

DoD ECA  
Medium Assurance & Medium Token  
Assurance Foreign Certificate  
Forms Packet

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



## Foreign Subscribers Instructions for the Applicant

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

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](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 Authorized DOD Employee (ADE) approved to complete your identity verification. All non-U.S. Citizens must present a valid passport **and** one additional official form of identification with a photo. Insure that all fields are filled in accurately.

- **Valid Passport** issued by your country of citizenship

**-AND-**

#### **Additional, Valid Official Photo ID such as:**

- Driver's license with photo
- Government-issued ID Card with photo
- Employment ID card from current employer with photo
- Military ID with photo
- Other official photo ID

### COMPLETE THE REGISTRATION PROCESS

Please check your email for a verification email request sent from [Support@IdenTrust.com](mailto:Support@IdenTrust.com) and follow the steps laid out.

The ADE must send a scanned copy via signed email to [Registration@IdenTrust.com](mailto:Registration@IdenTrust.com) before the application can be processed.

**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.

**Part 1: Subscribing Organization Authorization Agreement**

Subscribing Organization ("Organization"), identified below, acknowledges that IdenTrust Services, LLC ("IdenTrust") (www.IdenTrust.com), an External Certification Authority ("ECA") for the Department of Defense, will issue Digital Certificates ("Certificates") to employees of Organization. The Certificate will identify the employee(s) ("Applicant" or "Subscriber"), identified herein, as being employed by Organization.

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 Terms and Conditions attached as Appendix A hereof and the Part 2: In-Person Identification Form (<https://secure.identrust.com/certificates/policy/eca/>) ("ID Form"), are incorporated by reference herein and comprise this Agreement, as that term is used herein. IdenTrust reserves and Organization acknowledges and accepts IdenTrust's right to modify the CPS, which modifications shall become a part of this Agreement.

**1. IdenTrust and Organization agree that:**

- (a) IdenTrust or Organization, in its sole discretion, may revoke the Certificate issued hereunder at any time and for any reason;
- (b) IdenTrust will revoke the Certificate promptly upon confirming that the person making the revocation request is authorized to do so or upon otherwise determining that the Certificate should be revoked; and
- (c) With respect to US Government Subscribers or 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 U.S.C. § 601 et seq.). With respect to State governments, 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. 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.

**2. Organization warrants, represents, and agrees that:**

- (a) Organization agrees to be bound by the Terms and Conditions set forth in Appendix A to this Part 1;
- (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) Subscriber is a duly-authorized employee of the Organization and IdenTrust is hereby authorized to issue a Certificate to Subscriber that identifies Subscriber as being employed by Organization;
- (d) Federal agencies, and other authorized recipients of messages signed with Subscriber's Private Key, may rely on such messages to the same extent as though they were manually signed by the Subscriber listed in a valid, unrevoked and unexpired Certificate issued by IdenTrust; and
- (e) All information provided to IdenTrust by Organization is and will be accurate, current, complete, and not misleading and Organization will immediately notify IdenTrust and request that the Certificate be revoked if: (1) any information or fact material to the reliability of the Certificate is no longer accurate, current, complete or becomes misleading, (2) Organization suspects any loss, disclosure, or other compromise of the Subscriber's Private Key, or (3) Subscriber is no longer employed by, associated with, authorized by or affiliated with Organization.

The undersigned personally warrants and represents that he or she is an officer of the Organization 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 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

***Appendix A to Part 1  
Terms and Conditions***

**1. Certification Services from IdenTrust**

- a. Issuance and Revocation of Certificates. On request by the Subscribing Organization and one or more individual Subscribers employed by the Subscribing Organization, IdenTrust agrees to issue ECA Certificates as specified in the ECA CPS. IdenTrust also agrees to revoke an ECA Certificate that it has issued on receipt of a request by either the Subscribing Organization or the Subscriber listed in that Certificate. With respect to the issuance and revocation of ECA Certificates, IdenTrust and the Subscribing Organization agree to perform as required of each in the ECA CP and the public version of IdenTrust's ECA CPS. Moreover, IdenTrust in providing ECA certification services, and the Subscribing Organization in accepting them, is subject to the ongoing oversight of the EPMA as provided in the ECA CP.
- b. Individual Subscriber Agreements. In connection with registration of each Subscriber employed by the Subscribing Organization, Subscriber enters into a separate agreement, which is legally binding on each Individual Subscriber. The current form of Subscriber Agreement and IdenTrust's public version of the CPS are publicly available on IdenTrust's web site.
- c. IdenTrust Verification of Identity. Section 4 of the Subscriber Agreement is hereby incorporated by reference.

