

ACES Trusted Agent Instructions

Thank you for choosing Digital Signature Trust (DST), 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 – Complete the “ACES Appointment as Trusted Agent” form. Take this form to an officer who can sign on behalf of your organization and represent to IdenTrust that you are authorized to electronically submit bulk loads and business agreement forms. Return the form to IdenTrust.

Step 2 – Complete “Part I - ACES Business Representative Authorization” form. Take this form to an officer who can sign on behalf of your organization and represent to IdenTrust that you are a duly-authorized representative of the organization. Return the form to IdenTrust.

Step 3 – Complete “Part II - ACES Notary” form and take it to a licensed Notary. This can be someone employed by your organization or a financial institution (most banks have notaries on staff) to verify your identity credentials. Present the Notary with the form and a current valid driver's license or state issued ID card, and sign the form in the presence of the Notary.

Once the Notary has verified your identity by reviewing and recording the information from your photo ID card, please make sure the Notary has properly notarized your signature and affixed his or her raised seal or colored ink stamp to the form.

Finally, record the name and place where you had the form notarized. Keep a copy of all three forms (ACES Appointment as Trusted Agent, Part I - ACES Business Representative Authorization, and Part II - ACES Notary) and send the **signed originals** to IdenTrust.

MAILING ADDRESS / OVERNIGHT COURIER ADDRESS:

IdenTrust, Inc.
Attn: ACES Registration
255 North Admiral Byrd Road
Salt Lake City, UT 84116
1-888-339-8904

EXPEDITE CERTIFICATES

To help expedite the processing of your digital certificates, please send the Forms via overnight services to the above address and also include a pre-filled air bill for FedEx, UPS, DHL or Airborne Express so that we can expedite your Approval Letters back to you.

Step 4- Apply for your ACES Business Representative Digital Certificate at:

<https://secure.digsigtrust.com/tsapp/bus-start.jsp?AT=212&CT=520000>

When you apply, the registration will ask you to print the ACES Business Representative Agreement Form. ***You do not need to download and print those forms*** because they are part of step 2 of these instructions.

Step 5- Await your “Approval Letter” which will be mailed to you at the address you indicated on the application. An e-mail notification will be sent to you immediately upon receipt of your application and upon its approval.

ACES Appointment as Trusted Agent

Digital Signature Trust, LLC ("DST"), a limited liability company organized under the laws of Delaware, with its principal place of business at 255 North Admiral Byrd Road, Salt Lake City, Utah, hereby appoints:

_____, an employee of _____, ("Trusted Agent" or "You"), to serve as DST's Trusted Agent under the ACES Certificate Policy. As a Trusted Agent You will assist DST in performing such identity verification tasks as may be required by the terms of our Bulk Submission Agreement, the ACES CP and DST'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 DST 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 DST of your intent to terminate your Trusted Agent status.

You warrant to DST that you have read the relevant provisions of the ACES CP and DST's ACES CPS and understand your obligations as described in those documents.

As a Trusted Agent of Digital Signature Trust, 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 DST.
- 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 DST; 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 DST 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: _____

Phone Number: (_____) _____

Date: _____

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.

DST's ACES CPS Provisions (Edited)

1.3.2

Registration Authorities

In its role as an ACES/ECA, DST will function as the Registration Authority ("RA"). As RA, DST 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 DST."* *Banks, financial institutions and employers of Subscribers may enter into an agency contract with DST so that their employees can serve as Registration Agents for DST.* DST 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. DST will provide notaries and Registration Agents with information and/or instruction on in-person identification responsibilities, procedures and controls. DST will oversee the performance of registration activities through DST's "RA Operators."

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

DST will collect information from, and distribute information to, applicants via a web interface. Through notaries, Registration Agents and/or the use of databases, DST will verify the identity of the subject that desires to obtain a Certificate from DST. Applicants will be instructed to take the ID form to a notary or other DST-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, DST 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. DST 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 DST'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 DST (e.g., a verified postal address or telephone number). Certificate retrieval from DST 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 DST. Communication of DST'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 DST, 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), or
- 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.

