



Forms Packet

Copyright © IdenTrust 2010

ACES Trusted Agent Application Form

Print only what is needed

The instructions and terms/conditions must be read but do not need to be printed. Please print only the pages you need to send to IdenTrust. For most applicants, this includes two pages; Part 1: Sponsoring Organization Authorization Form and Part 2: Notary Form.

If you would like us to expedite your retrieval materials, please also print and send in the Expedited Shipping Request Form.

ACES DIGITAL CERTIFICATE PROGRAM ACES Trusted Agent

Instructions for Trusted Agent

Thank you for choosing IdenTrust Services, LLC ("IdenTrust"), a subsidiary of IdenTrust, Inc., to meet your company's digital certificate needs. We appreciate your willingness to serve your company as a Trusted Agent and assist in the issuance of ACES Business Representative digital certificates to individuals such as employees, officers, and agents authorized to act on behalf of your company.

To become an ACES Trusted Agent for IdenTrust, you must demonstrate that your company has authorized you for the role, and you must apply for and receive your own ACES Business Representative certificate. Simply follow these steps:

Step 1: Online Application

Apply for your ACES Business Representative Certificate at: http://www.identrust.com/certificates/buy_aces_business.html
You will be prompted to download the necessary forms at the end of the online application.

Step 2: ACES Appointment as Trusted Agent

Complete the **ACES Appointment as Trusted Agent** form. Take this form to an officer who can sign on behalf of your organization and represent that you are authorized to electronically submit bulk loads and business agreement forms.

Step 3: ACES Business Representative Authorization

Complete and Sign **Part I - Sponsoring Organization Authorization Form**. Take it to an officer in your Organization who can sign on behalf of your Organization and represent to IdenTrust that you are a duly-authorized representative of the Organization and that it agrees to be bound by the terms described in Part III - Certificate Agreement for Organization. Have the officer sign Part I - Sponsoring Organization Authorization Form and return it to you for submission to IdenTrust.

Step 4: Notary Form

Complete and Sign **Part II-Notary Form**. Take this form to a licensed Notary employed by your Organization or by a financial institution (most banks have notaries on staff) to verify your identity credentials. You have two options for presenting your ID:

- **Option 1** - one Federal Government-issued photo ID
- **Option 2** - two forms of ID issued by a state or local government. Of which, one must be a photo ID.

All forms of ID must be verifiable. Examples of acceptable forms of ID are as follows:

Federal Government-issued Photo IDs

- Passport
- Federal Employee ID card
- US Military Photo ID
- DoD CAC Card
- Certificate of US Citizenship (w/

State or Local Government-issued Photo ID

- State-issued Driver's License
- State-issued ID Card
- Student ID from a State College or University

Other acceptable forms of ID

- Original or Certified Copy of Birth Certificate
- Social Security Card
- Concealed Weapons Permit
- State-issued Pilot's License

Other official forms of ID will be considered on a case-by-case basis provided that they meet the above requirements.

Note: Please ensure that all information matches the information you submitted in the online application, including Subscriber information and Organization information.

Step 5: Send Forms to IdenTrust

For your records, make a copy of your Part 1 and Part 2 forms, then send the signed (ink-on-paper) originals to IdenTrust.

Mailing Address

ACES Registration
IdenTrust Services
P.O. Box 22930
Salt Lake City, UT 84122-0930

Overnight Courier Only (FedEx, UPS, Etc.)

ACES Registration
IdenTrust Services
255 Admiral Byrd Road, Suite 200
Salt Lake City, UT 84116 JFI

If you should have any questions during the process and would like to speak with a customer service representative, please call (888) 339-8904 or by email at helpdesk@identrust.com

ACES DIGITAL CERTIFICATE PROGRAM ACES Trusted Agent

Appointment as Trusted Agent:

IdenTrust, LLC a limited liability company organized under the laws of Delaware, with its principal place of business at 55 Hawthorne Street, Suite 400 San Francisco, CA 94105, hereby appoints:

_____, an employee of _____, ("Trusted Agent" or "You"), to serve as IdenTrust's Trusted Agent under the ACES Certificate Policy. As a Trusted Agent You will assist IdenTrust in performing such identity verification tasks as may be required by the terms of our Bulk Submission Agreement, the ACES CP and IdenTrust's ACES Certification Practices Statement. A summary of these requirements has been provided in the ACES BUSINESS REPRESENTATIVE CERTIFICATE AGREEMENT form below but, in the event of any discrepancy between the requirements described in ACES BUSINESS REPRESENTATIVE CERTIFICATE AGREEMENT and the ACES CP and ACES CPS, the terms of the ACES CP and ACES CPS shall govern. The ACES Policy Management Authority or IdenTrust may amend the ACES CP and ACES CPS from time to time. Any such amendments and any required notices will be pursuant to the terms of those documents and shall be binding upon You unless You notify IdenTrust of your intent to terminate your Trusted Agent status.

