IdenTrust
part of HID Global

DoD ECA
Medium Assurance TLS/SSL Certificate
Forms Packet

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 ECA SSL/TLS certificate. Unless otherwise defined on this page, capitalized terms have the meaning provided such term in Part 3: IdenTrust Services ECA SSL/TLS Certificate Subscriber Agreement.

Enrollment for an ECA digital certificate requires that you complete an online application as well as complete and return the following forms:

1. Part 1 – Subscribing Organization Authorization Agreement
2. Part 2 – In-person Identification Form

PLEASE NOTE: YOU HAVE ***30 DAYS*** AFTER YOU SIGN THESE FORMS TO COMPLETE THE APPLICATION PROCESS *AND* RETRIEVE YOUR CERTIFICATE.

Follow these instructions to successfully apply and complete paperwork for the ECA digital certificate.

THE ONLINE APPLICATION:

Please select one of the certificate options located here: http://www.identrust.com/certificates/eca/buy_eca.html and complete the online registration process.

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 to verify your identity credentials. You will need to present an ID for 2 of the 3 lists below.

US Citizens: One from List A *and* one from list B or C, – or – One from List B *and* one from List C.
Non-US Citizens: Valid Passport *and* one from List B.

If you made more than one citizenship assertion in your certificate request, you must provide a valid passport for each.

List A – Photo ID document that establishes identity and citizenship

- Passport from country of citizenship
- Certificate of U.S. Citizenship issued by USCIS (formerly INS)
- Certificate of Naturalization issued by a court of competent jurisdiction prior to October 1, 1991 or the USCIS (INS) since that date

List B – Photo ID document that establishes identity

- Military ID w/ photo
- Driver's license or government-issued ID card w/ photo
- Permanent or Unexpired Temporary Resident Card issued by the USCIS w/ photo

List C – Document that establishes US Citizenship

- Consular Report of Birth from a US Consulate (Form FS-240)
- Certificate of Birth Abroad issued by the US Department of State (Form DS-1350)
- Original or certificated copy of birth certificate issued by County, State or government authority bearing an official seal

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.

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. You have 30 days after you sign these forms to complete the application process and retrieve your certificate.

Part 1: Subscribing Organization Authorization Agreement

Subscribing Organization ("Organization"), identified below, acknowledges that IdenTrust Services, LLC ("IdenTrust"), an External Certification Authority ("ECA") for the Department of Defense, may, if IdenTrust accepts the application for an ECA SSL/TLS Certificate of which this agreement is part, issue one or more ECA SSL/TLS Certificates (each, a "Certificate") to a device or system identified herein below by its “Component Identifier” and which is owned or controlled by Organization (such device or system, the “Applicant” and, if an ECA SSL/TLS Certificate is issued to such Applicant, the “Subscriber”). Certificates, if issued by IdenTrust, will identify the Applicant as being owned or controlled by Organization and include Organizations name for such purpose. This Part 1: Subscribing Organization Authorization Agreement is referred to herein as the “Agreement”.

Except where otherwise defined herein, capitalized terms used herein shall have the meaning given to them in the public version of IdenTrust's DOD ECA Certification Practices Statement (https://secure.identrust.com/certificates/policy/eca/) ("the CPS") and the ECA Certificate Policy (http://iase.disa.mil/pki/eca/Documents) ("the CP"). The public version of the CPS, the CP, the Appendix A to Part 1: Terms and Conditions attached hereto and the Part 2: In-Person Identification Form submitted by Applicant to IdenTrust in connection herewith ("ID Form"), are incorporated by reference herein. Organization acknowledges and accepts that IdenTrust has the right to modify the CPS from time to time and that the CPS as so modified shall automatically supersede the prior version of the CP integrated herein. IdenTrust and Organization acknowledge and accept that the Department of Defense (or its designee) has the right to modify the CP from time to time and that the CP as so modified shall automatically supersede the prior version of the CP integrated herein.

IdenTrust and Organization agree that with respect to US government affiliated Applicants, US government affiliated Subscribers and US government Relying Parties, this Agreement and its attached Terms and Conditions shall be governed by the Contracts Disputes Act of 1978, as amended (41 US.C. § 601 et seq.). Subject to the foregoing sentence and to the extent not in conflict with the provisions of the CP, with respect to State governments affiliated Applicants, State government affiliated Subscribers, and State government Relying Parties, this Agreement and its attached Terms and Conditions shall be construed, interpreted, and enforced in accordance with the substantive laws of that State, without regard to its conflicts of law rules. Subject to the foregoing provisions of this paragraph and to the extent not in conflict with the provisions of the CP, in all other cases, irrespective of the place of performance, this Agreement and its attached Terms and Conditions shall be construed, interpreted, and enforced in accordance with the substantive laws of the State of Utah, without regard to its conflicts of law rules. The parties agree that the United Nations Convention on Contracts for the International Sale of Goods shall not apply to this Agreement.

