AKCESK | AUTORITETI KOMBËTAR PËR CERTIFIKIMIN ELEKTRONIK DHE SIGURINË KIBERNETIKE

# RFC 2350 description for AKCSESK

# (National Cyber Security Incident Response Team)

Autoriteti Kombetar per Certifikim Eletrokin dhe Sigurine Kibernetike
Rruga. "Papa Gjon Pali II", Nr. 3, Kati I Tiranë Shqipëri 04-22-21039
Email: info@cesk.gov.al
Web: www.cesk.gov.al

# Contents

# 1. About this document

This document contains a description for the National CSIRT of Republic of Albania according to RFC 2350. It provides basic information about the National CSIRT, the ways it can be contacted, describes its responsibilities and the services offered.

## 1.1 Date of Last Update

This is version 1 of 20/03/2020

## 1.2. Distribution List for Notifications

There is a distribution list for notifications only for the Critical and Important Information Infrastructures' point of contacts in the Republic of Albania. Any other specific questions or remarks please address to the AKCESK mail address.

## 1.3. Locations Where This Document May Be Found

The current version of this CSIRT description document is available from the AKCESK website – https://cesk.gov.al/legjislacioni/index.html

# 2. Contact Information

## 2.1. Name of the Team

In Albanian: AKCESK, Autoriteti Kombetar per Certifikimin Elektronik dhe Sigurine Kibernetike

In English: NAECCS, National Authority for Electronic Certification and Cyber Security

## 2.2. Address

Autoriteti Kombetar per Certifikimin Elektronik dhe Sigurine Kibernetike

Rruga: "Papa Gjon Pali II", Nr 3, Kati I, Tirane, Shqiperi

## 2.3. Time Zone

GMT, Greenwich Mean Time (GMT+01, from the last Sunday in October to the last Saturday in March)
GMT, Greenwich Mean Time (GMT+02, from the last Sunday in March to the last Saturday in October)

## 2.4. Telephone Number

+355-(0) 422 21 039

## 2.5. Facsimile Number

+355-(0) 422 21 039

## 2.6. Other Telecommunication

None available

## 2.7. Electronic Mail Address

For the incident reports, please use the address info@cesk.gov.al

## 2.8. Public Keys and Encryption Information

For the incident related communication, you can use this key:

-----BEGIN PGP PUBLIC KEY BLOCK-----

Comment: User-ID: Info CESK <info@cesk.gov.al>

Comment: Created: 3/24/2020 10:07 PM

Comment: Expires: 3/24/2022 12:00 PM

Comment: Type: 2048-bit RSA (secret key available)