Applicant warrants, represents and agrees that:

You warrant to IdenTrust that you have read the relevant provisions of the ACES CP and IdenTrust's ACES CPS and understand your obligations as described in those documents. As a Trusted Agent of IdenTrust, LLC, you will be performing a key role in the identification and authentication of Subscribers for ACES certificates. In the capacity as our Trusted Agent, you agree to do the following:

- 1) Gather and record all subscriber registration data as required for the bulk load submission on the bulk load templates provided by IdenTrust.
- 2) Complete the Business Agreement found in the bulk load templates. By checking the box, you attest that all applications contained in the template are for employees or other individuals affiliated with the business named on the Business Agreement who are authorized by the business to hold a certificate. This attestation is in accord with the Acknowledgement form The terms of this Acknowledgement are incorporated as part of the Bulk Submission Template and apply to all subscribers entered on the template.
- 3) Ensure that each applicant receives a copy of the Instructions for Applicant This provides information about the In-person Identification form and the responsibility to review and accept the subscriber agreement and policies.
- 4) When performing the In-person Identification and signing the form, ensure that the applicant signs the form in your presence, and presents the required identification credentials as stated in the In-person Identification by Trusted Agent form
- 5) When the In-person Identification is performed by a Notary, ensure that the In-person Identification by Notary form has been completed correctly including required signatures, information and required identification credentials.
- 6) Forward the following to IdenTrust; the Bulk Load template and for each subscriber a completed In-person Identification form, either by Notary or by Trusted Agent.
- 7) Supply the appropriate Human Resource Department(s) in your organization with the provided Instruction Form to ensure that IdenTrust is notified in the event of certificate revocation events, such as separation of subscriber from your organization. Irrespective of the place of performance, this Trusted Agent Agreement shall be constructed, interpreted, and enforced in accordance with the substantive laws of the State of Utah, without regard to its conflicts of law principles.

Trusted Agent Applicant Signature: _____

Print Name: _____ Date: _____

Organization Officer Sign Here: _____

Print Name: _____ Date: _____

Organization Officer's Title: _____ Telephone Number: (_____) _____

ACES DIGITAL CERTIFICATE PROGRAM ACES Trusted Agent

Summary of Relevant Policy Provisions

ACES CP Provisions (Edited)

1.3.2

Trusted Agents

CAs may choose to use the services of Trusted Agents to assist CAs in performing identity verification tasks. Trusted Agents do not have privileged access to CA functions, but are considered agents of the CA.

2.1.3

Trusted Agent Obligations

A Trusted Agent shall perform Subscriber identity verification in accordance with this CP.

3.1.9.1

In-Person Authentication

The CA shall ensure that the applicant's identity information and public key are bound adequately. Each CA shall specify in its CPS procedures for authenticating a Subscriber's identity. Additionally, a CA shall record the process that was followed for each certificate.

The process documentation must include a declaration of identity. The declaration shall be signed with a handwritten signature by the certificate applicant in the presence of the person performing the identity authentication.

For CLASS 3, applicant identity proofing requires the applicants to provide at least one federal government official picture identification credential (such as a ACES identification card or passport), or two non-federal government issued official identification credentials, at least one of which must be a photo ID, such as a drivers license. As an alternative to presentation of identification credentials, other mechanisms of equivalent or greater assurance (such as comparison of biometric data to identities pre-verified to the standards of this policy, and obtained via authenticated interaction with secured databases) may be used.

5.2.1.5

Trusted Agent

A Trusted Agent is a person authorized to act as a representative of a CA in providing Subscriber identity verification during the registration process. Trusted Agents do not have automated interfaces with CAs; they act on the behalf of the CA or the RA to only verify the identity of the Subscriber.

IDENTRUST's ACES CPS Provisions (Edited)

1.3.2

Registration Authorities

In its role as an ACES/ECA, IDENTRUST will function as the Registration Authority ("RA"). As RA, IDENTRUST may establish agents to perform registration functions including "**employees of banks, financial institutions or the employers of Subscribers who have entered into contractual relationships with IDENTRUST.**" **Banks, financial institutions and employers of Subscribers may enter into an agency contract with IDENTRUST so that their employees can serve as Registration Agents for IDENTRUST.** IDENTRUST will use legal relationships with banks, financial institutions and employers of Subscribers: 1) as a means of identifying authorized Registration Agents; 2) to control the responsibilities delegated to and by Registration Agents; 3) to establish the procedures for gathering Subscriber information and authenticating Subscriber identities; and 4) to specify other procedures and controls applicable to

Registration Agents. IDENTRUST will provide notaries and Registration Agents with information and/or instruction on in-person identification responsibilities, procedures and controls. IDENTRUST will oversee the performance of registration activities through IDENTRUST's "RA Operators."

IDENTRUST as RA and its RA Operators will use a secure, reliable and trustworthy system to process the application. Upon application approval, IDENTRUST will notify the applicant and provide instructions for Certificate retrieval.