Organization warrants, represents, and agrees that:
(a) Organization agrees to be bound by the Terms and Conditions set forth in the Appendix A to this Part 1: Terms and Conditions;
(b) It is duly-organized and validly-existing under the laws of its jurisdiction of organization and has full right and authority to use the Organization's name, given below, to grant this authorization, and to perform all obligations required of it hereunder;
(c) PKI Sponsor is a duly-authorized employee, contractor, or agent of the Organization;
(d) IdenTrust is hereby authorized by Organization to issue a Certificate to Subscriber that identifies Subscriber as (1) a system or device owned or controlled by Organization and (2) affiliated with organization;
(e) Federal agencies, and other recipients of messages signed with Subscriber's Private Key, may rely on such messages to the same extent as though they were sent by the Subscriber listed in a valid, unrevoked, and unexpired Certificate issued by IdenTrust; and
(f) All information provided to IdenTrust by Organization is and will be accurate, current, complete, and not misleading.

The undersigned personally warrants and represents that he or she is an officer or similarly authorized representative of the Organization (such officer or other authorized representative, an “Officer”) and has authority to make the representations and warranties in this Agreement on behalf of the Organization and to bind the Organization to the Terms and Conditions attached hereto by his or her signature.

Print Device Name (i.e. Fully Qualified Domain Name)	Organization Officer’s signature
Print PKI Sponsor (Human Applicant) Name	Print Organization Officer’s name
Print Organization name	Print Organization Officer’s title
Address line 1	Organization Officer’s telephone number
Address line 2	Organization Officer Email
City, State/Province, Country, Postal Code	Date Organization Officer signed

ALL FIELDS MUST BE COMPLETED

Appendix A to Part 1
Terms and Conditions

1. Certification Services from IdenTrust

a. Provided IdenTrust approves the application of Applicant and on request by the Subscriber, IdenTrust agrees to issue an ECA SSL/TLS Certificate as specified in the ECA CPS. With respect to the issuance and revocation of ECA SSL/TLS Certificates, IdenTrust and the Subscribing Organization agree to perform as required of each in the CP, the CPS, and the Subscribing Organization Authorization Agreement, inclusive of all terms integrated therein by reference. IdenTrust and the Subscribing Organization agree that with respect to IdenTrust's provision of ECA certification services and the Subscribing Organization's use or enjoyment of them are subject to the ongoing oversight and authority of the EPMA as provided for in the ECA CP.

b. In connection with registration of each Subscriber affiliated with the Subscribing Organization, Subscriber enters into an agreement with each Subscriber, separate from other Subscribers, if any, affiliated with Subscribing Organization.

2. Obligations of the Subscribing Organization

Organization agrees that it will require each of its Subscribers to carefully and fully comply with each of the provisions of the Subscriber Agreement.

3. Fees

Fees of IdenTrust for Certificates are published on the IdenTrust website. There is no fee for Certificate revocation. When a Subscriber applies for a Certificate, the initial fee is charged in connection with the application and shall be due and payable upon submission of the application and is not subject to refund, even if such application is abandon by the Applicant or Subscribing Organization or it is determined by IdenTrust, in its sole discretion, that Applicant is not eligible for to become a Subscriber. Renewal fees for Certificates are charged upon renewal. If Certificates are to be applied for via a "bulk load" procedure, an aggregate fee for all such Certificates applied for will be charged to the Subscribing Organization.

