PROGRAMME OF THE EUROPEAN UNION

NAVIGATION MADE IN EUROPE

PKI SYSTEM CERTIFICATE POLICY AND CERTIFICATION PRACTICE STATEMENT FOR ICA-001 (ICA-001 CP/CPS)

Issue 1.1 | January 2024

#EUSpace

TERMS OF USE AND DISCLAIMERS

Authorised Use and Scope of Use

This Certificate Policy and Certification Practice Statement for the EUSPA OSNMA ICA-001 infrastructure (hereinafter referred to as CPS EUSPA OSNMA ICA-001 or CPS) and the information contained herein is made available to the public by the European Union (hereinafter referred to as Publishing Authority) for information, standardisation, research and development and commercial purposes for the benefit and the promotion of the European Global Navigation Satellite Systems programmes (European GNSS Programmes) and according to terms and conditions specified thereafter.

General Disclaimer of Liability

With respect to the CPS EUSPA OSNMA ICA-001 and any information contained in the CPS EUSPA OSNMA ICA-001, neither the EU as the Publishing Authority nor the generator of such information make any warranty, express or implied, including the warranty of fitness for a particular purpose, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information hereby disclosed or for any product developed based on this information, or represents that the use of this information would not cause damages or would not infringe any intellectual property rights. No liability is hereby assumed for any direct, indirect, incidental, special or consequential damages, including but not limited to, damages for interruption of business, loss of profits, goodwill or other intangible losses, resulting from the use of the CPS EUSPA OSNMA ICA-001 or of the information contained herein. Liability is excluded as well for consequences of the use and / or abuse of the CPS EUSPA OSNMA ICA-001 or the information contained herein.

Copyright

The CPS EUSPA OSNMA ICA-001 is protected by copyright which belongs to the European Union. Any alteration or translation in any language of the CPS EUSPA OSNMA ICA-001 as a whole or parts of it is prohibited unless the Publishing Authority provides a specific written prior permission.

The CPS EUSPA OSNMA ICA-001 may only be partly or wholly reproduced and/or transmitted to a third party in accordance with the herein described permitted use and under the following conditions: the present “Terms of Use and Disclaimers”, are accepted, reproduced and transmitted entirely and unmodified together with the reproduced and/or transmitted information; the copyright notice “© European Union 2024” is not removed from any page.

Miscellaneous

No failure or delay in exercising any right in relation to the CPS EUSPA OSNMA ICA-001 or the information contained therein shall operate as a waiver thereof, nor shall any single or partial exercise preclude any other or further exercise of such rights. The disclaimers contained in this document apply to the extent permitted by applicable law.

Reference is made in this CPS EUSPA OSNMA ICA-001 to documents, standards or other information from third parties, in particular the ETSI. The use of these documents, standards or other information is under the sole responsibility of the users and such use may be subject to terms and conditions determined by these third parties.

Updates

The CPS EUSPA OSNMA ICA-001 could be subject to modification, update and variations.

The publication of updates will be subject to the same terms as stated herein unless otherwise evidenced.

Although the Publishing Authority will deploy its efforts to give notice to the public for further updates of CPS EUSPA OSNMA ICA-001, it does not assume any obligation to advise on further developments and updates of the CPS EUSPA OSNMA ICA-001, nor to take into account any inputs, comments proposed by interested persons or entities, involved in the updating process.

DOCUMENT CHANGE RECORD

REASON FOR CHANGE	ISSUE	REVISION	DATE
First public version of the document	1	0	August 2023
Version provided in the view of the OSNMA initial service declaration	1	1	January 2024

FOREWORD

This Certificate Policy and Certification Practice Statement for the Galileo Open Service Navigation Message Authentication (OSNMA) Issuing Certification Authority (ICA) 001 infrastructure (hereinafter referred to as CPS ICA-001 or CPS) details the certification policy and practices that EUSPA applies for the issuance of digital certificates by the EUSPA OSNMA ICA-001 infrastructure for End Entities (EE).

The structure and content of the CPS EUSPA OSNMA ICA-001 are compliant with [RD-3], [RD-4] and [RD-5].

The EUSPA OSNMA ICA-001 infrastructure is classified and most of the organisational, technical and process details are only delivered on a need-to-know basis and in compliance with applicable regulations ([RD-8]).

TABLE OF CONTENTS

1 INTRODUCTION 8
1.1 Overview 8
1.2 Document identification 8
1.2.1 Reference documents 8
1.3 PKI participants 8
1.3.1 Certification authorities 8
1.3.2 Registration authority 9
1.3.3 Subscribers 9
1.3.4 Relying parties 9
1.3.5 Other participants 9
1.4 Certificate usage 10
1.4.1 Appropriate certificate uses 10
1.4.2 Prohibited certificate uses 10
1.5 Policy administration 11
1.5.1 Organization administering the document 11
1.5.2 Point of contact 11
1.5.3 Entity determining CPS suitability for the policy 11
1.5.4 CPS approval procedures 11
1.6 Acronyms, Abbreviations and Definitions 12
2 PUBLICATION AND REPOSITORY RESPONSIBILITIES 14
2.1 Repositories 14
2.1.1 EUSPA Web Portal 14
2.1.2 GSC Web Portal 15
2.2 Publication of certification information 15
2.3 Time or frequency of publication 15
2.4 Access controls on repositories 15
3 IDENTIFICATION AND AUTHENTICATION 16
3.1 Naming 16
3.1.1 Types of names 16
3.1.2 Need for names to be meaningful 16
3.1.3 Anonymity or pseudo anonymity of subscribers 16
3.1.4 Rules for interpreting various name forms 16
3.1.5 Uniqueness of names 16
3.1.6 Recognition, authentication and role of trademarks 16
3.2 Initial identity validation 17
3.2.1 Method to prove possession of private key 17
3.2.2 Authentication of organization identity 17

