

CISRI  
Collaborative Inter-governmental Scientific Research Institute



IEMO  
International Emergency Management Organization



BAID  
Bank for International Development



---

## CISRI-IEMO-BAID Certification Practice Statement

Date: 26/05/21

Version: v.1.0

---

Document ID: CRT-CPS\_1.0  
URL: <https://baid.international/CPS>  
Date: 26/05/21



**CISRI-IEMO Joint Secretariat**  
*Secrétariat Conjoint CISRI-OIAU*

<https://www.cisri.org>  
<https://www.iemo.int>  
<https://baid.international>



**CISRI**

Collaborative Inter-governmental Scientific Research Institute



**IEMO**

International Emergency Management Organization



**BAID**

Bank for International Development

# Table of Contents

Table of Contents.....	2	1.6 Document Name and Identification.....	23
Document History.....	4	1.7 PKI Participants.....	23
Acknowledgments.....	5	1.7.1 CISRI-IEMO-BAID Certification Authority.....	24
Links.....	5	1.7.2 Subscribers.....	25
		1.7.3 Relying Parties.....	25
<b><u>1. Introduction.....</u></b>	<b>6</b>	1.8 Certificate Use.....	26
1.1 Overview.....	8	1.8.1 Appropriate Certificate Usage.....	26
1.2 CISRI-IEMO-BAID Certificate types.....	11	1.8.2 Prohibited Certificate Usage.....	26
1.2.1 Issuing Certificates.....	11	1.8.3 Certificate Extensions.....	27
1.2.2 Authoritative Certificates.....	11	1.8.4 Critical Extensions.....	27
1.2.3 Acceptable Subscriber Names.....	12	1.9 Policy Administration.....	28
1.2.4 Pseudonyms.....	12	1.9.1 Scope.....	28
1.2.5 Registration Procedures.....	12	1.9.2 CISRI-IEMO-BAID Policy Management Authority.....	28
1.3 Issuer Certificates.....	13	1.9.3 Acceptance of Updated Versions of the CPS .....	29
1.3.1 General.....	13	1.9.4 Version Management and Denoting Changes.....	29
1.3.2 Certificate Request.....	13	1.10 Definitions and Acronyms.....	30
1.3.3 Content.....	14		
1.3.4 Information Submitted to Verify Ownership or Right to Use of the Domain Name.....	15	<b><u>2. Publication and Repository Responsibilities</u></b>	<b>31</b>
1.3.5 Issuing Procedure.....	15		
1.3.6 Limited Warranty.....	16	<b><u>3. Identification and Authentication</u></b>	<b>32</b>
1.3.7 Relevant CISRI-IEMO-BAID Documents.....	16	3.1 Initial Identity Validation.....	32
1.4 Authoritative Certificates.....	17	3.2 Subscriber Registration Process.....	32
1.4.1 General.....	17	3.2.1 Documents Used for Subscriber Registration .....	33
1.4.2 Certificate Request.....	17	3.2.2 Records for Subscriber Registration.....	33
1.4.3 Content.....	18	3.2.3 Identification and Authentication for Revocation Requests.....	34
1.4.4 Documents Submitted to Identify the Applicant.....	19		
1.4.5 Issuing Procedure.....	19	<b><u>4. Certificate Life-Cycle Operational Requirements</u></b>	<b>35</b>
1.4.6 Limited Warranty.....	20		
1.4.7 Relevant CISRI-IEMO-BAID Documents.....	20		
1.5 Certificate usages.....	21		



Document ID: CRT-CPS\_1.0  
URL: <https://baid.international/CPS>  
Date: 26/05/21

Certification Practice Statement  
Version v1.0

**CISRI-IEMO Joint Secretariat**  
*Secrétariat Conjoint CISRI-OIAU*

<https://www.cisri.org>  
<https://www.iemo.int>  
<https://baid.international>



4.1 Certificate Application Processing and Issuance.....	36	6. Certificate and CRL Profiles.....	55
4.2 Certificate Generation.....	36	6.1 Certificate Profile.....	55
4.3 Certificate Acceptance.....	37	6.2 CRL Profile.....	55
4.4 Key Pair and Certificate Usage.....	37	7. Compliance Audit And Other Assessment.....	56
4.4.1 Subscriber.....	38	8. Other Business and Legal Matters.....	57
4.4.2 Relying Party.....	41	8.1 Financial Responsibility.....	57
4.5 Certificate Renewal.....	42	8.2 Confidentiality of Business Information..	58
4.6 Certificate Revocation.....	43	8.2.1 Disclosure Conditions.....	59
4.7 Certificate Status Services.....	44	8.3 Privacy of Personal Information.....	59
4.8 End of Subscription.....	45	8.4 Intellectual Property Rights.....	60
4.9 Certificates Problem Reporting and Response Capability.....	45	8.5 Representations and Warranties.....	61
5. Management, Operational, And Physical Controls.....	46	8.5.1 CISRI-IEMO-BAID Repository and Web Site Conditions.....	61
5.1 Physical Security Controls.....	46	8.5.2 Information Incorporated by Reference into a Digital Certificate.....	63
5.2 Procedural Controls.....	47	8.5.3 Pointers to Incorporate by Reference....	64
5.3 Personnel Security Controls.....	48	8.6 Disclaimers of Warranties.....	64
5.3.1 Qualifications, Experience, Clearances..	48	8.6.1 Limitation for Other Warranties.....	64
5.3.2 Training Requirements and Procedures....	48	8.6.2 Exclusion of Certain Elements of Damages	64
5.3.3 Retraining Period and Retraining Procedures.....	48	8.7 Indemnities.....	65
5.3.4 Sanctions against Personnel.....	49	8.8 Term and Termination.....	67
5.3.5 Controls of Independent Contractors....	49	8.9 Individual Notices and Communications with Participants.....	67
5.3.6 Documentation for Initial Training and Retraining.....	49	8.10 Amendments.....	68
5.4 Audit Logging Procedures.....	49	8.11 Dispute Resolution Procedures.....	68
5.5 Records Archival.....	51	8.12 Governing Law.....	69
5.5.1 Types of Records.....	52	8.13 Compliance with Applicable Law.....	69
5.5.2 Retention Period.....	52	8.14 Miscellaneous Provisions.....	70
5.5.3 Protection of Archive.....	52	8.14.1 Survival.....	70
5.5.4 Archive Collection.....	53	8.14.2 Severability.....	70
5.5.5 Procedures to Obtain and Verify Archive Information.....	53	9. List of definitions.....	71
5.6 Compromise and Disaster Recovery.....	54	10. List of acronyms.....	76





**CISRI**

Collaborative Inter-governmental Scientific Research Institute



**IEMO**

International Emergency Management Organization



**BAID**

Bank for International Development

---

## Document History

Version	Release Date	Author	Description
V1.0	2021-05-26	Alessandro Gubitosi	Initial version, Rev.



Document ID: CRT-CPS\_1.0  
URL: <https://baid.international/CPS>  
Date: 26/05/21

Certification Practice Statement  
Version v1.0

**CISRI-IEMO Joint Secretariat**  
*Secrétariat Conjoint CISRI-OIAU*

<https://www.cisri.org>  
<https://www.iemo.int>  
<https://baid.international>



---

## Acknowledgments

This CISRI-IEMO-BAID CPS endorses in whole or in part the following industry standards:

- [RFC 3647](#): Internet X.509 Public Key Infrastructure - Certificate Policies and Certification Practices Framework (obsoletes RFC 2527)
- [RFC 2459](#): Internet X.509 Public Key Infrastructure - Certificate and CRL Profile
- [RFC 3279](#): Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and CRI Profile
- The [ISO 1-7799](#) standard on security and infrastructure

## Links

- RFC 3647: <https://datatracker.ietf.org/doc/html/rfc3647>
- RFC 2459: <https://datatracker.ietf.org/doc/html/rfc2459>
- RFC 3279: <https://datatracker.ietf.org/doc/html/rfc3279>
- The ISO 1-7799 standard: <https://www.enisa.europa.eu/topics/threat-risk-management/current-risk/laws-regulation/rm-ra-standards/iso-iec/standard-17799>





**CISRI**

Collaborative Inter-governmental Scientific Research Institute



**IEMO**

International Emergency Management Organization



**BAID**

Bank for International Development

---

## 1. Introduction

This Certification Practice Statement (CPS) of the CISRI-IEMO-BAID Joint Secretariat Certification Authority (hereinafter, CISRI-IEMO-BAID) applies to the services of the BAID - Bank for International Development that are associated with the issuance of and management of digital certificates.

This CPS can be found on the following repositories:

- <https://www.baid.international/CPS>
- <https://www.iemo.int/BAID/CPS>

This CPS may be updated from time to time, please keep track of the version revision.

This CPS addresses the technical, procedural personnel policies and practices of the CA in all services and during the complete life cycle of certificates as issued by BAID.

BAID - Bank for International Development is operated and owned by CISRI-IEMO Joint Secretariat with provide it the legal jurisdiction and personality as their subsidiary institution. Therefore what referred to BAID is simultaneously referred to CISRI and IEMO Joint Secretariat, and explicitly provided by its International Personality under Headquarters Agreement of 17/03/2014. All officers and personnel of CISRI-IEMO-BAID, in the performance of the present CPS are included on the above mentioned provisions, regardless to their nationality, rank or sex.



Document ID: CRT-CPS\_1.0  
URL: <https://baid.international/CPS>  
Date: 26/05/21

Certification Practice Statement  
Version v1.0

**CISRI-IEMO Joint Secretariat**  
*Secrétariat Conjoint CISRI-OIAU*

<https://www.cisri.org>  
<https://www.iemo.int>  
<https://baid.international>



Inquiries on this CISRI-IEMO-BAID CPS can be addressed to:

Organization name	CISRI-IEMO Joint Secretariat - Secrétariat Conjoint CISRI-OIAU
Registered office	Seat-Siège: 144 E-Nord Tévragh Zeina - Nouakchott - RIM
Head Office	
Legal Representative	Alessandro Gubitosi, as IEMO DIRECTOR of IT BAID COMPTROLLER, Financial Services
Telephone number	+2224486341
Companies Register Registration No	
Website	<a href="https://www.baid.international">https://www.baid.international</a>

This CPS is final and binding between CISRI-IEMO Joint Secretariat (operating and owning the BAID – Bank for International Development), an Organization under public law, with registered office at Seat-Siège: 144 E-Nord Tévragh Zeina - Nouakchott - Mauritanie, (Hereinafter referred to as "CISRI-IEMO-BAID")

and

the subscriber and/or relying parties, who use rely or attempt to rely upon certification services made available by the CISRI-IEMO-BAID.

For subscribers this CPS becomes effective and binding by accepting a subscriber agreement.

For relying parties this CPS becomes binding by merely addressing a certificate related request on a CISRI-IEMO-BAID certificate to a CISRI-IEMO Joint Secretariat directory.

The subscriber agreement forfeits the consent of the relying party with regard to accepting the conditions laid out in this CPS.





