SOGEI CERT OPERATING MODEL
(RFC 2350)

Prepared:	Scherin De Cesaris, Valentina Lavore
Reviewed:	Fabrizio Maria Bernini
Approved:	Alessandro Brunacci
Date:	2026-04-03
Version:	1.4
Classification:	Public

INDICE

Document version

Review	Date	Change Summary
1.4	2026-04-03	CERT Personnel Organization and Services Provided

1. DOCUMENT INFORMATION

This document provides a description of Sogei CERT in accordance with the provisions of "RFC 2350 - Expectations for CSIRTs", supplying basic information, contact details, and a general overview of its tasks and the services it provides.

RFC 2350 establishes guidelines regarding the organization and communication methods of a Computer Security Incident Response Team (CSIRT), i.e., an organization that prevents and supports the management of security incidents affecting the information systems of a community of stakeholders, referred to as the Constituency.

In particular, the team is named "Sogei CERT" and delivers services for the prevention of and support to incident management for the organization's Constituency.

The CERT is established in compliance with the Italian Cyber Strategy, as defined in the Prime Ministerial Decree (DPCM) of 27 January 2014 – National Cyber Security Strategy, and follows the guidelines set out in the National Plan for Cyber Protection and ICT Security and the National Strategic Framework for Cyberspace Security.

Sogei CERT is composed of Sogei personnel working in synergy to achieve the security objectives of both the Constituency and the organization itself, with particular focus on incident management support and the execution of Cyber Threat Intelligence activities. Incidents of interest to the CERT include those regulated by Decree-Law No. 105 of 21 September 2019, as they are relevant to services falling within the National Cybersecurity Perimeter (PSNC), as well as significant incidents identified pursuant to Legislative Decree No. 138 of 4 September 2024, implementing Directive (EU) 2022/2555 (NIS2).

The following sections of this document describe in detail the organization of Sogei CERT and explain its operational model.

1.1 VERSION

Version 1.4 of 03 April 2026.
Compared to the previous version (1.3 of 25 January 2023), updates have been made to the personnel organization and to the services provided by the CERT.

1.2 AVAILABILITY

The current version of this document is published on the Sogei website at the following URL:
https://www.sogei.it/it/sogei-homepage/azienda/governance/it-governance/sicurezza-e-tutela-dei-dati/computer-emergency-response-team.html

1.3 ACRONYMS

CERT Sogei - Computer Emergency Response Team of Sogei S.p.A.

CSIRT - Computer Security Incident Response Team.

GPG - GNU Privacy Guard. Free software designed to replace the PGP cryptographic suite. It is fully compatible with the IETF OpenPGP standards and is supported by the German government. GNU Privacy Guard is distributed under the GNU General Public License and is part of the GNU Project.

GNU - GNU (a recursive acronym for "GNU's Not Unix") is a Unix-like operating system created in 1984 by Richard Stallman and developed by the community that adheres to the GNU Project.

MEF - Ministry of Economy and Finance.

PSNC - National Cybersecurity Perimeter, established by Decree-Law No. 105 of 21 September 2019, converted into Law No. 133 of 18 November 2019, aims to ensure a high level of security of networks, information systems, and IT services of public administrations, entities, and public and private operators established within the national territory.

RFC 2350 – Request for Comments 2350. The University of Auckland - Network Working Group. This document specifies an Internet Best Current Practices for the Internet Community, and requests discussion and suggestions for improvements.

2. OFFICIAL CONTACTS OF THE SOGEI CERT

2.1 NAME

The name of the Team is "CERT Sogei", in accordance with the provisions of the National Cyber Protection and ICT Security Plan and the National Strategic Framework for Cyberspace Security.

2.2 ADDRESS

CERT Sogei
Sogei SpA - Via Mario Carucci, 99 e 85 Roma – 00143 Italy

2.3 TIME ZONE

Central European Time (CET, GMT+1) (GMT+2 during daylight saving time, from the last Sunday in March to the last Sunday in October).