IDENTRUST will collect information from, and distribute information to, applicants via a web interface. Through notaries, Registration Agents and/or the use of databases, IDENTRUST will verify the identity of the subject that desires to obtain a Certificate from IDENTRUST. Applicants will be instructed to take the ID form to a notary or other IDENTRUST-authorized person employed by their company or a financial institution. The applicant will proceed to the location and present the pre-printed ID form and acceptable photo identification. The applicant must appear personally before a notary, IDENTRUST or a Registration Agent and present a valid, government-issued photo ID, such as a passport or driver's license. The ID form will contain pre-printed documentation including: a Subscriber agreement, notary/agent instructions, and boxes or lines for the agent or notary to initial or fill in when verifying the accuracy of the identifying information presented. The applicant and the notary or Registration Agent will sign the ID form. The Registration Agent or notary will make a record and log entry of the documentation presented by the applicant. The Registration Agent or notary will verify that the identification information is protected against forgery, modification, or substitution, and that the identity information is securely bound to the applicant. IDENTRUST will supplement this process with out-of-band identity checking and/or database cross-checking, as described below in this document. Any handwritten signatures used for this process shall, at a minimum, be verified against signatures on any valid, government-issued photo ID cards (e.g., passport or driver's license). A need for the Certificate must be identified on the form, but the Subscriber will not be required to identify a specific program.

The information collected from the applicant will be submitted to IDENTRUST's RA Operator who will review the information submitted (including, where applicable, the authenticity of the notary's seal), verify the identifying information, and inform the applicant upon approval or rejection of the application. On approval, instructions and an activation code for Certificate retrieval will be delivered to the applicant at a delivery point independently obtained or verified by IDENTRUST (e.g., a verified postal address or telephone number). Certificate retrieval from IDENTRUST will require two-factor authentication by requiring the use of both the personal passphrase and the activation code, both of which were previously exchanged between the applicant and IDENTRUST. Communication of IDENTRUST's Root Certificate and the Subscriber's Class 3 Certificate will occur over an SSL-encrypted connection.

3.1.9

Authentication of Individual Identity

All applicants are required to appear in person before IDENTRUST, a licensed notary or a Registration Agent, and present the following official (government-issued) photo ID:

- One federal government official picture identification credential (such as a ACES identification card or passport),
- Two non-federal government issued official identification credentials, at least one of which must be a photo ID, such as a drivers license.

Applicants must fill out and sign a form acknowledging understanding and acceptance of the responsibilities associated with accepting a Certificate. The form will also serve as a testimonial to the accuracy of the information provided in the Certificate request.

ACES DIGITAL CERTIFICATE PROGRAM Business Representative Certificate

Part I – Sponsoring Organization Authorization Form

THIS AUTHORIZATION is given by the Sponsoring Organization ("Organization"), identified below, to IdenTrust Services, LLC an IdenTrust company ("IdenTrust"). The principal place of business of IdenTrust is located at 255 North Admiral Byrd Road, Salt Lake City, Utah 84116-3703 U.S.A (www.IdenTrust.com). IdenTrust is a Certification Authority ("CA") under contract with the U.S. federal government for the ACES (Access Certificates for Electronic Services) program.

WHEREAS Organization desires to authorize, and IdenTrust desires to perform under its contract with the General Services Administration, the issuance of an ACES Business Representative Certificate ("Certificate") that will identify the "Subscriber," identified below, as being employed, associated, affiliated with or authorized by Organization and will certify Subscriber's Public Key. (In "Public Key Infrastructures" like ACES, a Public/Private Key Pair is held by the Subscriber, the Private Key is kept secure and used to create Digital Signatures, and the Public Key is held openly, certified by a CA, and used to authenticate network access and Digital Signatures).

1. IdenTrust and Organization agree that:

- (a) IdenTrust or Organization, in its sole discretion, may terminate this Authorization and revoke the Certificate 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) Irrespective of the place of performance, this Authorization 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 of the Certificate Agreement for Organization set forth in Part III;
- (b) Organization is duly-organized and validly-existing under the laws of its state of organization and has full right and authority to use the Organization's name, stated below, to grant this authorization, and to perform all obligations required of it hereunder;
- (c) Organization has duly authorized Subscriber as a Business Representative of the Organization (whether as an officer, employee, partner, member, agent, or other associate) to use a Business Representative Certificate and its associated Private Key to transact business and make Digital Signatures on behalf of the Organization, and Organization hereby authorizes IdenTrust to issue a Business Representative Certificate to Subscriber that identifies Subscriber as such;
- (d) All information provided to IdenTrust by Organization will, to the best of Organization's knowledge, be accurate, current and complete and that Organization will immediately notify IdenTrust and request that the Certificate be revoked if: (1) Organization suspects any loss, disclosure, or other compromise of the Subscriber's Private Key; (2) information contained in the Certificate is no longer accurate or current (e.g., the Subscriber changes his or her name); or (3) Subscriber is no longer employed by, associated with, authorized by or affiliated with Organization; and

The undersigned personally warrants and represents that he or she has authority to accept the terms and conditions of this Authorization and to bind the Organization by his or her signature.