4. Use and Disclosure of Information

IdenTrust agrees to take reasonable care to ensure that private information submitted or obtained during the application, identification and authentication, and certificate issuance processes will be kept confidential. Such information includes, but is not limited to, contact information, billing, and payment details, and sometimes information gained in the course of providing consulting, implementation, sales or other support services to the Subscribing Organization. This agreement restricts IdenTrust's use of that information solely to the purposes for which it was collected, and prohibits its disclosure to third parties, except as may be required by law, court order, or as required for IdenTrust to comply with the CP and CPS. Access to sensitive Subscriber-related information within IdenTrust is limited to (a) IdenTrust employees with a "need to know" such information for the uses described in the immediately preceding sentence, and (b) IdenTrust's and the DoD's auditors on a need-to-know basis. Access to that information in IdenTrust customer databases is limited accordingly using the structure and access limits of those databases. Notwithstanding the foregoing provisions of this Section 6, the following information is not confidential: (i) information contained in any ECA SSL/TLS Certificate; (ii) status (e.g. valid, invalid, revoked) information regarding any ECA SSL/TLS Certificate; and (iii) if revocation has occurred, information identifying the reason for revocation where such information is consistent with the standards set forth in RFC 5280 (as published at https://www.ietf.org/rfc/rfc5280.txt) (or any successor standard published by the Internet Engineering Task Force which supersedes it) relative to describing the reason for revocation. Accordingly and without forming any limitation on the immediately preceding sentence, it is understood that (y) IdenTrust may disclose the Subscriber's name, Public Key, email address, Organization name, certificate serial number, and certificate expiration date to any person and for any purpose, and (z) information disclosed by IdenTrust via any "repository", OCSP response, or CRL as such are provided for in the CP and CPS is also not confidential, and, where not prohibited in the CP, IdenTrust may also disclose such information by other means in response to requests made to IdenTrust. Subscriber and Subscribing Organization each agree that with respect to information of Subscriber and information of Subscribing Organization held treated as confidential under the provision of this Section, IdenTrust may disclose such information to each of Subscriber and Subscribing Organization, separately.

5. Incorporation by Reference

Section 2, Section 5 and Sections 7 through 12 of the Part 3: IdenTrust Services ECA SSL/TLS Certificate Subscriber Agreement are hereby incorporated by reference as though fully set forth herein.

Part 2: In-person Identification Form

Terms and Conditions

The undersigned ("PKI Sponsor")attests that all facts and information provided in Part 1: Subscribing Organization Authorization Agreement and this Part 2: In-person Identification Form are accurate, current, complete, and not misleading and that he or she: a) authorized by his or her Subscribing Organization (as identified on the Part 1: Subscribing Organization Authorization Agreement naming him or her as "PKI Sponsor" in connection with the application made for a digital certificate in connection with this Part 2: In-person Identification Form) to apply for, be issued, and use an ECA SSL/TLS Certificate issued by IdenTrust; b) has reviewed and accepts as identifying himself or herself the personal identifying information set forth below on this Part 2 – In-person Identification Form; c) is who he or she represents himself or herself to be; and d) has read, understood, and accepts the terms and conditions set forth in Part 3: IdenTrust Services ECA SSL/TLS Certificate Subscriber Agreement.

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)

Identification – All fields must be complete for List A and B, List A and C, or List B and C. See Page 2 'Instructions for the Applicant' for approved IDs.

LIST A – Photo ID for Identity & Citizenship	List B – Government-issued Photo ID Card	List C – Certified Birth Certificate or Record (U.S. Citizens Only)
Doc. Type/ Title:	Doc. Type/ Title:	Doc. Type/ Title:
Issuer:	Issuer:	Issuer:
Serial or Unique #:	Serial or Unique #:	Serial or Unique #:
Full Name:	Full Name:	Full Name:
Issue Date:	Issue Date:	Issue Date:
Expire Date:	Expire Date:	*See Note Below

***Note**: If the name on your Photo ID is different from the name on your Second ID, please send a **notarized** copy of a 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 _____

Additional Citizenship Addendum
(ECA In-Person Identification Form)

THIS SECTION TO BE VERIFIED BY THE NOTARY.

If applicant has more than one citizenship, it must be asserted in the certificate, and the applicant must present one valid passport for each citizenship.

Second Citizenship (Valid Passport)	Third Citizenship (Valid Passport)
Passport Country:	Passport Country:
Issuing Agency:	Issuing Agency:
Serial No.:	Serial No.:
Exact Name:	Exact Name:
Issue Date:	Issue Date:
Expire Date:	Expire Date:

The undersigned applicant swears under penalty of perjury that all facts and information provided above are accurate and that he or she is the subject and holder of the above-referenced passports and is who he or she represents himself or herself to be.

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: IdenTrust Services ECA SSL/TLS Certificate Subscriber Agreement

IMPORTANT NOTICE: This IdenTrust Services ECA SSL/TLS Certificate Subscriber Agreement (the "Agreement") is a legal agreement between IdenTrust Services, LLC ("IdenTrust") and the Applicant or Subscriber of the ECA SSL/TLS Certificates ("Applicant"/"Subscriber"). "Sponsoring Organization" shall mean the Organization identified in the application for ECA SSL/TLS Certificates and for whom Subscriber will act under the terms of this Agreement and the Subscribing Organization Authorization Agreement in using the Private Key corresponding to the Public Key listed in each ECA SSL/TLS Certificate. As used herein, "Component" shall mean a non-human system or device identified by the information in the subject field within an ECA SSL/TLS Certificate, which system or device is owned or controlled by the Subscribing Organization, and which system or device is administered by the PKI Sponsor identified on the Part 2: In-Person Identification Form submitted to IdenTrust in connection with the application for an ECA SSL/TLS Certificate to which this Agreement relates.

