KEYES

TYPE DE DIFFUSION
Public [1]

RESPONSABLE **ROSETTTE Arnaud**
DATE DE DIFFUSION 24/04/2026
DATE DE PÉREMPTION
VERSION 1.2

Security Management

KEYES-CSIRT RFC-2350

1 Document information

This document is the public RFC 2350 profile for the KEYES (previously known as NRB) Computer Security Incident Response Team or KEYES-CSIRT. It provides an overview of how to contact the team, its mission and constituency, its high-level operating policies (including information handling and secure communication expectations), and the security services it can provide. It also explains how to report incidents and where to find and authenticate the latest official version of this document. Certain operational details are intentionally limited for security reasons; support is provided to KEYES and, where applicable, to customers and partners under an appropriate agreement.

1.1 Date of last update

Please see section 8.1 Document management.

1.2 Distribution list for notifications

There is no distribution list for changes to this document. The latest version of this document can be found at the location listed in section 1.3.

1.3 Locations where this document may be found

The current version of this CSIRT description document is from the KEYES-CSIRT site; its URL is:
https://www.keyes.eu/fr/TBD
Please make sure you are using the latest version.

1.4 Authenticating this document

This document has been signed with the KEYES-CSIRT's PGP key.
The signature is available are on our website, its URL is https://www.keyes.eu/fr/TBD

2 Contact information

2.1 Name of the team

KEYES (previously known as NRB) Computer Security Incident Response Team or KEYES-CSIRT.

2.2 Address

KEYES-CSIRT
Parc Industriel des Hauts Sarts
2e Avenue 65
4040 Herstal
Belgium

2.3 Time zone

- In the winter: CET (Central European Time, UTC+1)
- In the summer: CEST (Central European Summer Time, UTC+2)

2.4 Telephone number

Belgian phone number +32 4 249 44 44.

2.5 Facsimile number

None available.

2.6 Other telecommunication

None available.

2.7 Electronic mail address

csirt@keyes.eu
This is a mail alias that relays mail to the human(s) on duty for the KEYES-CSIRT.

2.8 Public keys and other encryption information

The KEYES-CSIRT has a PGP key whose Key ID is **B5F6BE07DB354D12393AF822191E0D4191CA58D8**
Use: `gpg --recv-key 191E0D4191CA58D8`
The key and its signatures can be found at the usual large public key servers:

- keys.openpgp.org → linked to csirt@keyes.eu
- keyserver.ubuntu.com
- pgp.surfnet.nl
- pgp.circl.lu

2.9 Team Members

The Head of KEYES-CSIRT is Arnaud Rosette.
The team is composed of several staff members, and the list is not publicly available.

2.10 Other Information

KEYES-CSIRT is a member of:

- Belgian Cyber Security Coalition since 2022
- TF-CSIRT (listed member) since 2023

General information about KEYES can be found at https://www.keyes.eu/en/about

2.11 Points of Customer Contact

The preferred method for contacting the KEYES-CSIRT is via e-mail at csirt@keyes.eu; e-mail sent to this address will "biff" the responsible human, or be automatically forwarded to the appropriate backup person, immediately.
If you require urgent assistance, please call the KEYES-CSIRT on the emergency hotline 24x7 (phone number listed in 2.4).
The KEYES-CSIRT hours of operation are generally restricted to regular business hours (08:00-18:00 Monday to Friday except Belgian public holidays).
If possible, when submitting your report, use the form mentioned in section 6.

3 Charter

3.1 Mission statement

KEYES-CSIRT is a private team that delivers security services to KEYES entities as well as its customers since 01 Jan 1987. KEYES is a non-financial commercial organization.
The purpose of the KEYES-CSIRT is to assist its members and customers in implementing proactive measures to reduce the risks of computer security incidents, as well as responding to such incidents when they occur.

3.2 Constituency

KEYES-CSIRT's primary constituency is KEYES, including all its entities, subsidiaries, and the systems and infrastructure it operates. KEYES is located in Belgium and in several countries in Europe.
The secondary constituency consists of KEYES customers who have an existing service agreement covering cybersecurity support, as well as external organizations that seek to engage KEYES-CSIRT's services by establishing a formal agreement for incident response or related support activities.

