Certificate Policy for ISS SCMS Pilots and Testing
Version 1.01

ISS Policy Authority (IPA)

03-07-2024

Contents

1   Revision History

Version	Date	Description
1.0	Oct 13, 2023	• First Revision
1.01	Mar 7, 2024	• Added revision history

2   Introduction

This Certificate Policy (CP) defines certificate policies to facilitate testing of INTEGRITY Security Services LLC SCMS public key cryptography and public key infrastructures. This CP, based on the National Institute of Standards and Technology(NIST) test policy (Computer Security Division (CSD) 2012), is consistent with the Internet Engineering Task Force (IETF) X.509 Public Key Infrastructure (PKIX) Certificate Policy and Certification Practices Framework (Chokhani et al. 2003).

INTEGRITY Security Services LLC disclaims any liability that may arise from the use of this CP.

2.1   Overview

This policy pertains to certificates issued for testing and evaluation ONLY.

2.2   PKI participants

No stipulation.

2.3   Certificate usage

2.3.1   Appropriate certificate uses

Certificates issued under this policy should be used for testing purposes ONLY.

2.3.2   Prohibited certificate uses

This CP does not guarantee any particular level of assurance. These certificates should not be used to implement security for real-world applications.

2.4   Policy administration

2.4.1   Organization administering the document

The ISS Policy Authority (IPA) is responsible for all aspects of this CP.

2.4.2   Contact person

Questions regarding this CP shall be directed to the IPA registrar via electronic mail at **sarah.paramore@ghsiss.com**.

2.4.3   Person determining CPS suitability for the policy

This CP may be used without a CPS.

2.4.4   CPS approval procedures

No stipulation.

3   Publication and repository responsibilities

No stipulation.

4   Identification and authentication

No stipulation.

5   Certificate life-cycle operational requirements

No stipulation.

6   Facility, management, and operational controls

No stipulation.

7   Technical security controls

No stipulation.

8   Certificate, CRL, and OCSP profiles

No stipulation.

9   Compliance audit and other assessments

No stipulation.

10   Other business and legal matters

No stipulation.

10.1   Fees

No stipulation.

10.2   Financial responsibility

No stipulation.

10.3   Confidentiality of business information

No stipulation.

10.4   Privacy of personal information

No stipulation.

10.5   Intellectual property rights

No stipulation.

10.6   Representations and warranties

No stipulation.

10.7   Disclaimers of warranties

No stipulation.

10.8   Limitations of liability

INTEGRITY Security Services LLC disclaims any liability that may arise from use of any certificate issued by any CA that asserts this policy.

10.9   Indemnities

No stipulation.

10.10   Term and termination

No stipulation.

10.11   Individual notices and communications with participants

No stipulation.

10.12   Amendments

No stipulation.

10.13   Dispute resolution provisions

No stipulation.

10.14   Governing law

No stipulation.

10.15   Compliance with applicable law

No stipulation.

10.16   Miscellaneous provisions

No stipulation.

10.17   Other provisions

No stipulation.

References

Chokhani, S., W. Ford, R. Sabett, C. Merrill, and S. Wu. 2003. "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework." RFC 3647. RFC Editor; Internet Requests for Comments; RFC Editor.

Computer Security Division (CSD), NIST -. 2012. "Test Certificate Policy to Support Pki Pilots and Testing." Washington, D.C.: U.S. Department of Commerce. https://csrc.nist.gov/CSRC/media/Projects/Computer-Security-Objects-Register/documents/test_policy.pdf.