**CISRI**

Collaborative Inter-governmental Scientific Research Institute



**IEMO**

International Emergency Management Organization



**BAID**

Bank for International Development

## 1.1 Overview

This CPS applies to the specific domain of the CISRI-IEMO-BAID - Bank for International Development.

The purpose of this CPS is to present the CISRI-IEMO-BAID practices and procedures in managing certificates and to demonstrate compliance with requirements pertaining to the issuance of digital certificates according to CISRI-IEMO-BAID's own and industry requirements pursuant to the standards set out above.

The certificate type addressed in this CPS is the following:

### Issuer Certificate

Country	MR
State or Province Name	Seat-Siège: 144 E-Nord Tevragh Zeina - Nouakchott
Locality Name	Nouakchott - Mauritanie
Organization	CISRI-IEMO-BAID - Bank for International Development
Organization	CISRI-IEMO Joint Secretariat - Secrétariat Conjoint CISRI-OIAU
Organizational Unit Name	Financial Direction - Direction Financière
Common Name	CISRI-IEMO-BAID Authoritative Certification
Email Address	<a href="mailto:certs@baid.international">certs@baid.international</a>



Document ID: CRT-CPS\_1.0  
URL: <https://baid.international/CPS>  
Date: 26/05/21

Certification Practice Statement  
Version v1.0

**CISRI-IEMO Joint Secretariat**  
*Secrétariat Conjoint CISRI-OIAU*

<https://www.cisri.org>  
<https://www.iemo.int>  
<https://baid.international>





## Authoritative Certificate

Country	MR
State or Province Name	CISRI-IEMO-BAID Seat-Siege 144 E-Nord Tévragh Zeina - Nouakchott
Locality Name	Nouakchott - RIM
Organization	Convertible by agreement - Transferable on consensus
Organization	Convertible by agreement - Transferable on consensus
Organizational Unit Name	Void if unlawfully utilized
Description	Authoritative Certificate 1(one) BAID Unit: <serial number>
Common Name	International Authoritative Certificate
Email Address	<a href="mailto:certs@baid.international">certs@baid.international</a>
issuerAltName	-
subjectAltName	Waiver of responsibility for improper use
nsComment	Legal use only/NonWithdrawable/NonDuplicable/NonAlterable
nsCertSequence	-
nsBaseUrl	<a href="https://www.baid.international/certs">https://www.baid.international/certs</a> <a href="https://www.iemo.int/certs">https://www.iemo.int/certs</a>
nsSslServerName	-
nsRenewalUrl	-
nsRevocationUrl	<a href="https://www.iemo.int/certs/rev/&lt;serial number&gt;">https://www.iemo.int/certs/rev/&lt;serial number&gt;</a>
nsCaPolicyUrl	<a href="https://www.baid.international/certs/policies">https://www.baid.international/certs/policies</a>
nsCaRevocationUrl	<a href="https://www.baid.international/certs/rev/&lt;serial number&gt;">https://www.baid.international/certs/rev/&lt;serial number&gt;</a>





**CISRI**

Collaborative Inter-governmental Scientific Research Institute



**IEMO**

International Emergency Management Organization



**BAID**

Bank for International Development

These certificates:

- Can be used for electronic signatures in order to replace handwritten signatures where transacting parties choose for them
- Can be used to authenticate web resources, such as servers and other devices.

This CPS identifies the roles, responsibilities and practices of all entities involved in the life cycle, use, reliance upon and management of CISRI-IEMO-BAID certificates. The provisions of this CPS with regard to practices, level of services, responsibilities and liability bind all parties involved including the BAID, IEMO and CISRI, subscribers and relying parties.

Certain provisions might also apply to other entities such as the certification service provider, application providers etc.

This CPS describes the requirements to issue, manage and use certificates issued by the CISRI-IEMO-BAID under a managed Brand Root. This Brand Root is the CISRI-IEMO-BAID Root CA (Hereinafter referred to as "Brand Root") which is managed according to practices described in the CISRI-IEMO-BAID Certificate Policy published under:

- <https://www.baid.international/certs/policies>
- <https://www.iemo.int/certs/policies>

This CPS does not address the Brand Root policies, but relies exclusively on the practices described in the CISRI-IEMO-BAID Certificate Policy.

A subscriber or relying party of a BAID certificate must refer to the CISRI-IEMO-BAID CPS in order to establish Trust. It is also essential to establish the trustworthiness of the entire certificate chain of the CISRI-IEMO-BAID certificate hierarchy, including the Brand Root.



Document ID: CRT-CPS\_1.0  
URL: <https://baid.international/CPS>  
Date: 26/05/21

Certification Practice Statement  
Version v1.0

**CISRI-IEMO Joint Secretariat**  
*Secrétariat Conjoint CISRI-OIAU*

<https://www.cisri.org>  
<https://www.iemo.int>  
<https://baid.international>



---

## 1.2 CISRI-IEMO-BAID Certificate types

According to its Authoritative Mandate the CISRI-IEMO-BAID may issue Certificates concerning property and or conformity of both public and/or private movable and immovable goods and services, of whichever legal technical and financial nature, issued (directly or on behalf), and/or requested to the Organization

### 1.2.1 Issuing Certificates

CISRI-IEMO-BAID certificates can be also used for various protocols based transactions. It is meant for entities that wish to participate in secure communication and transactions at the web-server level. By using Secure Socket Layer (SSL) technology these certificates are essential to web-based businesses engaging in secured transactions.

The identity of the certificate-holder is fully authenticated by CISRI-IEMO-BAID.

### 1.2.2 Authoritative Certificates

CISRI-IEMO-BAID certificates may be used to provide authentication services, secure e-mail capabilities, inter-organizational communications, access to personal financial information and to authenticate the subscriber in online Internet transactions.

They require professional context affiliation to be incorporated into the certificate. With the same authoritative character CISRI-IEMO-BAID may use them as collateral for whichever transitive operation of technical and/or economical nature, as for the establishment of the Public Development Assistance scriptural allowances for Member States and Third Parties





**CISRI**

Collaborative Inter-governmental Scientific Research Institute



**IEMO**

International Emergency Management Organization



**BAID**

Bank for International Development

---

### 1.2.3 Acceptable Subscriber Names

For publication in its certificates BAID accepts subscriber names that are meaningful and can be authenticated as required.

### 1.2.4 Pseudonyms

BAID may allow the use of pseudonyms, reserving its right to disclose the identity of the subscriber as may be required by law or a following a reasoned and legitimate request.

### 1.2.5 Registration Procedures

BAID reserves the right to update registration procedures and subscriber submitted data to improve the identification and registration process.



Document ID: CRT-CPS\_1.0  
URL: <https://baid.international/CPS>  
Date: 26/05/21

Certification Practice Statement  
Version v1.0

**CISRI-IEMO Joint Secretariat**  
*Secrétariat Conjoint CISRI-OIAU*

<https://www.cisri.org>  
<https://www.iemo.int>  
<https://baid.international>



## 1.3 Issuer Certificates

### 1.3.1 General

CISRI-IEMO-BAID certificates are meant for secure communication with, for example, a website through an SSL or TLS link.

The applicant is an individual or an organization that has an Internet Server such as a website.

CISRI-IEMO-BAID certificates are used to assure a confidential communication with the Internet Server.

CISRI-IEMO-BAID certificates validity period is between one and ninety-nine years, in such case, counting after the initial year of issuance.

CISRI-IEMO-BAID certificates are issued to entities and individuals who own a domain name, or have the right to request a CISRI-IEMO-BAID certificates certificate for a specific domain.

### 1.3.2 Certificate Request

A certificate request can be made in the following way:

The certificate applicant submits an application following a procedure provided by BAID. Additional documentation in support of the application may be required so that BAID verifies that the domain name belongs to the applicant, or that the applicant is authorized





**CISRI**

Collaborative Inter-governmental Scientific Research Institute



**IEMO**

International Emergency Management Organization



**BAID**

Bank for International Development

---

to request a certificate for that domain name. The applicant submits to BAID the additional documentation. Upon verification of ownership or right to use of the domain name, BAID issues the certificate and sends a notice to the applicant. The applicant downloads and installs the certificate on its machines. The applicant must notify CISRI-IEMO-BAID of any inaccuracy or defect in a certificate promptly after receipt of the certificate or earlier notice of changes to the information to be included in the certificate.

### 1.3.3 Content

Typical information published on a certificate includes the following elements

- Applicant's domain name
- Applicant's public key
- Issuing Certification Authority (CISRI-IEMO Joint Secretariat)
- CISRI-IEMO-BAID electronic signature
- Type of algorithm
- Validity period of the digital certificate
- Serial number of the digital certificate



Document ID: CRT-CPS\_1.0  
URL: <https://baid.international/CPS>  
Date: 26/05/21

Certification Practice Statement  
Version v1.0

**CISRI-IEMO Joint Secretariat**  
*Secrétariat Conjoint CISRI-OIAU*

<https://www.cisri.org>  
<https://www.iemo.int>  
<https://baid.international>



---

### 1.3.4 Information Submitted to Verify Ownership or Right to Use of the Domain Name

The applicant must provide contact details to CISRI-IEMO-BAID.

The CISRI-IEMO Joint Secretariat has the right to request a signed registration form or a signed subscriber agreement.

The CISRI-IEMO Joint Secretariat has the right to request proof of the ownership of the domain name or can ask the owner of the domain name to validate the request of the applicant.

### 1.3.5 Issuing Procedure

The issuing procedure for a CISRI-IEMO-BAID Authoritative Certificate is as follows:

1. The applicant creates Certificate Signing Request (CSR) and a key pair using appropriate server software.
2. The applicant follows the registration procedure.
3. The applicant submits the required information including technical contact and server information.
4. The applicant accepts the subscriber agreement.
5. BAID verifies the submitted information by checking domain ownership or domain right to use and any other information as it sees fit.





**CISRI**

Collaborative Inter-governmental Scientific Research Institute



**IEMO**

International Emergency Management Organization



**BAID**

Bank for International Development

- 
6. The CISRI-IEMO-BAID Joint Secretariat may positively verify the applicant.
  7. BAID may issue the certificate to the applicant.
  8. BAID may publish the issued certificate in an online database
  9. Renewal: allowed
  10. Revocation: allowed

The CISRI-EMO-BAID might apply variations of this procedure in order to meet service, standards or legal requirements.

### 1.3.6 Limited Warranty

The CISRI-IEMO-BAID accepts no liability per loss due to a false domain name (lack of ownership or lack of right to use domain) in a certificate issued according to the CPS.

### 1.3.7 Relevant CISRI-IEMO-BAID Documents

The applicant must take notice and is bound by the following documents available on <https://www.baid.international/> and <https://www.iemo.int/BAID/>:

1. CISRI-IEMO-BAID CPS
2. Subscriber Agreement



Document ID: CRT-CPS\_1.0  
URL: <https://baid.international/CPS>  
Date: 26/05/21

Certification Practice Statement  
Version v1.0

**CISRI-IEMO Joint Secretariat**  
*Secrétariat Conjoint CISRI-OIAU*

<https://www.cisri.org>  
<https://www.iemo.int>  
<https://baid.international>





## 1.4 Authoritative Certificates

### 1.4.1 General

CISRI-IEMO-BAID certificates are intended for certain communications and transactions that require a minimum verification of the identity. They can be distributed for communications and transactions with a need to authenticate the communicating parties and encrypt the exchanged communications.