**2. Obligations of the Subscribing Organization**

- a. Supervision of Subscribers. Organization agrees that it will require each of its Subscribers to carefully and fully comply with each of the provisions of the Subscriber Agreement.
- b. Duties. Subscribers and Subscribing Organizations are each required under the terms of the CP and the public version of the CPS to do the following, among other things:
  - (1) Accurately represent themselves in all communications relevant to the ECA system.
  - (2) Protect their private keys at all times as specified in the ECA CP and as required by IdenTrust's instructions given at the time of certificate acceptance or otherwise.
  - (3) Notify IdenTrust in a timely manner of any grounds for revocation of a Certificate issued by IdenTrust to a Subscriber employed by the Organization. Such grounds include termination of the employee or if ever a private key held by the Subscriber is suspected to have been compromised or lost. Such notification will be made through the means specified in the public version of the CPS.
  - (4) Notify IdenTrust whenever any information in a Certificate ceases to be accurate or should be changed.

**3. Fees**

Fees for Certificate issuance 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 with respect to its initial term, and renewal fees are charged upon renewal. If Certificates are to be issued via a Bulk Load procedure, an aggregate fee will be charged to the Subscribing Organization.

**4. Use of Information**

- a. Confidential Information and Disclosure. IdenTrust obtains certain sensitive information from Subscribers in providing certification services. That information includes 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. Access to sensitive Subscriber-related information within IdenTrust is limited to IdenTrust employees acting in Trusted Roles and 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. However, information contained in ECA Certificates and related status information are not confidential. (That would defeat the purpose of an ECA Certificate, which is to establish a person's identity.) Accordingly, IdenTrust may disclose the Subscriber's name, Public Key, email address, citizenship, Organization name, certificate serial number, and certificate expiration date to any person and for any purpose. Information listed in the repository provided by IdenTrust is also not confidential.
- b. Disclosure of Certificate Revocation/Suspension Information. IdenTrust discloses information concerning the revocation of a Certificate or events leading to such a revocation only to the Subscriber and/or Subscribing Organization of that Certificate, and only on request. However, the information disclosed in a CRL or OCSP response, such as the fact that a Certificate is revoked and date of revocation, is not confidential. IdenTrust discloses that information on request or, preferably, through online retrieval.

**5. Incorporation by Reference**

Sections 6 through 17 of the Subscriber Agreement are hereby incorporated by reference.

**Foreign Subscribers  
Part 2: In-person Identification Form**

**Terms and Conditions**

The undersigned applicant attests that all facts and information provided are accurate, current, complete, and not misleading and that he or she: a) is authorized to receive, and has applied for, a digital certificate to be issued by IdenTrust; b) has read and verified the personal identifying information to be contained in the certificate; c) is who he or she represents himself or herself to be; and d) has read, understood, and agrees to the responsibilities associated with being a certificate subscriber, including the terms and conditions found in the IdenTrust Services ECA Certificate Subscriber Agreement, the public version of IdenTrust's ECA Certification Practices Statement ("CPS"), and the ECA Certificate Policy ("the ECA CP"). The applicant agrees to: 1) accurately represent him or herself in all communications; 2) protect his or her private key(s) at all times; 3) immediately notify IdenTrust if he or she suspects his or her private keys to have been compromised, stolen or lost; and 4) use his or her private keys in accordance with the above-mentioned documents.

Signed By: \_\_\_\_\_ (Subscriber to sign only in the presence of the ADE)

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

**Identification – All fields must be complete. See Page 2 'Instructions for the Applicant' for approved IDs.**

You must present **two** forms of identification to an Authorized DOD Employee (ADE). All Non-US Citizens must present a valid passport from their country of citizenship **and** an official photo ID as described in the instructions above.

| VALID PASSPORT FROM COUNTRY of CITIZENSHIP |
|--|
| Doc. Type/Title:                           |
| Issuer:                                    |
| Serial No.:                                |
| Exact Name:                                |
| Issue Date:                                |
| Expire Date:                               |

| 2 <sup>nd</sup> VALID PHOTO ID |
|--------------------------------|
| Doc. Type/Title:               |
| Issuer:                        |
| Serial No.:                    |
| Exact Name:                    |
| Issue 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).