Print Applicant's Name

Organization Officer Signature

Print Organization Name

Print Organization Officer Name

Organization Headquarters Address

Print Organization Title

City, State, Zip

Date

ACES DIGITAL CERTIFICATE PROGRAM Business Representative Certificate

Part II - Notary Form

Terms and Conditions

The undersigned applicant warrants, represents, and attests that all facts and information provided in Parts I & II are, to the best of the undersigned applicant's knowledge, accurate, current and complete and that he or she: a) Is authorized by his or her Organization to receive and use an ACES digital certificate issued by IdenTrust; b) Has read and accepts the personal identifying information set forth herein; 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 Subscriber of an ACES Business Representative Certificate, including the terms and conditions found in the on-line ACES Business Representative Certificate Agreement.

The applicant agrees to: 1) accurately represent him or herself in all communications with IdenTrust and Relying Parties; 2) protect his or her private key at all times; 3) immediately notify IdenTrust if he or she suspects his or her private key to have been compromised, stolen or lost; and 4) use his or her key only for authorized business as allowed by the ACES Program.

Identification - Complete this section entirely. Incomplete forms will be returned.

You must present **either one** Federal Government-issued Photo ID **-OR-** **two** forms of ID issued by a state or local government. If presenting two IDs, at least one must be a Photo ID.

One verifiable Photo ID issued by the Federal Government such as Passport, Fed. Employee ID, US Military Photo ID, DoD CAC, etc.

Photo ID

Doc. Type/
Title: _____

Issuer: _____

Serial
No: _____

Exact
Name
Listed: _____

Issue Date: _____

Expir. Date: _____

Two verifiable forms of ID issued by a state or local government. At least one must be a photo ID (See "Instructions to Subscribers" on page 1 for acceptable forms of ID)

Photo ID

Doc. Type/
Title: Driver's License

Issuer: State of California

Serial
No: 12345678

Exact Name
Listed: John T. Doe

Issue Date: 02/13/2009

Expir. Date: 02/13/2011

Second ID

Doc. Type/
Title: Birth Certificate

Issuer: State of California

Serial
No: 12345678

Exact Name
Listed: John T. Doe

Issue Date: 02/13/1958

Expir. Date: _____

Signed By: _____

(Subscriber to sign only in the presence of Notary)

Print Name: John T. Doe

First Name

Middle Initial

Last Name

Email Address: john.doe@email.com

(Same email address as provided online)

Notarial Acknowledgement

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

- On 01/01/2010 (date), before me personally appeared John Doe (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 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

Signature _____

Mary Smith

(Seal)

ACES DIGITAL CERTIFICATE PROGRAM Business Representative Certificate

Part II - Notary Form

Terms and Conditions

The undersigned applicant warrants, represents, and attests that all facts and information provided in Parts I & II are, to the best of the undersigned applicant's knowledge, accurate, current and complete and that he or she: a) Is authorized by his or her Organization to receive and use an ACES digital certificate issued by IdenTrust; b) Has read and accepts the personal identifying information set forth herein; 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 Subscriber of an ACES Business Representative Certificate, including the terms and conditions found in the on-line ACES Business Representative Certificate Agreement.

The applicant agrees to: 1) accurately represent him or herself in all communications with IdenTrust and Relying Parties; 2) protect his or her private key at all times; 3) immediately notify IdenTrust if he or she suspects his or her private key to have been compromised, stolen or lost; and 4) use his or her key only for authorized business as allowed by the ACES Program.

Identification - Complete this section entirely. Incomplete forms will be returned.

You must present **either one** Federal Government-issued Photo ID **-OR-** **two** forms of ID issued by a state or local government. If presenting two IDs, at least one must be a Photo ID.

One verifiable Photo ID issued by the Federal Government such as Passport, Fed. Employee ID, US Military Photo ID, DoD CAC, etc.

Photo ID

Doc. Type/
Title: _____

Issuer: _____
Serial
No: _____
Exact
Name _____

Issue Date: _____
Expir. Date: _____

Two verifiable forms of ID issued by a state or local government. At least one must be a photo ID (See "Instructions to Subscribers" on page 1 for acceptable forms of ID)

Photo ID

Doc. Type/
Title: _____

Issuer: _____
Serial
No: _____
Exact Name
Listed: _____

Issue Date: _____
Expir. Date: _____

Second ID

Doc. Type/
Title: _____

Issuer: _____
Serial
No: _____
Exact Name
Listed: _____

Issue Date: _____
Expir. Date: _____

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

Print Name: _____ Email Address: _____
First Name Middle Initial Last Name (Same email address as provided online)

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 _____ (date), 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

Signature _____

(Seal)

ACES DIGITAL CERTIFICATE PROGRAM

Expedited Shipping Request

Once your application has been approved, you will be sent a retrieval letter with your activation code and instructions for retrieving your certificate. Our standard delivery method is through USPS and should take 3 to 10 days, depending on your location.

Many applicants have requested the ability to pay for expedited shipping such as overnight or 2nd day. If you would like to arrange expedited shipping, please complete this form and send it with your Part 1: Sponsoring Organization Authorization Form and your Part 2: Notary Form.

For all expedited shipping requests, you will be charged the actual amount of the shipping, using IdenTrust's discounted rates. You will not be charged a handling fee or a marked-up shipping rate.

