

IGC Basic Assurance Individual Identity Hardware or Software Certificate



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. These certificates are accepted by U.S. Government agencies for use by approved persons to provide digital signing of documents, encrypt email, and provide non-repudiation (ensuring signers cannot deny their digital signatures).

ASSURANCE LEVEL

The IGC Basic Assurance Level 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 basic level of trust in the issued certificates.

IDENTITY VERIFICATION

Individual Identity, whereas there is no direct affiliation or endorsement by an employer or sponsoring organization, is established by in-person proofing before a Registration Authority or Trusted Agent; or verified through automated means where the applicant provides identity data points including name, date of birth, address and other personal information.

STORAGE

The IGC Basic Assurance Individual Identity certificate is available with 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 application that 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 encrypt 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 & Professional — Individuals use IdenTrust certificates for secure email and electronic document signing, digital signing/sealing of documents such as plans and proposals

BENEFITS

The IGC Basic Assurance Individual Identity Hardware or Software Certificate delivers the following advantages for your organization:

Trusted Security: Government-accepted certificates ensure verified identities and tamper-proof communications, preventing unauthorized access and meeting compliance requirements

Operational Efficiency: Accelerate business processes with legally binding electronic signatures, reducing transaction times while enabling secure remote work

Cost Savings: Eliminate paper-based workflows, reduce administrative overhead, and simplify identity management across your organization

Risk Protection: Prevent data breaches with strong encryption, provide legal defensibility with non-repudiable signatures, and reduce fraud through verified digital identities

ABOUT IDENTRUST

IdenTrust, part of HID, is a leading provider of trusted identity solutions, delivering digital certificates that secure online transactions, encrypt communications and authenticate identities. Recognized by financial institutions, healthcare providers, government agencies and enterprises worldwide, IdenTrust ensures compliance, security and operational efficiency across industries.

As the only bank-developed identity authentication system, IdenTrust provides a legally and technologically interoperable environment for identity authentication in more than 175 countries. With millions of active certificates and supporting billions of validations per year, IdenTrust sets the gold standard in digital trust.

CORE PRINCIPLES

- **Trust & Compliance** — IdenTrust certificates comply with global security standards, including WebTrust, SOC2, DirectTrust, Federal PKI, GDPR and DEA EPCS mandates, ensuring businesses meet regulatory requirements
- **Scalability & Integration** — Offering SSL/TLS, client authentication, document signing, code signing, S/MIME for email signing and encryption, and IoT certificates, that are publicly trusted or trusted by the U.S. Government. IdenTrust provides seamless integration with enterprise and cloud-based systems.
- **Reliability & Automation** — With 99.9%+ system uptime, IdenTrust ensures uninterrupted validation and issuance while enabling certificate lifecycle management through web portal and APIs

Headquartered in Salt Lake City, UT, IdenTrust operates from its primary datacenter with additional support from its London, UK office, serving banking and financial customers in EMEA. By combining trusted identity authentication, global compliance and industry-leading reliability, IdenTrust empowers businesses, governments and individuals to transact securely with confidence in an increasingly digital world.

RELATED INFORMATION:

- [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



HID Regional Offices

North America: +1 512 776 9000 | Toll Free: 1 800 237 7769

Europe, Middle East, Africa: +44 1440 714 850

Asia Pacific: +852 3160 9800 | Latin America: +52 (55) 9171-1108

For more global phone numbers click here

© 2025 HID Global Corporation/ASSA ABLOY AB. All rights reserved.

2025-05-20-iams-identrust-igc-basic-assurance-iis-hsc-ds-en

Part of ASSA ABLOY