IdenTrust™
part of HID Global

DIGITAL CERTIFICATES

# IGC | Medium Assurance | Organization Identity | Device Certificate

IGC | Medium Assurance | Organization Identity | Device certificates are idea for:

- Identification of network devices
- Server to server authentication
- Client/server authentication within a known trusted environment
- Server level signing of EPCS messages.

They are also ideal for any systems that need to communicate with U.S. Federal Government systems.

## Product Summary

IGC | Medium Assurance | Organization Identity | Device certificates are compliant with U.S. FBCA Medium Device assurance levels and are ideal for securing devices that require digital signing and encryption protection functions. They are also suitable for any systems that need to communicate with U.S. Federal Government systems.

You will apply for the IGC | Medium Assurance | Organization Identity | Device certificate and act as the sponsor and manager of the device. Your role is sometimes referred to as a Primary Machine Operator. You can also designate other individual(s) who can act in the role of a Secondary Machine Operator.

This is a software certificate and is stored in the device to which it is issued.

| | |
|---|---|
| Identity Authentication Method: | Your identity must be verified by a Notary Public or Trusted Agent |
| Identity Proofing Requirements: | Proof of identity, verification of the device and affiliation with the Sponsoring Organization |
| Forms Packet Required: | Yes – You are required to submit a complete forms packet with your application |
| CSR Submission: | You will need to provide a Certificate Signing Request (CSR), known as PKSC#10. Visit our How to Generate a CSR page if you need assistance |
| Trust Model: | This certificate is both publicly and government trusted |
| Assurance Level: | Organization and Device |
| Certificate Type: | This is a business certificate issued to you and the device that you will manage |
| Validity Periods: | Available up to a three (3) year validity period |
| Storage Type: | Stored in the associated device |
| Available to Non-U.S. Residents: | Yes – This certificate is available to applicants in a limited number of foreign countries, view our Supported Countries list |

## Sample Use Cases

- Identification of network devices
- Device to device authentication
- Client/device authentication within a known trusted environment
- Device level signing of EPCS messages

## Certificate Usage

The main purpose of this certificate is to secure websites interacting with the U.S. Federal government via:

- Data and Communications Encryption
- Server Authentication
- Client Authentication

Technical Specifications:

- X509 v3 digital certificate
- 2048 RSA bit key length
- SHA-256 signature hash algorithm
- CRL and OCSP validation
- Natively trusted by above mentioned browsers

## Other Resources

Related information:

- Acceptable Forms of Identification
- IGC Forms, Agreements and Policies
- IGC FAQs

**For IdenTrust Sales inquiries: +1 (801) 384-3481 | IGCsales@identrust.com**