Comment: Usage: Signing, Encryption, Certifying User-IDs

Comment: Fingerprint: D33B17157924238925B6ECDB3EFE3C05D05B070F


mQENBF56dogBCADQZtGXteS365RwTk80Ar4qZ/gu2E/kyULWQO9EuNnoZpxnhgdY

dPuFcjA2ht9kw7cZVEEvGuqe8viRNKuIJY/1fpdOH03Zbs+S3sc1H4ddg9MRCbts

yWBSRGje/TTfedRZq2Ih8YoL5AqMpGLXVQnV+PTPtHNyreqM3Hai0yOYofGMfMb3

YYmd05ee3MYX4KxOXJwPxazXGymppVpYNR+NJd7RRyKa6weQYO4wc+XGAaGIOEpF

I5yF1K1MhuNiWsutTCwd6gDCBaGObmrYQA5OKt+gntG6yeo1gc26cfPlxYFF8FTZ

MVnq3OJED5qg5MYIeFH8feWcoTeHJ3uOsp71ABEBAAG0HEluZm8gQ0VTSyA8aW5m

b0BjZXNrLmdvdi5hbD6JAVQEEwEIAD4WIQTTOxcVeSQjiSW27Ns+/jwF0FsHDwUC

Xnp2iAIbAwUJA8HYqAULCQgHAgYVCgkICwIEFgIDAQIeAQIXgAAKCRA+/jwF0FsH

D0/PB/9TIfWJg2XmcWXrp+kKMThzkRTjMBaaJoOgFHzE9aEmJ+LRYEMlF7NZPsv/

X6m9T9F7tG7iOUoAwYCddSKWWYzFzm76TUdbyYt93eL7LmqnsvcAV8qxQjN92XJd

DHGcel+uqawbPDQUBWX05rlM25H4NwOXy95yGJZOHyAUj3Wjo9rvUSCduwbfkymn

ARtCoXu9QBuY2ejuNAg4Ok5tlJGHyEj/PffmCbn2KfAnz6j0qVUggfIHgDbxIP5m

sJ9sj4Ea3Dc79kjhoOIJJD04N3s09przchPAeo7gCyNDG2X+vmz58MagSgjW+boj

ljqfDCPJRxFosXMDC6GLgL1+UQGSuQENBF56dogBCADYsihlUJRwhVN+aq6vWxQ0

1542AXIOo+CU9E6asD+VY7Ac7GsFQWYAKTA6OvkhZb8tAkBl4XN7i2ClSXQ1G4S4

+L8ceL6AAVxkjpy65lOylRc3CLosHESV4BghnaN5AbF2amoPMRajhot50QvnntRr

Usy6IfEOrEEMIJHwt6BdI1j+CBspbtZ3bj5fGvO3Xnp1jtUJIfjE/1PyyKLs6ri7

ydQYHjY0eNQ+tQDfPAL0E0xcsnrPOEBzaKRo3LDxPSh0GZLkftok8kaWFLJ2fNRY

ofxJRMh4YFp1UN4w/lnjEt12mo9/DesSF1fCZi1xuxlz9pyejI/luc1QtfGQL29J

ABEBAAGJATwEGAEIACYWIQTTOxcVeSQjiSW27Ns+/jwF0FsHDwUCXnp2iAIbDAUJ

A8HYqAAKCRA+/jwF0FsHD2MMB/kBpofk2Y+i5v44G18wsdZY5cxlPOIHr8Xbu31v

Ez79mBiaVDt0Ba/0Zzt7BjaPDtybeeFGYoOd3Cbvn4GC2kuTXa5zgPDRMJb6HkgU

Ibj3LB6i8rz5BaV3HlDyizGabJM0qBY1UcrGgyXozHxtym9v8gzmtlNfVH2TzlcL

vNBG8KrfJZRa6lS4Txv5cvszf3l7qHMcCYKTTuC5mjuGQi6Hh7nYZP5KfRDAJUlJ

kATzsqKP+7t9BlWdEqKq6fzOesyq4zq2bQfmbbvMifaAbzru5FcxK/L6MxOEkla8

BlYrkDT5tSMNGp6+TKTafmIqWr98h8orJvMrUF48b2j+tK4M

=cyHL

-----END PGP PUBLIC KEY BLOCK-----

## 2.9. Team Members

The AL-CSIRT Monitoring Unit team leader is Mrs. Argena Prendi. The AL-CSIRT Management Unit team leader is Mr. Rexhion Qafa.

A full list of AKCESK team members is not publicly available. Team members will identify themselves to the reporting party with their full name in an official communication regarding an incident. General Management, liaison and supervision are provided by Mrs. Vilma Tomco, General Director, National Authority for Electronic Certification and Cyber Security.

## 2.10. Other Information

General information about the AKCESK can be found at www.cesk.gov.al

## 2.11. Points of Customer Contact

The preferred method for contacting AKCESK for all the issues related to incidents on CII is through internal portal administrated by AKCESK. For all other entities is via online form found on AKCESK page : https://cesk.gov.al/raportoincident.html. This will create a ticket in our tracking system and alert the person on duty.

For general questions please send an e-mail to info@cesk.gov.al. If it is not possible (or not advisable for security reasons) to use e-mail, the CSIRT can be reached by telephone at + 355 (0)422-21-039. The AKCESK hours of operation are generally restricted to regular business hours (08:00-16:00 Monday to Thursday and 08:00-14:00 on Friday).

