CERT Finanziario Italiano (CERTFin) - RFC 2350

1. Document Information

This document contains a description of CERT Finanziario Italiano (in the following referred to as CERTFin according to RFC 2350 (https://www.rfc-editor.org/rfc/rfc2350.txt).

It defines the basic information related to CERTFin, including a brief explanation of the tasks and services offered and how it can be contacted.

1.1. DATE OF LAST UPDATE

This is version `1.3.1` published on September 28th, 2023.

1.2. DISTRIBUTION LIST FOR NOTIFICATIONS

Notifications will be sent to the representatives of the Constituency.

1.3. LOCATIONS WHERE THIS DOCUMENT MAY BE FOUND

The document is available on CERTFin's website at the following URLs:

- HTML **https://www.certfin.it/rfc2350.html** (**md5 hash**)
- PDF **https://www.certfin.it/rfc2350.pdf** (**md5 hash**)

Make sure to always use the updated version.

2. Contact Information

2.1. NAME OF THE TEAM

CERT Finanziario Italiano
Short name: CERTFin

2.2. ADDRESS

CERTFin c/o ABI Lab
Via del Gesù, 62
00186 Roma
Italy

2.3. TIME ZONE

Central European Time (UTC+1), and observing Daylight Saving Time (UTC+2) from the last Sunday of March to the last Sunday of October.

2.4. TELEPHONE NUMBER

Entry Point

(+39) 331 662.8967

Emergency Points of Contact

(+39) 346 218.6137

(+39) 338 684.4818

Business Continuity

(+39) 348 429.0304

Subscription, Partnership, Collaborations

(+39) 345 162.1558

2.6. OTHER TELECOMMUNICATION

None

2.7. ELECTRONIC MAIL ADDRESS

CERTFin can be reached at **isac@certfin.it**.
Messages sent to this address can be read by all members of the team of CERTFin

2.8. PUBLIC KEYS AND ENCRYPTION INFORMATION

PGP/GPG is supported for secure communication.

CERTFin has a public PGP/GPG key for **isac@certfin.it** which is available at the usual public key servers such as **http://pgp.mit.edu**.

PGP/GPG Key:

- ID: FinISAC <isac@certfin.it>
- Fingerprint: 7E4B B1EE 4230 8560 35D5 E9ED B3DA 72A4 0664 0DCF

All team members of CERTFin have a personal PGP/GPG key for exchange of classified information.

2.9. TEAM MEMBERS

CERTFin team consists of qualified cyber security and fraud analysts.
The Chief Operating Officer is Romano Stasi.
The Technical Coordinator is Mario Trinchera.

2.10. OPERATING HOURS

The preferred method for contacting CERTFin is via email at **isac@certfin.it**. The mailbox is monitored from Monday to Friday 09.00 - 17.00, except during public holidays in Italy.

A telephone number (operating 24/7) has been provided to representatives of the Constituency. Please use PGP/GPG if you intend to send sensitive information.

2.11. OTHER INFORMATION

General information about CERTFin can be found at **https://certfin.it**.

3. Charter

3.1. MISSION STATEMENT

CERTFin is the focal point for the collection, analysis and sharing of information related to cyber threats, and for the coordination of activities to prevent and support response to cyber emergencies that could harm IT-assets of the Italian financial and assurance organizations participating in the Constituency.

The main goals of CERTFin are:

- to provide prompt information regarding potential cyber-threats that could damage banks and insurance organizations;
- to act as Point of Contact between financial operators and other relevant public institutions as far as cyber protection;
- to facilitate the response to large-scale security incidents;
- to support crisis management process in case of cyber incidents;
- to cooperate with national and international institutions and other actors, from both public and private sector, which are involved in cyber security, by promoting the cooperation among them;
- to improve cyber-security awareness and culture.

3.2. CONSTITUENCY

Constituency Type: External

Constituency Sector: Financial Services

The CERTFin's Constituency includes financial and insurance organizations adherent to CERTFin.

3.3. SPONSORSHIP AND/OR AFFILIATION

The CERTFin was created through a special agreement between the Italian Banking Association, the Bank of Italy and ABI Lab signed on 20 December 2016.

3.4. AUTHORITY

CERTFin operates under the auspices of, and with authority delegated by, Bank of Italy and ABI.

CERTFin is not an authoritative body. It performs its functions through cooperation agreements and protocols.

4. Policies

4.1. TYPES OF INCIDENTS AND LEVEL OF SUPPORT

CERTFin is authorized to support and coordinate relevant cyber security incidents which occur, or threaten to occur, at participants to the Constituency. Depending on the security incident's nature, CERTFin will gradually roll out its services which include incident response coordination, alerting, and escalation to the central bank.

The level of support given by CERTFin will vary depending on the type and severity of the incident or issue, its potential or assessed impact, and the CERTFin's resources available at the time.

The CERTFin is committed to keeping its Constituency updated on potential vulnerabilities, possibly before they are actively exploited.

