IGC Medium Assurance

Organization Identity
Device Certificate

PROGRAM

The IdenTrust Global Common (IGC) certificates are issued under the IGC Certification Policy program and are cross-certified with the U.S. Federal PKI Common Policy Framework. These certificates are accepted by U.S. Government agencies for use by approved system devices to provide encryption protection and to communicate with U.S. Federal Government systems.

ASSURANCE LEVEL

IGC Medium Assurance is one of the assurance levels defined by the Certificate Policy. It specifies the minimum requirements for identity proofing, certificate issuance and management processes to ensure a medium level of trust in the issued certificates. This assurance level supports environments where authenticated device identity and validated organizational control are essential for secure federal and enterprise operations.

IDENTITY VERIFICATION

Organization Identity, whereas there is a direct affiliation or endorsement by a sponsoring organization, a completed Certificate Signing Request (CSR) and, applicant identity, also known as the Primary Machine Operator, is established by in-person proofing before a Trusted Agent or Notary Public and verified through automated means where the applicant provides identity data points including name, date of birth, address and other personal and organizational information.

STORAGE

The IGC Medium Assurance Organization Identity certificate is available in one storage option:

Device — Stored directly to the system's device for which it was applied, to deliver strong assurance for systems, servers and high trust network components.

USE CASES:

The IGC Medium Assurance Level Organization Identity device certificate offers a variety of use cases across multiple industries:

- **Government —** Federal, state, and local agencies utilize IdenTrust device certificates to provide interoperability with U.S. Federal systems through U.S. FBCA compliance, identification of network devices, server-to-server authentication and client/server authentication within a known, trusted environment.
- **Healthcare — Device certificates ensure compli**ance with DEA mandates for server-level signing of Electronic Prescriptions for Controlled Substances (EPCS) messages. Helps to safeguard protected health information by securing communication paths between clinical systems, applications and connected devices.
- **Enterprise —** Encrypting data and establishing secure links between organization servers and third parties. Ideal for zero trust architectures, automated workflows and environments requiring strong device authentication across cloud, hybrid and on premises infrastructures.

IdenTrust part of HID

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

Acceptable Forms of Identification
IGC Policies
IGC FAQs

FOR IDENTRUST INQUIRIES:

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

IdenTrust part of HID

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

2026-02-24-iams-identrust-igc-medium-assurance-organization-identity-device-certificate-ds-en
Part of ASSA ABLOY