# 3. Charter

## 3.1. Mission Statement

Ensures the security of trusted services, in particular ensuring the reliability and security of electronic transactions between citizens, businesses and public authorities, enhancing the effectiveness of public and private services and e-commerce and setting minimum technical standards for data and network security/information society computer systems, in accordance with international standards in this field, with the aim of creating a secure electronic environment

## 3.2. Constituency

Our constituencies are stated by Law on Cyber Security 2/2017 and Defined by DCM Nr 222 Date 26/04/2018 which lists all the Critical and Important Information Infrastructure operators in the Republic of Albania

## 3.3. Sponsorship and/or Affiliation

AKCESK is a Governmental Institution under the Prime Minister's Office

## 3.4. Authority

The National Authority for Electronic Certification and Cyber Security, exercises its activity, pursuant to Law 9880, dated 25.02.2008 "On Electronic Certification", Law No.107 / 2015 "On Electronic Identification and Trusted Services" and Law no. 2/2017 "On Cyber Security", as well as other bylaws that regulate the area of trusted services and cyber security. AKCESK works cooperatively with CII operators of the Republic of Albania, public and private sectors as well as International Institutions which focus on Cyber Security

# 4. Policies

## 4.1. Types of Incidents and Level of Support

AKCESK in the role of National CSIRT is authorized to address all types of cyber security incidents which occur, or threaten to occur, in its constituencies, which are the Critical Information Infrastructure Operators in the Republic of Albania. The level of support given by AKCESK will vary depending on the type and severity of the incident or issue, the type of constituent, the size of the user community affected, and AKCESK's resources at the time, though in all cases some response will be made within one working day

AKCESK is committed to keeping its constituencies, public and private companies as well as citizens of the Republic of Albania informed of potential vulnerabilities, and where possible, will inform all communities of such vulnerabilities before they are actively exploited.

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

All incoming information is handled confidentially by AKCESK, regardless of its priority. Information that is evidently very sensitive in nature is only communicated and stored in a secure environment, if necessary using encryption technologies.

AKCESK will use the information you provide to help incident response coordination. Information will only be distributed further to other teams and members on a need-to-know base, and preferably in an anonymized fashion.

AKCESK operates within the bounds of the Republic of Albania legislation.

## 4.3. Communication and Authentication

For all CII's operating in the Republic of Albania and identified by DCM 222, 26/4/2018 the communication is done through internal system managed by AKCESK.

E-mails and telephones are considered sufficiently secure to be used even unencrypted for the transmission of low-sensitivity data. If it is necessary to send highly sensitive data by e-mail, PGP will be used.

If it is necessary to authenticate a person before communicating, this can be done either through existing webs of trust (e.g. TI, FIRST) or by other methods like call-back, mail-back or even face-to-face meeting if necessary.

# 5. Services

## 5.1. Incident response coordination

AKCESK coordinates the response effort among constituencies involved in the incident. This includes CII operators listed by DCM 222, 26/4/2018 of Republic of Albania. The coordination work may involve collecting contact information, notifying sites of their potential involvement (as victim or source of an attack), collecting statistics about the number of sites involved, and facilitating information exchange.

Part of the coordination work may involve notification and collaboration with law enforcement agencies and other local and national CERTs with the focus protection of CII systems, networks and services.

This service does not involve direct, on-site incident response.

## 5.2. Awareness Building

AKCESK Unit will prepare a security alerts including:

- Safety warnings for specific needs of the constituency. These alerts provide timely information on the current situation and the activities that pose a threat to operators of electronic communication networks and services and their users.

- Safety warnings for the public. These alerts contain brief information that is clear for understanding from home computers user, in order to protect themselves to the internet.

Performing this service seek opportunities to increase security awareness through developing articles, posters, newsletters, web sites, or other informational resources that explain security best practices and provide advice on precautions to take. Activities may also include scheduling meetings and seminars to

keep constituents up to date with ongoing security procedures and potential threats to organizational systems.

## 6. Incident Reporting Forms

CII Operators report incidents through internal Incident Management System which is managed by AKCESK.

Other institutions that do not have access on this system should report through web report.The form is available on the following https://cesk.gov.al/rreth-nesh/raportoincident.html

## 7. Disclaimers

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