1. Acceptance and Payment. By signing the ID Form or by clicking the checkbox next to "I accept the complete terms and conditions of the Subscriber Agreement" during the online certificate application process, Applicant agrees that the information provided during the application process is accurate, current, complete, and not misleading and that Applicant will be bound by the terms and conditions of this Agreement. Applicant is also requesting that IdenTrust issue ECA SSL/TLS Certificates that will contain Subscriber's identifying information and the name of the Subscribing Organization. IdenTrust will begin processing the application as soon as it has received: (a) preauthorization to charge the credit card, purchase order or voucher number provided; (b) fully completed paper forms, i.e. the Part 1: Subscribing Organization Authorization Agreement and the Part 2: In-Person Identification Form. By proceeding with the application process, Applicant authorizes IdenTrust to bill the Subscribing Organization or the credit card for the applicable certificate issuance fee. Credit card information is transmitted securely to IdenTrust in an encrypted format and is securely stored by IdenTrust. Upon certificate approval, IdenTrust will process the credit card charge or purchase order. IdenTrust will revoke any ECA SSL/TLS Certificates not paid for within 60 days of certificate issuance. If Applicant does not accept this Agreement, then Applicant must choose "Cancel" during the online application process, and the application will be terminated.

2. Integration; Amendment. Except where otherwise defined herein, capitalized terms used herein shall have the meaning given to them in the public version of IdenTrust's ECA Certification Practices Statement (https://secure.identrust.com/certificates/policy/eca/) ("the CPS") and the current ECA SSL/TLS Certificate Policy (http://iase.disa.mil/pki/eca/Documents) ("the CP"). The CPS, the CP, the Part 2: In-Person Identification Form (the "ID Form") submitted to IdenTrust in connection herewith, and the Subscribing Organization Authorization Agreement submitted to IdenTrust in connection herewith, are incorporated by reference herein. Applicant acknowledges and accepts that IdenTrust has the right to modify the CPS from time to time and that the CPS as so modified shall automatically supersede the prior version of the CP integrated herein. IdenTrust and Applicant acknowledge and accept that the Department of Defense (or its designee) has the right to modify the CP from time to time and that the CP as so modified shall automatically supersede the prior version of the CP integrated herein. IdenTrust and the Subscriber agree that with respect to IdenTrust's provision of ECA certification-related services and the Applicant's use or enjoyment of them, including but not limited to any resulting issuance of an ECA SSL/TLS Certificate SSL/TLS to Applicant, are subject to the ongoing oversight and authority of the EPMA as provided for in the ECA CP. This Agreement constitutes the entire agreement related to the subject matter hereof between PKI Sponsor, Subscriber, Subscribing Organization, as applicable, on the one hand, and IdenTrust on the other hand.

3. Identification Procedure. After Applicant has completed the electronic portion of the application process, IdenTrust provides Applicant with a Subscribing Organization Authorization Agreement and an In-Person Identification Form (the "ID Form"). The Applicant must sign the ID Form in the presence of a Registrar, i.e. a person authorized under Section 1.3.2 of the CPS to perform the in-person confirmation of identity. As part of the ECA SSL/TLS Certificate issuance process, the Applicant must present the Registrar with a valid, government-issued photo ID and another government-issued ID. At least one of the documents must establish country of citizenship. For non-U.S. citizens, a passport is required. The documents presented to the Registrar must be the same as those reported to IdenTrust during the electronic application process. Sign the ID Form in the presence of the Registrar, the Registrar must review the Applicant's credentials and also sign the ID Form. The ID Form contains instructions to follow in submitting confirmation of identity to IdenTrust. If IdenTrust accepts an application for ECA SSL/TLS Certificates and confirms the information submitted during the application process, IdenTrust will issue ECA SSL/TLS Certificates to Subscriber for use by Subscriber on behalf of the Subscribing Organization.

4. ECA Key Generation, Certificate Issuance, and Term. Certificates will be valid for the Validity Period specified therein. The term of this Agreement shall correspond to the term of the ECA SSL/TLS Certificates' validity. IdenTrust will keep a copy of the Private Key corresponding to the Encryption Certificate in a secure, encrypted database for Key Recovery purposes. HOWEVER, IN NO EVENT SHALL IDENTRUST EVER HAVE ACCESS TO, OR STORE, THE SUBSCRIBER'S DIGITAL SIGNATURE PRIVATE KEY. IdenTrust will provide Key Recovery services for the Private Key corresponding to the Encryption Certificate in the event that it becomes unavailable or is subject to disclosure by an authorized party, e.g., by the Subscribing Organization. IdenTrust charges additional key recovery fees for such services in accordance with its published fee schedule or by separate agreement with IdenTrust.

