

Research and Development for  
Space Data System Standards

|  |
| --- |
| Intergovernmental certification authority |

Proposed Draft recommended practice

CCSDS 000.0-W-1

DRAFT ORANGE BOOK

May 2024

AUTHORITY

|  |  |  |  |
| --- | --- | --- | --- |
|  | | | |
|  | Issue: | Proposed Draft Recommended Practice |  |
|  | Date: | May 2024 |  |
|  | Location: | Not Applicable |  |
|  | | | |

**(WHEN THIS EXPERIMENTAL SPECIFICATION IS FINALIZED, IT WILL CONTAIN THE FOLLOWING STATEMENT OF AUTHORITY:)**

This document has been approved for publication by the Consultative Committee for Space Data Systems (CCSDS). The procedure for review and authorization of CCSDS documents is detailed in *Organization and Processes for the Consultative Committee for Space Data Systems* (CCSDS A02.1-Y-4).

This document is published and maintained by:

CCSDS Secretariat

National Aeronautics and Space Administration

Washington, DC, USA

Email: secretariat@mailman.ccsds.org

FOREWORD

INTERGOVERNMENTAL CERTIFICATION AUTHORITY will harmonize the credentialing process for unclassified interactions between space agencies and spacecraft.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CCSDS shall not be held responsible for identifying any or all such patent rights.

Through the process of normal evolution, it is expected that expansion, deletion, or modification of this document may occur. This document is therefore subject to CCSDS document management and change control procedures, which are defined in *Organization and Processes for the Consultative Committee for Space Data Systems* (CCSDS A02.1-Y-4). Current versions of CCSDS documents are maintained at the CCSDS Web site:

http://www.ccsds.org/

Questions relating to the contents or status of this document should be addressed to the CCSDS Secretariat at the address indicated on page i.

At time of publication, the active Member and Observer Agencies of the CCSDS were:

Member Agencies

* Agenzia Spaziale Italiana (ASI)/Italy.
* Canadian Space Agency (CSA)/Canada.
* Centre National d’Etudes Spatiales (CNES)/France.
* China National Space Administration (CNSA)/People’s Republic of China.
* Deutsches Zentrum für Luft- und Raumfahrt (DLR)/Germany.
* European Space Agency (ESA)/Europe.
* Federal Space Agency (FSA)/Russian Federation.
* Instituto Nacional de Pesquisas Espaciais (INPE)/Brazil.
* Japan Aerospace Exploration Agency (JAXA)/Japan.
* National Aeronautics and Space Administration (NASA)/USA.
* UK Space Agency/United Kingdom.

Observer Agencies

* Austrian Space Agency (ASA)/Austria.
* Belgian Science Policy Office (BELSPO)/Belgium.
* Central Research Institute of Machine Building (TsNIIMash)/Russian Federation.
* China Satellite Launch and Tracking Control General, Beijing Institute of Tracking and Telecommunications Technology (CLTC/BITTT)/China.
* Chinese Academy of Sciences (CAS)/China.
* China Academy of Space Technology (CAST)/China.
* Commonwealth Scientific and Industrial Research Organization (CSIRO)/Australia.
* Danish National Space Center (DNSC)/Denmark.
* Departamento de Ciência e Tecnologia Aeroespacial (DCTA)/Brazil.
* Electronics and Telecommunications Research Institute (ETRI)/Korea.
* European Organization for the Exploitation of Meteorological Satellites (EUMETSAT)/Europe.
* European Telecommunications Satellite Organization (EUTELSAT)/Europe.
* Geo-Informatics and Space Technology Development Agency (GISTDA)/Thailand.
* Hellenic National Space Committee (HNSC)/Greece.
* Hellenic Space Agency (HSA)/Greece.
* Indian Space Research Organization (ISRO)/India.
* Institute of Space Research (IKI)/Russian Federation.
* Korea Aerospace Research Institute (KARI)/Korea.
* Ministry of Communications (MOC)/Israel.
* Mohammed Bin Rashid Space Centre (MBRSC)/United Arab Emirates.
* National Institute of Information and Communications Technology (NICT)/Japan.
* National Oceanic and Atmospheric Administration (NOAA)/USA.
* National Space Agency of the Republic of Kazakhstan (NSARK)/Kazakhstan.
* National Space Organization (NSPO)/Chinese Taipei.
* Naval Center for Space Technology (NCST)/USA.
* Netherlands Space Office (NSO)/The Netherlands.
* Research Institute for Particle & Nuclear Physics (KFKI)/Hungary.
* Scientific and Technological Research Council of Turkey (TUBITAK)/Turkey.
* South African National Space Agency (SANSA)/Republic of South Africa.
* Space and Upper Atmosphere Research Commission (SUPARCO)/Pakistan.
* Swedish Space Corporation (SSC)/Sweden.
* Swiss Space Office (SSO)/Switzerland.
* United States Geological Survey (USGS)/USA.

PREFACE

This document is a CCSDS Experimental Specification. Its experimental status indicates that it is part of a research or development effort based on prospective requirements and, as such, it is not considered a Standards Track document. Experimental specifications are intended to demonstrate technical feasibility in anticipation of future requirements that have not yet emerged. Experimental work may be rapidly transferred onto the Standards Track in the future.

DOCUMENT CONTROL

|  |  |  |  |
| --- | --- | --- | --- |
| **Document** | **Title and Issue** | **Date** | **Status** |
| CCSDS 000.0-W-1 | Intergovernmental Certification Authority, Proposed Draft Recommended Practice, Issue 1 | May 2024 | Current proposed draft |

CONTENTS

Section Page

[1 INTRODUCTION 1-7](#_Toc157408986)

[1.1 Structure of this document 1-7](#_Toc157408987)

[1.2 Purpose of the document 1-7](#_Toc157408988)

[1.3 SCOPE OF THE DOCUMENT 1-8](#_Toc157408989)

[1.4 key words and definitions 1-9](#_Toc157408990)

[1.5 References 1-11](#_Toc157408991)

[2 INTERGOVERNMENTAL CREDENTIAL AUTHORITY 2-13](#_Toc157408992)

[2.1 Private key encryption and its relation to a CA 2-13](#_Toc157408993)

[2.2 IGCA CONCEPT 2-14](#_Toc157408994)

[2.3 IGCA DESCRIPTION 2-15](#_Toc157408995)

[2.4 GENERAL CONSTRAINTS 2-17](#_Toc157408996)

[2.5 Post-Quantum encryption considerations 2-17](#_Toc157408997)

[3 Requirements 3-18](#_Toc157408998)

[3.1 policy requirements 3-18](#_Toc157408999)

[3.2 QUALITY REQUIREMENTS 3-20](#_Toc157409000)

[3.3 TECHNICAL VETTING REQUIREMENTS FOR ISSUING CAs 3-22](#_Toc157409001)

[3.4 OPERATIONAL VERIFICATION 3-23](#_Toc157409002)

[3.5 DOCUMENTATION 3-23](#_Toc157409003)

[ANNEX A DEFINITION OF ACRONYMS (INFORMATIVE) A-1](#_Toc165454207)

[ANNEX B IMPLEMENTATION CONFORMANCE STATEMENT PROFORMA (NORMATIVE) B-1](#_Toc165454208)

[ANNEX C SECURITY, SANA, AND PATENT CONSIDERATIONS (Informative) C-1](#_Toc165454209)

[ANNEX D Possible implementation EXAMPLE (Informative) D-4](#_Toc165454210)

Figures

[Figure 2‑1. Asymmetric key use in relation to a Certificate Authority. 2-13](#_Toc157408769)

[Figure 2‑2. IGCA operations enable the security interconnection services. 2-14](#_Toc157408770)

[Figure 2‑3. Illustration of the CA functions and their operational use. 2-16](#_Toc157408771)

# INTRODUCTION

Certificate Authorities (CA) are trusted third-party entities that create, issue, store, and sign digital certificates. These digital certificates are afforded both integrity and authentication by virtue of the CA digital signature on the certificate. As a result, the authentication and integrity of the information contained in the certificate is assured as long as the CA, and the root certificates they generate, are secure and uncompromised.