The validity period is between one and ninety-nine years, in such case, counting after the initial year of issuance.

CISRI-IEMO-BAID certificates are issued to natural persons (individuals) within their professional context, companies, institutes and governments.

### 1.4.2 Certificate Request

A certificate request can be made by the following means:

- The certificate applicant submits an application according to a procedure provided by CISRI-IEMO-BAID.  
Additional documentation in support of the application may be required so that BAID can verify the identity of the applicant.
- The applicant submits to CISRI-IEMO-BAID such additional documentation.





**CISRI**

Collaborative Inter-governmental Scientific Research Institute



**IEMO**

International Emergency Management Organization



**BAID**

Bank for International Development

- 
- Upon verification of identity, the CISRI-IEMO-BAID issues the certificate and sends a notice to the applicant.
  - The applicant downloads and installs the certificate to the applicant's device.
  - The applicant must notify BAID of any inaccuracy or defect in a certificate promptly after receipt of the certificate or earlier notice of changes to the information to be included in the certificate.

### 1.4.3 Content

Typical content of information published on a CISRI-IEMO-BAID certificate includes the following elements:

- Subscriber's e-mail address
- Subscriber's name
- Applicant's professional organization
- Applicant's public key
- Code of applicant's country
- Issuing Certification Authority (CISRI-IEMO Joint Secretariat)
- CISRI-IEMO Joint Secretariat electronic signature
- Type of algorithm
- Validity period of the digital certificate
- Serial number of the digital certificate



Document ID: CRT-CPS\_1.0  
URL: <https://baid.international/CPS>  
Date: 26/05/21

Certification Practice Statement  
Version v1.0

**CISRI-IEMO Joint Secretariat**  
*Secrétariat Conjoint CISRI-OIAU*

<https://www.cisri.org>  
<https://www.iemo.int>  
<https://baid.international>



## 1.4.4 Documents Submitted to Identify the Applicant

In all cases, the applicant must submit to BAID a signed subscriber agreement. BAID must have access to a copy of identity proof.

BAID may require additional proof of identity in support of the verification of the applicant.

## 1.4.5 Issuing Procedure

The issuing procedure for a CISRI-IEMO-BAID certificate is as follows:

1. The applicant submits the required information: e-mail address, common name, organizational information and country code.
2. The applicant accepts the subscriber agreement.
3. A key pair is generated on an applicant's device (e.g. computer, smart card device etc.).
4. Applicant must provide to CISRI-IEMO-BAID proof of identity, if required.
5. CISRI-IEMO-BAID may positively verify the applicant.
6. CISRI-IEMO-BAID may issue the certificate to the applicant.
7. Renewal: allowed.
8. Revocation: allowed.

CISRI-IEMO-BAID might apply variations of this procedure in order to meet service, standards or legal requirements.





**CISRI**

Collaborative Inter-governmental Scientific Research Institute



**IEMO**

International Emergency Management Organization



**BAID**

Bank for International Development

---

## 1.4.6 Limited Warranty

CISRI-IEMO-BAID accepts no liability per loss due to a false identity in a certificate issued following the CPS.

## 1.4.7 Relevant CISRI-IEMO-BAID Documents

The applicant must take notice and is bound by the following documents available on <https://www.baid.international/> and <https://www.iemo.int/BAID/>:

3. CISRI-IEMO-BAID CPS
4. Subscriber Agreement



Document ID: CRT-CPS\_1.0  
URL: <https://baid.international/CPS>  
Date: 26/05/21

Certification Practice Statement  
Version v1.0

**CISRI-IEMO Joint Secretariat**  
*Secrétariat Conjoint CISRI-OIAU*

<https://www.cisri.org>  
<https://www.iemo.int>  
<https://baid.international>



## 1.5 Certificate usages

Certain limitations apply to the use of CISRI-IEMO-BAID certificates.

An authoritative certificate can only be used for purposes explicitly permitted as they are listed below:

### Electronic signature

Electronic signature can only be used for specific electronic transactions that support electronic signing of electronic forms, electronic documents, electronic mail etc. The signature certificate is only warranted to produce electronic signatures in the context of applications that support digital certificates. To describe the function of an electronic signature, the term non-repudiation is often used.

CISRI-IEMO-BAID Certificates are appropriate for electronic signatures.

### Authentication (Users)

User authentication certificates can be used for specific electronic authentication transactions that support accessing web sites and other online content, electronic mail etc. The Authentication function of a digital certificate can be ascertained in any transaction context with the purpose of authenticating the end user subscriber to a digital certificate.

To describe the function of authentication, the term digital signature is often used.

CISRI-IEMO-BAID Certificates are appropriate for user authentication.





**CISRI**

Collaborative Inter-governmental Scientific Research Institute



**IEMO**

International Emergency Management Organization



**BAID**

Bank for International Development

---

## Authentication (Devices)

Device authentication certificates can be used for specific electronic authentication transactions that support the identifying of web sites and other on line resources. The Authentication function of a digital certificate can be ascertained in any transaction context with the purpose of authenticating a device that the subscriber seeks to secure through a digital certificate. To describe the function of authentication, the term digital signature is often used.

CISRI-IEMO-BAID Certificates certificates are appropriate for user authentication.

## Confidentiality

All certificate types can be used to ensure the confidentiality of communications effected by means of digital certificates. Confidentiality is required to assure the confidentiality of business and personal communications as well as for purposes of personal data protection and privacy.

All CISRI-IEMO-BAID Certificates are appropriate for confidentiality.

Any other use of a digital certificate is not supported by this CPS. When using a digital certificate the functions of electronic signature (non repudiation) and authentication (digital signature) are permitted together with the same certificate.



Document ID: CRT-CPS\_1.0  
URL: <https://baid.international/CPS>  
Date: 26/05/21

Certification Practice Statement  
Version v1.0

**CISRI-IEMO Joint Secretariat**  
*Secrétariat Conjoint CISRI-OIAU*

<https://www.cisri.org>  
<https://www.iemo.int>  
<https://baid.international>



## 1.6 Document Name and Identification

CISRI-IEMO-BAID ensures compliance of its certificates with the requirements and assertions of this CPS.

## 1.7 PKI Participants

The BAID makes its services available to the CISRI-IEMO-BAID certificate subscribers. These subscribers include without limitation entities that uses the CISRI-IEMO-BAID certificates for the purposes of:

- Authentication (digital signature)
- Encryption





**CISRI**

Collaborative Inter-governmental Scientific Research Institute



**IEMO**

International Emergency Management Organization



**BAID**

Bank for International Development

---

## 1.7.1 CISRI-IEMO-BAID Certification Authority

A Certification Authority, such as BAID - Bank for International Development and the CISRI-IEMO Joint Secretariat, is an organization that issues Digital Certificates to be used in public or private domains, within a business framework, a transaction context etc.

A Certification Authority is also referred to as the Issuing Authority to denote the purpose of issuing certificates.

The CISRI-IEMO-BAID drafts and implements the policy prevailing in issuing a certain type or class of digital certificates.

The CISRI-IEMO-BAID ensures the availability of all services pertaining to the management of CISRI-IEMO Joint Secretariat certificates, including without limitation the issuing, revocation, status verification of a certificate, as they may become available or required in specific applications.

Appropriate publication is necessary to ensure that relying parties obtain notice or knowledge of functions associated with the revoked and/or suspended certificates. Publication is manifested by including a revoked or suspended certificate in a certificate revocation list that is published in an online directory.

The domain of responsibility of the CISRI-IEMO-BAID's comprises the overall management of the certificate lifecycle including the following actions:

- Issuance
- Revocation
- Renewal
- Status validation

## Role of CISRI-IEMO-BAID

CISRI-IEMO-BAID operates as a Trust Service Provider to deliver Trust Services to a user community.



Document ID: CRT-CPS\_1.0  
URL: <https://baid.international/CPS>  
Date: 26/05/21

Certification Practice Statement  
Version v1.0

**CISRI-IEMO Joint Secretariat**  
*Secrétariat Conjoint CISRI-OIAU*

<https://www.cisri.org>  
<https://www.iemo.int>  
<https://baid.international>





## 1.7.2 Subscribers

Subscribers of the CISRI-IEMO-BAID services may be Governments, Organizations, Companies or natural persons that successfully apply for a certificate.

Subscribers are parties that have ultimate authority over the private key corresponding to the public key that is listed in a subject certificate.

Natural persons that are subscribers typically hold a valid identification document, which might be used as credential in order to issue CISRI-IEMO-BAID Certificates.

Additional credentials are required as explained in the process for the application for a certificate.

## 1.7.3 Relying Parties

Relying parties are natural or legal persons that rely on a certificate and/or a digital signature verifiable with reference to a public key listed in a subscriber's certificate.

To verify the validity of a digital certificate, relying parties must always refer to CISRI-IEMO-BAID revocation information such as a Certificate Revocation List (CRL).

Certificate validation takes place prior to relying on information featured in a certificate.

Relying parties meet specific obligations as described in this CPS.





**CISRI**

Collaborative Inter-governmental Scientific Research Institute



**IEMO**

International Emergency Management Organization



**BAID**

Bank for International Development

---

## 1.8 Certificate Use

Certain limitations apply to the use of CISRI-IEMO-BAID certificates.

### 1.8.1 Appropriate Certificate Usage

CISRI-IEMO-BAID certificates can be used for public domain transactions that require:

- Authentication and
- Confidentiality

Additional uses are specifically designated once they become available to end entities.

### 1.8.2 Prohibited Certificate Usage

End entity certificate use is restricted by using certificate extensions on key usage and extended key usage.

Any usage of the certificate inconsistent with these extensions is not authorized.



Document ID: CRT-CPS\_1.0  
URL: <https://baid.international/CPS>  
Date: 26/05/21

Certification Practice Statement  
Version v1.0

**CISRI-IEMO Joint Secretariat**  
*Secrétariat Conjoint CISRI-OIAU*

<https://www.cisri.org>  
<https://www.iemo.int>  
<https://baid.international>



## 1.8.3 Certificate Extensions

CISRI-IEMO-BAID issues certificates that might contain extensions defined by the X.509 v3 standard as well as any other formats including those used in the OpenSource ecosystem.

## 1.8.4 Critical Extensions

CISRI-IEMO-BAID CA uses certain critical extensions in the certificates it issues such as:

- A basic constraint in the certificate to show whether a certificate is meant for a CA or not.
- To show the intended usage of the key.