5. IdenTrust Verification of Identity. IdenTrust may seek to verify the identity of the Applicant, Component, and that of the Subscribing Organization by any reasonable means. IdenTrust may make inquiry with public or private databases or other sources, for the purpose of verifying the information that Applicant and Subscribing Organization provide in order to determine whether to issue an ECA SSL/TLS Certificate to the Subscriber. IdenTrust is hereby also authorized to store and keep any information generated during the application, identification, authentication, certificate issuance and certificate management processes, which shall become the property of IdenTrust. IdenTrust, in its sole discretion and without incurring liability for any loss arising out of such denial or refusal, may deny an application for, or otherwise refuse to issue, an ECA SSL/TLS Certificate. IdenTrust shall have no liability for any delay experienced during the certificate issuance process, including but not limited to Applicant's inability to retrieve a Certificate because more than thirty (30) days have passed since the Applicant appeared before the registrar for in-person identity proofing.

6. Privacy. IdenTrust agrees to take reasonable care to ensure that private information submitted or obtained during the application, identification and authentication, and certificate issuance processes will be kept confidential. This agreement restricts IdenTrust's use of that information solely to the purposes for which it was collected, and prohibits its disclosure to third parties, except as may be required by law, court order, or as required for IdenTrust to comply with the CP and CPS. Access to sensitive Subscriber-related information within IdenTrust is limited to (a) IdenTrust employees with a "need to know" such information for the uses described in the immediately preceding sentence, and (b) IdenTrust's and the DoD's auditors on a need-to-know basis. Access to that information in IdenTrust customer databases is limited accordingly using the structure and access limits of those databases. Notwithstanding the foregoing provisions of this Section 6, the following information is not confidential: (i) information contained in any ECA SSL/TLS Certificate; (ii) status (e.g. valid, invalid, revoked) information regarding any ECA SSL/TLS Certificate; and (iii) if revocation has occurred, information identifying the reason for revocation where such information is consistent with the standards set forth in RFC 5280 (as published at https://www.ietf.org/rfc/rfc5280.txt) (or any successor standard published by the Internet Engineering Task Force which supersedes it) relative to describing the reason for revocation. Accordingly and without forming any limitation on the immediately preceding sentence, it is understood that (y) IdenTrust may disclose the Subscriber's name, Public Key, email address, Organization name, certificate serial number, and certificate expiration date to any person and for any purpose, and (z) information disclosed by IdenTrust via any "repository", OCSP response, or CRL as such are provided for in the CP and CPS is also not confidential, and, where not prohibited in the CP, IdenTrust may also disclose such information by other means in response to requests made to IdenTrust. Subscriber and Subscribing Organization each agree that with respect to information of Subscriber and information of Subscribing Organization held treated as confidential under the provision of this Section, IdenTrust may disclose such information to each of Subscriber and Subscribing Organization, separately.

7. Subscriber Obligations

7.1. Submit Correct Information. Applicant warrants and represents that he or she is obtaining the ECA SSL/TLS Certificate for use in compliance with one of the reasons stated in Section 1.3.5 of the CP (e.g. an employee of a business or governmental entity administering a component used in conducting business with a US government agency at the local, state or Federal level); that all of the information provided during the application process is accurate, current, complete, and not misleading; and that Applicant has provided IdenTrust with all facts material to IdenTrust's ability to confirm Applicant's identity and material to the reliability of the ECA SSL/TLS Certificates to be issued. Applicant represents that he or she will immediately inform IdenTrust if any information submitted in any application form or during the application process changes or becomes false or misleading.

7.2. Key Protection and Certificate Use. IdenTrust issues an ECA SSL/TLS Certificate based on a Public Key that the Applicant sends to IdenTrust. In Public Key Cryptography, a Key Pair of two mathematically related keys is generated by computer software whereby a Public Key has a corresponding Private Key. The Key Pair is stored on a computer, smart card, or some other cryptographic hardware device. To obtain an ECA SSL/TLS Certificate, Applicant will need to submit an ECA SSL/TLS Certificate request to IdenTrust containing the Applicant's Public Key. When IdenTrust creates the ECA SSL/TLS Certificate, the Public Key is included in the ECA SSL/TLS Certificate.

