MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

Gendarmerie nationale

RFC – 2350

(DESCRIPTION OF SERVICES)

TLP	**TLP:CLEAR** TLP:CLEAR information may be shared without restriction
Reference	CERT-GN-UNCYBER-RFC2350-EN
Version	8.0
Date	June 3rd, 2025

Unité Nationale Cyber
5 boulevard de l'Hautil
95001 CERGY-PONTOISE Cedex - FRANCE
cert@gendarmerie.interieur.gouv.fr

Table of content

Version history

Version	Date	Author	Change description	Add.	Change	Remov.
1.0	18-Sep-22	AMARCHAND	Document creation	X		
2.0	22-Sept-22	AMARCHAND	Document update		X	
3.0	22-Sept-22	AMARCHAND	Document update		X	
4.0	04-Oct-22	AMARCHAND	Document update		X	
5.0	06-Oct-22	AMARCHAND	Document update		X	
6.0	06-Dec-22	GLEONE	Document update		X	
7.0	13-Dec-22	GLEONE	Document update		X	
7.1	08-Feb-23	GLEONE	Document update		X	
7.2	14-Mar-23	GLEONE	Document update		X	
7.3	31-Mar-23	GLEONE	Document update		X	
8.0	03-Jun-25	ALEFEBVRE	Document update		X	

1 ABOUT THIS DOCUMENT

Foreword : This document describes the CERT-GN services in compliance with the RFC 2350 document[1].

1.1 Date of Last Update

The current version of this document is version 8.0 and was released on June, 3rd 2025.

1.2 Distribution List for Notifications

There is no Distribution List, or other dissemination mechanism, to inform of changes made to this document.

1.3 Location where this Document May be Found

The current and latest version of this document is available from Gendarmerie Nationale's website. Its URL is :
https://www.gendarmerie.interieur.gouv.fr/contact/cert/CERT-GN-UNCYBER-RFC2350-EN.pdf

1.4 Authenticating this Document

This document has been signed with the CERT-GN PGP key and the signature file is available at the same location as the document itself.

CERT-GN public PGP key is given at chapter 2.7 below.

2 CONTACT INFORMATION

2.1 Name of the Team

Short name : **UNCyber**
Full name : "**U**nité **N**ationale **Cyber**"

2.2 Address

Unité Nationale Cyber
5 boulevard de l'Hautil
95001 CERGY-PONTOISE Cedex
France

1 RFC 2350 is an IETF Best Current Practice available at : https://www.ietf.org/rfc/rfc2350.txt

2.3 Time Zone

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

2.4 Telephone Number

+33 (0) 787 417 671

2.5 Other Telecommunication

None available

2.6 Electronic Email Address

cert@gendarmerie.interieur.gouv.fr

2.7 Public Keys and Other encryption Information

CERT-GN PGP public key information are :

- KeyID : 0x7AB2122A
- Fingerprint : 34EA 0E93 F0C7 2626 E568 A71A FE46 690A 7AB2 122A

CERT-GN public PGP key is available at the following location :
https://keys.openpgp.org/search?q=FE46690A7AB2122A

2.8 Team Members

The team is composed of security experts who work on CERT-GN activities.
The list of the team members is not publicly available.

2.9 Operating Hours

CERT-GN can be joined on business hours : Monday to Friday, 9:00AM to 6:00PM.
CERT-GN is closed on French public holidays.

2.10 Additional Contact Info

General information about CERT-GN can be found at the following URL :
https://www.gendarmerie.interieur.gouv.fr/contact/cert

The section "Contact" on the Gendarmerie nationale public website provides advice to contact us :
https://www.gendarmerie.interieur.gouv.fr/contact

3 CHARTER

3.1 Mission statement

CERT-GN is a multidisciplinary composent that brings the expertise of the various services of the french 'Gendarmerie Nationale', including the **National Cyber Unit** (Unité Nationale Cyber / **UNCyber**) which constitutes its entry point.

The **National Cyber Unit (UNCyber)** is an operational entity with national jurisdiction. Its aim is to tackle serious and organised cybercrime.

The **UNCyber** is in charge of conducting judicial investigations, carrying out technical aspects of investigations and gathering operational intelligence.

Its area of expertise covers various aspects, such as national and international cooperation, cybercrime intelligence, complex cybercrime investigations, cyberattacks, online traffickings and child abuse. The unit also conducts open source investigations in order to provide additional intelligence to the ongoing cases.

A UNCyber detachment is embedded in the National Operations Center (CNO) at the French Gendarmerie Headquarters.

In addition to its capabilities, the UNC can benefit from the support of other units of the Gendarmerie, and ministerial components, to strengthen its actions.