**CISRI**

Collaborative Inter-governmental Scientific Research Institute



**IEMO**

International Emergency Management Organization



**BAID**

Bank for International Development

---

## 1.9 Policy Administration

The Policy Managing Authority of the CISRI-IEMO Joint Secretariat manages this BAID - Bank for International Development CPS.

The CISRI-IEMO Joint Secretariat registers, observes the maintenance, and interprets this CPS.

The CISRI-IEMO Joint Secretariat makes available the operational conditions prevailing in the life-cycle management of CISRI-IEMO-BAID certificates.

### 1.9.1 Scope

CISRI-IEMO-BAID may make revisions and updates to its policies as it sees fit or required by the circumstances. Such updates become binding for all certificates that have been issued or are to be issued 30 days after the date of the publication of the updated version of the CPS.

### 1.9.2 CISRI-IEMO-BAID Policy Management Authority

New versions and publicized updates of CISRI-IEMO-BAID policies are approved by the CISRI-IEMO Joint Secretariat Policy Management Authority.

The CISRI-IEMO Joint Secretariat Policy Management Authority in its present organizational structure comprises of members as indicated below:

- At least one member of the management of CISRI-IEMO-BAID
- At least one authorized agents directly involved in the drafting and development of CISRI-IEMO Joint Secretariat practices and policies



Document ID: CRT-CPS\_1.0  
URL: <https://baid.international/CPS>  
Date: 26/05/21

Certification Practice Statement  
Version v1.0

**CISRI-IEMO Joint Secretariat**  
*Secrétariat Conjoint CISRI-OIAU*

<https://www.cisri.org>  
<https://www.iemo.int>  
<https://baid.international>



### 1.9.3 Acceptance of Updated Versions of the CPS

Upon approval of a CPS update by the CISRI-IEMO Joint Secretariat Policy Management Authority, that CPS is published in the CISRI-IEMO Joint Secretariat online Repository at:

- <https://www.baid.international/CPS>
- <https://www.iemo.int/BAID/CPS>

The updated version is binding against all existing and future subscribers unless notice is received within 30 days after communication of the notice.

After such period the updated version of the CPS is binding against all parties including the subscribers and parties relying on certificates that have been issued under a previous version of the CISRI-IEMO Joint Secretariat CPS.

CISRI-IEMO-BAID publishes on its web site at least the two latest versions of its CPS.

### 1.9.4 Version Management and Denoting Changes

Changes are denoted through new version numbers for the CPS. New versions are indicated with an integer number followed by one decimal that is zero. Minor changes are indicated through one decimal number that is larger than zero. Minor changes include:

- Minor editorial corrections
- Changes to contact details





**CISRI**

Collaborative Inter-governmental Scientific Research Institute



**IEMO**

International Emergency Management Organization



**BAID**

Bank for International Development

---

## 1.10 Definitions and Acronyms

A list of definitions can be found at the end of this CPS.



Document ID: CRT-CPS\_1.0  
URL: <https://baid.international/CPS>  
Date: 26/05/21

Certification Practice Statement  
Version v1.0

**CISRI-IEMO Joint Secretariat**  
*Secrétariat Conjoint CISRI-OIAU*

<https://www.cisri.org>  
<https://www.iemo.int>  
<https://baid.international>



---

## 2. Publication and Repository Responsibilities

CISRI-IEMO-BAID publishes information about the digital certificates that it issues in an online repository. CISRI-IEMO-BAID reserves its right to publish certificate status information on third party repositories.

CISRI-IEMO-BAID retains an online repository of documents where it makes certain disclosures about its practices, procedures and the content of certain policies including this CPS.

CISRI-IEMO-BAID reserves its right to make available and publish information on its policies by any appropriate means within the CISRI-IEMO Joint Secretariat repository.

All parties who are associated with the issuance, use or management of CISRI-IEMO Joint Secretariat certificates are hereby notified that CISRI-IEMO-BAID may publish submitted information on publicly accessible directories in association with the provision of electronic certificate status information.

CISRI-IEMO-BAID refrains from making publicly available certain elements of documents including security controls, procedures, internal security policies etc.





**CISRI**

Collaborative Inter-governmental Scientific Research Institute



**IEMO**

International Emergency Management Organization



**BAID**

Bank for International Development

---

## 3. Identification and Authentication

CISRI-IEMO-BAID maintains appropriate procedures to address naming practices, including the recognition of trademark rights in certain names.

CISRI-IEMO-BAID authenticates the requests of parties wishing to revoke certificates under this policy.

### 3.1 Initial Identity Validation

The identification of the applicant for a certificate is carried out according to a documented procedure.

For the identification and authentication procedures of the initial subscriber registration, CISRI-IEMO-BAID might rely on such resources as third party databases.

### 3.2 Subscriber Registration Process

CISRI-IEMO-BAID ensures that:

- Subscribers of certificates are properly identified and authenticated
- Subscriber certificate requests are complete, accurate and duly authorized.



Document ID: CRT-CPS\_1.0  
URL: <https://baid.international/CPS>  
Date: 26/05/21

Certification Practice Statement  
Version v1.0

**CISRI-IEMO Joint Secretariat**  
*Secrétariat Conjoint CISRI-OIAU*

<https://www.cisri.org>  
<https://www.iemo.int>  
<https://baid.international>





### 3.2.1 Documents Used for Subscriber Registration

CISRI-IEMO-BAID typically verifies certificate request by appropriate means and on the basis of a documented procedure: the applicant must submit to CISRI-IEMO-BAID a Subscriber Agreement, both accepted and agreed to.

CISRI-IEMO-BAID may prescribe additional identification proof in support of the verification of the applicant ownership or right to use of the domain.

### 3.2.2 Records for Subscriber Registration

CISRI-IEMO-BAID maintains records of the executed subscriber agreement and any material or documents that support the application which also include but are not limited to:

- CISRI-IEMO-BAID subscriber agreement as approved of, and executed by, the applicant.
- Consent to the keeping of a record by CISRI-IEMO-BAID of information used in registration and any subsequent certificate status change and passing of this information to third parties under the same conditions as required by this CPS in the case of the CA terminating its services.
- That information held in the certificate is correct and accurate.
- A specifically designed attribute that uniquely identifies the applicant within the context of the CISRI-IEMO-BAID.





**CISRI**

Collaborative Inter-governmental Scientific Research Institute



**IEMO**

International Emergency Management Organization



**BAID**

Bank for International Development

---

The records identified above shall be kept for a period of no less than 2 years following the expiration of a certificate.

### 3.2.3 Identification and Authentication for Revocation Requests

For the identification and authentication procedures of revocation requests, CISRI-IEMO-BAID requires using an online authentication mechanism and/or a request addressed to the CISRI-IEMO-BAID.



Document ID: CRT-CPS\_1.0  
URL: <https://baid.international/CPS>  
Date: 26/05/21

Certification Practice Statement  
Version v1.0

**CISRI-IEMO Joint Secretariat**  
*Secrétariat Conjoint CISRI-OIAU*

<https://www.cisri.org>  
<https://www.iemo.int>  
<https://baid.international>



## 4. Certificate Life-Cycle Operational Requirements

The following operational requirements apply to Certificate Life-Cycle.

All entities within the CISRI-IEMO Joint Secretariat domain including subscribers or other participants have a continuous duty to inform the CISRI-IEMO-BAID of all changes in the information featured in a certificate during the operational period of such certificate and until it expires or revoked.

To carry out its tasks CISRI-IEMO Joint Secretariat may use third party agents for which CISRI-IEMO-BAID assumes responsibility.

Subscribers undergo an enrollment process that requires:

- a) Generating a key pair.
- b) Delivering the generated public key corresponding to a private key to CISRI-IEMO-BAID.
- c) Accepting the subscriber agreement.

The subscriber is required to accept the issuance terms by a subscriber agreement that will be executed with the CISRI-IEMO-BAID. The subscriber agreement incorporates by reference this CPS.

### 4.1 Certificate Application Processing and Issuance

CISRI-IEMO-BAID acts upon a CISRI-IEMO Joint Secretariat certificate application to validate the submitted information. Subsequently, the application is either approved or rejected.





**CISRI**

Collaborative Inter-governmental Scientific Research Institute



**IEMO**

International Emergency Management Organization



**BAID**

Bank for International Development

---

Such approval or rejection does not necessarily have to be justified to the applicant or any other party.

For rejected applications of certificate requests, CISRI-IEMO-BAID notes the reason for rejecting the application.

Following issuance of the approved certificate, the CISRI-IEMO-BAID delivers the issued certificate to the subscriber.

## 4.2 Certificate Generation

With reference to the issuance and renewal of certificates, CISRI-IEMO-BAID represents towards all parties that certificates are issued securely according to the conditions set below:

- The procedure to issue a certificate is securely linked to the associated registration, including the provision of any subscriber generated public key.
- The confidentiality and integrity of registration data is ensured at all times through appropriate SSL (Secure Socket layer) links...
- Certificate requests and generation are also supported by robust and tested procedures that have been scrutinized for compliance with the prevailing standards.



Document ID: CRT-CPS\_1.0  
URL: <https://baid.international/CPS>  
Date: 26/05/21

Certification Practice Statement  
Version v1.0

**CISRI-IEMO Joint Secretariat**  
*Secrétariat Conjoint CISRI-OIAU*

<https://www.cisri.org>  
<https://www.iemo.int>  
<https://baid.international>



## 4.3 Certificate Acceptance

An issued CISRI-IEMO Joint Secretariat certificate is deemed accepted by the subscriber when no objection is received by CISRI-IEMO Joint Secretariat from the subscriber within three (3) working day after it being received. Any objection to accepting an issued certificate must explicitly be notified to the CISRI-IEMO-BAID. The reasoning for rejection including any fields in the certificate that contain erroneous information must also be submitted.

The CISRI-IEMO-BAID might post the issued certificate on a repository. The CISRI-IEMO-BAID also reserves its right to notify the certificate issuance by the CISRI-IEMO-BAID to other entities.

## 4.4 Key Pair and Certificate Usage

The responsibilities relating to the use of keys and certificates include the ones addressed below:

### 4.4.1 Subscriber

The obligations of the subscriber include the following ones:





**CISRI**

Collaborative Inter-governmental Scientific Research Institute



**IEMO**

International Emergency Management Organization



**BAID**

Bank for International Development

---

### 4.4.1.1 Subscriber Duties

Unless otherwise stated in this CPS, the duties of subscribers include the following:

1. Accepting all applicable terms and conditions in the CPS of CISRI-IEMO-BAID published in the CISRI-IEMO Joint Secretariat repository.
2. Notifying the CISRI-IEMO-BAID of any changes in the information submitted that might materially affect the trustworthiness of that certificate.
3. Ceasing to use a CISRI-IEMO Joint Secretariat certificate when it becomes invalid.
4. Using a CISRI-IEMO Joint Secretariat certificate, as it may be reasonable under the circumstance.
5. Preventing the compromise, loss, disclosure, modification, or otherwise unauthorized use of their private key.
6. Using secure devices and products that provide appropriate protection to their keys.
7. Refraining from submitting to CISRI-IEMO-BAID or any CISRI-IEMO Joint Secretariat directory any material that contains statements that violate any law or the rights of any party.
8. Requesting the revocation of a certificate in case of an occurrence that materially affects the integrity of a CISRI-IEMO Joint Secretariat certificate.
9. Refraining from tampering with a certificate.
10. Only using certificates for legal and authorized purposes in accordance with the CPS.
11. Refrain from using a certificate outside possible license restrictions imposed by CISRI-IEMO-BAID.



