificate"), and 18 – 37 of this Agreement will survive the termination or expiration of this Agreement.

15. Permitted Uses of the Certificate.

The Signing Certificate may be used (a) in applications where a message or file needs to be bound to the identity of its originator (i.e. You) by a Digital Signature, (b) to support verification of Digital Signatures, or (c) the integrity of the message or file is to be determined by the use of a Digital Signature.

The Encryption Certificate may be used for encryption services, such as encrypting electronic messages, files, documents, or data transmissions.

The Identity Certificate may be used for purposes of authentication of You by any Relying Party.

The Identity Certificate may be used by a Relying Party to authenticate You.

The Card Auth Cert may be used for purposes of identifying that the Cryptomodule which is associated with such Card Auth Cert during activation as provided for under Section 8 is a Cryptomodule of Sponsoring Organization.

Notwithstanding the foregoing provisions of this Section 15, any use of the Certificate by You must be consistent with the use described in the "Key usage extension" and "extended Key usage extension" in such Certificate.

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 a Certificate 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;

IGC CERTIFICATE PROGRAM

- (ii) to protect the Private Keys corresponding the Certificate that You are issued in connection herewith, including but 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 the Certificate in violation of this Agreement;
- (iv) to respond in a timely manner to IGC-related notices issued by IdenTrust;
- (v) that You will protect all passwords and personal identification numbers used to access the Cryptomodule corresponding to the Certificate; and
- (vi) that the Private Keys corresponding to the Certificate that corresponds to the Cryptomodule never exist in plain text outside the Cryptomodule.

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 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.

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 IdenTrust Support at 1-888-248-4447;
- (iii) request made to IdenTrust via the IdenTrust online certificate management interface system, if such system are made available to You and You have signed up for access to such IdenTrust online system, 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 for herein or under the CPS. Unless prohibited by law or government rule, regulation, or order, in the event IdenTrust revokes the Certificate under this Section 19, 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. IdenTrust shall have no liability related to or arising from revocation of the Certificate as provided for under herein or under the CPS. The revocation of any one of the Digital Certificates that are referenced by the term "Certificate" hereunder shall be deemed and construed to require the revocation of all Digital Certificates associated with the definition of the term "Certificate" hereunder.

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;

IGC CERTIFICATE PROGRAM

- (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 his or herself in all communications with IdenTrust;
- (ii) You will protect the Private Keys corresponding the Certificate that You are issued in connection herewith, including by 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 uses 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., You changes his or her name, Your email address changes), or (b) You are 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;

IGC CERTIFICATE PROGRAM

- (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 – General.

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 OMITTS 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 AN IMPROPERLY USED OR IMPROPERLY RELIED UPON CERTIFICATE.

IN NO EVENT SHALL IDENTRUST'S TOTAL, AGGREGATE LIABILITY UNDER THIS AGREEMENT EXCEED AN AMOUNT EQUAL TO THE ACTUAL 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. Limitation of Liability – Federal and State Sovereign Immunity-Based Limitations.

In the event the Sponsoring Organization is an entity formed and existing under the Federal laws of the United States of America and is designated under Federal law as a part or agency of the Federal government of the United States under Federal law relating to the doctrine of sovereign immunity (the "Federal Sovereign Immunity Law"), then liability of Sponsoring Organization under Section 23 and liability of You under Section 21 shall be limited solely to the extent necessary to comply with the Federal Sovereign Immunity Law insofar as such laws apply to and limit the liability of, respectively, the Sponsoring Organization and You.

In the event the Sponsoring Organization is an entity formed and existing under the laws of a State among the United States of America (the "SO State") and is designated under the laws of the SO State as a part or agency of the government of the SO State under laws of the SO State relating to the doctrine of sovereign immunity (the "State Sovereign Immunity Law"), then liability of Sponsoring Organization under Section 23 and liability of You under Section 21 shall be limited solely to the extent necessary to comply with the State Sovereign Immunity Law insofar as such laws apply to and limit the liability of, respectively, the Sponsoring Organization and You.

27. Export.

IGC CERTIFICATE PROGRAM

The laws of some countries restrict the use, import, or export of encryption hardware and software. Where You receive or take the Certificate outside of the United States of America, You and Subscribing Organization each assume the risk for doing so and also undertake to fully comply with applicable laws and regulations relating to export and import and, without forming limitation on the foregoing, undertake to obtain any license, permit, or any approval that may be required.

28. 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 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.

29. Choice of Law; Conflicts. 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.

30. 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.

31. 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. Other than as provided in Section 21 and this Section 31, there are no third party beneficiaries to this Agreement. IdenTrust shall have neither liability nor responsibility under this Agreement to any Relying Party.

32. 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.

33. 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.

34. 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.

35. 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.

36. Entire Agreement. This Agreement represents the entire agreement of the parties, and supercedes 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.

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

IGC CERTIFICATE PROGRAM

“Card Auth Cert” means a Digital Certificate intended to be used to authenticate the Cryptomodule as being associated with the Subscribing Organization; provided, however, when “Card Auth Certificate” is used herein, such use is to be constructed to include an “if issued” condition.

“Certificate” means each of the following Digital Certificates, interchangeably:

- (i) An Encryption Certificate that is one of three Digital Certificates that together are identified as an “IGC PIV-I Harder” Digital Certificate under the CPS;
- (ii) An Identity Certificate that is one of three Digital Certificates that together are identified as an “IGC PIV-I Harder” Digital Certificate under the CPS;
- (iii) A Signing Certificate that is one of three Digital Certificates that together are identified as an “IGC PIV-I Harder” Digital Certificate under the CPS; and
- (iv) A Digital Certificate of the type named “IGC PIV-I Card Authorization Certificate” in the CPS, which consists of a single Card Auth Cert.

“Digital Certificate” means “Certificate” as defined in the CPS.

“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 that is compliant with the requirements set forth in Section 11 of the CPS.

“Digital Signature” means the transformation of an electronic record by one person using a Private Key and Public Key Cryptography so that a 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 Digital 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; provided, however, when “Encryption Certificate” is used herein, such use is to be constructed to include an “if issued” condition. See “Certificate” for more information.

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

“Identity Certificate” means a Digital Certificate that is intended to be used to by a Relying Party to authenticate You and intended to be used to log You into computer applications and computers; provided, however, when “Identity Certificate” is used herein, such use is to be constructed to include an “if issued” condition.. See “Certificate” for more information.

“IdenTrust” means IdenTrust Services, LLC.

“IdenTrust Privacy Policy” means the then-current version of the Privacy Policy located at the following address: <https://www.identrust.com/privacy.html>

“IGC Medium Hardware Certificate” has the meaning given “Certificate” herein.

“Key Pair” means two mathematically related keys, one of which is a Private Key and the other the Public Key corresponding to such Private Key), with such two keys 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, with respect to a Key Pair, the key that is 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, with respect to a Key Pair, the key that is 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.

IGC CERTIFICATE PROGRAM

“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.

“Relying Party” means an entity (natural or otherwise) that fulfills and complies with all the duties and obligations of a “Relying Party” (as provided for in the CPS).

“Repository” means the information and data repository of IdenTrust located at the following address: <https://secure.identrust.com/certificates/policy/igc/index.html>

“Signing Certificate” means a Public Key Cryptography certificate that provides authentication of the identity claimed by the certificate holder named in such certificate and is intended to be used to create Digital Signatures; provided, however, when “Signing Certificate” is used herein, such use is to be constructed to include an “if issued” condition. See “Certificate” for more information.

“Subscribing Organization” shall mean the entity described as such in the Subscribing Organization Authorization Form completed and signed 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.