

NAMESHIELD CERT

Established according to
RFC2350

Version History			
Document Version	Date	Document validation	Change Step
V 1.0	20210210	PB	Creation
V 1.1	20210223	PB	Requested changes
V 2.0	20210409	PB	Version for pre-submission
V 2.1	20210504	PB	Refining constituency
V 2.2	20210723	BS	Corrections according to the security team
V 3.0	20210906	BS	Evolution of provided services
V 3.1	20211012	BB	Requested changes
V 3.2	20211029	QA	Requested changes



Sources may use **TLP: WHITE** when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.

TLP : WHITE Information may be distributed without restriction, subject to copyright controls.

Table of Contents

- 1. DOCUMENT INFORMATION..... 3
 - 1.1 Date of last update..... 3
 - 1.2 Distribution list for notifications..... 3
 - 1.3 Locations where this document may be found..... 3
 - 1.4 Authenticating this document..... 3
 - 1.5 Document Identification..... 3
- 2. CONTACT INFORMATION..... 4
 - 2.1 Name of the team..... 4
 - 2.2 Address..... 4
 - 2.3 Time Zone..... 4
 - 2.4 Telephone Number..... 4
 - 2.5 Other Communication..... 4
 - 2.6 Electronic Mail Address..... 4
 - 2.7 Public Keys and Encryption Information..... 5
 - 2.8 Team Members..... 5
 - 2.9 Other Information..... 5
 - 2.10 Points of Reports for Incidents..... 5
- 3. CHARTER..... 6
 - 3.1 Mission Statement..... 6
 - 3.2 Constituency..... 6
 - 3.3 Affiliation..... 6
 - 3.4 Authority..... 6
- 4. POLICIES..... 7
 - 4.1 Types of Incidents and Level of Support..... 7
 - 4.2 Co-Operation, Interaction and Disclosure of Information..... 7
 - 4.3 Communication and Authentication..... 7
- 5. SERVICES..... 9
 - 5.1 Incident Handling..... 9
 - 5.2 Security Consulting..... 9
 - 5.3 Awareness Building..... 9



6. INCIDENT REPORTING FORMS.....10

7. DISCLAIMERS.....11



1. DOCUMENT INFORMATION

This document contains a description of CERT-NS according to RFC 2350. RFC 2350 is an IETF Best Current Practice available at: <https://www.ietf.org/rfc/rfc2350.txt>.

We provide therein basic information about the CERT-NS team, the way it is operated and how it can be contacted. It also describes its missions, roles and responsibilities, and offered services.

1.1 Date of last update

The current version of this document is V 3.2 as of October 20th 2021. It corresponds to a version that defines more specifically provided missions of CERT-NS.

1.2 Distribution list for notifications

There is no Distribution List to inform of changes made to this document.

1.3 Locations where this document may be found

The current and latest version of this document is available from CERT-NS' website at :

<https://cert.nameshield.net/rfc2350.pdf>

1.4 Authenticating this document

This document has been signed with the CERT-NS' PGP key. The signature is available from the same location as the document itself on the CERT website at :

<https://cert.nameshield.net/rfc2350.pdf.sig>

Cert-NS' public PGP key is given at chapter [2.7](#) below.

1.5 Document Identification

- Title : NAMESHIELD CERT - RFC 2350
- Version : 3.2
- Document Date : 2021-10-29
- Expiration: this document is valid until superseded by a later version.



2. CONTACT INFORMATION

This section describes how to contact CERT-NS

2.1 Name of the team

- Short Name : CERT-NS
- Official Name : NAMESHIELD CERT

2.2 Address

CERT-NS
NAMESHIELD CERT
79 rue Desjardins
49100 ANGERS

FRANCE

2.3 Time Zone

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

DST: Daylight Saving Time or Summer Time, starts on the last Sunday in March and ends on the last Sunday in October.

2.4 Telephone Number

This is the direct ligne to join a member of Nameshield CERT. It is mean to be used for urgent case only.

CERT-NS : +33 2 85 29 32 52

2.5 Other Communication

Other channels for contacts is communicated to third parties once a trustful relationship has been established. Initial contact may be established via phone, but most preferably via email. See Electronic Mail Address in 2.6.

2.6 Electronic Mail Address

Please, contact us at: [cert \[at\] nameshield.net](mailto:cert@nameshield.net)



2.7 Public Keys and Encryption Information

CERT-NS uses the following PGP Key:

- USER-ID : CERT Nameshield (CERT-NS) <[cert \[at\] nameshield.net](mailto:cert@nameshield.net)>
- KEY-ID : **0xb5051da5fdec46ef**
- Fingerprint : **F107 B07E 70C2 87DA 0C0C 333D B505 1DA5 FDEC 46EF**

The current CERT-NS' key can be found at the URL: <https://cert.nameshield.net/cert-ns.pub>

The key can also be retrieved from the usual public key servers, such as <https://pgp.mit.edu/>. The key shall be used whenever information must be sent to CERT-NS in a secure manner.

2.8 Team Members

The head of CERT-NS is Arnaud Jolivet.

The rest of CERT-NS team members is not publicly available. Full identity of team members is communicated to third parties during resolution of incidents, once a trustful relationship has been established.

The team consists of IT Security Analysts.

