# AXA CERT RFC 2350

## Document control

**From** AXA CERT
**Entity** AXA CYBER DEFENCE
**Date** 2019-08-07

Document location https://cert.axa/sources/AXA-CERT-RFC2350.pdf
Document Classification Public / TLP: WHITE

# Table of Content

# 1 Document Information

This document contains a description of AXA CERT according to RFC 2350.

It provides information about the CERT, how to contact the team, and describes its responsibilities and the services offered by AXA CERT.

## 1.1 Document Identification

Title: 'AXA CERT RFC 2350'
Version: 1.2
Document Date: 2019-08-07
Expiration: this document is valid until superseded by a later version.

## 1.2 Date of Last Update

Version 1.2, published on 2019-08-07.

## 1.3 Distribution List for Notifications

There is no distribution list for notifications.

## 1.4 Locations where this Document May Be Found

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

https://cert.axa/sources/AXA-CERT-RFC2350.pdf

## 1.5 Document Authenticity

This document has been signed with the PGP key of AXA CERT. The signature is available on AXA CERT's website. Its URL is:

https://cert.axa/sources/AXA-CERT-RFC2350.pdf.sig

# 2 Contact Information

## 2.1 Name of the Team

AXA CERT

## 2.2 Address

AXA CERT
81 rue Mstislav Rostropovitch
75 017 Paris
France

## 2.3 Time Zone

CET/CEST (UTC +1/UTC +2), Central European Time / Central European Summer Time.

## 2.4 Telephone Number

+33 1 42 29 08 15

## 2.5 Facsimile Number

None available.

## 2.6 Other Telecommunication

None.

## 2.7 Electronic Mail Address

Shall you need to notify us about a cyberthreat or an information security incident targeting or involving AXA or any of its subsidiaries, please contact us at:

cert@axa.com

## 2.8 Public Keys and Encryption Information

To send us information securely, please use our PGP key:

- ID: **0x676D7D05**
- Fingerprint: **3C3E 08E3 FDC8 1473 CD4B DCE6 B2A5 A31D 676D 7D05**

The key is available on the usual public key servers such as http://pgp.mit.edu/.

## 2.9 Team Members

The team leader is Marcos Orallo. The team consists of IT security professionals.

## 2.10 Other Information

The AXA CERT webpage is available at: https://cert.axa.

## 2.11 Points of Customer Contact

AXA CERT prefers to receive incident reports via e-mail. Please use our cryptographic keys above to ensure integrity and confidentiality.

AXA CERT's hours of operation are usually restricted to regular French business hours (09:00-18:00 Monday to Friday). For out of business hours support in case of critical security incidents, AXA CERT has Incident Response Specialist available on on-call duty.

# 3 Charter

## 3.1 Mission Statement

AXA CERT is responsible for providing alerts and warnings, intrusion detection services, incident handling, artifact handling and development of security tools for AXA Group companies and subsidiaries.

## 3.2 Constituency

AXA CERT constituency is composed of all AXA Group companies and subsidiaries. For more details please refer to https://www.axa.com/en/about-us/axa-world-map.

## 3.3 Sponsorship and/or Affiliation

AXA CERT is the Global Security Incident Response Team (SIRT) for AXA Group.

## 3.4 Authority

We coordinate security incidents involving our constituency.

# 4 Policies

## 4.1 Types of Incidents and Level of Support

AXA CERT addresses all types of security incident which occur, or threaten to occur, within AXA Group companies and subsidiaries.

Depending on the type and severity of the security incident, AXA CERT will roll out its services which include incident response and digital forensics.

The level of support given by AXA CERT depends on the severity of the security incident, its impact and the availabilities of AXA CERT's resources at the time.

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

AXA CERT value the importance of operational coordination and information sharing between CERTs, CSIRTs, SOCs and similar entities.

AXA CERT will exchange all necessary information with these entities with the respect of the French and European legal frameworks.

AXA CERT also complies with CCoP (CSIRT Code of Practice) version 2.4[1].

## 4.3 Communication and Authentication

AXA CERT complies with French and European regulations for securing and protecting sensitive information.

AXA CERT mainly ensures the security of communications by using PGP. Other agreed means could be used depending on the sensitivity level and context.

AXA CERT also supports the ISTLP[2] (Information Sharing Traffic Light Protocol).

# 5 Services

## 5.1 Reactive Activities

The team offers the following reactive services:

- Alerts and Warnings
- Incident Handling

[1] https://www.trusted-introducer.org/TI-CCoP.pdf
[2] https://www.trusted-introducer.org/ISTLPv11.pdf

- Artifact Handling

## 5.2 Proactive Activities

The team offers the following proactive services:

- Intrusion detection services
- Development and deployment of Security Tools

# 6 Incident Reporting Forms

No incident reporting form has been developed to report incidents to AXA CERT. Please report security incidents via encrypted e-mail to cert@axa.com with at least the following information:

- Contact details and organizational information
- IP address(es), FQDN(s), and any other relevant technical element with associated observation
- Any relevant information about a threat or an incident related to AXA CERT constituency

# 7 Disclaimers

While all precautions are taken in the preparation of information, notifications and alerts, AXA CERT assumes no responsibility for errors or omissions, or for damages resulting from the use of the information it provides.