A digital certificate binds an identity to a public key using a digital signature. A digital certificate establishes the identity of the owner of the certificate and is used to distribute the owner’s public key.

When a certificate is signed by a trusted Certificate Authority (CA), the public key in the certificate can be used to establish secure communications with another entity or to validate information that has been digitally signed. Certificates contain an owner’s identity (e.g., individual’s name, hostname, organization) and a public key. Certificates enable secure connectivity between entities, providing confidentiality, authenticity, and integrity.

When secure communication is required, an entity uses either a cached copy of another entity’s certificate or attempts to obtain a certificate for that entity from a Certificate Authority. The communicating entities use the public keys contained in the certificates to communicate with each other using asymmetric cryptographic methods or to generate a symmetric key via a key agreement protocol, ensuring the authentication, integrity, and confidentiality of the exchanged information.

From a CCSDS space mission perspective, substantial coordination is required to establish secure connections between Agencies, or between Agencies and their commercial partners, and specified endpoints for cross support and interoperability. An *Intergovernmental Certification Authority* (IGCA) enables coordination, connection, and provides secure validation processes between entities in space or on the ground. Certificates may be used to provide secure identities for: systems, software, spacecraft, instruments, ground stations, relay spacecraft, people, and other entities that may participate in space systems.

## Structure of this document

This section describes the structure of this document. Section 1 is the introduction, including the purpose and scope of the document. Section 2 describes the IGCA and its intended operations. Section 3 provides the specifications for the creation and operation of the IGCA. The Annexes provide the Definition of Acronyms; Implementation Conformance Statement; and Security, SANA, and Patent Considerations.

## Purpose of the document

This document specifies the requirements for an Intergovernmental Certification Authority (IGCA). This document establishes the requirements for governing, administrating, and operating an IGCA.

The requirements described in this document will provide the structure of management and governance for the use of the digital credentials documented in CCSDS 357.0-B-1, CCSDS Authentication Credentials [3], which are the basis for security services authentication, confidentiality, integrity, and nonrepudiation.

This document also specifies requirements for the development of a CCSDS Public Key Infrastructure (PKI). It defines the terms and conditions under which the IGCA and affiliated Certification Authorities (CAs) operate. It defines how the IGCA can serve as a CA bridge between member space agencies and for CAs to issue digitally signed certificates that can be used to secure access and communications paths.

## SCOPE OF THE DOCUMENT

This document describes the overall business, legal, and technical infrastructure of the Intergovernmental Certification Authority. More specifically, this document will specify requirements for the following:

* Appropriate applications for, and the assurance levels associated with CCSDS-issued digital certificates,
* Obligations of Certification Authorities,
* Requirements for audit and related security reviews,
* Methods to confirm the identity of certificate applicants,
* Operational procedures for certificate lifecycle services:
  + certificate application,
  + issuance,
  + acceptance,
  + revocation,
  + expiration,
  + storage, and
  + renewal.
* Operational security procedures for audit logging, records retention, and disaster recovery,
* Physical, personnel, key management, and logical security, and
* Certificate Profile and Certificate Revocation List contents.

## key words and definitions

### Normative text

The following conventions apply for the normative specifications in this Recommended Standard:

1. the words ‘shall’ and ‘must’ imply a binding and verifiable specification;
2. the word ‘should’ implies an optional, but desirable, specification;
3. the word ‘may’ implies an optional specification;
4. the words ‘is’, ‘are’, and ‘will’ imply statements of fact.

NOTE: These conventions do not imply constraints on diction in text that is clearly informative in nature.

### definitions

**These definitions are unique to this Intergovernmental Certification Authority recommendation and do not appear in the CCSDS Information Security Glossary [5]. Some definitions are sourced from the CA/Browser Forum [1]**.

**Applicant**: The natural person or Legal Entity that applies for (or seeks renewal of) a Certificate. Once the Certificate is issued, the Applicant is referred to as the Subscriber. For Certificates issued to devices, the Applicant is the entity that controls or operates the device named in the Certificate, even if the device is sending the actual certificate request.

**Audit Report**: A report from a Qualified Auditor stating the Qualified Auditor’s opinion on whether an entity’s processes and controls comply with the mandatory provisions of these Requirements.

**Bridge**: An agency or corporation whose CA is cross certified, allowing that agency or corporation issuing CA to issue valid and interoperable certificates.

**Certification Practice Statement (CPS)**: One of several documents forming the governance framework under which Certificates are created, issued, managed, and used.

**Control**: “Control” (and its correlative meanings, “controlled by” and “under common control with”) means possession, directly or indirectly, of the power to: (1) direct the management, personnel, finances, or plans of such entity; (2) control the election of a majority of the directors; or (3) vote that portion of voting shares required for “control” under the law of the entity’s Jurisdiction of Incorporation or Registration but in no case less than 10 percent.

**Cross Certificate**: A certificate that is used to establish a trust relationship between two Root CAs.

**Expiry Date**: The “Not After” date in a Certificate that defines the end of a Certificate’s validity period.

**Government Entity**: A government-operated legal entity, agency, department, ministry, branch, or similar element of the government of a country, or political subdivision within such country (such as a state, province, city, county, etc.).

**Legal Entity**: An association, corporation, partnership, proprietorship, trust, government entity, or other entity with legal standing in a country’s legal system.

**Nation State:** A bounded sovereign polity.

**Object Identifier (OID)**: A unique alphanumeric or numeric identifier registered under the International Organization for Standardization’s (ISO’s) applicable standard for a specific object or object class.

**Qualified Auditor**: A Qualified Auditor means a natural person, Legal Entity, or group of natural persons or Legal Entities that collectively possesses the following qualifications and skills:

* Independence from the subject of the audit
* The ability to conduct an audit that addresses the criteria specified in an Eligible Audit Scheme
* Employs individuals who have proficiency in examining PKI technology, information security tools and techniques, information technology and security auditing, and the third-party attestation function
* (For audits conducted in accordance with any one of the European Telecommunications Standards Institute (ETSI) standards) Accredited in accordance with ISO 17065 applying the requirements specified in ETSI EN 319 403
* (For audits conducted in accordance with the WebTrust® standard) Licensed by WebTrust®
* Bound by law, government regulation, or professional code of ethics
* Except in the case of an Internal Government Auditing Agency, maintains Professional Liability/Errors & Omissions insurance

**Registration Authority (RA)**: An entity that is responsible for one or more of the following functions: the identification and authentication of certificate applicants, the approval or rejection of certificate applications, initiating certificate revocations or suspensions under certain circumstances, processing subscriber requests to revoke or suspend their certificates, and approving or rejecting requests by subscribers to renew or rekey their certificates. RAs, however, do not sign or issue certificates [13].

**Relying Party**: Any natural person or Legal Entity that relies on a Valid Certificate. An Application Software Supplier is not considered a Relying Party when software distributed by such Supplier merely displays information relating to a Certificate.

**Root CA**: The top-level Certification Authority whose Root Certificate is distributed by Application Software Suppliers and that issues Subordinate CA Certificates.

**Root Certificate**: The self-signed Certificate issued by the Root CA to identify itself and to facilitate verification of Certificates issued to its Subordinate CAs.