2.9 Other Information

General information about CERT-NS can be found at the following URL: <https://cert.nameshield.net>

Operating hours of CERT-NS:

- Business days : Monday to Friday 9 am to 6 pm
- French public holidays : *closed*

2.10 Points of Reports for Incidents

CERT-NS will preferentially receive incident reports via e-mail at [cert \[at\] nameshield.net](mailto:cert@nameshield.net). Use of our cryptographic key will ensure integrity and confidentiality. E-mail will be processed by a member of the CERT-NS team, and then a ticket will be created automatically in our tracking system.



In case of emergency, please specify URGENT in the subject field in your e-mail. Urgent cases may also be reported by phone, although we better recommend mailing.



3. CHARTER

This section describes CERT-NS' mandate.

3.1 Mission Statement

As a key actor of Domain Name System cybersecurity, Nameshield commits itself to reach the best levels of security for its customers, by anticipating and treating all the threats that concern them. That's why it became ISO27001 certified in 2017, which was a mean to engage all of its collaborators in a never-ending security improvement process.

In order to gain an upper level of excellence in terms of security, Nameshield has decided to create a Security Team, a CERT, that can bring security experience, skills and professionalism in all the processes that are handled by the collaborators : Incident Response, Risk management, Technology Watch and others.

3.2 Constituency

CERT-NS' primary constituency is composed of all the elements of NAMESHIELD Information System: its users, its systems, its applications and its networks.

3.3 Affiliation

CERT-NS is affiliated to NAMESHIELD group: <https://www.nameshield.com>

CERT-NS maintains contact with various national and international CSIRT and CERT teams, on an as-needed basis.

3.4 Authority

CERT-NS coordinates incidents on behalf of its constituency, and only at its constituents' request. Consequently, CERT-NS operates under the auspices of, and with authority delegated by its constituents.

Generally, CERT-NS expects to work co-operatively with its constituents' system and application administrators and users.

CERT-NS operates under the authority of Information Systems Division.



4. POLICIES

This section describes CERT-NS' policies.

4.1 Types of Incidents and Level of Support

CERT-NS handles all types of incidents met by Nameshield, i.e. incidents within the cyber space impacting online assets of customers, as well as cyberattacks impacting the integrity and availability of Nameshield's IT systems.

The level of support given by CERT-NS will vary depending on the severity of the incident or issue, its potential or assessed impact and the availability of the CERT-NS' resources at the time of the incident.

4.2 Co-Operation, Interaction and Disclosure of Information

CERT-NS considers the paramount importance of operational coordination and information sharing between CERTs, CSIRTs, SOCs and similar bodies, and also with other organizations, which may aid to deliver its services or which provide benefits to CERT-NS' constituency.

Consequently, CERT-NS exchanges all necessary information with affected parties, as well as with other CSIRTs, on a need-to-know basis using the Traffic Light Protocol. However, neither personal nor overhead data are exchanged unless explicitly authorized. Moreover, CERT-NS will protect the privacy of its constituents, and therefore pass on information in an anonymized way only.

All incoming information is handled confidentially by CERT-NS, regardless of its priority.

All sensible data, such as personal data, system configurations, known vulnerabilities with their locations, are stored in a secure environment, and are encrypted if they must be transmitted over unsecured environment as stated below.

CERT-NS operates within the current French legal framework.

4.3 Communication and Authentication

CERT-NS protects sensitive information in accordance with relevant French, European and international regulations and policies for applicable jurisdictions. Communication security, including both encryption and authentication, is



achieved by using PGP or any other agreed and tested means, depending on sensitivity and context.

The preferred method of communication is email. Unencrypted email will not be considered particularly secure, but will be sufficient for the transmission of low-sensitivity data. For the exchange of sensitive information and authenticated communication, CERT-NS uses several encryption solutions. By default, all sensitive communication to CERT-NS should be encrypted with our public PGP key detailed in Section 2.8.

Telephones will be considered sufficiently secure to be used (even unencrypted), in view of the types of information that CERT-NS deals with. Network file transfers will be considered to be similar to email for these purposes: sensitive data should be encrypted for transmission.



5. SERVICES

This section describes CERT-NS' services. These services are primarily delivered to CERT-NS' constituency.

5.1 Incident Handling

Providing *Incident Handling* service means that the security team receives, triages and responds to incident requests or vulnerability reports. As the security team works in the same building than Nameshield, it is able to provide physical on-site assistance to help the constituency recover from an incident.

5.2 Security Consulting

CERT-NS helps technical teams of its constituency in detection and evaluation of security risks by carrying an expert vision of threats, vulnerabilities and counter-measures at different steps of projects. By this way, the team provide guidance for Risk Analysis, Business Continuity and Disaster Recovery Planning, or other formal or informal security workshop.

5.3 Awareness Building

The CERT team has the mission to increase the general security awareness of its constituency. It means that the team does not only have to improve understanding of security issues by Nameshield employees, but also helps them perform their day-to-day operations in a more secure manner.



6. INCIDENT REPORTING FORMS

CERT-NS does not provide any incident report form for its constituency. All contacts will be established by email or phone.

To report an incident, please provide the following details to CERT-NS:

- Contact details and organizational information.
- Email address, phone number, PGP key if available.
- IP address(es), FQDN(s), and any other relevant technical element.
- Supporting technical elements such as logs, proof of concept, screenshots, or any artefact that can help our analysts to process your report.



7. DISCLAIMERS

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