By requesting ECA SSL/TLS Certificates from IdenTrust, Applicant:

(i) Agrees to protect each Private Key corresponding to each Public Key submitted to IdenTrust;

(ii) Warrants and represents that he or she has kept and will keep the Private Keys private and will safeguard and maintain the Private Keys (and any user IDs, passphrases, passwords or PINs used to activate the Private Keys) in strict secrecy and take reasonable security measures to prevent unauthorized access to, or disclosure, loss, modification, compromise, or use of, the Private Keys and the computer system or media on which the Private Keys are stored;

(iii) Agrees to use ECA SSL/TLS Certificates only in accordance with this Agreement and in conjunction with the uses permitted by the CP;

(iv) Agrees not to use the ECA SSL/TLS Certificate(s) issued by IdenTrust for purposes of fraud, any other illegal scheme, or any use requiring fail-safe performance where failure could lead directly to death, personal injury, or severe environmental damage;

(v) Agrees during initial registration and subsequent key recovery requests to provide accurate identification and authentication information;

(vi) Agrees that when notified that the escrowed Private Key corresponding to the Subscriber's Encryption Certificate has been recovered, to determine whether revocation of such Certificate is necessary and request revocation, if necessary; and

(vii) Agrees that whenever the Subscriber's Private Key has been compromised, or is suspected of compromise, the Subscriber will immediately contact IdenTrust and request that the ECA SSL/TLS Certificate be revoked. A revocation request may be sent in a signed email (containing the reason for revocation and using the key for which revocation is requested) to support@identrust.com, by calling the IdenTrust Support at 1-888-882-1104 (U.S.) or 1-801-384-3474 (International) or by facsimile at 801-384-3610.

(viii) Agrees that the ECA SSL/TLS Certificate(s) issued by IdenTrust may only be used on workstations, guards and firewalls, routers, trusted servers (e.g., database, FTP, and WWW), and other infrastructure components for the purpose of facilitating communications with or for a US government agency at local, state, or Federal level. Such infrastructure component must be the Component and must be under the cognizance of the PKI Sponsor.

NOTICE IS HEREBY GIVEN THAT THE THEFT, COMPROMISE, OR MISUSE OF THE PRIVATE KEY MAY CAUSE THE PKI SPONSOR (AS THE HUMAN ACTING ON BEHALF OF THE SUBSCRIBER) OR THE SUBSCRIBING ORGANIZATION SERIOUS ADVERSE LEGAL CONSEQUENCES.

IF SECURITY OF THE PRIVATE KEY HAS BEEN OR IS IN DANGER OF BEING COMPROMISED IN ANY WAY, SUBSCRIBER AND/OR THE SUBSCRIBING ORGANIZATION MUST IMMEDIATELY NOTIFY IDENTRUST AND REQUEST THAT IDENTRUST REVOKE THE ECA SSL/TLS CERTIFICATE.

7.3. Review the ECA SSL/TLS Certificate; ECA SSL/TLS Certificate Acceptance. The contents of the ECA SSL/TLS Certificates issued to the Subscriber will be based on information provided by the Subscriber and the Subscribing Organization. After downloading the ECA SSL/TLS Certificates from the Web site designated by IdenTrust, the Subscriber shall examine the contents of his or her ECA SSL/TLS Certificates. The Subscriber shall promptly review and verify the accuracy of the information contained in the ECA SSL/TLS Certificates. Subscriber acknowledges that downloading or using the ECA SSL/TLS Certificate constitutes acceptance of the Certificate and its contents. If the Subscriber fails to notify IdenTrust of any errors, defects, or problems with an ECA SSL/TLS Certificate within 24 hours after downloading it, it will be considered to have been accepted. By accepting the ECA SSL/TLS Certificate, the Subscriber further acknowledges that all information in the ECA SSL/TLS Certificate is accurate, current, complete, and not misleading and that he or she is not aware of any fact material to the reliability of that information that has not been previously communicated to IdenTrust. Upon acceptance, and upon each occasion thereafter when the Subscriber uses the ECA SSL/TLS Certificate or the Private Key corresponding to the ECA SSL/TLS Certificate, the responsibilities identified herein, as well as those in the public version of the CPS and in the ECA CP, are reaffirmed.

7.4. Revoke the ECA SSL/TLS Certificate If Necessary.

(a) Permissive Revocation

(1) The Subscriber may request revocation of the Certificate at any time for any reason, and in such event IdenTrust will revoke the Certificate promptly upon confirming that the person making the revocation request is authorized to do so.

(2) The Subscribing Organization may request revocation of a Certificate issued to it Subscriber at any time for any reason, and in such event IdenTrust will revoke the Certificate promptly upon confirming that the person making the revocation request is authorized to do so.

