

## **CERT-NEXTER RFC 2350**

### **1. Document Information**

This document contains a description of CERT-NEXTER in accordance with RFC 2350<sup>1</sup> specification. It provides basic information about CERT-NEXTER, describes its responsibilities and services offered.

#### **1.1. Date of Last Update**

This is the version 1.0 released on CERT-NEXTER published on 2021-04-26.

#### **1.2. Distribution List for Notifications**

There is no distribution list for notifications.

#### **1.3. Locations where this Document May Be Found**

The current and latest version of this document is available at:

[https://www.nexter-group.fr/sites/default/files/CERT/RCF\\_2350.pdf](https://www.nexter-group.fr/sites/default/files/CERT/RCF_2350.pdf)

#### **1.4. Authenticating this Document**

This document has been signed with the PGP key of CERT-NEXTER

The PGP public key, ID and fingerprint are available on the CERT-NEXTER's website at:

[https://www.nexter-group.fr/sites/default/files/CERT/public\\_key.asc](https://www.nexter-group.fr/sites/default/files/CERT/public_key.asc)

#### **1.5. Document Identification**

Title: CERT-NEXTER\_RFC\_2350

Version: 1.0

Document Date: 2021-04-26

Expiration: this document is valid until superseded by a later version

---

<sup>1</sup> <https://tools.ietf.org/html/rfc2350>

## CERT-NEXTER RFC 2350

### 2. Contact Information

#### 2.1. Name of the Team

Short name: CERT-NEXTER  
Full name: Nexter Group CERT

#### 2.2. Address

Groupe Nexter  
13 Route de la Minière  
78034 Versailles

#### 2.3. Time Zone

CET/CEST: Europe/Paris (GMT+01:00, and GMT+02:00 on DST)

#### 2.4. Telephone Number

+33 1 39 49 85 85

#### 2.5. Facsimile Number

None available

#### 2.6. Other Telecommunication

None available

#### 2.7. Electronic Mail Address

[cert@nexter-group.fr](mailto:cert@nexter-group.fr)

#### 2.8. Public Keys and Encryption Information

PGP is used for functional exchanges with CERT-NEXTER

- User ID: CERT Nexter
- Key ID: 0x715FAEA2
- Fingerprint:

The public PGP key is available at:

[https://www.nexter-group-contrib.fr/sites/default/files/CERT/public\\_key.asc](https://www.nexter-group-contrib.fr/sites/default/files/CERT/public_key.asc)

It can be retrieved from one of the usual public key servers.

#### 2.9. Team Members

The CERT-NEXTER representative is Christophe DUBOIS.  
The full list of the team members is not publicly available.  
The team is made of Cybersecurity analysts.

**TLP:WHITE**

## **CERT-NEXTER RFC 2350**

### **2.10. Other Information**

See our web site at CERT-NEXTER for additional information about CERT-NEXTER

### **2.11. Points of Customer Contact**

CERT-NEXTER prefers to receive incident reports via e-mail at [cert@nexter-group.fr](mailto:cert@nexter-group.fr).

Please use our PGP key to ensure integrity and confidentiality.

In case of emergency, please specify the [URGENT] tag in the subject field in your e-mail.

CERT-NEXTER operates during regular business hours (8:30AM to 5:30PM UTC+1 from Monday to Friday).

## CERT-NEXTER RFC 2350

### 3. Charter

#### 3.1. Mission Statement

Nexter Group CERT is the Computer Emergency Response Team for Nexter Group. Its mission is to manage incident response for the member of its constituency.

#### 3.2. Constituency

Our constituency is detailed at the following link :

<https://www.nexter-group.fr/en/filiales/nexter.html>

#### 3.3. Sponsorship and/or Affiliation

CERT-NEXTER is owned, operated and financed by the Nexter Group. It maintains relationships with different CSIRTs in France.

#### 3.4. Authority

CERT-NEXTER operates under the authority of the Nexter Group CISO.

## CERT-NEXTER RFC 2350

### 4. Policies

#### 4.1. Types of Incidents and Level of Support

CERT-NEXTER manages all type of cybersecurity incident within its constituency.

The level of support depends on the incident severity.

#### 4.2. Co-operation, Interaction and Disclosure of Information

CERT-NEXTER shares information with other CSIRTs. Incident information is not publicly disclosed without the agreement of all involved parties.

#### 4.3. Communication and Authentication

CERT-NEXTER supports the Information Sharing Traffic Light Protocol.

The preferred method of communication is email. Sensitive information should be encrypted using our PGP key.

## CERT-NEXTER RFC 2350

### 5. Services

#### 5.1. Incident response

The following incident response activities are supported by CERT-NEXTER:

- Incident handling
- Digital forensics
- Incident response coordination

#### 5.2. Proactive activities

The following proactive activities are supported by CERT-NEXTER:

- Exercises
- Network and systems monitoring
- Threat hunting
- Internal communication for specific threats

## CERT-NEXTER RFC 2350

### 6. Incident Reporting Forms

No incident response form is in use in CERT-NEXTER.

Any report should include:

- Date/time of the incident or events, including the timezone
- IP/hostname/username involved in the incident
- Factual description of the incident
- Contact name
- Any other relevant information

Any sensitive information should be encrypted using either the CERT-NEXTER PGP public key or any other encryption method supported by CERT-NEXTER.

### 7. Disclaimers

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