CERT SI-nerGIE CERT RFC 2350

1 DOCUMENT INFORMATION ... 2

1.1 Date of the Last Update ... 2

1.2 Distribution List for notification ... 2

1.3 Location where the document May be found ... 2

1.4 Document authenticity ... 2

1.5 Document Identification ... 2

2 CONTACT INFORMATION ... 2

2.1 Name of the team ... 2

2.2 Postal adress ... 2

2.3 Time Zone ... 2

2.4 Telephone Number ... 2

2.5 Facsimile Number ... 2

2.6 Electronic Mail Adress ... 3

2.7 Public keys and Encryption Information ... 3

2.8 Team Members ... 3

2.9 Other Information ... 3

2.10 Points of Contact ... 3

3 CHARTER ... 3

3.1 Mission Statement ... 3

3.2 Constituency ... 3

3.3 Sponsoring Organization / Affiliation ... 3

3.4 Authority ... 3

4 POLICIES ... 4

4.1 Types of Incidents and Level of Support ... 4

4.2 Co-operation, Interaction and Disclosure of Information ... 4

4.3 Communication and Authentication ... 4

5 SERVICES ... 4

5.1 Digital Forensics and Incident Response ... 4

5.2 Proactive Activities ... 4

6 INCIDENT REPORTING FORMS ... 5

7 DISCLAIMERS ... 5

1 DOCUMENT INFORMATION

This document contains a description of SI-nerGIE CERT according to RFC 2350. It provides basic information about SI-nerGIE CERT, its responsibilities and services offered.

1.1 Date of the Last Update

This is the initial version 1.0 published on July 13th, 2022.

1.2 Distribution List for notification

There is no distribution list for notifications.

1.3 Location where the document May be found

The current and latest version of this document are available on the following web sites:
https://www.framatome.com/fr/cert
https:///www.orano.group/fr/cert

1.4 Document authenticity

The document has been signed with the PGP Key of SI-nerGIE CERT.
The PGP public key, ID and fingerprint are available on the Framatome web site at https://www.framatome.com/fr/cert and Orano website at https://www.orano.group/fr/cert

1.5 Document Identification

Title: Cert_SI-nerGIE_ RFC _2350_v1.0
Version: V1.0
Document Date: July 13th, 2022
SHA-256
Expiration: this document is valid until superseded by a later version.

2 CONTACT INFORMATION

2.1 Name of the team

Official name: CERT-A
Usual name: CERT SI-nerGIE

2.2 Postal adress

CERT SI-nerGIE
2 place des Vosges
92400 Courbevoie
Cedex

2.3 Time Zone

CET/CEST

2.4 Telephone Number

Main number (duty office): +33 1 34 96 95 95

2.5 Facsimile Number

Not available

2.6 Electronic Mail Adress

If you need to notify us about an information security incident or a cyber-threat targeting or involving SI-nerGIE CERT, please contact us at: csirt[at]si-nergie.tech.

2.7 Public keys and Encryption Information

User ID: csirt[at]si-nergie.tech
Fingerprint : F5C942E48F96DE6CD9614437992153271E7D4F3E
Key ID : 0x992153271E7D4F3E

2.8 Team Members

Team members identity is not publicly available. It might be communicated according need to know restrictions.

2.9 Other Information

General information about SI-nerGIE CERT can be found at the following URLs:
https://www.framatome.com/fr/cert or https://www.orano.group/fr/cert

2.10 Points of Contact

The preferred method to contact SI-nerGIE CERT is by sending an email to the following address:

csirt[at]si-nergie.tech.

Urgent cases can be reported by phone (+33 1 34 96 95 95) during French business hours. SI-nerGIE CERT hours of operation are aligned with regular French business hours (Monday to Friday 08:00 to 18:30).

3 CHARTER

3.1 Mission Statement

SI-nerGIE CERT manages cybersecurity incident response for both Framatome and Orano companies.

SI-nerGIE CERT coordinates incident response operations from investigations to mitigations measures implementation for the benefit of Framatome and Orano including their affiliates.

SI-nerGIE CERT is also in charge of other activities among them cyber watch, vulnerability management, hunting.

3.2 Constituency

Our constituency is composed of Framatome and Orano groups and affiliates

3.3 Sponsoring Organization / Affiliation

SI-nerGIE CERT is a private Computer Incident Response Team. It maintains relationships with different national and international CSIRTs and CERTs.

3.4 Authority

SI-nerGIE CERT operates under SI-nerGIE Cybersecurity director authority.

4 POLICIES

4.1 Types of Incidents and Level of Support

SI-nerGIE CERT's assistance may be requested in all types of cybersecurity incidents that may occur within its constituencies.

The level of support depends on the type and severity of the given security incident, the amount of affected entities, and our resources at the time.

4.2 Co-operation, Interaction and Disclosure of Information

SI-nerGIE CERT can collaborate with other CSIRTs and CERTs as well as with other affected third parties to the extent they are involved in the incident or incident response process.

Information received by SI-nerGIE CERT may be shared with Framatome Group or Orano Group entities as well as to cybersecurity service providers, on a need-to-know basis.

4.3 Communication and Authentication

All e-mails sent to the SI-nerGIE CERT should be signed using PGP. All e-mails containing confidential information should be encrypted and signed using PGP. Information received in encrypted form should not be stored permanently in unencrypted form.

For other communication, a phone call, postal service, or unencrypted e-mail may be used.

SI-nerGIE CERT respects the Information Sharing Traffic Light Protocol (TLP) that comes with the tags with the tags WHITE, GREEN, AMBER or RED.

5 SERVICES

5.1 Digital Forensics and Incident Response

SI-nerGIE CERT manages technical and organizational aspects of security incidents:

- Third party security incidents
- Cyber crisis coordination
- Incident triage (report assessment and verification) and analysis
- Incident categorization and incident response coordination
- Incident response support, technical assistance, eradication et recovery
- Technical crisis unit in case of cyberattacks
- Vulnerability management
- Evidence collection and digital forensic

5.2 Proactive Activities

SI-nerGIE CERT coordinates and maintains the following services to the extent possible depending on its resources:

- Cybersecurity assessment
- Threat management
- Threat intelligence
- Security awareness

6 INCIDENT REPORTING FORMS

There is no specific incident reporting form. Please report security incidents via encrypted e-mail to Csirt csirt[at]si-nergie.tech

- Incident reports should contain the following information:
- Incident date and time (including time zone)
- Source IPs, ports, and protocols
- Destination IPs, ports, and protocols
- Incident type
- And any relevant information

7 DISCLAIMERS

While every precaution will be taken in the preparation of information, notifications and alerts, CERT SI-nerGIE assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained within.