DIGITAL CERTIFICATES

IdenTrust™
part of HID Global

IGC Medium Assurance Device Certificate

Product Summary

IGC Medium 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 a 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 individuals who can act as your back up to manage the device and 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:	As the device sponsor, your identity must be verified by a Notary Public
Identity Proofing Requirements:	Proof of identity, vetting of the device and confirmation of affiliation with the sponsoring organization
Forms Packet Required:	Yes - You are required to submit a forms packet with your application
CSR Submission:	You will need to provide a Certificate Signing Request (CSR), known as PKCS#10. Visit our **How To Generate a CSR** page if you need assistance. **Link TBD**
Trust Model:	This certificate is publicly and government trusted
Assurance Level	Device and Organization
Certificate Type:	An affiliated certificate that it is issued to you and the device that you will manage
Validity Periods:	Issued for one (1), two (2) or three (3) year validity periods
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 the **IGC Device Foreign Countries** list. **Link TBD**
Certificate Delivery Time:	3-5 business days after Forms Packet submission

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 using via:

- Data and Communications Encryption
- Server Authentication
- Client Authentication

Other Resources

Related information available at the following links:

- How to Apply **(link to URL TBD)**
- Acceptable Forms of Identification **(link to URL TBD)**
- TrustID Forms, Agreements and Policies **(link to URL TBD)**
- TrustID FAQs **(link to URL TBD)**