Your Name: _____

Shipping Method Requested: Priority Overnight Standard Overnight 2nd Day 3rd Day

Option 1: Shipping label

If you already have an existing account with UPS or FedEx, you may complete a shipping label, with your account number, and include it when you send your forms.

Option 2: Your courier account number

If you already have an existing account with UPS or FedEx, you may include that information here and we will create a shipping label for your shipment.

Account Number: _____ UPS FedEx

Option 3: Credit Card on file

If you used a credit card to apply for your digital certificate and would like us to use that credit card to pay for the expedited shipping, sign this section to authorize use of that card.

I authorize you to use my credit card information on file, signed: _____

Option 4: Credit Card not on file

If you did not pay for your certificate using a credit card or if you would like to pay for expedited shipping using a different card, please call our support representatives at 888-339-8904.

**A receipt for the amount charged to your card will be emailed to you when your letter is sent.

ACES DIGITAL CERTIFICATE PROGRAM Business Representative Authorization Form

Part III - Certificate Agreement for Organization

IMPORTANT NOTICE: This ACES Certificate Agreement for Organization is a legal agreement between IdenTrust Services, LLC an IdenTrust company ("IdenTrust," "Us," "We," or "Our") and the Sponsoring Organization identified in Part I (or "Organization") that has authorized IdenTrust to issue an ACES Business Representative Certificate ("Certificate") to the Subscriber identified in Part I (the "Subscriber"). IdenTrust performs its ACES Certification Authority ("CA") functions as a government contractor in accordance with its contract with the General Services Administration ("GSA"). The purpose of the Certificate is to identify the Subscriber as being employed, associated or affiliated with Organization and to authenticate his or her Digital Signature, or to permit the online transaction of business, on behalf of the Organization.

Definitions of terms may be found below in Part IV. For further understanding of any terms or concepts not defined or explained herein, please refer to IdenTrust's ACES Certification Practice Statement ("the CPS") and the ACES Certificate Policy ("the CP") (both available at: http://www.identrust.com/certificates/aces_policies.html).

1. Certificate Issuance Process; Term; Amendment.

1.1 Certificate Issuance Process. After Subscriber has entered and submitted all data required during the online portion of the application process, Subscriber must download this ACES Business Representative Authorization Form (<http://www.identrust.com/pdf/ACESBusRepForm.pdf>) and take it to an official in Organization designated to sign on behalf of Organization and represent to IdenTrust that Subscriber is a duly-authorized representative and that the Organization has agreed to the terms set forth in Part III. Subscriber must also fill out and sign Part II of the Authorization Form in the presence of a notary employed by Organization or a financial institution. If IdenTrust accepts the application for a Certificate and confirms the information Subscriber and Organization submitted during the application process, IdenTrust will issue a Certificate to Subscriber for use in accordance with the terms of this Agreement and the ACES CP. As the Subscriber of an ACES Certificate, Subscriber must respond in a timely manner to ACES-related notices issued by IdenTrust. Subscriber may use the Certificate only for authorized purposes (to authenticate him- or herself and Organization with Relying Parties, to conduct business-related activities electronically, and to digitally sign electronic documents or initiate transactions or to gain access to Web sites or pages requiring certificate-controlled access). Such purposes include, but are not limited to, a) retrieving or updating business or restricted information, b) filing electronic documents with government agencies, c) applying for government licenses, loans or government benefits, or d) engaging in financial transactions with government agencies. The Certificate may not be used for purposes of fraud, any other illegal scheme, or any unauthorized purpose. If IdenTrust is also issuing the Subscriber an Encryption Certificate, then during key generation and Certificate issuance, the Private Key corresponding to the Encryption Certificate is securely escrowed by IdenTrust to allow for its recovery in case Subscriber loses the Private Key or in cases where an applicable law or policy requires key recovery. The Private Key corresponding to the Subscriber's Signing Certificate is never stored or escrowed. This Agreement (together with the applicable provisions of the CP and CPS) constitutes the entire agreement between Organization and IdenTrust, unless otherwise provided in a written agreement between Organization and IdenTrust.

1.2 Term. ACES Certificates are valid for two years from the date of issuance. Except for the provisions identified in Section 9 as surviving the termination of this Agreement, the term of this Agreement shall be contemporaneous with the Certificate's validity and shall terminate two years from the date the Certificate is issued, unless the Certificate is revoked prior to such time. Ninety days prior to expiration of Subscriber's Certificate, IdenTrust will provide Subscriber notice of renewal. Therefore, Subscriber should notify IdenTrust if his or her street address or e-mail address changes.

1.3 Amendment. The terms of this Agreement may be amended upon renewal of the Certificate, or at any time effective thirty (30) days after amended terms have been posted on the IdenTrust ACES Website. Use by any Business Representative of your Organization of any IdenTrust ACES Certificate after the effective date of any such amendment shall constitute notice of Organization's acceptance of the amended terms. Organization may decline to accept any such amended terms by directing its Business Representatives to refrain from use of their Certificates after the effective date of the amendment.