3.2.3 Authentication of individual identity 17
3.2.4 Non-verified subscriber information 17
3.2.5 Validation of authority 17
3.2.6 Criteria for interoperation 17
3.3 Identification and authentication for re-key requests 17
3.3.1 Identification and authentication for routine re-key 17
3.3.2 Identification and authentication for re-key after revocation 17
3.4 Identification and authentication for revocation request 17
4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS 18
4.1 Certificate application 18
4.1.1 Who can submit a certificate application 18
4.1.2 Enrolment process and responsibilities 18
4.2 Certificate application processing 18
4.2.1 Performing identification and authentication functions 18
4.2.2 Approval or rejection of certificate applications 18
4.2.3 Time to process certificate applications 18
4.3 Certificate issuance 18
4.3.1 CA actions during certificate issuance 18
4.3.2 Notification to subscriber by the CA of issuance of certificate 18
4.4 Certificate acceptance 19
4.4.1 Conduct constituting certificate acceptance 19
4.4.2 Publication of the certificate by the CA 19
4.4.3 Notification of certificate issuance by the CA to other entities 19
4.5 Key pair and certificate usage 19
4.5.1 Subscriber private key and certificate usage 19
4.5.2 Relying party public key and certificate usage 19
4.6 Certificate renewal 19
4.7 Certificate re-key 19
4.8 Certificate modification 20
4.9 Certificate revocation and suspension 20
4.9.1 Circumstances for revocation 20
4.9.2 Who can request revocation 20
4.9.3 Procedure for revocation request 20
4.9.4 Revocation request grace period 20
4.9.5 Time within which CA must process the revocation request 20
4.9.6 Revocation checking requirements for relying parties 21
4.9.7 CRL issuance frequency 21
4.9.8 Maximum latency for CRLs 21
4.9.9 On-line revocation/status checking availability 21
4.9.10 On-line revocation checking requirements 21
4.9.11 Other forms of revocation advertisements available 21
4.9.12 Special requirements regarding key compromise 21

4.9.13 Circumstances for suspension 21
4.9.14 Who can request suspension 21
4.9.15 Procedure for suspension request 21
4.9.16 Limits on suspension period 22
4.10 Certificate status services 22
4.10.1 Operational characteristics 22
4.10.2 Service availability 22
4.10.3 Optional features 22
4.10.4 End of subscription 22
4.10.5 Key escrow and recovery 22
4.11 CA termination 22
5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS 23
6 TECHNICAL SECURITY CONTROLS 24
6.1 Key pair generation and installation 24
6.1.1 Key pair generation 24
6.1.2 Private key delivery to subscriber 24
6.1.3 Public key delivery to the certificate issuer 24
6.1.4 CA public key delivery to relying parties 24
6.1.5 Key sizes 24
6.1.6 Public keys parameters generation and quality checking 24
6.1.7 Key usage purposes (as per X.509 v3 key usage field) 24
6.2 Private key Protection and Cryptographic Module Engineering Controls 25
6.2.1 Cryptographic module standards and controls 25
6.2.2 Private key (n out of m) multi-person control 25
6.2.3 Private key escrow 25
6.2.4 Private key backup 25
6.2.5 Private key archival 25
6.2.6 Private key transfer into or from a cryptographic module 25
6.2.7 Private key storage on cryptographic module 25
6.2.8 Method of activating the private key 25
6.2.9 Method of deactivating private key 25
6.2.10 Method of destroying private key 25
6.2.11 Cryptographic Module Rating 25
6.3 Other aspects of key pair management 26
6.3.1 Public key archival 26
6.3.2 Certificate operational periods and key pair usage periods 26
6.4 Activation data 26
6.5 Computer security controls 26
6.6 Life cycle technical controls 26
6.6.1 System development controls 26
6.6.2 Security Management Controls 26

6.6.3 Life cycle security controls 26
6.7 Network security controls 27
6.8 Time stamping 27
7 CERTIFICATE AND CRL PROFILES 28
8 OCSP PROFILE 29
9 COMPLIANCE AUDIT AND OTHER ASSESSMENTS 30
9.1 Frequency or circumstances of assessment 30
9.2 Identity/qualifications of assessor 30
9.3 Topics covered by assessment 30
10 OTHER BUSINESS AND LEGAL MATTERS 31
10.1 Fees 31
10.1.1 Certificate issuance and renewal fees 31
10.1.2 Certificate access fees 31
10.1.3 Revocation or status information access fees 31
10.1.4 Fees for other services 31
10.1.5 Refund policy 31
10.2 Financial responsibility and limited liability 31
10.2.1 Insurance coverage 31
10.2.2 Other assets 31
10.2.3 Insurance or warranty coverage for end-entities 31
10.3 Confidentiality of business information 31
10.4 Privacy of personal information 32
10.4.1 Privacy Plan 32
10.4.2 Information Treated as Private 32
10.4.3 Information not Deemed Private 32
10.4.4 Responsibility to Protect Private Information 32
10.4.5 Notice and Consent to use Private Information 32
10.4.6 Disclosure Pursuant to Judicial or Administrative Process 32
10.4.7 Other Information Disclosure Circumstances 32
10.5 Intellectual Property Rights 32
10.6 Representations and warranties 32
10.6.1 CA representations and warranties 33
10.6.2 RA representations and warranties 33
10.6.3 Subscriber representations and warranties 33
10.6.4 Relying Party representations and warranties 33
10.6.5 Representations and warranties of other participants 33
10.7 Disclaimers of warranties 33
10.8 Limitations of liability 33
10.9 Indemnities 33
10.10 Term and termination 33