**Acknowledgement by Authorized DOD Employee**

Country: \_\_\_\_\_

On \_\_\_\_\_ (MM/DD/YY), before me, \_\_\_\_\_ (name of the ADE), 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.

I certify under PENALTY OF PERJURY under federal laws of the United States of America that the foregoing paragraph is true and correct.

\_\_\_\_\_  
Signature of Authorized DoD Employee

**Additional Citizenship Addendum  
(ECA In-Person Identification Form)**

THIS SECTION TO BE VERIFIED BY THE AUTHORIZED DOD EMPLOYEE (ADE).

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.

| <b>Second Citizenship (Valid Passport)</b> | <b>Third Citizenship (Valid Passport)</b> |
|--|---|
| 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.

**Acknowledgement by Authorized DOD Employee**

Country: \_\_\_\_\_

On \_\_\_\_\_ (MM/DD/YY), before me, \_\_\_\_\_ (name of the ADE), 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.

I certify under PENALTY OF PERJURY under federal laws of the United States of America that the foregoing paragraph is true and correct.

\_\_\_\_\_  
Signature of Authorized DoD Employee

**COMPLETE TERMS OF IDENTRUST SERVICES ECA CERTIFICATE SUBSCRIBER AGREEMENT:**

**IMPORTANT NOTICE:** This IdenTrust Services ECA Certificate Subscriber Agreement is a legal agreement between IdenTrust Services, LLC ("IdenTrust") and the Applicant or Subscriber of the ECA Certificates ("Applicant"/"Subscriber"). "Subscribing Organization" shall mean the Organization identified in the application for ECA 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 Certificate.

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 Certificate Policy (<http://iase.disa.mil/pki/eca/Documents>) ("the CP"). The public version of the CPS, the CP, the In-Person Identification Form (<https://secure.identrust.com/certificates/policy/eca/>) submitted to IdenTrust in connection herewith ("ID Form") and the Subscribing Organization Authorization Agreement submitted to IdenTrust in connection herewith, are incorporated by reference herein and comprise this "Agreement", as that term is used herein. IdenTrust reserves, and Applicant acknowledges and accepts IdenTrust's right to modify the CPS, which modifications shall become a part of this Agreement.

**1. Acceptance and Payment.**

If this Agreement is presented to Applicant as a "click-through" as part of the IdenTrust online certificate application process, then by clicking the checkbox next to "I accept the complete terms and conditions of the Subscriber Agreement" during the online certificate application process, Applicant accepts this Agreement, agrees that Applicant is bound by the terms and conditions of this Agreement, and requests that IdenTrust approve Applicant's application made in connection herewith and, provided IdenTrust approves such application, issues ECA Certificates that will contain Applicant's name and the name of the Subscribing Organization.

If Applicant signed an In-person Identification Form in connection herewith, by so signing the Applicant accepts this Agreement, agrees that Applicant will be bound by the terms and conditions of this Agreement, and requests that IdenTrust approve Applicant's application made in connection herewith and, provided IdenTrust approves such application, issues ECA Certificates that will contain Applicant's name 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 Subscribing Organization Authorization Form and the 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 Certificates not paid for within 60 days of certificate issuance.

**2. Identification Procedure.** After Applicant has completed the online portion of the certificate 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 to perform the in-person confirmation of identity. As part of the ECA 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 and approves an application for ECA Certificates and confirms the information submitted during the application process, IdenTrust will issue ECA Certificates to Applicant for use by Applicant on behalf of the Subscribing Organization.

**3. 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 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.

**4. IdenTrust Verification of Identity.** IdenTrust may seek to verify the identity of the Applicant 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

## ECA DIGITAL CERTIFICATE PROGRAM

to issue an ECA Certificate to the Applicant. 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 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.