2. IdenTrust Verification of Subscriber and Organization Identity. Organization agrees to allow Us to verify Subscriber's and Organization's identity by any reasonable means. We may make inquiry with public or private databases or other sources, solely for the purpose of verifying the information Subscriber and Organization give Us in order to assist Us in making a determination regarding the issuance of a Certificate to Subscriber. We may also contact Organization's human resources department to verify employment. Organization and Subscriber each also authorize Us to store and keep any information generated during the application, identification and authentication, and Certificate issuance 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 approve the issuance of, an ACES Certificate.

3. PRIVACY ACT AND PAPERWORK REDUCTION ACT NOTICE AND DISCLOSURE. In accordance with the Privacy Act of 1974 and the Paperwork Reduction Act of 1980, the following notice explains how the information that Subscriber submits in order to obtain a Certificate is used and maintained: <http://www.identrust.com/privacy.html>. Section 9 of IdenTrust's ACES CPS (see above) also contains IdenTrust's Privacy Policies and Practices for ACES.

4. IdenTrust's Obligations as an ACES CA. In performing its duties as a government contractor under ACES, IdenTrust warrants that: a. it has issued, and will manage, Subscriber's ACES Certificate and related information in accordance with the requirements of the CP; b. it has complied with all requirements of the CP when identifying Subscriber and issuing Subscriber an ACES Certificate; c. it knows of no misrepresentations of fact in the ACES Certificate and that it has verified the information in the ACES Certificate; d. it has accurately transcribed information provided by Subscriber into the ACES Certificate; and e. the ACES Certificate meets the material requirements of the CP.

5. Organization's Obligations

5.1. Submit Correct Information. Organization represents and warrants to IdenTrust that all of the information Organization submits during the application process - including but not limited to Organization name – is, to the best of Organization's knowledge, accurate, current and complete and that Organization has provided IdenTrust with all Material Facts (as defined in Part IV, below) necessary to confirm the identities of Subscriber and Organization and to the reliability of the Certificate to be issued. Organization further agrees that for purposes of Certificate validity, if any of Subscriber's registration information changes (e.g., Subscriber has a change of employment, change of e-mail address or a change in legal name) Organization will immediately request revocation of Subscriber's Certificate(s). If Subscriber is still affiliated with Organization, then Subscriber may request issuance of new Certificate(s) with his or her updated registration information.

5.2. Binding Effect of Signed Message. Organization agrees that any Digital Signature made (i) with a Private Key verified to correspond to an ACES Signing Certificate validated as required in the CP (ii) upon identified data with the intent to signify the consent, agreement, approval or adoption of the content of such data by the Subscriber to whom the ACES Signing Certificate has been registered, shall have the same legal effect, validity and enforceability as if such content had been expressed in a writing manually signed by such person. Organization acknowledges that All Digital Signatures made, or transactions undertaken, using a Private Key verified to correspond to a Business Representative Certificate validated as required in the ACES CP shall be deemed to have been made by the Subscriber in a representative capacity on behalf of the Organization, unless, however, Subscriber is not employed by Organization at the time a Digital Signature was made or a transaction undertaken, or if the Relying Party has actual knowledge at the time of signature verification that Subscriber no longer has the authority to represent the organization.

5.3. Protecting Private Key(s). Organization acknowledges and agrees that Subscriber is responsible for protecting and maintaining sole possession and control of the Private Key corresponding to each Public Key for which IdenTrust issues a Certificate (subject to any escrow of Subscriber's Private Encryption Key for key recovery, if applicable, under Section 1). In addition, Organization represents and warrants to IdenTrust that, in regard to such Certificate, Organization will require Subscriber to keep his or her Private Key private and to safeguard and maintain Subscriber's Private Key (and any user IDs, passphrases, shared secrets, etc.) in strict secrecy and take reasonable security measures to prevent unauthorized access to, or disclosure, loss, modification, compromise, or use of, Subscriber's Private Key and the computer system or media on which Subscriber's Private Key is stored. If Organization ever suspects or discovers that Subscriber's Private Key has been compromised, Organization should immediately contact IdenTrust and request that the Certificate be revoked. ORGANIZATION CAN INITIATE A REVOCATION REQUEST BY SENDING A SIGNED E-MAIL (CONTAINING THE REASON FOR REVOCATION) TO ACESERVICES@IDENTRUST.COM, BY REVOKING IT ONLINE AT THE ACES CERTIFICATE MANAGEMENT CENTER, OR BY CALLING THE IDENTRUST HELP DESK AT 1-888-339-8904. IF ORGANIZATION EVER SUSPECTS OR DISCOVERS THAT THE SECURITY OF SUBSCRIBER'S PRIVATE KEY HAS BEEN OR IS IN DANGER OF BEING COMPROMISED IN ANY WAY, ORGANIZATION MUST IMMEDIATELY REQUEST THAT IDENTRUST REVOKE SUBSCRIBER'S ACES BUSINESS REPRESENTATIVE CERTIFICATE. SUBSCRIBER MUST THEN IMMEDIATELY CEASE USING HIS OR HER PRIVATE SIGNING KEY.