**Subject**: The natural person, device, system, unit, or Legal Entity identified in a Certificate as the Subject. The Subject is either the Subscriber or a device under the control and operation of the Subscriber.

**Subject Identity Information**: Information that identifies the Certificate Subject in the X.509 certificate. Subject Identity Information does not include a domain name listed in the subjectAltName extension or the Subject commonName field.

**Subordinate CA**: A Certification Authority whose Certificate is signed by the Root CA or another Subordinate CA.

**Subscriber**: A natural person or Legal Entity to whom a Certificate is issued and who is legally bound by a Subscriber Agreement or Terms of Use.

**Subscriber Agreement**: An agreement between the CA and the Applicant/Subscriber that specifies the rights and responsibilities of the parties.

**Terms of Use**: Provisions regarding the safekeeping and acceptable uses of a Certificate issued in accordance with these Requirements when the Applicant/Subscriber is an Affiliate of the CA or is the CA.

**Valid Certificate**: A Certificate that passes the validation procedure specified in RFC 5280 [15].

**Validity Period**: The period of time measured from the date when the Certificate is issued until the Expiry Date.

## References

The following publications contain provisions that, through reference in this text, constitute provisions of this Experimental Specification. At the time of publication, the editions indicated were valid. All publications are subject to revision, and users of this Experimental Specification are encouraged to investigate the possibility of applying the most recent editions of the documents indicated here. The CCSDS Secretariat maintains a register of currently valid CCSDS publications.

[1] CA/Browser Forum, Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates BR-1.6.5. October 2018.

[2] Security Threats Against Space Missions Issue 2. Recommendation for Space Data System Standards (Green Book) CCSDS 350-1-G-2 Washington, D.C.: CCSDS, September 2015.

[3] Authentication Credentials, Recommendation for Space Data System Standards (Blue Book) CCSDS 357-0-B-1 Washington, D.C.: CCSDS, July 2019.

[4] WebTrust Principles and Criteria for Certification Authorities, 277 Wellington St. West Toronto, ON March 2019.

[5] Information Security Glossary of Terms Issue 2 Recommendation for Space Data System Standards (Magenta Book) CCSDS 350.8-M-2 Washington, D.C.: CCSDS, February 2020.

[6] International Federation of Accountants (IFAC), International Standard on Assurance Engagements (ISAE) 3000, 529 5th Avenue New York, New York, December 2015.

[7] International Organization for Standardization/International Electrotechnical Commission ISO/IEC 29115 Information technology Security techniques, Chemin de Blandonnet 8, 1214 Vernier, Geneva Switzerland. 2013.

[8] Cryptographic Algorithms Issue 2, Recommendation for Space Data System Standards (Blue Book) CCSDS 352-0-B-2 Washington, D.C CCSDS 352.0-B-2, August 2019.

[9] Internet Engineering Task Force (IETF) Automatic Certificate Management Environment (ACME) RFC 8555, Fremont, CA, March 2019.

[10] National Institute of Standards and Technology, Security Requirements for Cryptographic Modules NIST FIPS 140-3 Gaithersburg, MD, March 2019.

[11] CA/Browser Forum, Intellectual Property Rights Policy, July 2018.

[12] Creative Commons Attribution 4.0 International license, Creative Commons Corporation (“Creative Commons”), 211 Hope St PO Box 1866 Mountain View, CA, Current version.

[13] Internet Engineering Task Force (IETF) Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework RFC 3647, Fremont, CA, November 2003.

[14] IOAG Lunar Comm Architecture Report v1.3, January 2022.

[15] Internet Engineering Task Force (IETF) Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, RFC 5280, Fremont, CA, May 2008.

[16] NIST publication <https://csrc.nist.gov/CSRC/media/Presentations/Update-on-the-NIST-Post-Quantum-Cryptography-Proje/images-media/2_post-quantum_dmoody.pdf> 100 Bureau Drive Gaithersburg, MD 20899

[17] Recommended Standard CCSDS 352.0-B-2 Blue Book August Washington, D.C.: CCSDS, September 2015.

[18] PKCS #3: Diffie-Hellman Key-Agreement Standard. Revised ed. Bedford, Massachusetts: RSA Laboratories, November 1993.

[19] PKCS #1 v2.1: RSA Cryptography Standard. Bedford, Massachusetts: RSA Laboratories, June 2002.

[Only references required for the implementation of the specification are listed in the References subsection. (See [1] for additional information on this subsection.)]

# INTERGOVERNMENTAL CREDENTIAL AUTHORITY

The IGCA provides trust through standard security processes by providing authenticated information to enable the privacy of communication. The IGCA is a separate, authenticated and managed, entity that interoperates with existing National Space Agency Certificate Authorities (CAs) based on trust agreements between the agencies. This is implemented via the addition of an IGCA root certificate to their trust stores.

## Private key encryption and its relation to a CA

Asymmetric keys are the basis of operational security on the Internet. The IGCA leverages this functionality, along with the vetting processes already provided by commercial CAs, for a large-scale deployment to space assets. As will be described in subsequent sections, the CA performs a primary bridging function between Agencies and other organizations. Figure 2‑1 illustrates the CA relationship to asymmetric keys and how authentication and privacy between two parties is ensured.