10.10.1 Term 33
10.10.2 Termination 33
10.10.3 Effect of termination and survival 34
10.11 Individual notices and communications with participants 34
10.12 Amendments 34
10.12.1 Procedure for amendment 34
10.12.2 Notification mechanism and period 34
10.12.3 Circumstances under which OID must be changed 34
10.13 Dispute resolution provisions 34
10.14 Governing law 34
10.15 Compliance with applicable law 34
10.16 Miscellaneous provisions 34
10.17 Other provisions 35
11 LIST OF REFERENCES 36

LIST OF TABLES

Table 1 - Organization administering the document 11
Table 2 - Point of contact 11
Table 3 - Entity determining CPS suitability for the policy 11
Table 4 - Acronyms and abbreviations 12
Table 5 – Key periods 26

LIST OF FIGURES

Figure 1: Certification Authority chain overview 9

1 INTRODUCTION

1.1 Overview

EUSPA, Certificate Authorities and associated Relying Parties' operation depend on the CPS EUSPA OSNMA ICA-001 for the issuance of digital certificates to End Entities. Also, this document describes the general rules for providing certificate services such as: registration, public key certification, key and certificates rekey and certificate revocation.

In this version of the document the EUSPA OSNMA ICA-001 certificates are provided in the view of the OSNMA service provision phase.

1.2 Document identification

This document is identified by EUSPA OSNMA ICA Policy 1 = {EUSPA}.1.1.1=1.3.6.1.4.1.60049.1.1.1, with:

- EUSPA RCA Policy 1 = {EUSPA}.1=1.3.6.1.4.1.60049.1
- GALILEO SCA Policy 1 = {EUSPA}.1.1=1.3.6.1.4.1.60049.1.1

The digital version of this document is available in the following repositories:

- HTTPS repository at https://www.gsc-europa.eu/gsc-products/OSNMA/PKI/ (please see [RD-2] for further details).

1.2.1 Reference documents

Please refer to chapter 11.

1.3 PKI participants

The CPS EUSPA OSNMA ICA-001 regulates the most important relations between entities belonging to EUSPA, advisory teams (including auditors) and customers (users of the services provided):

- Certification Authorities.
- Subscribers.
- Relying parties.
- Communication team for the repositories (§1.2).
- Relevant suppliers for EUSPA regarding issuance and management of digital certificates.
- Auditors.

Note: PKI administration contact is given in §1.5.2.

1.3.1 Certification authorities

EUSPA OSNMA ICA-001 is an Issuing Certification Authority part of the following hierarchy as shown in Figure 1:

- EUSPA Root CA.
- GALILEO Sub CA.
- OSNMA Issuing CA.

The EUSPA OSNMA ICA-001 can issue certificates only to End Entities that belong to the OSNMA domain with two possible entities:

⇨ External End Entity: certificates that are useful for users receivers only:
  - EUSPA OSNMA EE PKR.

- EUSPA OSNMA EE MERKLE TREE.

⇨ Internal End Entity: certificates that are useful for the EUSPA OSNMA ICA-001 infrastructure only:

- EUSPA OSNMA EE CMS.
- EUSPA OSNMA EE EGEP.

As a first step, the End Entity certificates are requested by the OSNMA EE system to the EUSPA OSNMA ICA-001 (see also the procedures described in §4.3).

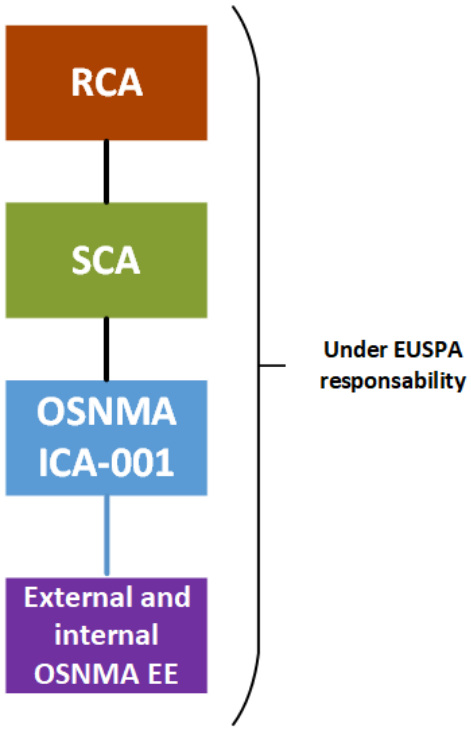

Figure 1: Certification Authority chain overview

1.3.2 Registration authority

There is no registration authority for this CA. Only EUSPA and EUSPA contracted/authorised operators can request and issue End Entity certificates only for the defined and specific needs of the OSNMA service provision.

1.3.3 Subscribers

The PKI subscriber is EUSPA.

1.3.4 Relying parties

A relying party is an entity that uses the ICA certificate. The digital signature of this certificate has to be controlled in order to insure the confidentiality, integrity and authenticity of the data exchanged relying on this certificate.

1.3.5 Other participants

EUSPA OSNMA ICA-001 and OSNMA EE system are operated by EUSPA and EUSPA contracted/authorised operators.

These entities may audit the EUSPA OSNMA ICA-001 and the OSNMA EE system:

- National Authorities.
- Independent audit team (e.g.: Security Accreditation Board tasks an audit team).

1.4 Certificate usage

The certificate policy defines the purpose for which a certificate may be used. This is defined by two elements:

- The certificate applicability (for example: electronic signature, confidentiality).
- A description of the allowed and prohibited applications.

1.4.1 Appropriate certificate uses

EUSPA OSNMA ICA-001 can issue certificates only to OSNMA EE system that can only sign data related to the provision of the OSNMA service.

1.4.2 Prohibited certificate uses

All certificate usages not listed in §1.4.1 are prohibited.