5.4. Review ACES Business Representative Certificate; Certificate Acceptance. The contents of the Certificate issued to Subscriber for use on behalf of Organization will be based on information provided by Subscriber and Organization. During the Certificate issuance process Subscriber is provided with the opportunity to review such information. All Subscribers agree to review and verify the accuracy of the information contained in their Certificates. Subscribers acknowledge that downloading or using the Certificate constitutes their acceptance of the Certificate and its contents. If Subscriber fails to notify IdenTrust of any errors, defects, or problems with your Certificate within 24 hours after downloading it, it will be considered to have been accepted by Subscriber. By accepting the Certificate, Subscriber further represents and warrants that all Material Facts in his or Certificate (i.e., Subscriber's Legal Name, Organizational Affiliation and Public/Private Key Pair) are accurate, current and complete. Upon acceptance, and at any time thereafter when a Subscriber uses his or her Certificate or the corresponding Private Key, Subscriber and Organization acknowledge and assent to the responsibilities identified herein (including those identified in the CP).

5.5. Situations Requiring Revocation of Subscriber Certificate(s). Organization must revoke a Subscriber's ACES Certificate if it discovers or suspects that Subscriber's Private Key (corresponding to your Public Key listed in Subscriber's ACES Certificate) has been or is in danger of being compromised or subjected to unauthorized use in any way, or if any Material Fact affecting the reliability of the Certificate changes or is no longer true (e.g., Subscriber's name changes, Subscriber is no longer employed, associated or affiliated with Organization, Subscriber no longer holds the Public/Private Key Pair, etc.) . Subscriber or Organization may also revoke Subscriber's Certificate at any time for any other reason. IdenTrust may also revoke Subscriber's Certificate without advance notice if IdenTrust, in its sole discretion, determines that: (a) the Certificate was not properly issued or was obtained by fraud; (b) the security of the Private Key corresponding to the Certificate has or may have been lost or otherwise compromised; (c) the Certificate has become unreliable; (d) Material Facts in the Certificate have changed or become untrue (e.g., Subscriber is no longer affiliated with Organization); (e) Subscriber or Organization have violated any applicable agreement or obligation; (f) Subscriber or Organization requests revocation; (g) a governmental authority has lawfully ordered IdenTrust to revoke the Certificate; (h) this Agreement terminates; or (j) there are any other grounds for revocation. Subscriber's right to use a Certificate ceases immediately upon revocation of the Certificate. Once a Certificate has been revoked, it cannot be used or reinstated.

5.6. Cease Use of an ACES Business Representative Certificate. Organization will require Subscriber to immediately cease using his or her Certificate in the following circumstances: (a) when Subscriber suspects or discovers that the Private Key corresponding to the Certificate has been or may be compromised or subjected to unauthorized use in any way; (b) when a Material Fact in the Certificate has changed or is no longer true, (c) upon the revocation or expiration of the Certificate, or (d) upon termination of this Agreement.

5.7. Risk of Loss and Indemnification. Organization agrees that it assumes the risk of any use of Subscriber's Private Key(s) or Certificates in violation of this Agreement. Organization also agrees, to the extent allowed by applicable law, to indemnify and hold IdenTrust and its affiliates harmless from any and all liabilities, costs, and expenses, including reasonable attorneys' fees, related to: any misrepresentation or omission of Material Fact, whether intentional or not, made by Subscriber or Organization to IdenTrust; any violation of this Agreement or the CP or the CPS by Organization or authorized users of the Certificate; or any misuse of Subscriber's ACES Certificate.

6. 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, FITNESS FOR A PARTICULAR PURPOSE, TITLE, AND NONINFRINGEMENT WITH REGARD TO IDENTRUST SERVICES OR ANY ACES BUSINESS REPRESENTATIVE CERTIFICATE ISSUED HEREUNDER.

7. LIMITATIONS ON IDENTRUST'S LIABILITY.

7.1 IDENTRUST SHALL HAVE NO LIABILITY FOR LOSS DUE TO USE OF SUBSCRIBER'S CERTIFICATES, UNLESS THE LOSS IS PROVEN TO BE A DIRECT RESULT OF A BREACH BY IDENTRUST OF THIS AGREEMENT OR THE CPS OR A PROXIMATE RESULT OF THE GROSS NEGLIGENCE, FRAUD OR WILLFUL MISCONDUCT OF IDENTRUST. IDENTRUST SHALL HAVE NO LIABILITY FOR CLAIMS ALLEGING ORDINARY NEGLIGENCE.

7.2 EXCEPT IN THE CASE OF IDENTRUST'S GROSS NEGLIGENCE, FRAUD, OR WILLFUL MISCONDUCT, IDENTRUST'S LIABILITY TO ORGANIZATION SHALL BE LIMITED TO THE AMOUNT PAID TO IDENTRUST BY ORGANIZATION WITH RESPECT TO THE YEAR IN WHICH THE CLAIM IS MADE FOR THE ISSUANCE OR RENEWAL OF THE CERTIFICATES ISSUED TO SUBSCRIBER PURSUANT TO THIS AGREEMENT.