3.3 Affiliation

KEYES- CSIRT is part of KEYES.

3.4 Authority

KEYES-CSIRT coordinates security incidents on behalf of its constituency and only at its constituents' request.
KEYES-CSIRT primarily acts as an advisor regarding local security teams and is expected to make operational recommendations. Therefore, KEYES-CSIRT may not have any specific authority to require specific actions. The implementation of such recommendations is not a responsibility of KEYES-CSIRT, but solely of those to whom the recommendations were made.
KEYES-CSIRT expects to work cooperatively with its constituents.

3.5 Domain, AS and IPs

3.5.1 Domains

- keyes.eu
- nrb.be

3.5.2 AS

- AS12942

3.5.3 IPs

- 217.117.32.0/19
- 2a02:7100::/32
- 2a02:7100:ffff::/48

4 Policies

4.1 Types of Incidents and Level of Support

KEYES-CSIRT addresses all types of cybersecurity incidents that occur within, or pose a threat to, its constituency (see section 3.2). This includes, but is not limited to, incidents such as malware infections, phishing attempts, ransomware attacks, data breaches, denial-of-service (DoS) attacks, unauthorized access, and vulnerabilities in systems or applications.
The level of support provided by KEYES-CSIRT depends on several factors, including the type and severity of the incident, its actual or potential impact, the criticality of the affected systems, the nature of the constituent involved, the size of the impacted community, and the available resources at the time of the request.

Depending on the incident, KEYES-CSIRT delivers a range of services, including incident triage and analysis, containment and eradication advice, recovery assistance, coordination with external partners, and digital forensic support.
Please note that KEYES-CSIRT does not provide direct support to individual end users. End users are expected to contact their local IT teams, Security Operations Center (SOC), or internal security contacts. KEYES-CSIRT provides support and guidance to these teams, helping them manage and resolve incidents effectively.

4.2 Co-operation, Interaction and Disclosure of Information

Information classification is based on the Traffic Light Protocol (TLP) version 2.0, for which the definition of the different levels can be found on the FIRST website.

4.3 Communication and Authentication

All communications classified “TLP:GREEN” and above MUST be sent through secure communication channels.

5 Services

The following services can be provided by KEYES-CSIRT. Those services are based on the FIRST CSIRT Services Framework (version 2.1)

5.1 Information Security Event Management

- Monitoring and detection
- Event analysis

5.2 Information Security Incident Management

- Information security incident report acceptance
- Information security incidents analysis
- Artefact and forensic evidence analysis
- Mitigation and recovery
- Information security incident coordination
- Crisis management support

5.3 Vulnerability Management

- Vulnerability discovery / research
- Vulnerability report intake
- Vulnerability analysis
- Vulnerability coordination
- Vulnerability disclosure
- Vulnerability response

5.4 Situational Awareness

- Data acquisition
- Analysis and synthesis
- Communication

5.5 Knowledge Transfer

- Awareness building
- Training and education
- Exercises
- Technical and policy advisory

6 Incident reporting forms

At present, KEYES-CSIRT has not developed dedicated local forms for incident reporting.
When reporting an incident to KEYES-CSIRT, please ensure that you provide sufficient information to facilitate effective handling and response. The following details are particularly important:

- Contact information (e.g., full name, email address, phone number, and PGP key if available)
- Organizational information (e.g., organization name and address)
- A clear description of the incident
- The observed or potential impact on business operations
- Identification of affected assets (systems, applications, data, etc.)
- A timeline of events leading up to and following the incident
- Actions already taken to mitigate or contain the incident
- Any relevant technical details (e.g., log files, indicators of compromise, system information)

Providing detailed and accurate information will significantly improve KEYES-CSIRT's ability to assist effectively.

7 Disclaimers

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

8 Appendices

8.1 Document management

Editor	Arnaud Rosette			
Updates	Version	Date	Description	
	1.0	23/10/2023	Initial version	
	1.1	23/10/2024	Updated version	
	1.2	18/03/2026	Updated version	
Validation	1.2	18/03/2026	Arnaud Rosette	Head of CSIRT
Approval	1.2	18/03/2026	Arnaud Rosette	Head of CSIRT
Document status	Final			