1.5 Policy administration

1.5.1 Organization administering the document

Table 1 - Organization administering the document

Name	European Union Agency for the Space Programme (EUSPA) Office: Janovského 438/2 170 00 Prague 7 – Holesovice Czech Republic
e-mail	helpdesk@gsc-europa.eu
Web	https://www.gsc-europa.eu/

1.5.2 Point of contact

Table 2 - Point of contact

Name	GSC Helpdesk
e-mail	helpdesk@gsc-europa.eu

Contact person should also be used for any concern about the certificate (e.g.: revocation §4.9.3).

1.5.3 Entity determining CPS suitability for the policy

Table 3 - Entity determining CPS suitability for the policy

Name	GSC Helpdesk
e-mail	helpdesk@gsc-europa.eu
Web	https://www.gsc-europa.eu/

1.5.4 CPS approval procedures

The document change procedure is under the responsibility of the PKI Project Manager.

Document changes are approved by internal EUSPA boards before being published online..

1.6 Acronyms, Abbreviations and Definitions

Table 4 - Acronyms and abbreviations

Abbreviation	Definition
{EUSPA}	EUSPA base OID=1.3.6.1.4.1.60049
BSI	Bundesamt für Sicherheit in der Informationstechnik
CA	Certificationion Authority
CMS	Cryptographic Message Syntax
CN	Common Name
CP	Certification Policy
CPS	Certification Practice Statement: Statement of the practices which a Certification Authority employs in issuing managing, revoking, and renewing or re-keying certificates
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DN	Distinguished Name
EC	European Commission
ECSS	European Cooperation for Space Standardization
EE	End Entity with two possible activities:: ⇨ External End Entity:: certificate that are useful for users receivers only ⇨ Internal End Entity:: certificate that are useful for the EUSPA OSNMA ICA-001 infrastructure only.
EGEP	Extended GSC Encryption Protocol
ETSI	European Telecommunications Standards Institute
EU	European Union
EUCI	EU classified information
EUSPA	European Union Space Programme Agency
GNSS	Global Navigation Satellite System (e.g. GPS, Galileo, GLONASS etc.)
HSM	Hardware Security Module
ICA	Issuing Certificate Authority
LACP	List of Approved Cryptographic Products

Abbreviation	Definition
NAGU	Notice Advisory to Galileo Users
NAV	Navigation
OID	Object identifier Alphanumeric / numeric identifier registered in accordance with the ISO/IEC 9834 standard and uniquely describing a specified object or its class
PKI	Public Key Infrastructure
RCA	Root Certificate Authority
SCA	Subordinate Certificate Authority
SDD	Service Definition Document
SIS	Signal In Space
VS-NfD	VerSchlusssache-Nur für Dienstgebrauch

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

The status of certificates (new certificates, CRL updates) will be announced on the Web Portal and sent by email to registered users via e-mail, consenting to such notification and on the GSC Web Portal.

The repositories are available online:

- EUSPA Web Portal (public): https://www.euspa.europa.eu/about/how-we-work/pki

  Note: only for RCA and SCA elements.
- GSC Web Portal (only for registered users):
  - HTTPS repository: https://www.gsc-europa.eu/gsc-products/OSNMA/PKI/
  - SFTP repository:
    - Hostname: osnma.gsc-europa.eu
    - Port: 2222
    - Directory: /OSNMA_PublicKey/Applicable/

The content of the SFTP directory is described in [RD-2].

EUSPA and EUSPA contracted/authorised organisations:

- Make all necessary efforts to ensure that all certificates published in the repositories belong to EUSPA.
- Ensure that the certificates of Certification Authorities belong to each domain and that the certificates are published on time.
- Ensure the publishing of the CPS.
- Provide access to information about the certificate status by publishing Certificate Revocation Lists (CRL) for instance through an HTTP service.
- Secure constant access to information in the repositories.
- Ensure secured and controlled access to repositories.
- Make all necessary efforts to ensure that all personal information are treated according to the GDPR.

2.1.1 EUSPA Web Portal

The following elements are available in the EUSPA Web Portal:

1. All required elements to trust the RCA (i.e.: RCA certificate, RCA CRL and RCA CPS).
2. All required elements to trust the SCA (i.e.: SCA certificate, SCA CRL and SCA CPS).

   Note: For the sake service continuity, when renewing a certificate, active and future certificates and the CRL can be present in the repositories as described in [RD-2].

2.1.2 GSC Web Portal

The following elements are available in the GSC Web Portal:

1. All required elements to trust the ICA (i.e.: ICA certificate, ICA CRL and ICA CPS).
2. All required elements needed by relying parties to authenticate NAV messages and described in [RD-2].

Notes:

- Besides the repositories, OSNMA elements needed to authenticate NAV messages will also be transmitted periodically through the SIS, see [RD-1] (e.g.: active Public Key).
- For the sake of service continuity, when renewing a certificate, active and future certificates and the CRL may be present in repositories as described in [RD-2].

2.2 Publication of certification information

Online repositories providing the CPS, issued certificates, CRL and any other elements necessary to authenticate navigation messages are always available.

2.3 Time or frequency of publication

The information published in repositories is updated following specific events like:

- CPS updates.
- After issuing a new certificate.
- CRL is updated either periodically or when a certificate is revoked.
- Fixing of non-conformities found by audits.
- Additional information – after every update.

2.4 Access controls on repositories

All information published in relation with the EUSPA OSNMA ICA-001 is available in the GSC Web portal.

Logical and physical protection measures are implemented to protect against unauthorised addition, deletion or modification of data published in the GSC repositories.

Relying parties have read-only access via Internet to the GSC repositories.

In case of voluntary or involuntary alteration or compromise of information in GSC repositories, appropriate actions will be taken to re-establish the repositories' data integrity. Actions (if appropriate) will be taken against those responsible for these acts. The affected relying parties will be notified.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

The structure and use of names in certificates comply with [RD-6].