4.2. CO-OPERATION, INTERACTION AND DISCLOSURE OF INFORMATION

CERTFin receives from its Constituency alerts related to incidents or threats. It evaluates their possible impact for the financial and insurance sector, informs all the involved actors and coordinates them in order to find the most suitable solutions

CERTFin regards the operational cooperation and information sharing with other CERTs and similar qualified organizations as of paramount importance. Therefore, while appropriate measures will be taken to protect the identity of members of the Constituency and of neighbouring sites where necessary, unless otherwise expressly stated, CERTFin ensures the confidentiality of its sources of information. The information received, possibly anonymized, may be shared with interested parties in order to solve or prevent specific issues.

CERTFin operates within the current Italian and European legal frameworks, with specific regard to the handling and disclosure of information.

4.3. COMMUNICATION AND AUTHENTICATION

Telephones and unencrypted emails are considered sufficiently secure for the transmission of low-sensitive data. If it is necessary to send highly sensitive data by email, PGP/GPG will be used. Network file transfers will be similar to email for these purposes: sensitive data will be encrypted for transmission.

CERTFin recognizes and supports the TLP (Information Sharing Traffic Light Protocol).

Where it is necessary to establish trust, for example before relying on information given to the CERTFin or before disclosing confidential information, the identity and *bona fide* of the other party will be ascertained to a reasonable degree of trust by use of appropriate methods (e.g.: referrals from known trusted sources, checks with the originator, digital signatures).

5. Services

5.1. INCIDENT RESPONSE

CERTFin will support the affected members in handling the technical and organizational aspects of relevant cyber security incidents.

In case of a large-scale national event, CERT Nazionale activates the coordination process for the incident resolution, including sending out alerts and warnings to its Constituency, for performing digital forensic analysis when necessary, and for providing assistance or advice with respect to the different incident response phases.

5.1.1 Incident Triage

CERTFin assesses the triage label of the reported incidents. The events are analysed, verifying the reliability of the source, finding any other available information. Then they are categorized according to their seriousness.

In case of a large-scale national event, CERTFin activates the escalation process for the incident resolution.

5.1.2 Incident Coordination

The steps for the Incident Coordination are following described:

1) To identify the organizations involved;
2) To establish contacts with all the stakeholders in order to analyse the incident and identify actions to be undertaken;
3) To facilitate contacts with other organizations that can provide support in solving the incident;
4) To promptly inform all the involved (or potentially involved) parties within the Constituency;
5) To write reports and send them to other CERTs or interested organizations.

CERTFin acts primarily as an information gathering centre. Information collected are readily sorted within the Constituency to facilitate the solution of cyber security incidents.

5.1.3 Incident Resolution

CERTFin disseminates the information needed to counteract the incident and to restore the state of normality as quickly as possible in cooperation with the involved member Constituency.

5.2. PROACTIVE ACTIVITIES

CERTFin coordinates and maintains the following services for its Constituency:

- Cyber Threat Intelligence based on the collection of intelligence using different external source intelligence with the aim of researching and analysing trends and technical developments in cyber areas.
- Information Sharing with the aim of exchanging and keeping updated information about threats and vulnerability and of preparing analysis about fraud end cyber-attacks (through MISP platform, periodical conference calls and reports delivery)
- Security Awareness for improving cyber security consciousness of banking and insurance customers
- Dissemination of useful information gathered through national and international main conferences and European projects

6. Incident Reporting Forms

CERTFin does not provide any public form for reporting incidents.

Any member of the Constituency can send information about security incidents, threats or related information to CERTFin by sending an email, possibly encrypted, to **isac@certfin.it**.

When reporting a cyber security incident to CERTFin, please provide at least the following information:

- contact details and organizational information;
- type and description of the incident or threat;
- time and date of reported event, including the time zone;
- source of information;
- possible impacts;
- any relevant technical element with associated observation.

Member of the Constituency can report incidents using the same reporting forms already used for communication to Institutional Bodies.

Please classify the information using the Traffic Light Protocol and apply encryption as appropriate.

Do not send malicious code or other attachments via email without having previously agreed the transmission mode with CERTFin.

7. Disclaimers

While every precaution will be taken in the preparation of information, notifications and alerts, CERTFin assumes no responsibility for errors or omissions, or for damages arising from the use of such information.

Appendix A: Glossary of Terms

Constituency: group of users, sites, networks or organizations served by the team. The team must be recognized by its Constituency in order to be effective.

Cyber Security Incident: any event, or series of related events, not planned by the member affecting its IT resources and which

i) has or could have a negative impact on the integrity, availability, confidentiality, authenticity and / or continuity of services o of its processes; or

ii) in any case it implies the violation or the imminent threat of violation of the company rules and practices on information security

A cyber security incident should be considered “serious” if resulting or likely to result in at least one of the following consequences:

a. high economic losses or prolonged inefficiencies for the organization, even as a result of repeated minor incidents;

b. significant disruptions on customers and other subjects (e.g., intermediaries or payment infrastructures); the severity assessment considers the number of customers or counterparties potentially involved and the amount at risk;

c. the risk of affecting the member's ability to comply with the conditions and obligations of the law or of the supervisory regulations;

d. reputational damage if it is made public (for example through the media and the press).

Vulnerability: a characteristic of a piece of technology which can be exploited to perpetrate a security incident.

For further terms please refer to the Cyber Lexicon of the Financial Stability Board (http://www.fsb.org/2018/11/cyber-lexicon/).