Document ID: CRT-CPS\_1.0  
URL: <https://baid.international/CPS>  
Date: 26/05/21

Certification Practice Statement  
Version v1.0

**CISRI-IEMO Joint Secretariat**  
*Secrétariat Conjoint CISRI-OIAU*

<https://www.cisri.org>  
<https://www.iemo.int>  
<https://baid.international>

CISRI  
Collaborative Inter-governmental Scientific Research Institute



IEMO  
International Emergency Management Organization



BAID  
Bank for International Development



---

The Subscriber has all above stated duties towards the CA at all times.





**CISRI**

Collaborative Inter-governmental Scientific Research Institute



**IEMO**

International Emergency Management Organization



**BAID**

Bank for International Development

---

### 4.4.1.2 Subscriber Duty Towards Relying Parties

Without limiting other subscriber obligations stated elsewhere in this CPS, subscribers have a duty to refrain from any misrepresentations they make in certificates to third parties that reasonably rely on the representations contained therein.

### 4.4.1.3 Reliance at Own Risk

It is the sole responsibility of the parties accessing information featured in the CISRI-IEMO-BAID repositories and web site to assess and rely on information featured therein. Parties acknowledge that they have received adequate information to decide whether to rely upon any information provided in a certificate. The CISRI-IEMO-BAID takes steps necessary to update its records and directories concerning the status of the certificates. Failure to comply with the conditions of usage of the CISRI-IEMO-BAID repositories and web site may result in terminating the relationship between the CISRI-IEMO-BAID and the party.



Document ID: CRT-CPS\_1.0  
URL: <https://baid.international/CPS>  
Date: 26/05/21

Certification Practice Statement  
Version v1.0

**CISRI-IEMO Joint Secretariat**  
*Secrétariat Conjoint CISRI-OIAU*

<https://www.cisri.org>  
<https://www.iemo.int>  
<https://baid.international>





## 4.4.2 Relying Party

The duties of a relying party are as follows:

### 4.4.2.1 Relying Party Duties

A party relying on a CISRI-IEMO Joint Secretariat certificate will:

- Validate a CISRI-IEMO Joint Secretariat certificate by using certificate status information (e.g. CRL) published by CISRI-IEMO-BAID.
- Trust a CISRI-IEMO-BAID certificate only if all information featured on such a certificate can be verified via such a validation procedure as being correct and up to date.
- Rely on a CISRI-IEMO Joint Secretariat certificate, only as it may be reasonable under the circumstances.
- Trust a certificate only if it has not been revoked.





**CISRI**

Collaborative Inter-governmental Scientific Research Institute



**IEMO**

International Emergency Management Organization



**BAID**

Bank for International Development

---

## 4.4.2.2 CISRI-IEMO-BAID Repository and Web Site Conditions

Parties, including subscribers and relying parties, accessing the CISRI-IEMO-BAID Repository and web site agree with the provisions of this CPS and any other conditions of use that the CISRI-IEMO-BAID may make available. Parties demonstrate acceptance of the conditions of usage of the CPS by submitting a query with regard to the status of a digital certificate or by using or relying upon any such information or services provided:

- Obtaining information as a result of the search for a digital certificate.
- Validating the status of a digital certificate before encrypting data using the public key included in a certificate
- Obtaining information published on the CISRI-IEMO-BAID web site.

## 4.5 Certificate Renewal

Subscribers may request the renewal of CISRI-IEMO Joint Secretariat certificates. To request the renewal of a CISRI-IEMO Joint Secretariat certificate, an end user lodges a request.

Requirements for renewal of certificates, where available, may vary from those originally required for subscribing to the service.



Document ID: CRT-CPS\_1.0  
URL: <https://baid.international/CPS>  
Date: 26/05/21

Certification Practice Statement  
Version v1.0

**CISRI-IEMO Joint Secretariat**  
*Secrétariat Conjoint CISRI-OIAU*

<https://www.cisri.org>  
<https://www.iemo.int>  
<https://baid.international>



## 4.6 Certificate Revocation

CISRI-IEMO-BAID shall use reasonable efforts to publish clear guidelines for revoking certificates, and maintain a 24/7 ability to accept and respond to revocation requests.

The identification of the subscriber who applies for a revocation or suspension of a certificate is carried out according to an internal documented procedure.

The CISRI-IEMO-BAID revokes a CISRI-IEMO Joint Secretariat certificate if:

- There has been loss, theft, modification, unauthorized disclosure, or other compromise of the private key of the certificate's subject.
- The certificate's subscriber has breached a material obligation under this CPS.
- The performance of a person's obligations under this CPS is delayed or prevented by a natural disaster, computer or communications failure, or other cause beyond the person's reasonable control, and as a result, another person's information is materially threatened or compromised.
- There has been a modification of the information contained in the certificate of the certificate's subject.





**CISRI**

Collaborative Inter-governmental Scientific Research Institute



**IEMO**

International Emergency Management Organization



**BAID**

Bank for International Development

---

## 4.7 Certificate Status Services

The CISRI-IEMO-BAID makes available certificate status checking services including CRLs, and appropriate Web interfaces.

### CRL

A CRL lists all revoked and suspended certificates during the application period. CRLs for the different products are pointed to from within the certificate through the CDP extension.



Document ID: CRT-CPS\_1.0  
URL: <https://baid.international/CPS>  
Date: 26/05/21

Certification Practice Statement  
Version v1.0

**CISRI-IEMO Joint Secretariat**  
*Secrétariat Conjoint CISRI-OIAU*

<https://www.cisri.org>  
<https://www.iemo.int>  
<https://baid.international>



## 4.8 End of Subscription

Subscriber subscription ends when a certificate is revoked, expired or the service is terminated.

## 4.9 Certificates Problem Reporting and Response Capability

In addition to certificate revocation, CISRI-IEMO-BAID provides subscribers, relying parties, and other third parties with clear instructions for reporting complaints or suspected Private Key compromise, certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to certificates. CISRI-IEMO-BAID shall use reasonable efforts to provide a timely capability to accept and acknowledge and respond to such reports.





**CISRI**

Collaborative Inter-governmental Scientific Research Institute



**IEMO**

International Emergency Management Organization



**BAID**

Bank for International Development

---

## 5. Management, Operational, And Physical Controls

This section describes non-technical security controls used by CISRI-IEMO-BAID to perform the functions of key generation, subject authentication, certificate issuance, certificate revocation, audit, and archival.

### 5.1 Physical Security Controls

The CISRI-IEMO-BAID implements physical controls on its own, leased or rented premises.

The CISRI-IEMO-BAID infrastructure is logically separated from any other certificate management infrastructure, used for other purposes.

The CISRI-IEMO-BAID secure premises are located in an area appropriate for high-security operations.

Physical access is restricted by implementing mechanisms to control access from one area of the facility to another or access into high-security zones.

The CISRI-IEMO-BAID implements prevention and protection as well as measures against fire exposures.

Media are stored securely. Backup media are also stored in a separate location that is physically secure and protected from fire and water damages.

The sites of the CISRI-IEMO-BAID host the infrastructure to provide the CISRI-IEMO-BAID services. The CISRI-IEMO-BAID sites implement proper security controls, including access control, intrusion detection and monitoring. Access to the sites is limited to authorized personnel listed on an access list...



Document ID: CRT-CPS\_1.0  
URL: <https://baid.international/CPS>  
Date: 26/05/21

Certification Practice Statement  
Version v1.0

**CISRI-IEMO Joint Secretariat**  
*Secrétariat Conjoint CISRI-OIAU*

<https://www.cisri.org>  
<https://www.iemo.int>  
<https://baid.international>



## 5.2 Procedural Controls

The CISRI-IEMO-BAID follows personnel and management practices that provide reasonable assurance of the trustworthiness and competence of the members of the staff and of the satisfactory performance of their duties in the fields of the electronic signature-related technologies.

The CISRI-IEMO-BAID obtains a signed statement from each member of the staff on not having conflicting interests, maintaining confidentiality and protecting personal data.

All members of the staff operating the key management operations administrators, security officers, and system auditors or any other operations that materially affect such operations are considered as serving in a trusted position.

The CISRI-IEMO-BAID conducts an initial investigation of all members of staff who are candidates to serve in trusted roles to make a reasonable attempt to determine their trustworthiness and competence.

Where dual control is required at least two trusted members of the CISRI-IEMO-BAID staff need to bring their respective and split knowledge in order to be able to proceed with an ongoing operation.

The CISRI-IEMO-BAID ensures that all actions with respect to the CISRI-IEMO-BAID can be attributed to the system and the person of the CA that has performed the action.

The CISRI-IEMO-BAID implements dual control for critical CA functions.





**CISRI**

Collaborative Inter-governmental Scientific Research Institute



**IEMO**

International Emergency Management Organization



**BAID**

Bank for International Development

---

## 5.3 Personnel Security Controls

### 5.3.1 Qualifications, Experience, Clearances

The CISRI-IEMO-BAID perform checks to establish the background, qualifications, and experience needed to perform within the competence context of the specific job.

### 5.3.2 Training Requirements and Procedures

The CISRI-IEMO-BAID makes available training for their personnel to carry out their functions.

### 5.3.3 Retraining Period and Retraining Procedures

Periodic training updates might also be performed to establish continuity and updates in the knowledge of the personnel and procedures.



Document ID: CRT-CPS\_1.0  
URL: <https://baid.international/CPS>  
Date: 26/05/21

Certification Practice Statement  
Version v1.0

**CISRI-IEMO Joint Secretariat**  
*Secrétariat Conjoint CISRI-OIAU*

<https://www.cisri.org>  
<https://www.iemo.int>  
<https://baid.international>





### 5.3.4 Sanctions against Personnel

CISRI-IEMO-BAID sanctions personnel for unauthorized actions, unauthorized use of authority, and unauthorized use of systems for the purpose of imposing accountability on a participant's personnel, as it might be appropriate under the circumstances.

### 5.3.5 Controls of Independent Contractors

Independent contractors and their personnel are subject to the same privacy protection and confidentiality conditions as CISRI-IEMO-BAID personnel.

### 5.3.6 Documentation for Initial Training and Retraining

The CISRI-IEMO-BAID make available documentation to personnel, during initial training, retraining, or otherwise.

## 5.4 Audit Logging Procedures

Audit logging procedures include event logging and audit systems, implemented for the purpose of maintaining a secure environment.





