RFC2350

The BNG-CERT was set up using the RFC2350 guideline developed by the Network Working Group of IETF.org.

Document information

- **Version**: 1.0
- **Date last update**: 05-03-2025
- **Date last review**: 28-02-2025
- **Distribution list notifications update:** Notifications for distribution of this document are not provided. For information, contact the BNG-CERT e-mail address.
- **Location of publication of this document:** https://www.bngbank.com/security.

Contact information

- **Team name**: 'BNG-CERT', Computer Emergency Response Team of BNG
- **Postal Address**: BNG Bank N.V.
  attn BNG-CERT
  Postbus 30305
  2500 GH The Hague
  The Netherlands
- **Time zone:** BNG-CERT uses Central European Time (CET), including daylight saving Time (DST). GMT+0100 in winter and GMT+0200 in summer.
- **Phone number:** +44 1736 802 045 (PagerDuty)
- **Facsimile number**: none
- **Other telecommunications:** none
- **Public keys and encryption:** CERT will use PGP for encryption and digital signing.
- **Team members**: The BNG-CERT team members are not publicly known, the team members identify themselves to the contact when a security incident occurs.
- **Contact information**: BNG-CERT can be reached from 08:00 to 18:00 on +44 1736 802 045 (PagerDuty), support outside these hours is on a best effort basis. BNG-CERT can be reached by email at bng-cert@bngbank.nl.
- **Additionional contact information**: valse-email@bngbank.nl.

Charter BNG-CERT

Definition of a CERT

A Computer Emergency Response Team (CERT) is a specialized team of ICT professionals, capable of acting quickly in the event of a security incident involving computers or networks. The goal is to reduce damage and promote rapid recovery of services.

Mission Statement

The mission of BNG-CERT is to minimize the impact of an incident or damage resulting from a (cyber) attack or digital break-in.

Target group (constituents)

The target group of the BNG-CERT is entirely BNG, including external suppliers who play a crucial role in the processing of BNG data.

Goals

The objectives of the BNG-CERT are:

- To be the first point of contact and the connecting factor in information security incidents;
- To be able to act directly in information security incidents in the field of computers and networks;
- To combine the technical and functional expertise of BNG Bank employees in the handling of an information security incident;
- To reduce damage and promote fast recovery of services;
- To contribute to information security awareness at BNG.

Governance & Mandate

The BNG-CERT is part of the BNG Bank organization and is directly controlled by the BNG Cyber Defense Center. The Executive Committee of BNG has established the foundation, role and mandate of the CERT.

Competence

The BNG-CERT registers information security incidents and coordinates their handling. The BNG-CERT works together with the responsible employees and departments, if necessary also those of its suppliers and customers, and has an advisory role. However, if the circumstances require it, the BNG-CERT has the mandate to take measures that are appropriate to handle an incident adequately.

Policies

Type of incidents: BNG-CERT responds to all information security incidents that occur within its target group, with a focus on:

- Cyber-related incidents and threats;
- Data leaks;
- Ransomware;
- Abuse, such as phishing, spam, viruses and malware.

Collaboration and information sharing: Information provided to BNG-CERT will be treated as confidential or higher where necessary and will not be shared with third parties without prior consent, unless required by law. BNG-CERT uses the Traffic Light Protocol (TLP) in its communications with external parties.

Communication and authentication: BNG-CERT prefers communication by e-mail. BNG-CERT will use PGP keys for encryption and digital signing of confidential traffic. The BNG-CERT public keys will be published soon on https://www.bngbank.com/security and on the public PGP key servers.

Services

Incident triage: All incidents are registered and assessed for impact and priority. The triage will determine:

- Who are the stakeholders in the incident;
- What is the experience of the incident reporter;
- What is the severity of the incident;
- What are the time constraints of the incident.

Incident coordination: During the course of the incident, the cause of the incident is determined, the relevant contacts are made with internal and external stakeholders and, if necessary, the escalation process is initiated.

Incident handling: The BNG-CERT provides support through coordination between the relevant parties, external intelligence, evaluation, reporting and any follow-up activities.

Incident reporting

After resolving an incident, all parties involved will be informed. The following information must be included in the communication as a minimum:

- A brief description of the incident;
- Overview of actions taken and the associated results;
- The most important findings and recommendations.

Disclaimer

BNG-CERT cannot fully guarantee the accuracy and availability of all information. The BNG-CERT accepts no liability for damage caused by the absence or inaccuracy of the information provided.