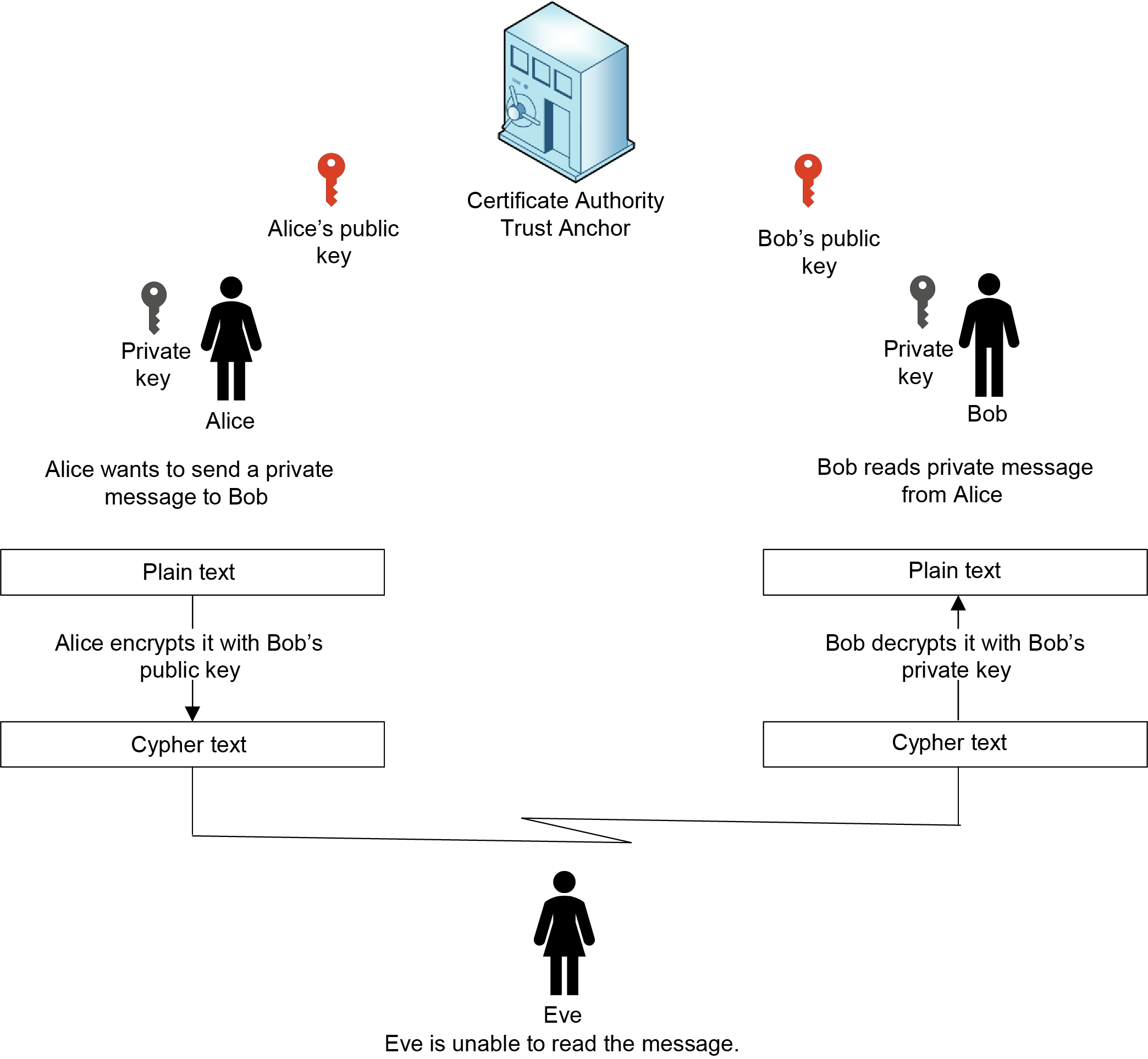


Figure 2‑1. Asymmetric key use in relation to a Certificate Authority.

## IGCA CONCEPT

This Recommended Practice specifies policy and specifies requirements for an integrated set of technologies, protocols, identity verification, management, and auditing requirements that are necessary for the IGCA and affiliated Certification Authorities (CAs) to issue and manage Trusted Certificates. The concept of operations depicted in Figure 2‑2 illustrates the IGCA’s use in a terrestrial environment.

The IGCA intends to use standard internet protocols created by Internet Engineering Task Force and standards developed by CCSDS to interact with subordinate CAs and nation state bridge CAs. The simplified concept of operation is shown without showing the built-in redundancies that are needed for fail-safe operations. The ICGA provides trust and PKI keys that can be used to facilitate the operation of CCSDS protocols such as Space Data Link Security (SDLS), DTN BPSec, or secured service interfaces. This document specifies the requirements for a Certification Practice Statement (CPS), which is used to govern the operation of CAs. The figure illustrates the functions and interactions facilitated by the IGCA. As a trust anchor it is the source of trusted certificates, and by way of contacts, vetting and review of security operations it can subsequently support cross-organization authentications in this way, the IGCA facilitates provisioning of identity services and therefore allowing a more efficient realization of security for protocols between different users and systems compared to the current treaty or single use agreements.

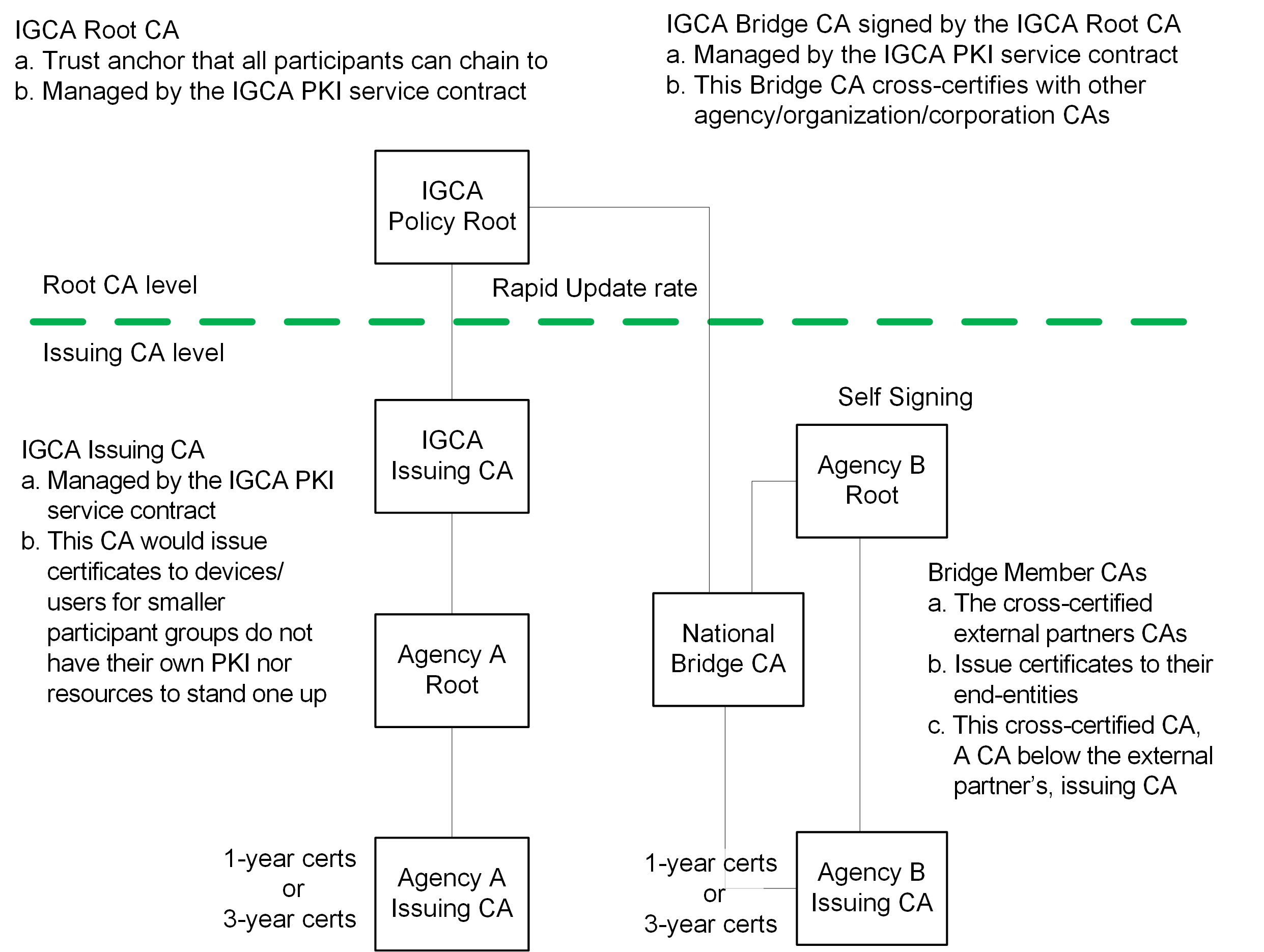


Figure 2‑2. IGCA operations enable the security interconnection services.

IGCA Certificates can be used for authentication, confidentiality, and nonrepudiation in a space public key infrastructure. The IGCA may be required to perform functions such as cross-signing to other root CAs or in conjunction with an international trust anchor (once one is developed), thereby increasing the reach of the IGCA certificates and users.

All certification paths start with a trust anchor/root CA. A trust anchor certificate:

* Is self-signed, that is, signed with the private key corresponding to the public key contained in the subject public key field of the certificate,
* Contains any needed parameters in the Subject Public Key Info field, where the digital signature algorithm used in the certificate requires the use of parameters,
* Contains few or no extensions, and
* Is transferred to the relying party in an authenticated manner. The signature on the trust anchor certificate cannot authenticate the certificate.

The trust anchor/root CA must be created and verified such that it can be implicitly trusted. As a trust anchor, the IGCA policy functions will verify each subscriber’s identity information. Authentication and identity verification are specified by the IGCA Certification Practice Statement (CPS). In general, the activities of the IGCA will include, but are not limited to:

* In-person identity verification,
* Verification and validation of identity documents,
* Enrollment and registration,
* Certificate issuance,
* Certificate usage,
* Certificate revocation, and
* Post-issuance updates and additions.

