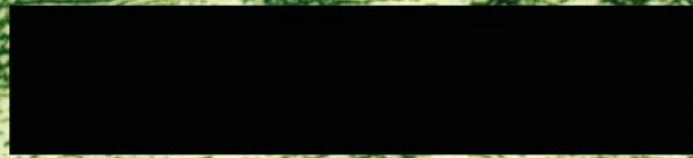


Everyone needs ACES Certificates
to work with the US Government.



IdenTrust™

IdenTrust
ACES Digital Certificates



Digital Identity Certificates Provide More Assurance for Electronic Communications

Interactions with the government have undergone enormous change in recent years. Transactions that were traditionally paper-based are being transferred to an electronic format, so that they are completed more rapidly. As a result, more information is being captured and stored electronically. As government agencies continue to integrate the Internet with agency systems that collect and maintain sensitive information about citizen-to-government, business-to-government and government-to-government relationships, it is critical that they ensure authenticity and accountability in processing these electronic transactions.

One of the government programs designed to reduce fraud and secure transactions is the ACES Digital Certificate Program. Any U.S. resident can obtain an ACES digital certificate from IdenTrust. An ACES digital certificate is an electronic "identification card" issued by IdenTrust, which establishes an individual's identity for online transactions—more securely than a simple username and password. (Username and password are single-factor authentication— "something you know"— while digital certificates are two-factor "something you know" plus "something you have").

IdenTrust leads in ACES certificate issuance

IdenTrust was the first Certificate Authority to receive GSA's approval to provide ACES certificates. Today, IdenTrust is the leading issuer of ACES certificates. By continuing to expand the number of agencies accepting and using ACES certificates, IdenTrust is a key driver in expanding electronic government.

IdenTrust provides three types of ACES certificates: Business Representative, Unaffiliated Individual and Device Certificates (both SSL/TLS and VPN).



The Role of ACES

Access Certificates for Electronic Services, or ACES, is a program administered by the U.S. General Services Administration (GSA) that provides strongly authenticated electronic identity credentials to citizens or business representatives. The ACES program combines standard digital signature solutions with carefully developed and audited identity authentication and validation policies. Numerous state and federal agencies have already implemented digital certificate authentication for systems that accept online transactions. The result is a trusted electronic credential that asserts the identity of the individual to the agency system or application and authenticates the transaction. ACES certificates can be used to authenticate users for controlled access to government systems, and more importantly, to submit government forms and documents with less risk to the agency that the person will repudiate the transaction.

The ACES program supports a government-wide approach, consistent with its e-Authentication Initiative, because an ACES digital certificate can be relied upon by any state or federal agency. Once authenticated, certificate holders can utilize these credentials at any other participating agency. This eliminates the hassle of managing different security credentials each time the person needs to conduct business. One certificate provides authentication and access to all systems that are "PKI-enabled" and have "trusted" the Federal Government's Root Certificate. IdenTrust's credential-issuing certificate has been cross-certified by the Federal Bridge Certification Authority at a medium assurance level.

Certificate Type	Feature
ACES Business Representative	<ul style="list-style-type: none">• Authenticate yourself to gain access to a PKI-enabled application on behalf of your organization at a medium level of assurance (e.g. a secure web server)• Digitally sign documents to replace "ink" signatures (e.g. signing a contract)
ACES Unaffiliated Individual	<ul style="list-style-type: none">• Authenticate yourself to gain access to a PKI-enabled application at a basic level of assurance (e.g. client-authenticated secure SSL/TSL connection)• Digitally sign documents to replace "ink" signatures (e.g. signing a form)
ACES Agency Application TLS/SSL Server Certificates and ACES VPN IPsec Client Certificates	<ul style="list-style-type: none">• Authenticates and encrypts data transmission• Enables authenticated, encrypted communications with servers and applications• Allows mutual authentication and/or encrypted TLS/SSL communications (or VPN communications using a VPN certificate) between devices operated by federal, state or local agencies or government contractors.

Experience and Reputation

IdenTrust is a partner in several significant certificate programs with state and federal government. Our experience and reputation is second to none.

Agencies currently using IdenTrust ACES certificates include:

NATIONAL INSTITUTES OF HEALTH – Electronic Grant Applications. ACES certificates, used in conjunction with the Federal Bridge Certificate Authority (FBCA) and the Higher Education Bridge Certificate Authority (HEBCA) enable the NIH to validate digitally signed electronic submissions from multiple institutions.

US DEPARTMENT OF LABOR – Electronic Submission of Annual Labor Management Financial Reports. Labor Unions are using ACES certificates to digitally sign and electronically file detailed annual financial reports with the Department of Labor. This provides improved and expedited access to more accurate data--lowering the cost for both the Department of Labor and the unions filing the reports.