(3) IdenTrust may revoke the Certificate:
- (i) Upon the Subscriber's failure, (or that of the Subscribing Organization, where applicable) to meet its obligations under the ECA CP, the public version of the CPS, or an applicable agreement, regulation, or law; or
- (ii) For any of the other reasons for Certificate revocation set forth in the CP, public version of the CPS, or any other reasonable grounds for revocation.

(b) Required Revocation

(1) The Subscriber and Subscribing Organization are separately responsible for promptly requesting revocation of a Certificate as soon as any of the following events occurs:
- (i) any information or fact material to the reliability of the Certificate, including but not limited to the Subscriber's name, becomes misleading or is no longer accurate, current, or complete;
- (ii) The private key corresponding to the public key in the ECA SSL/TLS Certificate, or the cryptographic module holding that private key has been compromised or such a compromise is suspected;
- (iii) Subscriber is no longer controlled or owned by, or is no longer affiliated with Organization; or

(iv) If there is no PKI Sponsor, including but not limited to fact of Organization no longer authorizing the person acting as PKI Sponsor to so act.

(2) The Subscriber and Subscribing Organization assume the risk of any failure to request a revocation required above.

(3) IdenTrust will revoke the Certificates:
- (i) If IdenTrust learns, or reasonably suspects, that the private key corresponding to the public key listed in a Certificate has been compromised;
- (ii) If IdenTrust determines that the Certificates were not issued in accordance with the ECA CP and/or IdenTrust's ECA CPS;
- (iii) Upon determining that the Certificates have become unreliable or that material information in the application for the Certificates or in the Certificates themselves have changed or have become false or misleading (e.g., the Subscriber changes his or her name);
- (iv) A governmental authority has lawfully ordered IdenTrust to revoke the Certificates; or
- (v) If other circumstances transpire that cause the Certificates to be misleading to a relying party or in violation of the ECA CP, the public version of the CPS, or other ECA requirements.

7.5. Cease Using the ECA SSL/TLS Certificate. Except for sending a signed e-mail requesting revocation of the Certificate, the Subscriber agrees to immediately cease using Subscriber's ECA SSL/TLS Certificate in the following circumstances: (i) when the Private Key corresponding to the ECA SSL/TLS Certificate has been or may be compromised or subjected to unauthorized use in any way; (ii) when any information in the ECA SSL/TLS Certificate is no longer accurate, current, or complete or becomes misleading, (iii) upon the revocation or expiration of the ECA SSL/TLS Certificate, or (iv) upon termination of this Agreement or any lapse in ownership or control, as applicable, of the Component by the Subscribing Organization.

7.6. Indemnification. If the Subscribing Organization is not a State government, the U.S. Government, or one of their political subdivisions, the PKI Sponsor and Subscribing Organization shall indemnify and hold IdenTrust and its officers, directors, employees, Trusted Correspondents, and affiliates harmless from any and all liabilities, costs, and expenses, including reasonable attorneys' fees, related to: any intentional misrepresentation or omission of material fact made by the Subscriber; any compromise or misuse of the Private Key or ECA SSL/TLS Certificate caused directly or indirectly by the PKI Sponsor's negligent or intentional conduct, unless prior to that compromise or misuse the PKI Sponsor or Subscribing Organization appropriately requested revocation of the Certificate; or any violation of this Agreement by the PKI Sponsor, Subscriber, or Subscribing Organization.

8. IdenTrust Warranties. IdenTrust warrants that the procedures it uses to issue and manage ECA SSL/TLS Certificates are in accordance with the CP and the CPS.

9. DISCLAIMER OF WARRANTIES. IDENTRUST DISCLAIMS ANY AND ALL WARRANTIES OF ANY TYPE, WHETHER EXPRESS OR IMPLIED, THAT ARE NOT SPECIFICALLY PROVIDED HEREIN, INCLUDING BUT NOT LIMITED TO ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, WITH REGARD TO IDENTRUST SERVICES OR ANY ECA SSL/TLS CERTIFICATE ISSUED HEREUNDER.

10. Limitation of Liability. IdenTrust shall not be liable for any consequential, indirect, special, remote, exemplary, punitive or incidental damages, including, without limitation, damages arising from loss of profits, revenues, savings, opportunities or data, injuries to customer relationships or business interruption, regardless of the cause of action, even if IdenTrust has been advised of the possibility of such loss. IDENTRUST SHALL HAVE NO LIABILITY FOR LOSS DUE TO USE OF AN IDENTRUST-ISSUED ECA SSL/TLS CERTIFICATE, UNLESS THE LOSS IS PROVEN TO BE A DIRECT RESULT OF A BREACH BY IDENTRUST OF THE CP OR THE CPS OR A PROXIMATE RESULT OF THE NEGLIGENCE, FRAUD OR WILLFUL MISCONDUCT OF IDENTRUST.