3.1.1 Types of names

Certificates generated by EUSPA OSNMA ICA-001 for EE are compliant with the X.509 v3 standard [RD-6] . Basic names of the Subjects and of the certificate issuers placed in EUSPA's certificates are in compliance with the Distinguished Names – DN, created following X.500 [RD-13] and X.520 [RD-14] recommendations.

3.1.2 Need for names to be meaningful

The names used in certificates are chosen so that:

- It is clear that the certificate issued is an EE certificate (not a CA certificate).
- The usage of the End Entity certificate is clear.

The names of End Entities certificates should be compliant with:

- commonName: An official unique identifier of the End Entity (as formatted in ETSI EN 319 412-1 [RD-15]).
- organizationName: EUSPA as it is the official registered name of the Subscribing CA as a corporation or organization.
- countryName: ES as it is the two-letter ISO 3166-1 country code for the country in which the EE is located.

3.1.3 Anonymity or pseudo anonymity of subscribers

The subscribers shall not be anonymous or pseudo anonymous.

3.1.4 Rules for interpreting various name forms

The interpretation of the fields within the certificates issued by EUSPA is done in accordance with the certificate profiles described in Certificates and CRLs profiles presented in §7 of this document. The creation and interpretation of the DN shall be performed according to the recommendations from § 3.1.2 of this document.

3.1.5 Uniqueness of names

The CN (and therefore the DN) must be unique for all certificates issued by the EUSPA OSNMA ICA-001.

3.1.6 Recognition, authentication and role of trademarks

Not applicable

3.2 Initial identity validation

3.2.1 Method to prove possession of private key

Possession of the private key is controlled by verifying the digital signature of the CSR (certificate signing request).

3.2.2 Authentication of organization identity

EUSPA OSNMA ICA-001 is the third tier Certification Authority of the EUSPA domain: its identity should be verified and authenticated regarding the chain of trust (with SCA and RCA certificates).

Only EUSPA and EUSPA contracted/authorised operators can operate the EUSPA OSNMA ICA-001 on behalf of EUSPA.

3.2.3 Authentication of individual identity

Authentication is done using only EUSPA and EUSPA contracted/authorised operators' credentials.

3.2.4 Non-verified subscriber information

The EUSPA PKI doesn't include unverified subject information in certificates.

3.2.5 Validation of authority

Each received certificate authority shall be verified through chain of trust.

3.2.6 Criteria for interoperation

Not applicable.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

Same identification and authentication will be used as per section 3.2.3.

3.3.2 Identification and authentication for re-key after revocation

Same identification and authentication will be used as per section 3.2.3.

3.4 Identification and authentication for revocation request

Same identification and authentication will be used as per section 3.2.3.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

This chapter describes the basic procedures that apply to all types of certificates issued directly by EUSPA OSNMA ICA-001.

4.1 Certificate application

4.1.1 Who can submit a certificate application

Only EUSPA and EUSPA contracted/authorised operators can request a certificate from the EUSPA OSNMA ICA-001.

4.1.2 Enrolment process and responsibilities

The enrolment process is performed according to internal procedures.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

Identification and authentication functions are done by trusted roles associated to EUSPA OSNMA ICA-001.

4.2.2 Approval or rejection of certificate applications

Approval or rejection of a certificate application is done according to internal procedures.

4.2.3 Time to process certificate applications

EUSPA and EUSPA contracted/authorised operators are the only persons ensuring the correct provision of the OSNMA service i.e. they manage the EUSPA OSNMA ICA-001 certificate besides the End Entity certificates. In this framework, the time to process End Entity certificate applications is without interest as the requester and the issuer are the same authorised operators.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

After receiving and processing a request, the EUSPA OSNMA ICA-001 issues a certificate. After the certificate is issued, EUSPA and EUSPA contracted/authorised operators will publish the certificate in the GSC repositories if necessary.

4.3.2 Notification to subscriber by the CA of issuance of certificate

Not applicable as the EUSPA OSNMA ICA-001 and the OSNMA EE system are operated by the same authorised operators.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

Acceptance of a certificate is done according to internal procedures.

4.4.2 Publication of the certificate by the CA

See §2 of the present document.

4.4.3 Notification of certificate issuance by the CA to other entities

Issued certificates are published in GSC repositories if needed.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

The private keys are protected (as described in §6) from access by unauthorised personnel or other third parties.

The private keys are used only in accordance with the usages specified in the key usage extension as stated in §1.4.1 and described in [RD-2].

4.5.2 Relying party public key and certificate usage

All user receiver software must be compliant with X.509 that enforces the requirements and set forth in this CPS. EUSPA does not warrant that any third party's software will support or enforce such controls or requirements, and all relying parties are advised to seek appropriate technical or legal advice.

Relying Parties shall use the certificates:

- In compliance with their stated purpose in the present CPS and in compliance with the certificate content (field keyUsage),
- Only after certificate validity/status control and validation of chain of trust.

Relying on an unverifiable digital signature may result in risks that the relying party assumes in whole and which EUSPA does not assume any responsibility for any way.

4.6 Certificate renewal

Prior to the expiration of an existing End Entity certificate, it is necessary to request a new certificate to maintain continuity of the OSNMA service provision.

A certificate renewal necessarily implies re-keying (public/private keys renewal or recomputation).

Other certificate attributes will not change between new and old certificates except in exceptional circumstances. For example in case of the use of a new algorithm, a new CPS will be published, in addition to a new certifcate.

Furthermore, if the Sub CA keys are revoked, all EUSPA OSNMA ICA-001 certificates become untrusted and must be renewed again.

4.7 Certificate re-key

See §4.6.

