CERT Banca d’Italia (CERTBI) - RFC 2350

1. Document Information

1.1. DATE OF LAST UPDATE

This is version 2.0.0 published on February 7, 2024.

1.2. DISTRIBUTION LIST FOR NOTIFICATIONS

There isn’t any distribution list for notifications.

1.3. LOCATIONS WHERE THIS DOCUMENT MAY BE FOUND

The document is available on CERTBI’s website at the following URLs:

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

2. Contact Information

2.1. NAME OF THE TEAM

CERT Banca d’Italia
Short name: CERTBI

1.2. ADDRESS

CERT Banca d’Italia
Divisione CERTBI
Servizio Pianificazione Informatica
Dipartimento Informatica

Largo Guido Carli, 1
00044 Frascati (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

+39 06 4792 9797

2.5. FACSIMILE NUMBER

+39 06 4792 8946 (*this is not a secure fax*)

2.6. OTHER TELECOMMUNICATION

None

2.7. ELECTRONIC MAIL ADDRESS

CERTBI can be reached at **cert@bancaditalia.it**.

2.8. PUBLIC KEYS AND ENCRYPTION INFORMATION

PGP/GPG is supported for secure communication.

CERTBI has a public PGP/GPG key for **cert@bancaditalia.it** which is available at **https://cert.bancaditalia.it/certbi.asc** and usual public key servers, such as **MIT PGP Key Server**.

PGP/GPG Key:

- ID: 0xF3B8890C
- Fingerprint: AAD8 26E6 51FD 597A 3EC8 4535 E6A3 94C3 F3B8 890C

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

2.9. TEAM MEMBERS

CERTBI team consists of qualified cyber security analysts. The team leader is the *pro tempore* head of the “Divisione CERTBI”.

2.10. OTHER INFORMATION

General information about CERTBI can be found at **https://cert.bancaditalia.it**.

2.11. POINTS OF CUSTOMER CONTACT

The preferred method for contacting CERTBI is via email at **cert@bancaditalia.it**. The mailbox is monitored during hours of operation. Please use PGP/GPG if you intend to send sensitive information.

The CERTBI’s hours of operation are generally restricted to regular business hours (9:00 - 17:00, Monday to Friday except Italian holidays).

If necessary, any urgent case can be reported by phone at **+39 06 4792 9797**.

3. Charter

3.1. MISSION STATEMENT

CERTBI is the focal point for the collection, analysis and sharing of information related to cyber threats, and for the coordination of activities aiming at preventing and supporting the response to cyber emergencies that could harm IT-assets of Banca d’Italia and IVASS. It is the one contact point for voluntary information sharing with the Bank’s external counterparts, running continuous cyber intelligence activities for the preventative and proactive countering of cyber threats. CERTBI cooperates with qualified counterparts at national, EU and extra-EU levels. It continuously produces intelligence on the evolution of cyber threats and delivers it to the Institute’s internal and external stakeholders, adopting an intelligence-led cyber security approach also in supporting the entire cyber security incident lifecycle.

3.2. CONSTITUENCY

The CERTBI's constituency includes people and IT-assets of Banca d'Italia and IVASS.

3.3. SPONSORSHIP AND/OR AFFILIATION

CERTBI is part of Banca d'Italia organization.

3.4. AUTHORITY

CERTBI operates under the auspices of, and with authority delegated by, the Director General of the Directorate General for Information Technology of Banca d'Italia.

4. Policies

4.1. TYPES OF INCIDENTS AND LEVEL OF SUPPORT

CERTBI is authorized to address relevant cyber security incidents which occur, or threaten to occur, at Banca d'Italia and IVASS. Depending on the security incident's nature, CERTBI will gradually roll out its services which include: managing information exchange and interactions with internal and external stakeholders; the production and dissemination of tactical, operational and strategic cyber threat intelligence, also to prevent and counteract cyber security incidents; alerting and artifact analysis.

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

The CERTBI is committed to keeping its constituency informed of potential vulnerabilities, possibly before they are actively exploited.

4.2. CO-OPERATION, INTERACTION AND DISCLOSURE OF INFORMATION

CERTBI 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

neighboring sites where necessary, the CERTBI will otherwise share information when this will assist others in resolving or preventing security incidents.

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

CERTBI observes the **CSIRT Code of Practice**.

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 considered to be similar to email for these purposes: sensitive data will be encrypted for transmission.

CERTBI 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 CERTBI 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

CERTBI is responsible for information security incident management, interacting with internal and external stakeholders in the context of cyber security incident response activities. CERTBI is responsible for the production and dissemination of tactical, operational and strategic cyber threat intelligence in order to prevent cyber security incidents and to effectively counter cyber threats, for sending out alerts and warnings to its constituency, for performing artifact analysis when necessary, and for providing assistance or advice with respect to the different incident response phases.

5.2. PROACTIVE ACTIVITIES

CERTBI services are based on FIRST CSIRT Services Framework and coordinates and maintains the following services for its constituency:

- Information Security Incident Management
    - Artifact and Forensic Evidence Analysis
    - Information Security Incident Coordination
    - Crisis Management Support
- Vulnerability Management
    - Vulnerability Discovery/Research
    - Vulnerability Report Intake
    - Vulnerability Disclosure
- Situational Awareness
    - Data Acquisition
    - Analysis and Synthesis
    - Communication
- Knowledge Transfer
    - Awareness Building
    - Training and Education
    - Exercises
    - Technical and Policy Advisory

6. Incident Reporting Forms

CERTBI does not provide any public form for reporting incidents.

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

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

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

7. Disclaimers

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