RFC2350

A2A-CERT

1. DOCUMENT INFORMATION

1.1. ABOUT THIS DOCUMENT

This document contains a description of A2A - Computer Emergency Readiness Team (hereinafter referred as to A2A-CERT) in according to RFC 2350. It defines the basic information related to A2A-CERT, including a brief explanation of the tasks and services offered and contacts to get in touch with us.

1.2. DATE OF LAST UPDATE

Version 1.0, updated on 15/12/2021.

1.3. LOCATIONS WHERE THIS DOCUMENT MAY BE FOUND

The current and latest version of this document is available on A2A website.

Its URL is https://www.a2a.eu/it/gruppo/chi-siamo/a2a-cert

1.4. AUTHENTICATING THIS DOCUMENT

This document has been signed with the GPG key of A2A-CERT.

The public GPG key is available in A2A-CERT website.

1.5. DOCUMENT IDENTIFICATION

Title: A2A-CERT_RFC 2350

Version: 1.0.

Document Date: 15/12/2021

Expiration: this document is valid until a later version is issued.

2. CONTACT INFORMATION

2.1. NAME OF THE TEAM

Full Name: A2A-Computer Emergency Readiness Team

Short Name: A2A-CERT

2.2. ADDRESS

Postal Address: Corso di Porta Vittoria 4, Milano, 20122, Italy

2.3. TIME ZONE

Central European (GMT+0100 and GMT+0200 from the last Sunday of March to the last Sunday of October).

2.4. TELEPHONE NUMBER

N/A

2.5. ELECTRONIC MAIL ADDRESS

The e-mail iris@a2a.eu is available to contact A2A-CERT. All members of A2A-CERT team can read the messages sent to this address.

2.6. PUBLIC KEYS AND OTHER ENCRYPTION INFORMATION

In order to guarantee the security of communications the GPG technology is employed. A2A-CERT's public GPG key for iris@a2a.eu is available on A2A-CERT website.

A2A-CERT's Public Key:

- USER-ID: A2A-CERT iris@a2a.eu
- KEY-ID: 4AEB A929 3358 EBC9
- Fingerprint: 4A87 60F5 C2C0 EC9D 1B99 7AB8 4AEB A929 3358 EBC9

Third parties shall use GPG public key to establish a secure communication with A2A-CERT

2.7. TEAM MEMBERS

A2A-CERT's Team is composed by the Managing Executive, namely Alessandro Marzi (Head of CERT) and the Operational Manager, namely Denis Tassone (Deputy Head of CERT and CERT Analysts leader).

3. OTHER INFORMATION

General information about A2A-CERT is available on A2A website: its URL is https://www.a2a.eu/it/gruppo/chi-siamo/a2a-cert.

3.1. POINTS OF CUSTOMER CONTACT

The email address iris@a2a.eu is the preferred method to contact A2A-CERT.

The mailbox is monitored 24/7.

The use of GPG is mandatory when confidential or sensitive information are involved.

If for security reasons it is not possible to get in touch with A2A-CERT via e-mail, the contact may take place via telephone.

3.2. CHARTER

3.2.1. MISSION STATEMENT AND CONSTITUENCY

A2A-CERT is the main reference point for monitoring, analyzing and sharing information on cyber threats that target the Group. In the event of a cyber incident, A2A-CERT takes action to contain and eradicate the threat and restore the systems impacted.

In collaboration with other national and international organizations, A2A promotes interaction and exchange of cyber security information to increase knowledge and capabilities to identify threats, anticipate related risks and respond effectively to cyber attacks.

3.2.2. CONSTITUENCY

The Constituency consists of the entire A2A Group. A2A-CERT provides the Group's companies - including subsidiaries and their assets - with the whole Cyber Defence service portfolio, as established within the service contracts. Furthermore, A2A-CERT focuses on protecting and safeguarding the Constituency's business infrastructures and services - as well as the confidentiality, integrity and availability of its information assets - from potential threats within the cyberspace, by preventing, containing and neutralizing malicious events both within the Information Technology (IT) and Operational Technology (OT) environments.

3.2.3. SPONSORSHIP AND/OR AFFILIATION

A2A-CERT is affiliated to A2A S.p.A.

It maintains contacts with various national and international CERT and CSIRT teams, with FIRST, TFCSIRT, ENISA and Carnegie Mellon University according to its needs and to its culture of information exchange.

3.2.4. AUTHORITY

The establishment of the A2A-CERT was mandated on 17/12/2020.

3.3. POLICIES

3.3.1. TYPE OF INCIDENT AND LEVEL OF SUPPORT

A2A-CERT manages and addresses information security incidents, which occur or threaten to occur within its constituency. The level of support given by A2A-CERT will vary depending on the severity of the information security incident, the assets impacted and the CERT's currently available resources.

3.3.2. CO-OPERATION, INTERACTION AND DISCLOSURE OF INFORMATION

A2A-CERT highly values the importance of operational coordination and information sharing among CERTs, CSIRTs, SOCs and similar parties, as well as other organizations, which may aid them in delivering their services or provide other benefits.
A2A-CERT recognizes and supports ISTLP (Information Sharing Traffic Light Protocol).

3.3.3. COMMUNICATION AND AUTHENTICATION

A2A-CERT protects sensitive information in accordance with relevant local regulations and policies. Communication security (which includes both encryption and authentication) is primarily achieved using GPG or any other agreed means, depending on the sensitivity level and context.

4. SERVICE

4.1. INCIDENT MANAGEMENT

A2A-CERT continuously monitors security events in order to identify and respond effectively and promptly to security incidents detected within its perimeter, containing the impacts and preventing their future occurrence. Incident management process as developed by A2A-CERT covers all the following steps:

- Preparedness and prevention;
- Detection;
- Analysis;
- Response;
- Recovery.

4.2. THREAT INTELLIGENCE

A2A-CERT collects and analyses information on known and emerging cyber threats within its Cyber Threat Landscape, in order to increase knowledge on tactics, techniques and procedures adopted by attackers and prevent or anticipate the occurrence of threats.

5. INCIDENT REPORTING FORM

A2A-CERT does not provide any incident reporting form in a public web page.
As for A2A-CERT's constituency, the incident reporting must follow the internal procedures.

6. DISCLAIMERS

While every precaution will be taken in the preparation of information, notifications and alerts, A2A CERT assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained within.