4.8 Certificate modification

No modification is allowed on an existing certificate (e.g.: validity extension): modifications shall be done through certificate renewal.

4.9 Certificate revocation and suspension

Certificates issued by EUSPA OSNMA ICA-001 can be revoked but they are never suspended. Certificate revocation is irreversible.

4.9.1 Circumstances for revocation

The EUSPA OSNMA ICA-001 will revoke End Entity Certificates for instance when:

1. EUSPA and EUSPA contracted/authorised operators obtain evidence that the End Entity's private key has been compromised or no longer complies with the requirements of §6.1.5 and §6.1.6.
2. EUSPA and EUSPA contracted/authorised operators obtain evidence that the EE certificate was misused.
3. EUSPA and EUSPA contracted/authorised operators are made aware that the EE certificate was not issued in accordance with this document.
4. EUSPA and EUSPA contracted/authorised operators determine that any of the information appearing in the EE certificate is inaccurate or misleading.
5. The EUSPA OSNMA ICA-001 or End Entity ceases operations for any reason.
6. The EUSPA OSNMA ICA-001's right to issue EE certificates under these requirements expires or is revoked or terminated, but EUSPA OSNMA ICA-001's right to publish CRL remains.

A compromised private key refers to:

1. Unauthorised access to the private key or a strong reason for suspecting such a thing.
2. Private key loss or occurrence of a reason to suspect such a loss.
3. Stolen private key or occurrence of a reason to suspect such a theft.
4. Accidental deletion of the private key.

4.9.2 Who can request revocation

Revocation can only be performed by EUSPA and EUSPA contracted/authorised operators.

4.9.3 Procedure for revocation request

The End Entity certificates will be revoked by EUSPA and EUSPA contracted/authorised operators who will also publish a new CRL.

4.9.4 Revocation request grace period

As soon as the revocation is decided and taking into account OSNMA service provision management, EUSPA and EUSPA contracted/authorised operators will revoke the certificate without any grace period.

4.9.5 Time within which CA must process the revocation request

Not available.

4.9.6 Revocation checking requirements for relying parties

Relying Parties shall use the repositories to verify the status of a certificate any time before relying on it:

- ICA CRL.
- SCA CRL.
- RCA CRL.

4.9.7 CRL issuance frequency

The CRL is updated and published every year at least. Furthermore, in case of a certificate revocation, a new Certificate Revocation List including the reference to the revoked certificate is generated.

4.9.8 Maximum latency for CRLs

The CRL should be published without delay.

4.9.9 On-line revocation/status checking availability

The provisions given in section 2.3 apply.

4.9.10 On-line revocation checking requirements

The provisions given in section 2.3 apply.

4.9.11 Other forms of revocation advertisements available

Not applicable.

4.9.12 Special requirements regarding key compromise

The End Entity certificate associated to a compromised private key shall be revoked.

By propagation, all cryptographic elements under EUSPA OSNMA ICA-001 (including all end entity certificates) shall be revoked in the case where the EUSPA OSNMA ICA-001 private key is compromised.

4.9.13 Circumstances for suspension

EUSPA and EUSPA contracted/authorised operators don’t suspend certificates.

4.9.14 Who can request suspension

Not applicable.

4.9.15 Procedure for suspension request

Not applicable.

4.9.16 Limits on suspension period

Not applicable.

4.10 Certificate status services

4.10.1 Operational characteristics

EUSPA OSNMA ICA-001 certificate status is provided through the CRL. CRL is available through GSC repositories as described in §2. The integrity and authenticity of the CRL is provided by the digital signature performed by the EUSPA OSNMA ICA-001.

4.10.2 Service availability

EUSPA and EUSPA contracted/authorised operators operate and maintain the EUSPA OSNMA ICA-001 CRL capability with resources sufficient to provide an HTTP and SFTP service under normal operating conditions.

The EUSPA OSNMA ICA-001 publication availability is described in §2.2.

4.10.3 Optional features

EUSPA certificate status services do not include or require any additional features.

4.10.4 End of subscription

Not applicable.

4.10.5 Key escrow and recovery

Not applicable.

4.11 CA termination

Before a CA ceases its activity, EUSPA and EUSPA contracted/authorised operators should:

- Inform the following about the decision to terminate its services: all relying parties who use active (unexpired and unrevoked) certificates issued by this authority and other entities with which EUSPA has agreements or other form of established relations, other trust service providers and relevant authorities such as supervisory bodies.
- Revoke the unexpired certificates that have been issued by the EUSPA OSNMA ICA-001.
- Assist with the orderly transfer of service, and operational records to a successor CA, if any.
- Destroy CA private keys, including backup copies, or withdraw them from use, in such a manner that the private keys cannot be retrieved.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

Facility, management, and operational controls are described in a Local Security Operations document.

Security incidents related to the certificate system, including reporting and mitigation procedures are handled following a business continuity plan.

6 TECHNICAL SECURITY CONTROLS

The EUSPA OSNMA ICA-001 PKI infrastructure is classified and complies with applicable EUCI regulations and [RD-11]. Some of the technical, organisational or processes measures are only communicated on a need-to-know basis and in compliance with applicable regulation [RD-8].

6.1 Key pair generation and installation

6.1.1 Key pair generation

All key pairs are generated by BSI-approved VS-NfD and Common Criteria EAL4+ certified HSM.

6.1.2 Private key delivery to subscriber

Not applicable.

6.1.3 Public key delivery to the certificate issuer

EE public key is delivered to the certificate issuer EUSPA OSNMA ICA-001 through CSR.

6.1.4 CA public key delivery to relying parties

Certification Authorities are available in the repositories §2.2.

6.1.5 Key sizes

All EUSPA PKI key sizes follow the recommendations provided by the French NSA (ANSSI) given in [RD-7]. The used values for EE certificates issued by the EUSPA OSNMA ICA-001 are the following:

- Digest Algorithm: SHA-256.
- ECC: NIST P-256.

