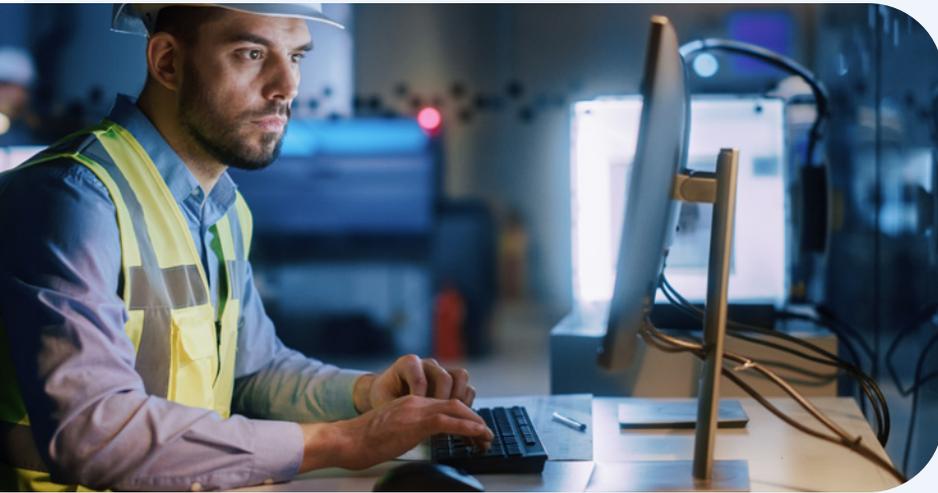# IGC Medium Assurance

Business Identity
Software & Hardware

PROGRAM

The IdenTrust Global Common (IGC) certificates are issued under the IGC Certification Policy that is cross-certified with the U.S. Federal PKI Common Policy Framework. This cross-certification ensures broad interoperability and allows IGC certificates to be trusted by U.S. Government agencies for secure digital signing, encrypted email, authentication and non repudiation — preventing the signer from repudiating digitally signed documents. IGC Medium Business combines individual identity, employer verification, federal cross certification and HID's global identity leadership — delivering higher trust assurance and easier deployment.

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. Supports federal compliance requirements and high trust organizational identity scenarios where employer verified roles are essential.

IDENTITY VERIFICATION

Business Identity, which involves a direct affiliation or endorsement by an employer or sponsoring organization, is established through 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 information.

STORAGE

The IGC Medium Assurance Business Identity certificate is available in two storage options:

Software — Downloaded directly to a laptop/PC browser store for secure storage on a single device

Hardware — Downloaded to a FIPS 140-2 compliant USB token or smart card, available to purchase from IdenTrust during the application, which provides portability and multi-factor authentication (MFA)

USE CASES:

The IGC Basic Assurance Level Individual Identity certificate offers a variety of use cases across multiple industries:

- **Government —** Federal, state, and local agencies use IdenTrust for secure application access, digital signing and encrypted email.

- **Healthcare —** Digital certificates ensure compliance with DEA mandates for EPCS prescribing, protect patient data and secure medical devices.

- **eNotary —** Notaries use IdenTrust certificates with select RON partners to meet state requirements for remote, online notarizations and document signing.

- **Personal and Professional —** Individuals use IdenTrust certificates for secure email and electronic document signing, as well as for the digital signing/sealing of documents such as plans and proposals.

- **Trusted by Adobe® —** Requiring hardware storage, IdenTrust IGC Medium certificates are cross-certified with the US Federal Bridge program as a member of the Adobe Approved Trusted List.

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™