## IGCA DESCRIPTION

The IGCA is the central certification authority that provides the basis for a CCSDS-wide public key infrastructure to support universal international mission security without usurping an individual national certificate or key management controls. The IGCA will reduce the years of negotiation between nation states and corporations that currently takes place by establishing a centralized organization to vet and disseminate Public Keying materials. A Public Key Infrastructure will greatly increase the authentication capacity of the CCSDS community, enhancing trust in the interactions, but also allows greater granularity in applying security controls. The IGCA will foster an environment of trusted cooperation and interoperability. The IGCA is a centralized management authority to perform needed policy and maintenance activities.

IGCA functions include acting as the Root CA (trust anchor), Bridges with the National Bridge CA, Subordinate/Issuing CA, Policy CA, Registration CA, Local Mirror, and providing combined operational functions for off- world IGCA System use. See Figure 2‑3 for definitions of the independent functions performed by the IGCA.

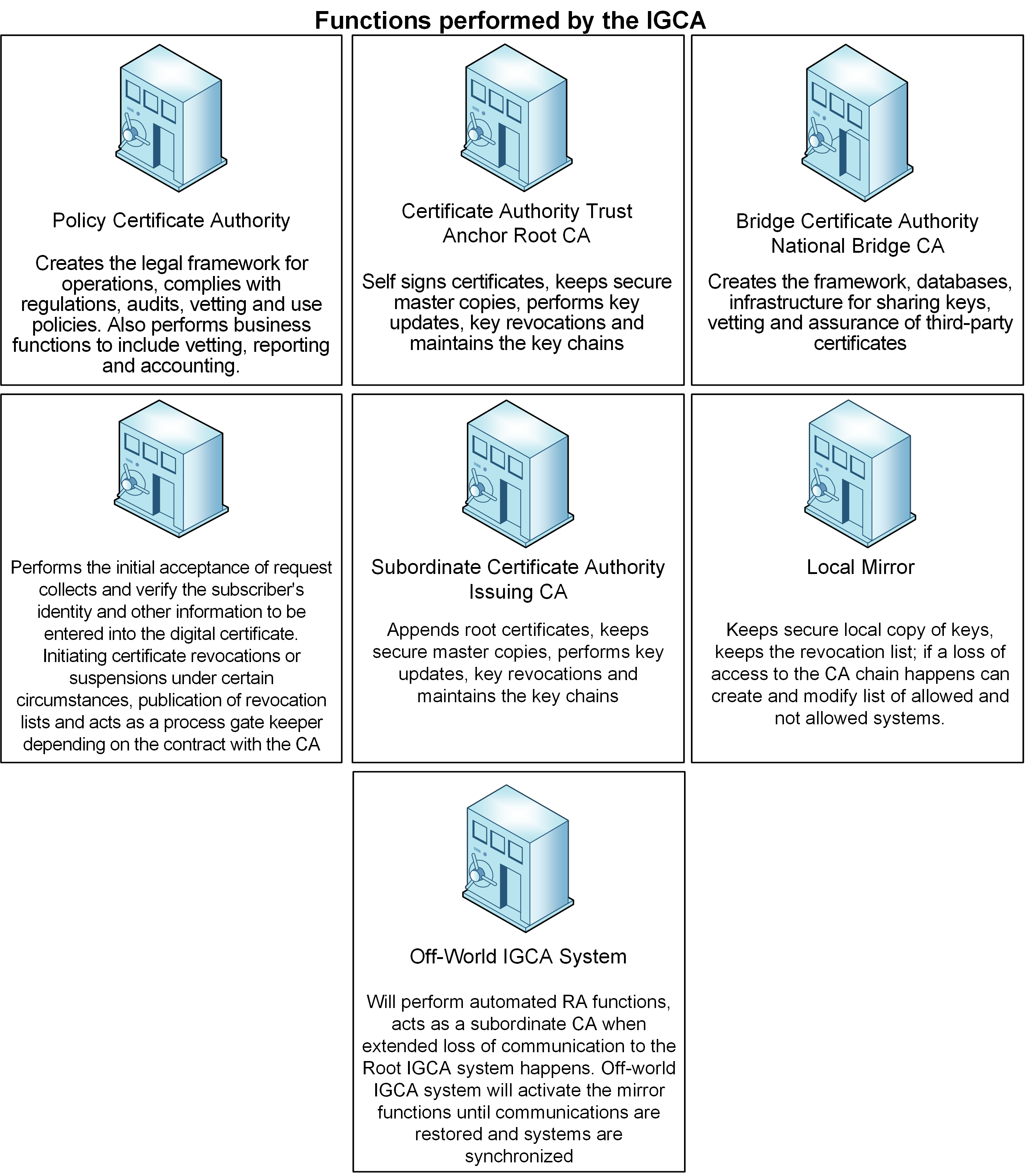


Figure 2‑3. Illustration of the CA functions and their operational use.

The root CA creates and signs certificates. To provide trust for public keys, the root CA cryptographically signs certificates, which provides assurance that the information contained in the certificate is valid, authentic, and bound to a subject.

## GENERAL CONSTRAINTS

Space communications may suffer from limited bandwidth and transmission delays. Space missions historically are relatively long-lived as compared with terrestrial systems and are not easily modified or upgraded after launch. Space is a uniquely harsh operating environment with radiation, thermal, shock, and vibrational effects. The overall mission, the processors, memory, and communications bandwidth must be taken into consideration with respect to the lifespan of the mission and potential cryptographic upgrades.

Space environmental constraints may affect the operation of the IGCA. Certificate updates and certificate revocations are two of the most critical operations to maintain security. Current terrestrial certificates are issued annually with a move towards shorter certificate validity periods to limit the attack window in the event of certificate compromise. Due to limited contact periods, low bandwidth links, limited memory, and limited processor capabilities in comparison to most terrestrial systems, update rates and processes may vary from what is the norm for terrestrial certificates.

## Post-Quantum encryption considerations

Quantum computers, when materialized, will allow exponential speed up of solving the mathematical problems used by typical asymmetric cryptography, resulting in recovering the keys even in a few hours; On the contrary, symmetric ciphers, like the Advanced Encryption Standard, used typically for encryption, or encrypted authentication, are less affected (using keys of 256 bit length is considered sufficient to mitigate the threat of quantum computers to symmetric cryptography).

Asymmetric cryptography is used for authentication, digital signatures, as well as key exchange and key authentication and digital signatures. Since PKI implementations heavily rely on asymmetric cryptography (e.g. for authentication, digital signatures of certificates), all current PKI solutions will be at risk when quantum computers materialize. Even if it will take several years until this happens (experts put it in the range of 10 to 30 years), the migration time (including the length time to design, develop, validate, qualify and deploy) of space systems, and their lifetime force us to consider the quantum threat to cryptography (and specifically to asymmetric cryptography algorithms such as RSA [16, 17, 19] and Diffie-Hellman [16, 17, 18]. As a result, the IGCA intends to remain cognizant of, and adoption of post-quantum-safe algorithms by CCSDS.

Post Quantum Cryptography (PQC) provides asymmetric cryptographic schemes which are quantum resistant. Several PQC algorithms have already been standardized by NIST, while more are expected to follow. However, PQC solutions typically require more processing power and memory, as well as the keys (public/private) and the signatures can become very lengthy, making multiple fragmentation inevitable. The standardization of quantum resistant PKI is still at an infancy, and more efforts, studies and testing are needed before a quantum resistant PKI solution is standardized.