US DEPARTMENT OF STATE – D-TRADE - The State Department enables companies to electronically file for munitions export licenses. ACES certificates control access to this highly sensitive website, and are used to digitally sign license applications.

INTERNAL REVENUE SERVICE – Secure Data Transfer – The IRS uses ACES Business Representative digital certificates to authenticate state agencies and financial institutions for data exchange.

US ENVIRONMENTAL PROTECTION AGENCY – Central Data Exchange – A central submission point for EPA reporting systems to receive legally acceptable data in various electronic formats.

WEST VIRGINIA DEPARTMENT OF ENVIRONMENTAL PROTECTION – WVDEP processes permits and applications electronically using an ACES digital certificate.

Not only does IdenTrust issue certificates under the ACES program, we have years of experience in other Government applications, at both federal and state levels. We issue certificates to the defense industry as an approved vendor of the Department of Defense's ECA program, as well as providing digital certificates used by the State of Washington's "Transact Washington" portal.

Benefits

Government-approved solution

- GSA owns and administers the ACES program
- Available on the GSA Multi-Award Schedule

Applicable both inside and outside of government agencies

- In fact, our largest customers are corporate entities conducting business with government
- Ideal for business-to-government solutions
- Works for citizen (or consumer)-to-government as well

Part of the E-Gov solution

- Enables compliance with the Government Paperwork Elimination Act
- An ACES subscriber can use the certificate with any participating Federal Agency
- Certificates meet NIST SP 800-63 multi-factor authentication requirements (Level 3) – a security level much higher than simple pin and password (Level 2)

Flexible registration

Identification and authentication aligned with the specific needs of small or large subscribing organizations, including online registration for individuals and bulk load registration for groups.

1. **Bulk Loading** – The IdenTrust Bulk Load process is intended to simplify the purchasing process when registering for 5 or more certificates in a single submission. In order to bulk load certificates to IdenTrust, you will need to appoint a representative from your organization as a Trusted Agent.
2. **Trusted Agent** – An individual within a subscribing organization who is appointed by the organization and approved by IdenTrust to act as a Trusted Agent and perform identity verification tasks on behalf of the organization.
3. **LRA Central** – A web-based interface that can be used by organizations to manage the accounts of its ACES subscribers.

When PIN and Password aren't enough

Many agencies routinely have access to or require the disclosure of Personally Identifiable Information or sensitive proprietary business information. ACES digital certificates can be used to secure the communication of:

- Financial disclosures
- License applications
- Medical information
- Social Security numbers
- Drivers License data
- Telephone numbers
- Street address
- E-mail address
- IP address (in some cases)
- Vehicle registrations
- Driver's license numbers
- Biometrics--face, fingerprints, or handwriting
- Credit card numbers
- Country, state, or city of residence
- Age, Gender or Race
- Name of school or workplace
- Grades, salary, or job position
- Criminal records
- Sensitive business records

There are multiple benefits to using an electronic versus paper-based form signed with a digital signature: reduced costs, improved process flows, detailed audit trail and lower risk environment

Cost benefits:

- Certificate costs: Usually businesses pay for their own certificates, not the agency
- Archiving: Manage document lifecycles without moving trucks and warehouses
- Postage: Some agencies spend tens of millions of dollars just on mailing forms alone

Work/Process flow benefits:

- Timeliness: When you digitize a form, the data is available instantaneously. Paper submittals depend on outside factors that are notoriously slow: mail, handling, routing, etc.
- Assurance: When a document is signed, a "hash" of that document is created, and if the document is altered in any way, that hash is broken, telling you it has been modified
- Lower Risk: Using Digital Certificates satisfies Multi-Factor Authentication (something you know and something you have) providing an audit trail of accountability

ACES Digital Certificates are an Immediate and Proven Solution to Authentication

The U.S. government will continue to require greater levels of online security and authentication from individuals wanting to conduct business electronically with its agencies. IdenTrust's experience with government digital certificate policies is proven and extensive. Digital certificates are about trust. With IdenTrust, you can trust that the certificates issued will stringently adhere to government policies and be provided with the highest level of customer service.

How To Get A Digital Certificate – A Simple 4-step Process

STEP 1:

Online Application

Go to www.IdenTrust.com

Select the certificate you need and fill out the online application and provide payment.

STEP 2:

Identification

IdenTrust confirms your identity. Documentation is submitted if necessary.

STEP 3:

Approval

IdenTrust validates your information with independent data sources and approves certificate issuance – typically takes 3 business days.

STEP 4:

Digital Certificate Retrieval

Once approved, you will receive a welcome letter with instructions on how to retrieve and use your digital certificate.

For more information, visit www.IdenTrust.com.

To contact ACES Sales, call (866) 763-3346 or send an email to ACESsales@IdenTrust.com