**CISRI**

Collaborative Inter-governmental Scientific Research Institute



**IEMO**

International Emergency Management Organization



**BAID**

Bank for International Development

---

CISRI-IEMO-BAID implements the following controls:

CISRI-IEMO-BAID audit records events that include but are not limited to:

- Issuance of a certificate
- Revocation of a certificate
- Publishing of a CRL

Audit trail records contain:

- The identification of the operation
- The data and time of the operation
- The identification of the certificate, involved in the operation
- The identification of the person that performed the operation
- A reference to the request of the operation.

Documents available include:

- Infrastructure plans and descriptions.
- Physical site plans and descriptions.
- Configuration of hardware and software.
- Personnel access lists.

CISRI-IEMO-BAID ensures that designated personnel review log files at regular intervals and detect and report anomalous events.



Document ID: CRT-CPS\_1.0  
URL: <https://baid.international/CPS>  
Date: 26/05/21

Certification Practice Statement  
Version v1.0

**CISRI-IEMO Joint Secretariat**  
*Secrétariat Conjoint CISRI-OIAU*

<https://www.cisri.org>  
<https://www.iemo.int>  
<https://baid.international>



---

Log files and audit trails are archived for inspection by the authorized personnel of CISRI-IEMO-BAID. The log files should be properly protected by an access control mechanism. Log files and audit trails are backed up and must be available to independent auditors upon request.

## 5.5 Records Archival

CISRI-IEMO-BAID keeps archives in a retrievable format.

CISRI-IEMO-BAID ensures the integrity of the physical storage media and implements proper copying mechanisms to prevent data loss.

Archives are accessible to authorized personnel of CISRI-IEMO-BAID as appropriate.

The CISRI-IEMO-BAID keeps internal records of the following items:

- All certificates for a period of a minimum of 2 years after the expiration of the certificate.
- Audit trails on the issuance of certificates for a period of a minimum of 2 years after issuance of a certificate.
- Audit trail of the revocation of a certificate for a period of a minimum of 2 years following the revocation of a certificate.
- CRLs for a minimum of 1 years after expiration or revocation of a certificate.





**CISRI**

Collaborative Inter-governmental Scientific Research Institute



**IEMO**

International Emergency Management Organization



**BAID**

Bank for International Development

- 
- Support documents on the issuance of certificates for a period of 2 years after expiration of a certificate. Support documents can be electronically stored.

## 5.5.1 Types of Records

CISRI-IEMO-BAID retains in a trustworthy manner records of CISRI-IEMO-BAID digital certificates, audit data, certificate application information, log files and documentation supporting certificate applications.

## 5.5.2 Retention Period

CISRI-IEMO-BAID retains in a trustworthy manner records of certificates for at least 2 years.

## 5.5.3 Protection of Archive

Conditions for the protection of archives include:

Only the records administrator (member of staff assigned with the records retention duty) may view the archive:

- Protection against modification of archive, such as storing the data on a write once medium.



Document ID: CRT-CPS\_1.0  
URL: <https://baid.international/CPS>  
Date: 26/05/21

Certification Practice Statement  
Version v1.0

**CISRI-IEMO Joint Secretariat**  
*Secrétariat Conjoint CISRI-OIAU*

<https://www.cisri.org>  
<https://www.iemo.int>  
<https://baid.international>



- 
- Protection against deletion of archive.
  - Protection against deterioration of the media on which the archive is stored, such as a requirement for data to be migrated periodically to fresh media.

## 5.5.4 Archive Collection

The CISRI-IEMO-BAID archive collection system is internal.

## 5.5.5 Procedures to Obtain and Verify Archive Information

To obtain and verify archive information CISRI-IEMO-BAID maintains records under clear hierarchical control.

The CISRI-IEMO-BAID retains records in electronic or in paper-based format. The CISRI-IEMO-BAID may require subscribers, or their agents to submit documents appropriately in support of this requirement.

Filing terms begin on the date of expiration or revocation. Such records may be retained in electronic or in paper-based format or any other format that the CISRI-IEMO-BAID may see fit.





**CISRI**

Collaborative Inter-governmental Scientific Research Institute



**IEMO**

International Emergency Management Organization



**BAID**

Bank for International Development

---

## 5.6 Compromise and Disaster Recovery

In a separate internal document, the CISRI-IEMO-BAID documents applicable incident, compromise reporting and handling procedures. The CISRI-IEMO-BAID documents the recovery procedures used if computing resources, software, and/or data are corrupted or suspected of being corrupted.

The CISRI-IEMO-BAID establishes the necessary measures to ensure full recovery of the service, in an appropriate time frame depending on the type of disruption, in case of a disaster, corrupted servers, software or data.



Document ID: CRT-CPS\_1.0  
URL: <https://baid.international/CPS>  
Date: 26/05/21

Certification Practice Statement  
Version v1.0

**CISRI-IEMO Joint Secretariat**  
*Secrétariat Conjoint CISRI-OIAU*

<https://www.cisri.org>  
<https://www.iemo.int>  
<https://baid.international>



## 6. Certificate and CRL Profiles

This section specifies the certificate format and CRL formats.

### 6.1 Certificate Profile

CISRI-IEMO Joint Secretariat certificate profiles are available upon request.

### 6.2 CRL Profile

The CISRI-IEMO-BAID maintains a record of the CRL profile it uses in an independent technical document. This will be made available at the discretion of the CISRI-IEMO-BAID, on request from parties explaining their interest.





**CISRI**

Collaborative Inter-governmental Scientific Research Institute



**IEMO**

International Emergency Management Organization



**BAID**

Bank for International Development

---

## 7. Compliance Audit And Other Assessment

CISRI-IEMO-BAID accepts under condition the auditing of practices and procedures it does not publicly disclose. CISRI-IEMO Joint Secretariat CA gives further consideration and evaluates the results of such audits before possibly implementing them.

Following its own approval with regard to the scope and content, CISRI-IEMO-BAID accepts compliance audits to ensure it meets requirements, standards, procedures and service levels according to this CPS and accreditation schemes it publicly claims compliance with.



Document ID: CRT-CPS\_1.0  
URL: <https://baid.international/CPS>  
Date: 26/05/21

Certification Practice Statement  
Version v1.0

**CISRI-IEMO Joint Secretariat**  
*Secrétariat Conjoint CISRI-OIAU*

<https://www.cisri.org>  
<https://www.iemo.int>  
<https://baid.international>





---

## 8. Other Business and Legal Matters

Certain legal conditions apply to the issuance of the CISRI-IEMO Joint Secretariat certificates under this CPS as described in this section.

### 8.1 Financial Responsibility

CISRI-IEMO-BAID maintains sufficient resources to meet its perceived obligations under this CPS. The CISRI-IEMO-BAID makes this service available on an “as is” basis..





**CISRI**

Collaborative Inter-governmental Scientific Research Institute



**IEMO**

International Emergency Management Organization



**BAID**

Bank for International Development

---

## 8.2 Confidentiality of Business Information

CISRI-IEMO-BAID observes personal data privacy rules and confidentiality rules as described in the CISRI-IEMO Joint Secretariat CPS. Confidential information includes:

- Any personal identifiable information on subscribers, other than that contained in a certificate.
- Reason for the revocation of a certificate, other than that contained in published certificate status information.
- Audit trails.
- Correspondence regarding CA services.
- CA Private key(s).

The following items are not confidential information:

- Certificate and their content.
- Status of a certificate.

CISRI-IEMO-BAID does not release nor is it required to release any confidential information without an authenticated and justified request specifying either:

- The party to whom the CISRI-IEMO-BAID owes a duty to keep information confidential is the party requesting such information.
- A court order.

Parties requesting and receiving confidential information are granted permission on the assumption that they use it for the requested purposes, secure it from compromise, and refrain from using it or disclosing it to third parties.



Document ID: CRT-CPS\_1.0  
URL: <https://baid.international/CPS>  
Date: 26/05/21

Certification Practice Statement  
Version v1.0

**CISRI-IEMO Joint Secretariat**  
*Secrétariat Conjoint CISRI-OIAU*

<https://www.cisri.org>  
<https://www.iemo.int>  
<https://baid.international>



---

## 8.2.1 Disclosure Conditions

Non-confidential information can be disclosed to any subscriber and relying party under the conditions below:

- Only a single certificate is delivered per inquiry by subscriber or relying party.
- The status of a single certificate is provided per inquiry by a subscriber or relying party.
- Subscribers can consult the information the CA holds about them.

Confidential information may not be disclosed to subscribers nor relying parties. CISRI-IEMO-BAID properly manages the disclosure of information to the CA personnel.

To incorporate information by reference, CISRI-IEMO-BAID might use computer-based and text-based pointers that include URLs, etc.

## 8.3 Privacy of Personal Information

CISRI-IEMO-BAID has an internal policy for the protection of personal data of the applicant applying for an CISRI-IEMO Joint Secretariat certificate.





**CISRI**

Collaborative Inter-governmental Scientific Research Institute



**IEMO**

International Emergency Management Organization



**BAID**

Bank for International Development

---

## 8.4 Intellectual Property Rights

CISRI-IEMO-BAID owns and reserves all intellectual property rights associated with its databases, web sites, CISRI-IEMO Joint Secretariat certificates and any other publication whatsoever originating from CISRI-IEMO-BAID including this CPS.

The distinguished names in use across CISRI-IEMO-BAID, remain the sole property of CISRI-IEMO-BAID, which enforces these rights.

Certificates are and remain property of CISRI-IEMO-BAID. CISRI-IEMO-BAID permits the reproduction and distribution of certificates on a non-exclusive, royalty-free basis, provided that they are reproduced and distributed in full, except that certificates are not published in any publicly accessible repository or directory without the express written permission of CISRI-IEMO-BAID. The scope of this restriction is also intended to protect subscribers against the unauthorized re-publication of their personal data featured on a certificate. CISRI-IEMO-BAID owns and reserves all intellectual property rights associated with its own products and services that it has not explicitly transferred or released to another party.



Document ID: CRT-CPS\_1.0  
URL: <https://baid.international/CPS>  
Date: 26/05/21

Certification Practice Statement  
Version v1.0

**CISRI-IEMO Joint Secretariat**  
*Secrétariat Conjoint CISRI-OIAU*

<https://www.cisri.org>  
<https://www.iemo.int>  
<https://baid.international>



## 8.5 Representations and Warranties

CISRI-IEMO-BAID uses this CPS and a subscriber agreement to convey legal conditions of usage of CISRI-IEMO Joint Secretariat certificates to subscribers and relying parties.

Participants that may make representations and warranties include CISRI-IEMO-BAID, subscribers, relying parties, and any other participants as it might become necessary.

All parties of the CISRI-IEMO Joint Secretariat domain, including the CISRI-IEMO-BAID and subscribers warrant the integrity of their respective private key(s). If any such party suspects that a private key has been compromised they will immediately notify CISRI-IEMO-BAID.

### 8.5.1 CISRI-IEMO-BAID Repository and Web Site Conditions

Parties (including subscribers and relying parties) accessing the CISRI-IEMO-BAID repository and web site agree with the provisions of this CPS and any other conditions of usage that CISRI-IEMO Joint Secretariat may make available. Parties demonstrate acceptance of the conditions of usage of the CPS by submitting a query with regard to the status of a digital certificate or by anyway using or relying upon any such information or services provided.