During the future transition period, post-quantum algorithms will not be supported by all systems. Therefore, various migration considerations must be taken into account, including backwards compatibility to continue supporting existing implementations that will not yet have been updated to support the post-quantum algorithms.

# Requirements

In order to trust each other’s communications interagency communications will require the use of the trust anchor method to authenticate their communications. Legal statues were reviewed based on the information held and information that is to transit the communications networks and it was determined that it was not classified, and the highest classification is Sensitive but Unclassified/Controlled Unclassified Information. The following requirements are specific for this trust level.

NOTE: The term “The IGCA and affiliated CAs” means that the IGCA is the policy/root CA and the affiliated CAs are the CAs that issue certificates that are tied to the IGCA policy/root CA.

## policy requirements

This section provides the policy requirements for the IGCA and affiliated CAs.

### Each agency shall use an IGCA subordinate issuing CAs or cross-certified related issuing CAs.

### The IGCA and affiliated CAs shall maintain insider threat monitoring and a mitigation policy.

### The IGCA and affiliated CAs shall maintain a vulnerability management plan.

### The IGCA and affiliated CAs shall maintain a patch management plan.

### The IGCA and affiliated CAs shall maintain a continuity of operations plan.

### The IGCA and affiliated CAs shall have a privacy plan that applies to a participant’s activities.

NOTE: The Plan is governed by applicable laws or polices.

### The IGCA and affiliated CAs shall have the capability of being audited manually and automatically.

NOTE: The IGCA is auditable by CCSDS member Agencies.

NOTE: The IGCA governing policies are agreed upon by consensus in CCSDS by the member Agencies.

### The IGCA and affiliated CAs shall follow the International Standard on Assurance Engagements (ISAE) 3000 for audit reporting [6].

### The IGCA and affiliated CAs shall follow the WebTrust® Principles and Criteria for Certification Authorities for audit exclusions [4].

### The IGCA shall allow each agency to apply for certificates.

### The IGCA may cross-certify with root Cas of nation states or corporative CAs.

NOTE: The arrangement between the IGCA and CAs is based on the acceptance of the others security procedures and practices.

### The IGCA and affiliated CAs shall have an approved enhanced vetting process and provide a level of assurance equal to or greater than level of assurance 3 in ISO/IEC 29115:2013 [7].

### The IGCA and affiliated CAs shall maintain an agreed Certificate Management process.

NOTE: This should include items such as physical security, environmental controls, system integrity controls, configuration management, integrity management of trusted code, malware detection/prevention, network security and firewall management, port restrictions, address filtering, user management, trusted roles, education awareness, training, logical access controls, activity logging, inactivity time-outs, and individual accountability. In addition, the certificate management and certificate monitoring are sufficient for preventing unmanaged certificate expiration.

### The IGCA and affiliated CAs shall maintain an agreed security program and conduct annual risk assessments.

NOTE: The risk assessment includes items such as identifying foreseeable internal and external threats that could result in an unauthorized access, disclosure, and misuse alteration or destruction of a certificate data or certificate management processes. It may also include a process to assess the likelihood and potential damage of threats and assessing the sufficiency of the certificate data and the certificate management processes, systems, technologies, and arrangements to counter threats.

### The IGCA and affiliated CAs shall create and maintain security log files.

NOTE: The security logs are used to confirm that all system actions can be attributed to an authenticated identity of a person or an automated process.

### The IGCA and affiliated CAs shall use Domain validation.

NOTE: Domain validation ensures against Man in the Middle (MitM) attacks. DNS validation prevents certificate mis-issuance due to DNS hijacking.

## QUALITY REQUIREMENTS

This section provides the IGCA quality requirements.

### IGCA Root-CA Lifetime. The Root-CA shall replace its certificate according to its security policy.

NOTE: IGCA Root-CAs are updated based on threat and vulnerability assessments, which are then put into the security policy.

### IGCA and affiliated CAs shall maintain 99.982% up time.

NOTE: 99.982% availability/reachability is a loss of operations of no more than 1.6 hours per year. Distributed Denial of Service (DDoS) attacks against the IGCA are included in the threat scenarios and should be considered in the performance parameters of the Service-Level Agreement.

NOTE: The availability requirement is bound to the ability to issue new certificates and validate existing certificates.

### The IGCA and affiliated CAs shall have reviewed and agreed Operational Protection Policies.

NOTE: The policies are intended to ensure that there are checks and balances to defend against attempts to insert misinformation at any point in the certificate issuing processes.

### The IGCA and affiliated CAs shall have two or more mirror sites.

NOTE: Mirrors are identical replicas of the IGCA for load balancing, speed, availability, and back-up purposes.

### The IGCA and affiliated CAs shall use certificate revocation lists (CRLs).

NOTE: The IGCA and affiliated CAs may use additional certificate revocation mechanisms.

### The IGCA and affiliated CAs should implement Automatic Certificate Management Environment (ACME) [9].

### The IGCA and affiliated CAs’ mirrors shall be geographically and logically diverse.

### The IGCA and affiliated CAs’ mirrors should comprise different technical solutions.

NOTE: The systems should be totally independent solutions (e.g., different data centers, technical solutions, software, hardware, etc.) for increased reliability of the IGCA architecture.

### The IGCA and affiliated CAs’ mirrors shall maintain the same configuration between all addressable instances.

### The IGCA and affiliated CAs shall maintain configuration control documentation with description and revisions.

### The IGCA and affiliated CAs shall use the CCSDS’s certification structure as outlined in Reference [3].

NOTE: Reference 3 provides the specification for the structure of the credentials to be used for authentication by CCSDS-compliant missions and ground systems.

### The IGCA and affiliated CAs shall issue a certificate revocation within 24 hours of detection of a compromised credential.

### IGCA and affiliated CAs shall issue End-Entity Certificate lifetimes of two lengths, 1 year or 3 years in duration.

NOTE: Shorter lifetimes are desirable for enhanced security. However, for space, the certificate exchange process is over a limited bandwidth channel and may require several transmissions to validate proper installation. It is envisioned that near-Earth missions would use 1-year certificates and deep space missions would use 3-year certificates. Nodes supporting both missions could have both types of certificates.

### IGCA and affiliated CAs’ End-Entity Certificate shall be issued 30 days prior to the end of the certificate lifetime.

### The IGCA and affiliated CAs may allow the use of overlapping End-Entity certificates for up to 30 days.

NOTE: Transmission delays and intermittent contact may require both an old and current certificate to be operational during the same time, because of the requirement to be able to command updates and key changes.

### The IGCA and affiliated CAs shall use the CCSDS’ Authentication Credentials IPsec profile, CCSDS 357.0-B-1, Blue Book [3].

### The IGCA and affiliated CAs shall use 256-bit keys and RSA Digital Signatures of at least 7680 bits as specified in CCSDS Cryptographic Algorithms, CCSDS 352.0-B-2 Blue Book [8].

### The IGCA and affiliated CAs must support key protection mechanisms as required in FIPS 140-3 or equivalent standards to protect the CA keys [10].

NOTE: FIPS 140-3 Cryptographic Module Validation Program (CMVP) utilizes the ISO/IEC 19790: 2012 requirements standard and ISO/IEC 24759: 2017 derived test methods. This requirement is to prevent or recognize compromise of cryptographic modules and cryptographic keys. Example of tamper detection includes tamper-evident coatings or seals that must be broken to attain physical access to the plaintext cryptographic keys and critical security parameters within the module, or pick-resistant locks on covers or doors to protect against unauthorized physical access.

### The IGCA and affiliated CAs shall have physical security mechanisms to provide a high probability of detection of attempts at physical access or modification of the cryptographic module.