In case of technical or functional constraints (except security considerations) that should be justified, internal EE certificates issued by the EUSPA OSNMA ICA-001 could have the following values:

- Digest Algorithm: SHA-384.
- ECC: NIST P-384.

6.1.6 Public keys parameters generation and quality checking

EUSPA and EUSPA contracted/authorised operators are responsible for checking the parameter quality of the generated key.

6.1.7 Key usage purposes (as per X.509 v3 key usage field)

Key usage of End Entity certificates is defined in §7 and shall be used only for ‘Digital Signature’.

6.2 Private key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

The cryptographic product is approved by the Secretary-General of the Council (LACP [RD-12], BSI-approved VS-NfD and Common Criteria EAL4+ certified HSM).

6.2.2 Private key (n out of m) multi-person control

CA Key Pairs are generated during a planned key ceremony and in accordance with a written ceremony procedure.

Ceremony procedures and associated records are retained at least for the lifetime of the generated key pairs.

6.2.3 Private key escrow

Private keys are not subjected to custody.

6.2.4 Private key backup

Private keys are backed-up and stored in a secured manner.

6.2.5 Private key archival

Private keys are archived in a secured manner.

6.2.6 Private key transfer into or from a cryptographic module

Private keys/backups are encrypted before extraction and the transfer into another HSM is performed in accordance with HSM manufacturer procedures.

6.2.7 Private key storage on cryptographic module

Private keys are stored in HSM as per HSM manufacturer procedures.

6.2.8 Method of activating the private key

Private keys are activated in accordance with the user manual of the HSM manufacturer.

6.2.9 Method of deactivating private key

Private keys are deactivated in accordance with the user manual of the HSM manufacturer.

6.2.10 Method of destroying private key

Private keys are destroyed in accordance with the user manual of the HSM manufacturer and internal procedures.

6.2.11 Cryptographic Module Rating

See §6.2.1.

6.3 Other aspects of key pair management

6.3.1 Public key archival

No stipulation.

6.3.2 Certificate operational periods and key pair usage periods

The validity periods of the keys are:

Table 5 – Key periods

Keys/certificates	Validity period
EUSPA OSNMA ICA-001	5 years
External End Entity certificate	2 years and 6 months
Internal End Entity certificate	4 years 11 months

6.4 Activation data

Not applicable.

6.5 Computer security controls

The entire infrastructure is hosted in a secure area. Physical controls, networks controls and system controls protect the system from unauthorised logical and physical accesses.

6.6 Life cycle technical controls

6.6.1 System development controls

The development of the system follows the ECSS standards defining all the steps to monitor, review, qualify, validate and accept the system.

6.6.2 Security Management Controls

Organization, procedures and technical measures are assessed during the development phase and during the operation all along the infrastructure lifetime through audits.

6.6.3 Life cycle security controls

Security controls are performed through the monitoring of the status of the entire infrastructure. Furthermore, internal audits are performed every year and external audits may be planned also to assess the security level of the infrastructure and improve it.

6.7 Network security controls

The controls include:

- A set of organization measures as, for example, separation of duties, right access control and management.
- A set of technical measures as, for example, firewalls, antivirus, hardened operating systems.
- A set of physical measures as, for example, badge access, seals, locks.
- Cyber/Security and operation trainings.
- Monitoring system with dashboards to control system health and security events.
- Constant vulnerability and patch management.

6.8 Time stamping

All events are timestamped.

7 CERTIFICATE AND CRL PROFILES

Certificate and CRL profiles comply with the format described in the ITU-T X.509 v.3 standard [RD-16]. [RD-2] describes the meaning of the respective certificate fields and CRL, of the applied standard and private extensions used by EUSPA.

8 OCSP PROFILE

Not applicable.

9 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

9.1 Frequency or circumstances of assessment

Compliance internal audits are performed at least once per year.

9.2 Identity/qualifications of assessor

The auditor can be internal to EUSPA and EUSPA contractor organisations or external and independent from EUSPA and EUSPA contractor (EUSPA Security Accreditation Department, National NSA, external accredited company).

The auditors have enough qualifications to audit PKI infrastructures.

9.3 Topics covered by assessment

The auditors assess the compliance level of the infrastructure to applicable cyber/security baselines, specifications, regulations or guidelines (e.g.: NSA guidelines).

10 OTHER BUSINESS AND LEGAL MATTERS

10.1 Fees

No fee as part of Galileo project.

10.1.1 Certificate issuance and renewal fees

Not applicable.

10.1.2 Certificate access fees

Not applicable.

10.1.3 Revocation or status information access fees

Not applicable.

10.1.4 Fees for other services

Not applicable.

10.1.5 Refund policy

Not applicable.

10.2 Financial responsibility and limited liability

For further details please refer to [RD-9].

10.2.1 Insurance coverage

Not applicable.

10.2.2 Other assets

Not applicable.

10.2.3 Insurance or warranty coverage for end-entities

Not applicable.

10.3 Confidentiality of business information

The Certificates and Certificate Revocation Lists do not contain confidential data.

10.4 Privacy of personal information

The privacy of personal information is governed by to [RD-10] which includes details on processing of personal information.

10.4.1 Privacy Plan

For details please refer to [RD-10].

10.4.2 Information Treated as Private

For details please refer to [RD-10].

10.4.3 Information not Deemed Private

The content of digital certificates is public information.

10.4.4 Responsibility to Protect Private Information

For details please refer to [RD-10].

10.4.5 Notice and Consent to use Private Information

If needed, in the process of issuing a digital certificate Subjects / Beneficiaries are informed about the need to use their personal data for the service and the need for consent. Consent is required forproviding the service.