Part I - ACES Business Representative Authorization Form

THIS AUTHORIZATION is given by the Sponsoring Organization ("Organization"), identified below, to Digital Signature Trust ("DST") an IdenTrust Company, a Utah corporation with its principal place of business at 255 North Admiral Byrd Road, Salt Lake City, Utah 84116-3703 U.S.A (www.IdenTrust.com) and 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 DST 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. DST and Organization agree that:

- (a) DST or Organization, in its sole discretion, may terminate this Authorization and revoke the Certificate at any time and for any reason;
- (b) DST 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 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, given below, to grant this authorization, and to perform all obligations required of it hereunder;
- (b) Subscriber is a duly-authorized representative of the organization as an employee, partner, member, agent, or other associate, and DST is hereby authorized to issue an ACES digital certificate to subscriber that identifies Subscriber as being employed, associated, affiliated with and/or authorized by Organization;
- (c) Federal agencies, and other government-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 DST (Certificates have a two-year lifetime)
- (d) All information provided to DST by Organization will be accurate, current and complete and that Organization will immediately notify DST 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
- (e) DST does not assume, nor should it be exposed to, the business and operational risks associated with Organization's business, and Organization will hold DST, its subcontractors, affiliates, and employees harmless from any and all liabilities, costs, and expenses, including reasonable attorneys' fees, related to the services provided to Subscriber or in connection with any performance under this Authorization.

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 Subscriber Name Organization

Officer Signs Here

Print Sponsoring Organization Name

Print Name Here

Address

Print Officer's Title Here

**Part II - ACES Notary Form
INSTRUCTIONS FOR NOTARY**

FOR THE PURPOSES OF THIS DOCUMENT, PERSONAL ACQUAINTANCE WITH THE INDIVIDUAL IS INSUFFICIENT. You must: 1) review a current government-issued ID containing the individual's name and photograph, 2) verify that such photo ID information is protected against forgery, modification, or substitution and 3) record below the serial number and type of government-issued ID presented by the applicant. You should also record in your "notary's journal" the ID serial number of the identification that was presented to you.

The undersigned applicant warrants, represents, and attests that all facts and information provided are accurate, current and complete and that he or she:

- a) Is authorized to receive, and has applied electronically for, an ACES digital certificate to be issued by DST;
- b) Has read and accepts 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 an ACES certificate subscriber, 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 DST/Identrus and Qualified Relying Parties; 2) protect his or her private key at all times; 3) immediately notify DST/Identrus 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.

Signed By: _____
(Sign Only In The Presence Of Notary)

Print _____
First Name, Middle Initial, Last Name

E-mail Address _____

ACKNOWLEDGEMENT

State of _____

County of _____

The foregoing instrument was acknowledged before me this ____ day of _____, _____, by the signer and subject of the above form, who personally appeared before me and signed or attested the same in my presence, and presented the following government-issued photo ID card as proof of their identity:

Exact Name Listed on Photo ID Serial Number of Photo ID Expiration ID Type

Notary Public _____

Residing in: _____

My Commission Expires: _____

Street Address of Branch or Office

Name of Organization Employing Notary



Terminology Used in the Business Representative Authorization Form

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 an Agency 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 DST that: (a) identifies DST as the Certification Authority issuing it; (b) names or identifies a Subscriber and the Subscriber's Organization; (c) contains the Public Key of the Subscriber; (d) identifies the Certificate's operational period; (e) is digitally signed by DST; 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.

Certification Authority: A Certification Authority is an entity that is responsible for authorizing and causing the issuance of a Certificate.

Certification Practice Statement: A "Certification Practice Statement" is a statement of the practices that a Certification Authority employs in issuing, suspending, revoking, and renewing Certificates and providing access to same, in accordance with the requirements of a contract for certificate services.

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.

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.

Qualified Relying Party: A federal agency or other recipient of a digitally signed message authorized by the CP to rely on an ACES Certificate and that has entered into a Memorandum of Understanding with the Government Services Administration to participate in the ACES Program to verify the Digital Signature on the message.

Responsible Individual: A trustworthy person designated by a Sponsoring Organization to Authenticate individual applicants seeking certificates on the basis of their affiliation with the Sponsoring Organization.

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.).

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