NOTE: The physical security mechanisms may include the use of anti-tamper enclosures and tamper-detection/response circuitry that zeroes all plaintext CSPs when the removable covers/doors of the cryptographic module are opened.

### The IGCA and affiliated CAs shall use the Space Assigned Numbers Authority (SANA) registry for Organizations, Contacts, Roles, Contents and Space Link Identifiers.

NOTE: IDs are located in the registries, and information structure/formats and Object Identifier numbers are specified.

### Registration Authorities (RA) shall be subordinate to the IGCA root CA or an Agency Root CA [13].

NOTE: It is envisioned that at remote locations, i.e., Mars, an RA will be used to provide the services for the CA.

### Registration Authority may perform the functions of its master CA except issuing or signing certificates.

NOTE: It is envisioned that at remote locations, i.e., Mars, an RA will be used to provide the services for the CA.

## TECHNICAL VETTING REQUIREMENTS FOR ISSUING CAs

This section provides the IGCA technical vetting requirements.

### IGCA-affiliated CAs shall validate the identity of applicants.

NOTE: The identity source documents shall be bound to that applicant and shall be neither expired nor cancelled. If the two identity source documents bear different names, evidence of a formal name change shall be provided.

### The IGCA-affiliated CAs shall use one of the following primary identity source documents in the identity identification process:

* Government issued proof of identity valid in the CA owner’s country
* Legally allowed proof of identity accepted by government institutions in the CA owner’s country

### The IGCA-affiliated CAs shall use a second source document that must be different than the primary identity source document.

NOTE: The requirements for proof of identity shall apply to citizens of foreign countries who are working within the resident country.

## OPERATIONAL VERIFICATION

This section provides the Operational IGCA verification requirements.

### IGCA, affiliated CAs, and cross-certified CAs shall perform interoperability testing.

### IGCA and affiliated CAs shall test that all the certificates issued are compliant with Reference [3].

### The affiliated CAs shall confirm the Applicant's control of their domain address.

## DOCUMENTATION

This section provides the IGCA documentation requirements.

### The ICGA and affiliated CAs’ documentation shall be auditable by CCSDS.

NOTE: Privacy of individuals is governed by applicable laws.

NOTE: Documentation includes policies, procedures and compliance records.

1. DEFINITION OF ACRONYMS  
     
   (INFORMATIVE)

**CA** Certification Authority

**CCSDS** Consultative Committee for Space Data Systems

**CP** Certificate Policy

**CPS** Certification Practice Statement

**CRL** Certificate Revocation List

**ETSI** European Telecommunications Standards Institute

**IGCA** Intergovernmental Certification Authority

**ISO** International Organization for Standardization

**OID** Object Identifier

**PKI** Public Key Infrastructure

**RA** Registration Authority

**RFC** Request for Comments

1. IMPLEMENTATION CONFORMANCE STATEMENT PROFORMA  
     
   (NORMATIVE)
   1. Introduction
      1. OVERVIEW

This annex provides the Implementation Conformance Statement (ICS) Requirements List (RL) for an implementation of Intergovernmental Certification Authority (IGCA). The ICS for an implementation is generated by completing the RL in accordance with the instructions below. An implementation claiming conformance must satisfy the mandatory requirements referenced in the RL.

* + 1. abbreviations and conventions

CRL distribution point: A directory entry or other distribution source for Certificate Revocation Lists (CRLs). A CRL distributed through a CRL distribution point may contain revocation entries for only a subset of the full set of certificates issued by one CA or may contain revocation entries for multiple CAs. It is a managed parameter within the X.509 credential.

* + 1. conformance

The Conformance Requirements List consists of information in tabular form. The status of features is indicated using the abbreviations and conventions described below.

Item Column

The item column contains sequential numbers for items in the table.

Feature Column

The feature column contains a brief descriptive name for a feature. It implicitly means “Is this feature supported by the implementation?”

Status Column

The status column uses the following notations:

* M mandatory
* O optional
* C conditional
* X prohibited
* I out of scope
* N/A not applicable

Support Column Symbols

The support column is to be used by the implementer to state whether a feature is supported by entering Y, N, or N/A, indicating:

* Y Yes, supported by the implementation
* N No, not supported by the implementation
* N/A Not applicable

The support column should also be used, when appropriate, to enter values supported for a given capability.

* + 1. INSTRUCTIONS FOR COMPLETING THE REQUIREMENTS LIST

An implementer shows the extent of compliance to the Recommended Standard by completing the RL; that is, the state of compliance with all mandatory requirements and the options supported are shown. The resulting completed RL is called an ICS. The implementer shall complete the RL by entering appropriate responses in the “support” or “values supported” column, using the notation described in A1.3. If a conditional requirement is inapplicable, N/A should be used. If a mandatory requirement is not satisfied, exception information must be supplied by entering a reference X*i*, where *i* is a unique identifier, to an accompanying rationale for the noncompliance.

* 1. ICS PROFORMA FOR CCSDS
     1. GENERAL INFORMATION
        1. Identification of ICS

Date of Statement (DD/MM/YY)

ICS serial number

System Conformance statement cross-reference

* + - 1. Identification of Implementation Under Test

Implementation Name

Implementation Version

Special Configuration

Other Information

* + - 1. Identification of Supplier

Supplier

Contact Point for Queries

Implementation Name(s) and Versions

Other information necessary for full identification, e.g., name(s) and version(s) for machines and/or operating systems

System Name(s)

* + - 1. Identification of Specification

Have any exceptions been required?

NOTE: A YES answer means that the implementation does not conform to the Recommended Standard. Non-supported mandatory capabilities are to be identified in the ICS, with an explanation of why the implementation is nonconforming.

Yes [ ] No [ ]