2.4 TELEPHON AND FAX CONTACTS

+390650255005 (landline)

+390650255005 (on-call)

2.5 EMAIL ADDRESS

<cert@sogei.it> is the official mail address of CERT Sogei

2.6 CERTIFIED EMAIL ADDRESS (PEC)

<cert@pec.sogei.it> is the certified mail address CERT Sogei

2.7 OTHER TYPES OF COMMUNICATION

Additional communication methods beyond those listed above can be made available upon request or when necessary.

2.8 PUBLIC KEYS AND ENCRYPTION MECHANISMS

Communications between Sogei CERT and its Constituency may also take place through the exchange of encrypted documents using GPG

Sogei CERT makes its public key available to representatives of accredited entities in order to receive communications containing confidential information protected by encryption. Public keys are exchanged through trusted channels, such as standard email using institutional mailboxes.

CERT members have access to the corresponding private key, which is used to decrypt received data.

The procedures for the use and exchange of information comply with Sogei security policies.

2.9 TEAM STRUCTURE

Sogei CERT, placed within the Digital Technologies and Services Directorate (DZT), under the responsibility of the Cybersecurity Area (CYS), is a structure operating within Sogei responsible for the handling of cyber security incidents.

Sogei CERT is organized in such a way as to comply with the provisions of:

- the National Cyber Protection and ICT Security Plan;
- the National Strategic Framework for Cyberspace Security;
- the Sogei CERT Charter.

2.10 USER CONTACT POINTS AND PROCEDURES

The preferred method for contacting Sogei CERT staff is via email at:

- cert@sogei.it

and via certified email (PEC) at:

- cert@pec.sogei.it

Emails sent to these addresses are handled by CERT staff as soon as possible, depending on the severity assigned to the report; however, if the communication is considered urgent, it is recommended to include the word “URGENT” in the subject line.

Sogei operational teams managing servers or application environments may contact the on-call CERT staff member in case of emergencies using the telephone number +39 320 431 4519.

The operating hours of Sogei CERT are generally limited to normal working hours (09:00–18:00, Monday to Friday).

3. CHARTER

3.1 MISSION

The mission of Sogei CERT is to prevent and support the management of cyber security incidents, by carrying out cyber threat intelligence activities and promoting awareness and training initiatives on cybersecurity topics.
Within Sogei CERT, the Head is responsible for supporting top management and staff in understanding cyber risks and threats, with particular reference to the protection of the organization's information assets.

3.2 CONSTITUENCY

The Constituency of Sogei CERT includes the set of internal and external stakeholders, as well as the organizational structures within the Sogei perimeter, to which the CERT provides services for the prevention and management support of cyber security incidents.

3.3 ACCREDITATIONS

Sogei CERT is officially accredited by:

- the National Anti-Crime Computer Centre for the Protection of Critical Infrastructures (CNAIPIC);
- CSIRT Italia – the Italian Computer Security Incident Response Team;
- the Department of Information for Security (DIS).

3.4 AUTHORITY

Sogei CERT operates on the basis of contracts/agreements established by the organization with accredited clients.

4. SOGEI CERT POLICY

4.1 TYPES OF INCIDENTS AND LEVELS OF SUPPORT

Sogei CERT provides support in relation to cyber security incidents that may compromise the confidentiality, integrity, or availability of the information systems and services within its Constituency.

4.2 COOPERATION, INTERACTION AND INFORMATION SHARING

During prevention activities and incident handling support, Sogei CERT will pay particular attention to the management of any confidential information it may come to know. In particular, the following information will be handled in a manner that ensures the highest possible level of confidentiality:

- users' personal information;
- information considered confidential for legal, contractual, or ethical reasons.

The following technical information shall also be considered highly confidential:

- information relating to sites or systems managed within the scope of responsibility;
- information relating to attacks or incidents, whether attempted or successful, within the scope of responsibility;
- statistical information, including anonymized data, that may be considered potentially sensitive or embarrassing for the organizations within the scope of responsibility;
- events classified as Data Breaches.