7.3 IN NO EVENT SHALL IDENTRUST BE LIABLE FOR ANY CONSEQUENTIAL, INDIRECT, REMOTE, EXEMPLARY, PUNITIVE, SPECIAL, OR INCIDENTAL DAMAGES, OR DAMAGES FOR BUSINESS INTERRUPTION, LOSS OF PROFITS, REVENUES, SAVINGS, OPPORTUNITIES OR DATA, OR INJURY TO CUSTOMER RELATIONSHIPS, REGARDLESS OF THE FORM OF ACTION AND REGARDLESS OF WHETHER IDENTRUST WAS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7.4 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 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.

8. Dispute Resolution Provisions. This Agreement shall be governed by, interpreted and construed under the laws of the United States and 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 is found to be invalid or unenforceable, then this Agreement shall be deemed amended by modifying such provision to the extent necessary to make it valid and enforceable while preserving its intent or, if that is not possible, by striking the provision and enforcing the remainder of this Agreement.

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

9. Survival. Sections 4, 5.6, 5.7, 6, 7, 8 and the Sponsoring Organization Authorization Form, which is incorporated into this Agreement by reference, shall survive any termination or expiration of this Agreement.

ACES DIGITAL CERTIFICATE PROGRAM

Business Representative Certificate

Part IV – Definitions

Agency: A federal agency, authorized federal contractor, agency-sponsored university or laboratory, or when authorized by law or regulation, a state, local, or tribal government.

Application: A computer program or web-based interface used by a Relying Party to interact with subscribers.

Business Representative: The Subscriber of a Certificate that identifies the Subscriber as being employed, associated, affiliated with or authorized by a Sponsoring Organization.

Certificate: A computer-based record or electronic message issued by IdenTrust pursuant to its role as a Certification Authority that: (a) identifies IdenTrust as the Certification Authority issuing it; (b) names or identifies a Subscriber and the Organization or Agency with which he or she is associated; (c) contains the Public Key of the Subscriber; (d) identifies the Certificate's operational period; (e) is digitally signed by IdenTrust; and (f) has the meaning ascribed to it in accordance with applicable standards. A Certificate includes not only its actual content but also all documents expressly referenced or incorporated in it. . A Signing Certificate is a Certificate corresponding to a Private Key used for creation of Digital Signatures, and an Encryption Certificate corresponds to a Private Key used for message encryption.

Digital Signature: A Digital Signature is a transformation of an electronic message using Public Key Cryptography so that a person having the communication and the Subscriber's Public Key can accurately determine (1) whether the transformation was created using the Private Key corresponding to the Subscriber's Public Key, and (2) whether the communication has been altered since the transformation was made. It does not involve a handwritten signature.

Key Pair: In Public Key Cryptography, a Key Pair is two mathematically related keys (a Private Key and its corresponding Public Key), having the properties that (i) one key can be used to encrypt a message that can only be decrypted using the other key, and (ii) even knowing one key, it is computationally infeasible to discover the other key.

Material Fact: The phrase, "Material Fact," shall have the following meanings for the following circumstances as used in this Agreement: For Certificate Issuance (§§1 & 5.1): Material Facts are all facts requested by IdenTrust as part of the enrollment, Certificate issuance, Certificate replacement and Certificate renewal processes, which are relied upon by IdenTrust to confirm a Subscriber's identity and to bind the Subscriber's identity to the Public/Private Key Pair certified. For Facts Contained in the Certificate and giving rise to the Subscriber's Duty to Request revocation of the Certificate (§§5.4 - 5.6): Material Facts are the Subscriber's Legal Name, Organizational Affiliation and Public/Private Key Pair. For misrepresentations or omissions of Material Fact giving rise to the Subscriber's duty to indemnify IdenTrust (§ 7): "Material Fact" means all of the above.

Organization (also, "Sponsoring Organization"): A business entity, government agency, or other organization with which a Business Representative is affiliated (e.g., as an employee, agent, member, user of a service, business partner, customer, etc.).

Private Key: In Public Key Cryptography, a Private Key is the key of a Key Pair kept secret by its holder and can be used by its holder to encrypt or decrypt messages corresponding to the Public Key. The Private Key is used to create a Digital Signature.

Public Key: In Public Key Cryptography, a Public Key is the key of a Key Pair publicly disclosed by the holder of the corresponding Private Key and is used by the recipient to encrypt or decrypt messages corresponding to the Private Key. The Public Key is used to verify a Digital Signature.

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

Relying Party: An agency or other recipient of a digitally signed message authorized by the CP to rely on an ACES Certificate and is authorized in writing by IdenTrust or the General Services Administration to verify the Digital Signature on the message.

Repository: A database containing information and data relating to ACES Certificates, including information relating to ACES Certificate status as valid or revoked.

Subscriber: A person (e.g. a Business Representative) that (a) is named or identified in a Certificate as the "subject" of the Certificate, and (b) holds a Private Key that corresponds to a Public Key listed in that Certificate.