* + 1. Requirements list

| **Feature** | **Reference** |
| --- | --- |
| Each agency shall use an IGCA subordinate issuing CAs or cross-certified related issuing CAs. | 3.1.1 |
| The IGCA and affiliated CAs shall maintain insider threat monitoring and a mitigation policy. | 3.1.2 |
| The IGCA and affiliated CAs shall maintain a vulnerability management plan. | 3.1.3 |
| The IGCA and affiliated CAs shall maintain a patch management plan. | 3.1.4 |
| The IGCA and affiliated CAs shall maintain a continuity of operations plan. | 3.1.5 |
| The IGCA and affiliated CAs shall have a privacy plan that applies to a participant’s activities. | 3.1.6 |
| The IGCA and affiliated CAs shall have the capability of being audited manually and automatically. | 3.1.7 |
| The IGCA and affiliated CAs shall follow the International Standard on Assurance Engagements (ISAE) 3000 for audit reporting [6]. | 3.1.8 |
| The IGCA and affiliated CAs shall follow the WebTrust® Principles and Criteria for Certification Authorities for audit exclusions [4]. | 3.1.9 |
| The IGCA shall allow each agency to apply for certificates. | 3.1.10 |
| The IGCA may cross-certify with root CAs of nation states or corporative CA. | 3.1.11 |
| The IGCA and affiliated CAs shall have an approved enhanced vetting process and provide a level of assurance equal to or greater than level of assurance 3 in ISO/IEC 29115:2013 [7]. | 3.1.12 |
| The IGCA and affiliated CAs shall maintain an agreed Certificate Management process. | 3.1.13 |
| The IGCA and affiliated CAs shall maintain an agreed security program and conduct an annual risk assessment.. | 3.1.14 |
| The IGCA and affiliated CAs shall create and maintain security log files. | 3.1.15 |
| The IGCA and affiliated CAs shall use Domain validation. | 3.1.16 |
| IGCA Root-CA Lifetime. The Root-CA shall replace its certificate according to its security policy. | 3.2.1 |
| The IGCA and affiliated CAs shall maintain 99.982% up time. | 3.2.2 |
| The IGCA and affiliated CAs shall have a reviewed and agreed Operational Protection Policies | 3.2.3 |
| The IGCA and affiliated CAs shall have two or more mirror sites. | 3.2.4 |
| The IGCA and affiliated CAs shall use certificate revocation lists (CRLs). | 3.2.5 |
| The IGCA and affiliated CAs should implement Automatic Certificate Management Environment (ACME). | 3.2.6 |
| The IGCA and affiliated CAs’ mirrors shall be geographically and logically diverse. | 3.2.7 |
| The IGCA and affiliated CAs’ mirrors should comprise different technical solutions. | 3.2.8 |
| The IGCA and affiliated CAs’ mirrors shall maintain the same configuration between all addressable instances. | 3.2.9 |
| IGCA and affiliated CAs shall maintain configuration control documentation with description and revisions. | 3.2.10 |
| The IGCA and affiliated CAs shall use the CCSDS certification structure as outlined in Reference [3]. | 3.2.11 |
| The IGCA and affiliated CAs shall issue a certificate revocation within 24 hours of detection of a compromised credential. | 3.2.12 |
| IGCA and affiliated CAs shall issue End-Entity Certificate lifetimes of two lengths, 1 year or 3 years in duration. | 3.2.13 |
| IGCA and affiliated CAs’ End-Entity Certificate shall be issued 30 days prior to the end of the certificate lifetime. | 3.2.14 |
| The IGCA and affiliated CAs may allow overlapping End-Entity use of certificates for up to 30 days. | 3.2.15 |
| The IGCA and affiliated CAs shall use the CCSDS Authentication Credentials IPsec profile, CCSDS 357.0-B-1, Blue Book. | 3.2.16 |
| The IGCA and affiliated CAs shall use 256-bit keys and RSA Digital Signatures of at least 7680 bits listed in the CCSDS Cryptographic Algorithms, CCSDS 352.0-B-2 Blue Book. | 3.2.17 |
| IGCA and affiliated CAs must support key protection mechanisms as required in FIPS 140-3 or equivalent standards to protect the CA keys. | 3.2.18 |
| IGCA and affiliated CAs shall have physical security mechanisms to provide a high probability of detection of attempts at physical access or modification of the cryptographic module. | 3.2.19 |
| The IGCA and affiliated CAs shall use the Space Assigned Numbers Authority (SANA) registry for Organizations, Contacts, Roles, Contents and Space Link Identifiers. | 3.2.20 |
| Registration Authorities (RA) shall be subordinate to the IGCA root CA or an Agency Root CA. | 3.2.21 |
| Registration Authority may perform the functions of its master CA except issuing or signing certificates. | 3.2.22 |
| IGCA-affiliated CAs shall validate the identity of applicants. | 3.3.1 |

|  |  |
| --- | --- |
| **Feature** | **Reference** |
| The IGCA-affiliated CAs shall use one of the following primary identity source documents in the identity identification process:   * Government-issued proof of identity, as valid in the CA owner’s country * Legally allowed proof of identity, as accepted by government institutions in the CA owner’s country | 3.3.2 |
| The IGCA-affiliated CAs shall use a second source document that must be different than the primary identity source document. | 3.3.3 |
| IGCA, affiliated CAs, and cross-certified CAs shall perform interoperability testing. | 3.4.1 |
| IGCA and affiliated CAs shall test that all of the certificates issued are compliant with Reference [3]. | 3.4.2 |
| The IGCA affiliated CAs shall confirm the Applicant’s control of their domain address. | 3.4.3 |
| The ICGA and affiliated CAs’ documentation shall be auditable by CCSDS. | 3.5.1 |

1. SECURITY, SANA, AND PATENT CONSIDERATIONS  
     
   (Informative)
   1. SECURITY CONSIDERATIONS
      1. Introduction

CCSDS will utilize the credential vetting process and mechanisms to validate the identities of users, applications, and devices.

CCSDS organizations employ technologies to convey identity and to attest to the claims of the trust models that are associated with those identities.

There are risks to CCSDS systems that utilize the IGCA credentials and the credential services; if an attacker gains control of the IGCA credential-management system, they can issue certificates. A compromised credential management process will result, requiring invalidating existing certificates and reissuance of all certificates.

A CCSDS IGCA credential-management program would result in higher levels of assurance of the credentials while ensuring interoperability and ease the deployments of systems that are pretested to integrate with the credential-management system. The system would provide unified administration, compliance, and auditing of the X.509 credentials.

* + 1. security concerns with respect to the ccsds document
       1. Overview

Standard credential service and certificate usage will provide CCSDS missions with a standard means of authentication of communicating entities.

* + - 1. Data Privacy

Certificates provide a means of identifying/authenticating entities to provide accurate access controls to ensure data privacy.

* + - 1. Data Integrity

Certificates provide a means whereby data integrity may be provided.

* + - 1. Authentication of Communicating Entities

Authentication is necessary to ensure that the exchange of information is between intended entities. This document specifies the vetting and certification process requirements for a trusted third party to provide CCSDS-compliant certificates for systems.

* + - 1. Control of Access to Resources

The identity contained in X.509 certificates is intended to be the basis for assigning access rights to individuals, groups, and system services.

* + - 1. Availability of Resources

This document deals with the functional requirements needed for a trusted third party to provide or exchange certificates to validate an entity and thus provide assurance that that entity is who or what they espouse to be.

* + - 1. Auditing of Resource Usage

The Certification Authority (CA) that generates CCSDS X.509 certificates must be trusted and thus must be auditable by all concerned parties to place trust in the credentials issued. The trust in the certificates and the system is frequently the basis for establishing accountability to specific individuals, for actions they have taken on a system. Nonrepudiation of user actions cannot be assured if credentials cannot be assured.

* + 1. POTENTIAL THREATS AND ATTACK SCENARIOS

The CA that generates the certificate and the authenticity of its CCSDS X.509 certificate is dependent upon the digital signature of the CA attesting to the authentication of the credential. If the digital signature algorithm used by the CA is of insufficient cryptographic strength, a credential may be spoofed.

Security Threats Against Space Missions (CCSDS 350.1–G–2) [2] is a CCSDS Informational Report that provides an overview of potential threats against various categories of civilian space missions and provides illustrative security threat data for mission planners. This document should be reviewed.

The IGCA provides vetting, keys, certificate management and distribution providing mechanisms for authentication, privacy and non-repudiation.

* + 1. CONSEQUENCES OF NOT APPLYING SECURITY TO THE TECHNOLOGY

If authentication is not implemented, an attacker could inject false or unauthorized commands into a communications path to the spacecraft’s command chain, and potentially take over control of the spacecraft. This could result in the loss of a mission.

* 1. SANA CONSIDERATIONS

This document may require action from SANA.

* 1. PATENT CONSIDERATIONS

Information and processes referenced in this document are in the public domain or have public use licensing, and there are no known patents that apply to the recommendations in this document.

The CA/Browser Forum allows free use of their work based on the IP policy statement and Creative Commons license.

CA/Browser Forum, Intellectual Property Rights Policy, July 2018 [1]

Creative Commons Attribution 4.0 International license, Creative Commons Corporation (“Creative Commons”), 211 Hope St, PO Box 1866, Mountain View, CA Current version [12]

1. Possible implementation EXAMPLE   
     
   (Informative)
   1. Depection of a conceptual implamentation
      1. Interagency Operations Advisory Group’s Concept

Lunar Communications Architecture work is going and it needs a method of validating trust and disseminating certificates and other security functions. The IGCA has been proposed to fill this gap and the below graphic is an overview of how this may be implemented.