**5. 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 private. Except as necessary to carry out the provisions of this Agreement, or for auditing purposes, or as otherwise required by law or court order, IdenTrust will protect the confidentiality of such private information and will not sell, rent, lease, or disclose such information in any manner to any person without prior permission. IdenTrust also agrees to protect such information in a manner designed to ensure its integrity and to make it available to the Subscriber or the Subscribing Organization, following an appropriate request. However, information contained in ECA Certificates and related status information are not private. (That would defeat the purpose of an ECA Certificate, which is to establish a person's identity.) Accordingly, IdenTrust may disclose the Subscriber's name, Public Key, email address, citizenship, Subscribing Organization's name, the certificate serial number, and the certificate expiration date to any person and for any purpose.

### 6. Subscriber Obligations.

**6.1. Submit Correct Information.** Applicant warrants and represents that he or she is obtaining the ECA Certificate for use in compliance with one of the reasons stated in Section 1.3.5 of the CP; 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 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.

**6.2. Key Protection and Certificate Use.** IdenTrust issues an ECA 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 Certificate, Applicant will need to submit an ECA Certificate request to IdenTrust containing the Applicant's Public Key. When IdenTrust creates the ECA Certificate, the Public Key is included in the ECA Certificate.

By requesting ECA Certificates from IdenTrust, Applicant:

- (a) Agrees to protect each Private Key corresponding to each Public Key submitted to IdenTrust;
- (b) 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;
- (c) Agrees to use ECA Certificates only in accordance with this Agreement and in conjunction with the uses permitted by the CP;
- (d) Agrees not to use the ECA 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;
- (e) Agrees during initial registration and subsequent key recovery requests to provide accurate identification and authentication information;
- (f) Agrees that when notified that the escrowed Private Key corresponding to his or her Encryption Certificate has been recovered, to determine whether revocation of such Certificate is necessary and request revocation, if necessary; and
- (g) 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 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.



## ECA DIGITAL CERTIFICATE PROGRAM

(h) Agrees that the ECA Certificate(s) issued by IdenTrust may only be used for one of the following purposes:

1. Employees of businesses acting in the capacity of an employee and conducting business with an agency of the Federal Government at a local, State, or Federal Government level;
2. Employees of a State conducting business with the an agency of the Federal Government at a local, State, or Federal Government level;
3. Employees of a Foreign State conducting business with the an agency of the Federal Government at a local, State, or Federal Government level;
4. Individuals communicating securely with the an agency of the Federal Government at a local, State, or Federal Government level; and
5. Workstations, guards and firewalls, routers, trusted servers (e.g., database, FTP, WWW), and other infrastructure components communicating securely with or for an agency of the Federal Government at a local, State, or Federal Government level. These components must be under the cognizance of humans, who accept the Certificate and are responsible for the correct protection and use of the associated private key.

NOTICE IS HEREBY GIVEN THAT THE THEFT, COMPROMISE, OR MISUSE OF THE PRIVATE KEY MAY CAUSE 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 CERTIFICATE.

**6.3. Review the ECA Certificate; ECA Certificate Acceptance.** The contents of the ECA Certificates issued to the Subscriber will be based on information provided by the Subscriber and the Subscribing Organization. After downloading the ECA Certificates from the Web site designated by IdenTrust, the Subscriber shall examine the contents of his or her ECA Certificates. The Subscriber shall promptly review and verify the accuracy of the information contained in the ECA Certificates. Subscriber acknowledges that downloading or using the ECA 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 Certificate within 24 hours after downloading it, it will be considered to have been accepted. By accepting the ECA Certificate, the Subscriber further acknowledges that all information in the ECA 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 Certificate or the Private Key corresponding to the ECA Certificate, the responsibilities identified herein, as well as those in the public version of the CPS and in the ECA CP, are reaffirmed.

### **6.4. Revoke the ECA Certificate If Necessary.**

#### **(a) Permissive Revocation.**

1. The Subscriber may request revocation of the Certificate at any time for any reason. The Subscribing Organization may request revocation of a Certificate issued to its Individual Subscriber at any time for any reason.
2. IdenTrust may also revoke the Certificates:
  - 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 responsible for promptly requesting revocation of a Certificate as soon as any of the following events occurs:
  - i. The Subscriber's name or any other information in the Certificate becomes inaccurate or is discovered to be inaccurate;
  - ii. The private key corresponding to the public key in the ECA Certificate, or the media holding that private key has been compromised or such a compromise is suspected; or
  - iii. The Subscriber's employment with the Subscribing Organization ends.
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;

## ECA DIGITAL CERTIFICATE PROGRAM

- 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.