IdenTrust's entire liability, in law or in equity, for losses due to its operations at variance with its procedures defined in the ECA CP or the CPS shall not exceed either of the following limits:

- One thousand U.S. dollars (USD $1,000) for all recoverable losses sustained by each person, whether natural or legal, as a result of a single transaction involving the reliance upon or use of a certificate.

- One million U.S. dollars (USD $1,000,000) maximum aggregate total liability for all recoverable losses sustained by all persons as a result of a single incident (i.e. the aggregate of all transactions) arising out of the reliance upon or use of a certificate.

IDENTRUST SHALL INCUR NO LIABILITY 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.

11. Dispute Resolution Provisions. With respect to US government affiliated Applicants, US government affiliated Subscribers and US government Relying Parties, this Agreement shall be governed by the Contracts Disputes Act of 1978, as amended (41 US.C. § 601 et seq.). Subject to the foregoing sentence and to the extent not in conflict with the provisions of the CP, with respect to State governments affiliated Applicants, State government affiliated Subscribers, and State government Relying Parties, this Agreement shall be construed, interpreted, and enforced in accordance with the substantive laws of that State, without regard to its conflicts of law rules. Subject to the foregoing provisions of this paragraph and to the extent not in conflict with the provisions of the CP, in all other cases, irrespective of the place of performance, this Agreement shall be construed, interpreted, and enforced in accordance with the substantive laws of the State of Utah, without regard to its conflicts of law rules. The parties agree that the United Nations Convention on Contracts for the International Sale of Goods shall not apply to this Agreement.

If any provision of this Agreement, the Subscribing Organization Authorization Agreement, the ID Form, or the CPS is found to be invalid or unenforceable, then such document 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.

The dispute resolution procedures specified in this Agreement shall provide the sole remedy for any claim against IdenTrust for any loss sustained by any Relying Party, Subscriber, or Subscribing Organization, whether that loss is claimed to arise from reliance on a Certificate, from breach of a contract, from a failure to perform according to the ECA CP and/or the CPS, or from any other act or omission. No Relying Party, Subscriber, or Subscribing Organization shall require IdenTrust to respond to any attempt to seek recourse through any other means.

11.1 Claims and Claim Determinations. Before making a claim to recover a loss for which IdenTrust may be responsible, a Subscriber, Relying Party, or Subscribing Organization who is not the U.S. Government, a State Government, or a Government employee (the "Claimant") shall make a thorough investigation. IdenTrust will cooperate reasonably in that investigation. The Claimant will then present to IdenTrust reasonable documented proof:

(i) That the Claimant has **suffered** a recoverable loss as a result of a transaction;

(ii) Of the amount and extent of the recoverable loss claimed; and

(iii) Of the causal linkage between the alleged transaction and the recoverable loss claimed, itemized as necessary.

Upon the occurrence of any loss arising out of a transaction, the Claimant shall file notice and all required proof of the claim (using a procedure accessed through IdenTrust's web site) not later than one year after the date of discovery of the facts out of which the claim arose. Notice of the claim must be given on an IdenTrust Claim-Loss Form downloadable from https://secure.identrust.com/certificates/policy/eca. Instructions for completion and submission of the claim form also appear in the Claim-Loss Form downloadable from that web page.

On receipt of a claim form, IdenTrust may determine to pay the claim or deny it. IdenTrust may also pay the claim in an amount less than the amount claimed if IdenTrust determines that the loss calculations exceed the amount that IdenTrust is obligated to pay. IdenTrust will notify the Claimant of its determination within 30 days of receipt of the claim form.

If the claimant is not satisfied with IdenTrust's determination of the claim, the Claimant may seek judicial relief as provided in the next section.

11.2 Judicial Review. A Relying Party, Subscriber, or Subscribing Organization who is not the U.S. Government, a State Government, or a Government Subscriber may contest the determination of the claim by IdenTrust under section 11.2 hereof by filing suit as provided herein within one year after IdenTrust's determination of the claim.

The courts of the State of Utah have exclusive subject matter jurisdiction over all suits and any other disputes arising out of or based on this Agreement, the ECA CP, or the public version of the CPS, including suits for judicial review of claims decided according to the preceding section. The parties hereby waive any right to trial by jury of any claim or suit arising out of the CP, the public version of the CPS, or this Agreement.

12. Survival. Section 2 and Sections 6 -12 of this Agreement and the provisions of the ID Form shall survive any termination or expiration of this Agreement and expiration or revocation of the ECA SSL/TLS Certificates.