CERT-GN missions are to :

- Monitor open and underground sources in order to identify any new major cyber threats and attacks within the French Cyberespace ;
- With the support of various stakeholders, gather information, analyse and provide cyber intelligence, thematic reports and synthesis ;
- Inform French Gendarmerie Nationale Cyber Units, at central and local levels of significant events in this field, and enhance their level of knowledge about the threats, authors and types of attacks ;
- Share cyber threat intelligence with other Public Actors and Private Companies and conduct actions to sensitize this ecosystem on Cyber threats ;
- Be the go-between between the Gendarmerie Nationale's national cyber unit and cyber security teams in France and around the world ;
- Act as an interface between the digital forensics and investigative high-level experts of the Gendarmerie Nationale's cyberspace command and the French CERT/CSIRT community ;
- Provide information and anticipation on threats, to proactively reduce the threat risk, and provide assistance, tools and know-how to assist in crisis management.

3.2 Constituency

The CERT-GN constituency is Gendarmerie Nationale investigation units.

3.3 Sponsorship / affiliation

CERT-GN is a public entity of the Law and Order sector. It is owned, operated and financed by the **UNCyber** (Gendarmerie nationale's national cyber unit).

It maintains relationships with different CSIRT-CERTs in France, Europe and beyond.

3.4. Authority

CERT-GN operate under the auspices of, and with the authority delegated by, the Commander of the National Cyber Unit (**UNCyber**). CERT-GN strives to work cooperatively with IT Managers, System Administrators, SOC, law enforcement agencies at the European and international level, etc.

CERT-GN services are performed by a technical team composed of officers, non-commissioned officers and specialised staff of the French Gendarmerie.

4 POLICIES

4.1. Types of incidents and level of support

CERT-GN may be involved in all types of cybersecurity incidents that may occur within its constituencies. The level of support depends on the type and severity of the given security incident, the amount of affected entities and available resources at the time.

CERT-GN can then provide contextualised intelligence on threats, attacks and threat actors, incident coordination service and crisis management support.

On a permanent basis, CERT-GN informs its constituencies about threats, modus operandi and vulnerabilities, especially new and emerging ones.

Anyone who is aware of a cyber-incident that might have a criminal purpose or origin may contact CERT-GN to share information on this incident, its characteristics and, if applicable, authors.

4.2. Co-operation, interaction and disclosure of information

To fulfill their missions, CERT-GN develop and maintain communication channels with other organisations and entities, among which other CERT or CSIRT teams, public administrations, private organisations, law enforcement agencies and anti-cybercrime units at the European and International level.

Information provided to CERT-GN may be shared with Gendarmerie Nationale entities, as well as with other public or private interlocutors, in compliance with the TLP defined by the information source and national legislation.

A such CERT-GN protect sensitive information in compliance with relevant law and regulations that may apply.

- CERT-GN apply Traffic Light Protocol (TLP - as define by FIRST : https://www.first.org/tlp/) when sharing information.
- The Gendarmerie is a Law and Order force. As a result, some of the information processed by CERT-GN is covered by various protective measures (National Defence Secret, Judicial Investigation Secret, etc...). These protection measures are imposed on the exchanges between CERT-GN and their various interlocutors.

4.3. Communication and authentification

The preferred means of communication is email.

For exchanges within the Gendarmerie, CERT-GN use the Gendarmerie's own secure messaging system. When sent on non-secure communication channels such as email, sensitive information is encrypted. Unencrypted email can only be used to submit non-sensitive information, and will not be considered as secure.

For the exchange of sensitive information and authenticated communication, CERT-GN prefers the use of PGP to encrypt data. CERT-GN public PGP key is detailed in Section 2.7.

In view of the types of information that CERT-GN usually deal with, telephone will be considered sufficiently secure to be used even unencrypted. However, CERT-GN will not exchange highly sensitive detailed information through telephone and ask counterparts to proceed with encrypted emails.

5 SERVICES

5.1. Incident Response

CERT-GN is informed about all security incident that occurs in its different constituencies.

CERT-GN will assist and liaise with Gendarmerie’s entities and affiliates in :

- Monitoring and knowledge of artifacts, incidents, threats and attacks ;
- Incident handling, including analysis, response, response support and response coordination ;
- Crisis management, preparation and training ;

- Liaison with counterparts, association, other CERTs and legal, communication and operational teams for ongoing technical security investigations.

The level of service provided by CERT-GN depends on the ecosystem (SOC, operational entities, forensic team) needs.

However, CERT-GN provides the collection, analysis and cross-checking of information on the threats and attacks and will ensure the relevant dissemination of the edited intelligence and related prevention tools.

5.2 Proactive Activities

With the support of various stakeholders, CERT-GN provide their interlocutors with a set of proactive Watch, Monitoring and Intelligence services on the basis of their right to know. This set can include :

- Annual reports on the threats landscape ;
- Security advisories ;
- Alerts ;
- Attack/Threats/Authors datasheets ;
- Prevention tools.

6 INCIDENT REPORTING FORMS

CERT-GN provide its interlocutors and associated services with the tools, forms and contact points necessary for the most effective, rapid and secure communication.

There is no specific security incident reporting form. Incidents should be reported via encrypted email or deposited in the various relevant databases to which CERT-GN has access.

7 DISCLAIMERS

While every precaution will be taken in the preparation of information, notifications and alerts, CERT-GN shall not be responsible for any errors or omissions, or for any damages resulting from or arising out of the use of the information contained herein and therein.

END OF DOCUMENT