The potential recipients of communications from the Sogei CERT include:

- Sogei;
- the Constituency;
- CERT-MEF;
- CSIRT Italia - the Italian Computer Security Incident Response Team;
- other national or international CERTs;

- the “National Anti-Crime Computer Centre for the Protection of Critical Infrastructures” (CNAIPIC).

4.3 COMMUNICATIONS: CONFIDENTIALITY AND AUTHENTICATION

The nature and confidentiality of the information handled by the CERT are such that standard telephone communications and email transmission are considered appropriate means for their exchange.

In the case of communications containing confidential information or potentially malicious programs, simple encryption (password-protected compressed archives) or GPG encryption shall be used.

5. SERVICES PROVIDED BY THE SOGEI CERT

5.1 SUPPORT FOR CYBER SECURITY INCIDENT MANAGEMENT

Sogei CERT provides support for the management of cyber security incidents within its organization, assisting the relevant internal units during the Triage, Analysis and Classification, and Communication and Notification phases. In particular, the CERT provides the necessary support to analyze threats and ensure that relevant information is properly handled, remaining informed and up to date throughout the entire incident management process.

More detailed information can be found in the following document:

- DP-78-Q4-36 - “Gestione incidenti di sicurezza informatica”

5.1.1 TRIAGE

During the Triage phase, the CERT forwards reports related to potential cyber security incidents (e.g., those arising from Cyber Threat Intelligence activities), performing an initial classification, to the relevant organizational units.

5.1.2 ANALYSIS AND CLASSIFICATION

During the Analysis and Classification phase of the incident, if necessary, the CERT conducts Cyber Threat Intelligence activities to support incident handling and provide a more comprehensive understanding of the nature of the threat.

5.1.3 COMMUNICATION AND NOTIFICATION

The CERT remains informed throughout the entire incident management process, supporting any communication between the involved parties. At the end of the process, it provides the final report to the relevant stakeholders.

If required, the CERT also notifies the incident to the competent authorities and to the Constituency, ensuring that all information is communicated in a timely manner and in compliance with applicable regulations and internal organizational processes.

5.2 PROACTIVE SERVICE

5.2.1 CYBER THREAT INTELLIGENCE

Within the scope of Cyber Threat Intelligence activities, CERT members perform, using CTI platforms and the consultation of open sources, daily monitoring of current and potential threats that may impact the organization and its Constituency.

In particular, Sogei CERT provides the following services to its Constituency:

- *Early Warning*: identification and timely reporting of emerging or critical vulnerabilities, with particular attention to cases of active exploitation or high likelihood of exploitation;
- *Third-Party Monitoring*: activities aimed at identifying threats, vulnerabilities, or security events that may affect suppliers, partners, or external entities relevant to the Constituency;
- *Digital Risk Protection (DRP):* activities aimed at identifying and monitoring threats and malicious activities related to the organization's digital exposure.

5.2.2 CYBER AWARENESS

Sogei CERT coordinates and maintains several services to support its Constituency in gaining deeper insight into cybersecurity topics, including:

- periodic in-depth seminars;
- planning and execution of white phishing campaigns;
- Cyber Newsletter: periodic distribution of updates and information on major threats and developments in the cyber landscape.

6. INCIDENT REPORTING FORMS

Sogei CERT does not provide a dedicated security incident reporting form.

Accredited Constituency contacts may use the agreed-upon methods and established points of reference.

All users who wish to report a security event may do so via the CERT email address <cert@sogei.it>, providing as much information as possible, including:

- the type of event or incident (malware, policy violation, system compromise, or others);
- the time and date when the event occurred or whether it is still ongoing;
- any available evidence (e.g., email messages or files), which should be sent in a password-protected compressed archive and/or with encrypted content.

7. DISCLAIMER

Although every possible precaution is taken in the preparation of prevention and incident handling reports, as well as in the production of advisories and bulletins, the Sogei CERT assumes no responsibility for any errors or omissions, nor for any damages resulting from the use of the information provided.

Furthermore, the presence of hyperlinks included within the information communicated by the Sogei CERT is intended solely as a means to facilitate further reference and research.