The CISRI-IEMO-BAID repositories include or contain:

- Information provided as a result of the search for a digital certificate.
- Information to verify the status of an CISRI-IEMO Joint Secretariat certificate.





**CISRI**

Collaborative Inter-governmental Scientific Research Institute



**IEMO**

International Emergency Management Organization



**BAID**

Bank for International Development

- 
- Information published on the CISRI-IEMO-BAID web site.
  - Any other services that CISRI-IEMO-BAID might advertise or provide through its web site.
  - If a repository becomes aware of or suspects the compromise of a private key, it will immediately notify CISRI-IEMO-BAID.

The CISRI-IEMO-BAID maintains a certificate repository during the application period and for a minimum of two years after the expiration or revocation of a certificate.

### 8.5.1.1 Reliance at Own Risk

It is the sole responsibility of the parties accessing information published on the CISRI-IEMO-BAID repositories and web site to assess and rely on information featured therein. Parties acknowledge that they have received adequate information to decide whether to rely upon any information provided in a certificate. CISRI-IEMO-BAID takes steps necessary to update its records and directories concerning the status of the certificates and issue warnings about. Failure to comply with the conditions of usage of the CISRI-IEMO Joint Secretariat repositories and web site may result in terminating the relationship between the CISRI-IEMO-BAID and the party.

### 8.5.1.2 Accuracy of Information

CISRI-IEMO-BAID makes every effort to ensure that parties accessing its repositories receive accurate, updated and correct information. CISRI-IEMO-BAID, however, cannot accept any liability beyond the limits set in this CPS and the CISRI-IEMO-BAID insurance policy.



Document ID: CRT-CPS\_1.0  
URL: <https://baid.international/CPS>  
Date: 26/05/21

Certification Practice Statement  
Version v1.0

**CISRI-IEMO Joint Secretariat**  
*Secrétariat Conjoint CISRI-OIAU*

<https://www.cisri.org>  
<https://www.iemo.int>  
<https://baid.international>



## 8.5.2 Information Incorporated by Reference into a Digital Certificate

CISRI-IEMO-BAID incorporates by reference the following information in every digital certificate it issues:

- Terms and conditions of the CISRI-IEMO-BAID CPS.
- Any other applicable certificate policy as may be stated on an issued CISRI-IEMO Joint Secretariat certificate.
- The mandatory elements of the standard X.509.
- Any non-mandatory but customized elements of the standard X.509.
- Content of extensions and enhanced naming that are not fully expressed within a certificate.
- Any other information that is indicated to be so in a field of a certificate.

## 8.5.3 Pointers to Incorporate by Reference

To incorporate information by reference CISRI-IEMO Joint Secretariat uses computer-based and text-based pointers. CISRI-IEMO Joint Secretariat may use URLs, OIDs etc.





**CISRI**

Collaborative Inter-governmental Scientific Research Institute



**IEMO**

International Emergency Management Organization



**BAID**

Bank for International Development

---

## 8.6 Disclaimers of Warranties

This section includes disclaimers of express warranties.

### 8.6.1 Limitation for Other Warranties

CISRI-IEMO-BAID does not warrant:

- The accuracy of any unverifiable piece of information contained in certificates.
- The accuracy, authenticity, completeness or fitness of any information contained in, free, test or demo certificates.

### 8.6.2 Exclusion of Certain Elements of Damages

In no event is CISRI-IEMO-BAID liable for:

- Any loss of profits.
- Any loss of data.
- Any indirect, consequential or punitive damages arising from or in connection with the use, delivery, license, and performance or non-performance of certificates or digital signatures.
- Any transactions or services offered or within the framework of this CPS.



Document ID: CRT-CPS\_1.0  
URL: <https://baid.international/CPS>  
Date: 26/05/21

Certification Practice Statement  
Version v1.0

**CISRI-IEMO Joint Secretariat**  
*Secrétariat Conjoint CISRI-OIAU*

<https://www.cisri.org>  
<https://www.iemo.int>  
<https://baid.international>





- 
- Any other damages except for those due to reliance on the verified information in a certificate, except for information featured on, free, test or demo certificates.
  - Any liability incurred in any case if the error in such verified information is the result of fraud or wilful misconduct of the applicant.

## 8.7 Indemnities

This section contains the applicable indemnities.

To the extent permitted by law, the subscriber agrees to indemnify and hold CISRI-IEMO-BAID harmless from any acts or omissions resulting in liability, any loss or damage, and any suits and expenses of any kind, including reasonable attorneys' fees that CISRI-IEMO Joint Secretariat may incur as a result of:

- Failure to protect the subscriber's private key,
- Use a trustworthy system as required
- Taking precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorized use of the subscriber's private key
- Attend to the integrity of the managed Branded Root.





**CISRI**

Collaborative Inter-governmental Scientific Research Institute



**IEMO**

International Emergency Management Organization



**BAID**

Bank for International Development

---

## 8.8 Term and Termination

This CPS remains in force until notice of the opposite is communicated by CISRI-IEMO-BAID on its web site or repository.

Notified changes are appropriately marked by an indicated version. Following publications, changes become applicable 30 days thereafter.

## 8.9 Individual Notices and Communications with Participants

CISRI-IEMO-BAID accepts notices related to this CPS by means of digitally signed messages or in paper form. Upon receipt of a valid, digitally signed acknowledgment of receipt from CISRI-IEMO-BAID the sender of the notice deems its communication effective. The sender must receive such acknowledgment within twenty (20) business days, or else written notice must then be sent in paper form through a courier service that confirms delivery or via certified or registered mail, postage prepaid, return receipt requested, addressed as follows. Individuals communications made to CISRI-IEMO-BAID must be addressed to [certs@baid.international](mailto:certs@baid.international) or by post to the CISRI-IEMO Joint Secretariat in the address mentioned in the introduction of this document.



Document ID: CRT-CPS\_1.0  
URL: <https://baid.international/CPS>  
Date: 26/05/21

Certification Practice Statement  
Version v1.0

**CISRI-IEMO Joint Secretariat**  
*Secrétariat Conjoint CISRI-OIAU*

<https://www.cisri.org>  
<https://www.iemo.int>  
<https://baid.international>



## 8.10 Amendments

Changes to this CPS are indicated by appropriate numbering.

## 8.11 Dispute Resolution Procedures

Before resorting to any dispute resolution mechanism including adjudication or any type of Alternative Dispute Resolution (including without exception mini-trial, arbitration, binding expert's advice, co-operation monitoring and normal expert's advice) parties agree to notify CISRI-IEMO-BAID of the dispute with a view to seek dispute resolution.

Upon receipt of a Dispute Notice, CISRI-IEMO-BAID convenes a Dispute Committee that advises CISRI-IEMO Joint Secretariat management on how to proceed with the dispute. The Dispute Committee convenes within twenty (20) business days from receipt of a Dispute Notice. The Dispute Committee is composed by a counsel, a member of CISRI-IEMO-BAID operational management and a security officer. The counsel or data protection officer chair the meeting. In its resolutions the Dispute Committee proposes a settlement to CISRI-IEMO-BAID executive management. CISRI-IEMO-BAID executive management may subsequently communicate the proposed settlement to the resting party.





**CISRI**

Collaborative Inter-governmental Scientific Research Institute



**IEMO**

International Emergency Management Organization



**BAID**

Bank for International Development

---

## 8.12 Governing Law

This CPS is governed, construed and interpreted in accordance with the International Law . This choice of law is made to ensure uniform interpretation of this CPS, regardless of the place of residence or place of use of CISRI-IEMO Joint Secretariat certificates or other products and services. The International Law apply to all CISRI-IEMO-BAID commercial or contractual relationships in which this CPS may apply or quoted implicitly or explicitly in relation to CISRI-IEMO-BAID products and services where CISRI-IEMO-BAID acts as a provider, supplier, beneficiary receiver or otherwise.

## 8.13 Compliance with Applicable Law

CISRI-IEMO-BAID complies with the International Law, as result of their intergovernmental nature, sanctioned by the United Nations Treaty Series UNTS nos. A-37542, I-42766



Document ID: CRT-CPS\_1.0  
URL: <https://baid.international/CPS>  
Date: 26/05/21

Certification Practice Statement  
Version v1.0

**CISRI-IEMO Joint Secretariat**  
*Secrétariat Conjoint CISRI-OIAU*

<https://www.cisri.org>  
<https://www.iemo.int>  
<https://baid.international>



## 8.14 Miscellaneous Provisions

All whatsoever instruments certified, authorised or created by means of the CISRI-IEMO BAID Certification Procedure are intended only for legal use, in strict observance with relevant International Rules and Procedures. Any unlawful use of the CISRI-IEMO-BAID Certification renders it void and nullified. CISRI-IEMO-BAID decline whatsoever responsibility for improper use. The Certificates are considered to be Non returnable, non amendable and non duplicable. Renewal and Transfer upon agreement.

### 8.14.1 Survival

The obligations and restrictions contained under section 8 Other Business and Legal Matters survive the termination of this CPS.

### 8.14.2 Severability

If any provision of this CPS, including limitation of liability clauses, is found to be invalid or unenforceable, the remainder of this CPS should be interpreted in such manner as to effect the original intention of the parties.





**CISRI**

Collaborative Inter-governmental Scientific Research Institute



**IEMO**

International Emergency Management Organization



**BAID**

Bank for International Development

---

## 9. List of definitions

**ACCEPT (A CERTIFICATE)** To approve of a digital certificate by a certificate applicant within a transactional framework.

**ACCREDITATION** A formal declaration by an approving authority that a certain function/entity meets specific formal requirements

**APPLICATION FOR A CERTIFICATE** A request sent by a certificate applicant to a CA to issue a digital certificate

**APPLICATION SOFTWARE VENDOR:** A developer of Internet browser software or other software that displays or uses certificates and distributes root certificates, such as KDE, Microsoft Corporation, Mozilla Corporation, Opera Software ASA, and Red Hat, Inc.

**ARCHIVE** To store records for period of time for purposes such as security, backup, or audit.

**ASSURANCES** A set of statements or conduct aiming at conveying a general intention.

**AUDIT** Procedure used to validate compliance with formal criteria or controls.

**AUTHENTICATION** A process used to confirm the identity of a person or to prove the integrity of specific information by placing them within the right context and verifying such relationship.

**AUTHORISATION** Granting of rights.

**AVAILABILITY** The rate of accessibility of information or resources.

**CERTIFICATE** The public key of a subject and the associated information, digitally signed with the private key of the issuer of the certificate. Unless explicitly specified, the certificates described here are the subscriber's certificates .

**CERTIFICATE REVOCATION LIST OR CRL** A list maintained by the CA of certificates that are revoked before their expiration time.

**CERTIFICATION AUTHORITY OR CA** An entity that is trusted to associate a public key to the information on the subject, contained in the certificate. Unless explicitly specified, the CA described herein is the CISRI-IEMO-BAID.