**6.5. Cease Using the ECA Certificate.** Except for sending a signed e-mail requesting revocation of the Certificate, the Subscriber agrees to immediately cease using his or her ECA Certificate in the following circumstances: (i) when the Private Key corresponding to the ECA Certificate has been or may be compromised or subjected to unauthorized use in any way; (ii) when any information in the ECA Certificate is no longer accurate, current, or complete or becomes misleading, (iii) upon the revocation or expiration of the ECA Certificate, or (iv) upon termination of this Agreement or employment with the Subscribing Organization.

### 6.6. Indemnification.

It is understood that where Subscribing Organization is the Federal Government, a State Government, or a Foreign State, indemnification obligations under the provisions below in this Section 6.6 may be restricted by statutory or common law within the law that governs this Agreement per Section 11, including but not limited statutes and common law that embody the doctrine of "sovereign immunity" within such governing law.

The Subscriber 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 Certificate caused directly or indirectly by the Subscriber's negligent or intentional conduct, unless prior to that compromise or misuse the Subscriber or Subscribing Organization appropriately requested revocation of the Certificates; or any violation of this Agreement by the Subscriber or the Subscribing Organization.

**7. IdenTrust Warranties.** IdenTrust warrants that the procedures it uses to issue and manage ECA Certificates are in accordance with the CP and the CPS.

**8. 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 CERTIFICATE ISSUED HEREUNDER.

### 9. Limitations of Liability.

#### 9.1. Limitation of Liability, IdenTrust.

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 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 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 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

## ECA DIGITAL CERTIFICATE PROGRAM

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. Applicable Law; Jurisdiction.

**11.1. Federal Government as Subscribing Organization.** Where the Subscribing Organization is the Federal Government, this Agreement shall be governed by the laws of the US, including but not limited to the Contracts Disputes Act of 1978, as amended (41 U.S.C. § 601 et seq.).

**11.2. State Government as Subscribing Organization.** Where the Subscribing Organization is a State Government, this Agreement shall be governed by the substantive laws of the State under which such State Government is established, without regard to its conflicts of law rules.

**11.3. Foreign State as Subscribing Organization.** Where the Subscribing Organization is a Foreign State, this Agreement shall be governed by the laws of the US, including but not limited to the Foreign Sovereign Immunity Act of 1976, as amended (28 U.S.C. § 1602 et seq.).

**11.4. Utah.** Except to the extent otherwise required under the provisions set forth above in this Section 11, this Agreement shall be governed by, and interpreted, and construed under the laws of the State of Utah without regard to its conflicts of law principles.

**11.5. Subscriber.** With respect to Subscriber, the Subscriber agrees that the law governing this Agreement is the law that governs this Agreement as determined by provisions above in this Section 11 as such provisions apply to the Subscribing Organization with which the Subscriber is affiliated in the ECA Certificate (or the ID Form if the ECA Certificate is not issued).

**11.6. Jurisdiction; Waiver of Jury Trial; Other.** The parties hereto, and each of them, unconditionally and irrevocably agree that the United States District Court for Utah and the Salt Lake City District Court of the State of Utah shall each have subject matter jurisdiction and personal jurisdiction over each of the parties, and hereby unconditionally and irrevocably consent to the exercise of such subject matter and personal jurisdiction. The parties hereto, and each of them, unconditionally and irrevocably waive any right they may have to: (i) assert the doctrine of forum non conveniens; and (ii) to object to venue to the extent that any proceeding is conducted in accordance with this provision. The parties hereto, and each of them, hereby waive any right to trial by jury of any claim or suit arising out of or relating to this Agreement. The parties hereto, and each of them, agree that the United Nations Convention on Contracts for the International Sale of Goods shall not apply to this Agreement. The parties hereto, and each of them, agree that the ECA Certificate and all activities of IdenTrust are commercial in nature and in purpose, and the substantial majority of activities of IdenTrust related to this Agreement take place in the State of Utah.

### 12. Dispute Resolution Provisions.

**12.1. Dispute Resolution – General.** 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 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.