10.4.6 Disclosure Pursuant to Judicial or Administrative Process

EUSPA is relieved of liability for the disclosure of personal data in the following situations:

- disclosure of personal information in accordance with the applicable law.
- to the competent institutions and bodies, based on the public law obligations EUSPA has, in accordance with the legal provisions.

10.4.7 Other Information Disclosure Circumstances

The following situations constitutes exceptions to the obligation to keep the confidentiality of personal data, that exonerate EUSPA of liability:

- disclosure of personal information to:
    - auditors in the audits to which EUSPA could be subject;.
    - a third party who relies on the certification services provided by EUSPA.

10.5 Intellectual Property Rights

For details please refer to §Terms Of Use And Disclaimers.

10.6 Representations and warranties

The PKI services are provided for the OSNMA service provision and no representations and warranties are provided (with exception of section 10.6.1) For further details please refer to [RD-9].

10.6.1 CA representations and warranties

EUSPA issues X509 v3 certificates.

10.6.2 RA representations and warranties

For details, please refer to section 1.3.2.

10.6.3 Subscriber representations and warranties

Not applicable.

10.6.4 Relying Party representations and warranties

Examples of Relying Parties' obligations and responsibilities include (without limitation):

- The successful performance of public key operations as a prerequisite for relying on a EUSPA Certificate.
- The validation of a EUSPA Certificate by using the (CRLs) or certificate validation services.
- The immediate termination of any reliance on a EUSPA Certificate if it has been revoked or when expired.

10.6.5 Representations and warranties of other participants

Not applicable.

10.7 Disclaimers of warranties

For details please refer to [RD-9].

10.8 Limitations of liability

For details please refer to [RD-9].

10.9 Indemnities

EUSPA assumes no financial responsibility for improperly used Certificates, CRLs, etc.

10.10 Term and termination

10.10.1 Term

This CPS and any amendments hereto shall become effective after publication in the repositories and in accordance with §10.12.2 and shall remain in effect perpetually until terminated in accordance with this section.

10.10.2 Termination

The CPS remains in force until replaced by a new version.

10.10.3 Effect of termination and survival

The conditions and effects resulting from termination of this CPS will be communicated via the repositories upon termination. That communication will outline the provisions that may survive termination of this CPS and remain in force. The responsibilities for protecting confidential information and private personal information shall survive termination, and the terms and conditions for all existing certificates shall remain valid for the remainder of the validity periods of such Certificates.

10.11 Individual notices and communications with participants

Participants shall use adequate methods to communicate with each other taking into account the classification of the information.

10.12 Amendments

10.12.1 Procedure for amendment

EUSPA is responsible for the approval and change of the present CPS. The CPS is reviewed when an update is needed.

Errors, updates, or suggested changes to this document shall be communicated as identified in the present CPS §1.5.2. Such communication will include a description of the change, a change justification, and contact information of the person requesting the change.

EUSPA shall accept, modify or reject the proposed change after completion of a review phase.

10.12.2 Notification mechanism and period

CPS will be published in the repositories.

10.12.3 Circumstances under which OID must be changed

Not applicable.

10.13 Dispute resolution provisions

All disputes associated with the present CPS will be settled before the French-speaking courts of Brussels.

10.14 Governing law

The present CPS shall be governed by European Union law, complemented, where necessary, by the law of Belgium.

10.15 Compliance with applicable law

The present CPS is subject to European Union law, complemented, where necessary, by the law of Belgium.

10.16 Miscellaneous provisions

Not applicable.

10.17 Other provisions

Not applicable.

11 LIST OF REFERENCES

ID	Title	Reference
[RD-1]	OSNMA SIS Interface Control Document https://www.gsc-europa.eu/sites/default/files/sites/all/files/Galileo_OSNMA_SIS_ICD_v1.0.pdf	October 2023 Issue 1.1
[RD-2]	OSNMA IDD ICD (OSNMA Internet Data Distribution) www.gsc-europa.eu/sites/default/files/sites/all/files/Galileo_OSNMA_IDD_ICD.pdf	January 2024 Issue 1.1
[RD-3]	RFC 3647 - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework	November 2003
[RD-4]	ETSI EN 319 411-1 - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements	V1.3.1 (2021-05)
[RD-5]	ETSI EN 319 411-2 - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates	V2.4.1 (2021-11)
[RD-6]	RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	May 2008
[RD-7]	Référentiel Général de Sécurité	V2.0
[RD-8]	Commission Decision (EU, Euratom) 2015/444 on the security rules for protecting EU classified information	13 March 2015
[RD-9]	https://www.gsc-europa.eu/support-to-developers/osnma-public-observation-test-phase/register[1]	
[RD-10]	https://www.gsc-europa.eu/sites/default/files/sites/all/files/GSC_Privacy_Statement.pdf	
[RD-11]	PROGRAMME SECURITY INSTRUCTION CONCERNING European GNSS Programmes	EU GNSS PSI v 4.1
[RD-12]	List of approved cryptographic products (LACP) for protecting EU Classified Information (EUCI)	5335/4/21 rev4
[RD-13]	Recommendation ITU-T X.500 Information technology – Open Systems Interconnection – The Directory: Overview of concepts, models and services	2005

[1] This will be replaced by the Service Definition Document (SDD) at the time of the OSNMA initial service declaration

ID	Title	Reference
[RD-14]	Recommendation ITU-T X.520 Information technology – Open Systems Interconnection – The Directory: Selected attribute types	2005
[RD-15]	ETSI EN 319 412-1 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures	V1.4.4 May 2021
[RD-16]	Recommendation ITU-T X.509 Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks	2005

LINKING SPACE TO USER NEEDS

www.euspa.europa.eu

@EU4Space

@EU4Space

EUSPA

@space4eu

EUSPA

#EUSpace