**CERTIFICATION PRACTICE STATEMENT OR CPS** A statement of the practices in the management of certificates during all life phases.



Document ID: CRT-CPS\_1.0  
URL: <https://baid.international/CPS>  
Date: 26/05/21

Certification Practice Statement  
Version v1.0

**CISRI-IEMO Joint Secretariat**  
*Secrétariat Conjoint CISRI-OIAU*

<https://www.cisri.org>  
<https://www.iemo.int>  
<https://baid.international>



**CERTIFICATE CHAIN** A hierarchical list certificates containing a subscriber certificate and CA certificates.

**CERTIFICATE EXPIRATION** The end of the validity period of a digital certificate.

**CERTIFICATE EXTENSION** A field in the digital certificate used to convey additional information on issues that include: the public key, the certified subscriber, the certificate issuer, and/or the certification process.

**CERTIFICATE HIERARCHY** A level based sequence of certificates of one (root) CA and subordinate entities that include, CAs and subscribers. CERTIFICATE MANAGEMENT Actions associated with certificate management include storage, dissemination, publication, revocation, and suspension of certificates.

**CERTIFICATE REVOCATION LIST (CRL)** A list issued and digitally signed by a CA that includes revoked and suspended certificates. Such list is to be consulted by relying parties at all times prior to relying on information featured in a certificate.

**CERTIFICATE SERIAL NUMBER A** sequential number that uniquely identifies a certificate within the domain of a CA.

**CERTIFICATE SIGNING REQUEST (CSR)** A machine-readable application form to request a digital certificate.

**CERTIFICATION** The process to issue a digital certificate.

**CERTIFICATION AUTHORITY (CA)** An authority, such as CISRI-IEMO-BAID that issues, suspends, or revokes a digital certificate.

**CERTIFICATE POLICY (CP)** A statement of the practices of a CA and the conditions of issuance, suspension, revocation etc. of a CA certificate.

**CERTIFICATE ISSUANCE** Delivery of X.509 v3 digital certificates.

**CERTIFICATE SUSPENSION** Online service used to temporarily disable a digital certificate and to automatically revoke it if no request for re-activating it is submitted within a certain time period

**CERTIFICATE REVOCATION** Online service used to permanently disable a digital certificate before its expiration date

**CERTIFICATE REVOCATION LISTS** Online publication of complete and incremental digital certificates revocation lists compliant with RFC 2459

**COMMERCIAL REASONABLENESS** A legal term from Common Law. In electronic commerce it means the usage of technology that provide reasonable assurance of trustworthiness.

**COMPROMISE** A violation of a security policy that results in loss of control over sensitive information.

**CONFIDENTIALITY** The condition to disclose data to selected and authorized parties only.

**CONFIRM A CERTIFICATE CHAIN** To validate a certificate chain in order to validate an end-user subscriber certificate.

**DIGITAL CERTIFICATE** A formatted piece of data that relates an identified subject with a public key the subject uses.

**DIGITAL SIGNATURE** To encode a message by using an asymmetric cryptosystem and a hash function such that a person having the initial message and the signer's public key can accurately determine whether the transformation was





CISRI

Collaborative Inter-governmental Scientific Research Institute



IEMO

International Emergency Management Organization



BAID

Bank for International Development

---

created using the private key that corresponds to the signer's public key and whether the initial message has been altered since the transformation was made.

**DISTINGUISHED NAME** A set of data that identifies a real-world entity, such as a person in a computer-based context.

**DIRECTORY SERVICE** Online publication of certificates allowing the retrieval of a certificate based on its certificate identifier.

**END-USER SUBSCRIBER** A subscriber other than another CA.

**EXTENSIONS** Extension fields in X.509 v.3.0 certificates.

**GENERATE A KEY PAIR** A trustworthy process to create private keys during certificate application whose corresponding public key are submitted to the applicable CA during certificate application in a manner that demonstrates the applicant's capacity to use the private key.

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

**HASH** An algorithm that maps or translates one set of bits into another (generally smaller) set in such a way that:

- A message yields the same result every time the algorithm is executed using the same message as input.
- It is computationally infeasible for a message to be derived or reconstituted from the result produced by the algorithm.
- It is computationally infeasible to find two different messages that produce the same hash result using the same algorithm.

**IDENTIFICATION** The process to confirm the identity of an entity. Identification is facilitated in public key cryptography by means of certificates.

**INCORPORATE BY REFERENCE** To make one document a part of another by identifying the document to be incorporated, with information that allows the recipient to access and obtain the incorporated message in its entirety, and by expressing the intention that it be part of the incorporating message. Such an incorporated message shall have the same effect as if it had been fully stated in the message.

**KEY GENERATION PROCESS** The trustworthy process of creating a private/public key pair. The public key is supplied to a CA during the certificate application process.

**KEY PAIR** A private key and its corresponding public key in asymmetric encryption.

**NOTICE** The result of notification to parties involved in receiving CA services in accordance with this CPS.

**NOTIFY** To communicate specific information to another person as required by this CPS and applicable law.

**OBJECT IDENTIFIER** A sequence of integer components that can be assigned to a registered object and that has the property of being unique among all object identifiers within a specific domain.

**PKI HIERARCHY** A set of CAs whose functions are organized according to the principle of delegation of authority and related to each other as subordinate and superior CA.



Document ID: CRT-CPS\_1.0  
URL: <https://baid.international/CPS>  
Date: 26/05/21

Certification Practice Statement  
Version v1.0

CISRI-IEMO Joint Secretariat  
*Secrétariat Conjoint CISRI-OIAU*

<https://www.cisri.org>  
<https://www.iemo.int>  
<https://baid.international>





**PRIVATE KEY** A mathematical key to create digital signatures and sometimes (depending upon the algorithm) to decrypt messages in combination with the corresponding public key.

**PUBLIC KEY** A mathematical key that can be made publicly available that is used to verify signatures created with its corresponding private key. Depending on the algorithm, public keys can also be used to encrypt messages or files which can then be decrypted with the corresponding private key.

**PUBLIC KEY CRYPTOGRAPHY** Cryptography that uses a key pair of mathematically related cryptographic keys.

**PUBLIC KEY INFRASTRUCTURE (PKI)** The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a certificate-based public key cryptographic system.

**REGISTERED AGENT** An individual or entity that is both authorized by the Applicant to receive service of process and business communications on behalf of the Applicant; and listed in the official records of the Applicant's Jurisdiction of Incorporation as acting in the role specified in (a) above.

**REGISTERED OFFICE** The official address of a company, as recorded with the Incorporating Agency, to which official documents are sent and legal notices received.

**REGISTRATION NUMBER** The unique number assigned to the Private organization Applicant or Subject entity by the Incorporating Agency in such entity's Jurisdiction of Incorporation.

**REGISTRATION AUTHORITY OR RA** An entity that has the responsibility to identify and authenticate subscribers. The RA does not issue certificates. It merely requests the issuance of a certificate on behalf of applicants whose identity it has verified.

**RELIANCE** To accept a digital signature and act in a way that shows trust in it.

**RELYING PARTY** Any entity that relies on a certificate for carrying out any action.

**REPOSITORY** A database and/or directory listing digital certificates and other relevant information accessible on-line.

**REVOKE A CERTIFICATE** To permanently end the operational period of a certificate from a specified time forward.

**SECRET SHARE** A portion of a cryptographic secret that has been divided among a number of physical tokens, such as smart cards etc.

**SECRET SHARE HOLDER** A person that holds a secret share.

**SIGNATURE** A method that is used or adopted by a document originator to identify himself or herself, which is either accepted by the recipient or its use is customary under the circumstances.

**SIGNER** A person who creates a digital signature for a message, or a signature for a document.

**SMART CARD** A hardware token that contains a chip to implement among others cryptographic functions.

**STATUS VERIFICATION** Online service based on the Online Certificate Status Protocol (RFC 2560) used to determine the current status of a digital certificate without requiring CRLs





CISRI

Collaborative Inter-governmental Scientific Research Institute



IEMO

International Emergency Management Organization



BAID

Bank for International Development

---

**SUBJECT OF A DIGITAL CERTIFICATE** The named party to which the public key in a certificate is attributable, as user of the private key corresponding to the public key.

**SUBSCRIBER** The subject of a digital certificate, or a party designated by the subject to apply for the certificate.

**SUBSCRIBER AGREEMENT** The agreement between a subscriber and a CA for the provision of public certification services.

**TRUSTED POSITION** A role within a CA that includes access to or control over cryptographic operations that may allow for privileged access to the issuance, use, suspension, or revocation of certificates, including operations that restrict access to a repository.

**TRUSTWORTHY SYSTEM** Computer hardware, software, and procedures that provide an acceptable level against security risks, provide a reasonable level of availability, reliability, and correct operation and enforce a security policy.

**CISRI-IEMO-BAID PUBLIC CERTIFICATION SERVICES** A digital certification system made available by CISRI-IEMO-BAID as well as the entities that belong to the CISRI-IEMO-BAID domain as described in this CPS.

**CISRI-IEMO-BAID PROCEDURES** A document describing the CISRI-IEMO-BAID's internal procedures with regard to registration of end users, security etc.

**WEB - WORLD WIDE WEB (www)** A graphics based medium for the document publication and retrieval of information on the Internet.

**WRITING** Information accessible and usable for reference.

**X.509** The standard of the ITU-T (International Telecommunications Union-T) for digital certificates.



Document ID: CRT-CPS\_1.0  
URL: <https://baid.international/CPS>  
Date: 26/05/21

Certification Practice Statement  
Version v1.0

CISRI-IEMO Joint Secretariat  
*Secrétariat Conjoint CISRI-OIAU*

<https://www.cisri.org>  
<https://www.iemo.int>  
<https://baid.international>



---

## 10. List of acronyms

**BAID:** Bank for International Development

**CISRI:** Collaborative Inter-governmental Scientific Research Institute

**CA:** Certification Authority

**RA:** Registration Authority

**CP:** Certificate Policy

**CPS:** Certification Practice Statement

**IEMO:** International Emergency Management Organization

**IETF:** Internet Engineering Task Force

**ISO:** International Standards organization

**ITU:** International Telecommunications Union

**PKI:** Public Key Infrastructure

**RFC:** Request for Comments

**SSCD:** Secure Signature Creation Device





**CISRI**

Collaborative Inter-governmental Scientific Research Institute



**IEMO**

International Emergency Management Organization



**BAID**

Bank for International Development

---

The CISRI-IEMO-BAID accept comments regarding this CPS addressed to the address mentioned above in the Introduction of this document.



Document ID: CRT-CPS\_1.0  
URL: <https://baid.international/CPS>  
Date: 26/05/21

Certification Practice Statement  
Version v1.0

**CISRI-IEMO Joint Secretariat**  
*Secrétariat Conjoint CISRI-OIAU*

<https://www.cisri.org>  
<https://www.iemo.int>  
<https://baid.international>