

ECA Medium Assurance Token Certificate



PROGRAM

The Department of Defense (DoD) External Certification Authority (ECA) program enables contractors, suppliers, partners and other approved external organizations to securely access DoD systems, exchange information and conduct trusted digital transactions using DoD-approved certificates. The ECA program supports various use cases, including secure email, digital signatures, and encryption, ensuring that external entities can interact securely with the DoD.

ASSURANCE LEVEL

The Medium Assurance level in the DoD ECA program is designed for applications handling sensitive, medium-value information. This level ensures a balance between security and usability for external entities interacting with the DoD.

AFFILIATION

To obtain a Medium Assurance certificate, applicants must be affiliated with a sponsoring organization, complete an online enrollment process, provide required identity information, and successfully complete in-person identity verification through a Trusted Agent or Notary Public.

STORAGE

The ECA | Medium Assurance | Token certificate is downloaded directly to a FIPS-compliant USB or smart card for secure storage.

ADDITIONAL INFORMATION

- Available in one-, two-, or three-year validity periods
- Certificate is stored on a single USB or Smartcard
- Available for both US and Non-US residences
- SHA-384 signature hash algorithm

USE CASES

The IdenTrust ECA Medium Assurance Token certificate offers a variety of uses with DoD contractors, Industrial Security Professionals, and foreign allies to securely interact with the Department of Defense to protect data and establish trust.

Access and Secure Authentication

- Authenticate into secure, restricted DoD Information Systems
- Log into Defense Partner web portals
- View and track electronic defense contracts within select systems of the Wide Area Work Flow (WAWF)

Encrypted Communications

- Satisfy CMMC requirements by enabling secure handling of Controlled Unclassified Information (CUI)
- Digitally sign and encrypt unclassified emails
- Encrypt files to prevent interception/modification by third parties
- Assure organization and sender identity with Identity Verification

Compliance and Document Control

- Apply digital signatures to DoD contracts, proposals, and submissions
- Prevent signatory denial of transactions or approvals with non-repudiation
- Support security and digital trust requirements associated with NIST SP 800-171

ABOUT IDENTRUST

IdenTrust, part of HID, is a leader in digital identity and PKI-based certificate solutions. With headquarters in Salt Lake City, Utah, and locations in Austin, TX; Paris, France; Stockholm, Sweden; and Vienna, Austria, IdenTrust has been securing the world's most critical systems for over two decades.

As a pioneer in identity-based security, IdenTrust empowers governments, enterprises, financial institutions, healthcare providers, and professionals to protect data, authenticate users and perform online transactions with confidence. Our PKI-based services are trusted by Fortune 500 companies, global banks and public sector organizations alike — securing everything from financial transactions and government communications to enterprise authentication and IoT deployments.

From TLS/SSL website security and S/MIME email encryption to digital signatures, code signing, IoT device authentication and EPCS-compliant certificates for digitally signing prescriptions, IdenTrust offers a comprehensive suite of identity-based digital certificates. Our solutions are designed to meet the evolving demands of a connected world while ensuring compliance with stringent standards, including DoD ECA, DEA EPCS, and other regulatory frameworks. Recognized for their reliability, interoperability and alignment with policies, IdenTrust certificates represent the gold standard in global digital trust.

As part of HID, IdenTrust is backed by the innovation and scale of a global identity leader — ensuring our customers benefit from world-class technology, support and vision.

WHAT SETS US APART

Proven Compliance: IdenTrust certificates meet or exceed the most rigorous industry standards, including CAB Forum Baseline Requirements, EV Guidelines and key RFCs. We're also cross-certified with the U.S. Federal Bridge, ensuring interoperability across federal and commercial ecosystems.

Global Reach, Local Trust: With millions of certificates issued worldwide, IdenTrust supports a diverse range of use cases — from TLS/SSL and document signing to code signing and device identity — backed by world-class support and regional expertise.

Security at Scale: Whether you're deploying a few certificates or managing millions of IoT devices, our infrastructure is built for performance, resilience, and automation.

Innovation with Integrity: As part of the HID family, IdenTrust is at the forefront of identity innovation — combining decades of cryptographic expertise with emerging technologies to meet the evolving needs of digital trust.

When trust is essential, and security is non-negotiable, organizations around the world choose IdenTrust to transact with confidence.

ADDITIONAL INFORMATION & RESOURCES

- [Identity Verification Requirements](#)
- [ECA Policies](#)
- [ECA FAQs](#)

FOR IDENTRUST INQUIRIES:

Sales — (888) 928-7974 or ECSales@IdenTrust.com
Support — (800) 748-5360 or Support@IdenTrust.com



North America: +1 512 776 9000 | Toll Free: 1 800 237 7769
Europe, Middle East, Africa: +353 (91) 414060
Asia Pacific: +852 3160 9800 | Latin America: +52 55 9171 1108
For more global phone numbers click here

© 2026 HID Global Corporation/ASSA ABLOY AB. All rights reserved.
2026-08-24-iams-identrust-emc-medium-assurance-token-certificate-ds-en
Part of ASSA ABLOY