### 12.2. Claims and Claim Determinations – Non-Excluded Entities.

Before making any claim in a court to recover a loss for which IdenTrust may be responsible, a Subscriber, Relying Party, or Subscribing Organization that is not an Excluded Entity (the “Claimant”) shall make a claim to IdenTrust and obtain a determination of such claim by IdenTrust as provided for under the provisions of this Section 12.2.

Before making any claim to IdenTrust to recover a loss for which IdenTrust may be responsible, the Claimant shall make a thorough investigation. IdenTrust will cooperate reasonably in that investigation. The Claimant will then present to IdenTrust reasonable documented proof:

- (a) That the Claimant has suffered a recoverable loss as a result of a transaction;
- (b) Of the amount and extent of the recoverable loss claimed; and
- (c) 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

## ECA DIGITAL CERTIFICATE PROGRAM

<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.

Subject to Section 11.6, if the Claimant is not satisfied with IdenTrust's determination of the claim, the Claimant may seek judicial relief in a court by filing suit no more than one year after IdenTrust's determination of the claim.

**12.3. Claims and Claim Determinations – Excluded Entities.** Excluded Entities shall only make a claim to recover a loss for which IdenTrust may be responsible where such claim is made in accordance with the provisions of Section 11.6.

**13. Additional Export-Related Restrictions.** No resale, transfer, or re-export of the ECA Certificate or any related cryptographic hardware device (e.g. USB token, smartcard) provided by IdenTrust to Subscriber in connection therewith is authorized without prior authorization from the United States government. No upgrades, enhancements, substitutions, or changes to the cryptographic functionality of the ECA Certificate or any related cryptographic hardware device provided by IdenTrust to Subscriber in connection therewith is authorized, including under any hardware or software updates.

**14. Hardware Storage Device.** In the event the application for an ECA Certificate submitted to IdenTrust in connection herewith (a) included as part of such application the selection among different ECA Certificate types of an ECA Certificate type that included the word "Hardware" or the word "Token" in the ECA Certificate type's name as presented in the IdenTrust materials or (b) was an application where only one ECA Certificate type was provided for and such ECA Certificate type included the word "Hardware" or "Token" in its name as presented in the IdenTrust materials, then in the event IdenTrust approves the issuance of such ECA Certificate, Applicant, as Subscriber, will be provided with a cryptographic hardware device (e.g. USB token, smartcard) by IdenTrust along with instructions regarding how to activate such device. With respect to any cryptographic hardware device provided by IdenTrust under this Agreement, Subscriber and Subscribing Organization shall rely only on such representations and warranties as are provided by the applicable original equipment manufacturer. ANY CRYPTOGRAPHIC HARDWARE DEVICE PROVIDED BY IDENTRUST IN CONNECTION WITH THIS AGREEMENT IS PROVIDED "AS IS"; provided, however, IdenTrust will use commercially reasonable efforts to facilitate any claims Subscriber may have with, and returns of any defective cryptographic hardware device to, the original equipment manufacturer during the warranty period, if any, provided by such manufacturer for such device. IdenTrust does not warrant that any cryptographic hardware device will meet the requirements of Subscribing Organization or Subscriber, or that use or operation of any cryptographic hardware device will be uninterrupted or error free.

**15. Entire Agreement; Severability.** This Agreement constitutes the entire agreement between Subscriber, Subscribing Organization, and IdenTrust related to its subject matter. 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.

**16. Survival.** Sections 5-17 of this Agreement and the provisions of the ID Form shall survive any termination or expiration of this Agreement or expiration or revocation of the ECA Certificates.

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

"Excluded Entity" means a: (i) Relying Party, Subscriber, or Subscribing Organization that is the Federal Government or a State Government; or (ii) Subscriber that is an employee of the Federal Government or a State Government.

"Federal Government" means the federal government of the US.

"Foreign State" means a "foreign state or government" under the Foreign Sovereign Immunity Act of 1976, as amended (28 U.S.C. § 1602 et seq.).

"Non-Excluded Entity" means an entity that is a Relying Party, Subscribing Organization, or Subscriber, but is not an Excluded Entity.

"State" means any state among the states that together make up the US.

"State Government" means the government of a State as established by the law of such State, or any part or agency of such government including but not limited to sub-divisions of such government such as counties, cities, and towns where such sub-divisions are expressly provided for in the law of such State.

"US" means the United States of America.