RFC 2350 Description for CERT-EE

1. Document Information

1.1. Date of Last Update

This is version 1.12, published 2025-10-13

1.2. Distribution List for Notifications

CERT-EE will not plan frequent modifications to this document, thus see p 1.3 for the download location.

1.3. Locations where this Document May Be Found

https://ria.ee/en/cyber-security/handling-cyber-incidents-cert-ee/rfc-2350-description-cert-ee

As PDF: https://www.ria.ee/en/media/1965/download

2. Contact Information

2.1. Name of the Teams

CERT-EE, Estonian national CERT

2.2. Address

Pärnu maantee 139a, Tallinn 15169, Estonia

2.3. Time Zone

- EET, Eastern European Time (UTC+2, between last Sunday in October and last Sunday in March)
- EEST, Eastern European Summer Time (UTC+3, between last Sunday in March and last Sunday in October)

2.4. Telephone Number

+372 663 0299

Backup Telephone: +372 5308 8299

2.5. Other Telecommunication

Available upon reasonable requests – GSM, SSL IRC etc

2.6. Electronic Mail Address

cert@cert.ee – e-mail messages are read 24/7.

2.7. Public Keys and Encryption Information

The CERT-EE has a PGP key (0xA32AFB7D), with KeyID B05DBD10A32AFB7D and fingerprint 7B96 A5C7 079D 0CAF 9BEA C713 B05D BD10 A32A FB7D.

The key can be found at https://cert.ee/.well-known/team-key.txt.

2.8. Team Members

The head of CERT-EE is Mr. Taavi Kupper.

Information about other team members is available by request.

2.9. Other Information

General information about CERT-EE is available at https://ria.ee/kuberturvalisus/kuberintsidentide-kasitlemine-cert-ee (in Estonian) and https://ria.ee/en/cyber-security/handling-cyber-incidents-cert-ee (in English).

CERT-EE Twitter profile (mostly in Estonian): https://x.com/CERT_EE
The blog of the Information System Authority (in Estonian): https://www.ria.ee/blogi

2.10. Points of Customer Contact

The preferred communication channel is the e-mail address cert@cert.ee. If it's not possible to use e-mail, please call the official phone number indicated in p.2.4. Appropriate communication channels are advised according to the nature of the request.

CERT-EE has one team member on duty 24/7.

3. Charter

3.1. Mission Statement

The main goals for CERT-EE as the national CERT are:

- promote secure networking;
- deal with computer security incidents;
- cooperation with internationally recognised information technology security incident prevention institutions (teams, CSIRTS, CERTS).

3.2. Constituency

The main areas of responsibility of CERT-EE are:

- dealing with information security incidents within AS8240 and AS56588 as well as with incidents in most of the state and municipal networks in .ee domain disregarding their exact affiliation or service provider.
- serving as the single point of contact for foreign CERTs/CSIRTs, as the national CERT.
- coordinating the activities in case of an elevated situation.
- educating the nation and national IT sector on cyber threats, commenting the cyber security situation as necessary.

3.3. Sponsorship and/or Affiliation

CERT-EE is a department of the Cyber Security Centre NCSC-EE of the Information System Authority (https://www.ria.ee/en) and is funded from state budget. The other departments of the NCSC-EE are Critical Information Infrastructure Protection Department, Information Security Standards Department, Supervision Department, Analysis and Prevention Department and R&D Coordination Department.

CERT-EE is affiliated with FIRST, the global Forum of Incident Response and Security Team, GÉANT and TI (Trusted Introducer for European CERTs) and CSIRT Network (established under the NIS Directive). CERT maintains affiliations with various CSIRTs around the world as needed.

3.4. Authority

CERT-EE has no formal authority to advise particular actions (except actions related to AS8240 and AS56588). CERT-EE participates in security driven decisions for .ee TLD (including AS2586, AS322, AS3249, AS3327, AS3332, AS8728, AS12563, AS12757, AS13272, AS16014, AS28955, AS31081, AS31602, AS34702, AS34729, AS39038, AS39211, AS39301, AS39632, AS39823, AS42012, AS42016, AS42300, AS42472, AS43881 and AS43958).

4. Policies

4.1. Types of Incidents and Level of Support

Incident information obtained as a national CERT, is parsed, systematised and forwarded to ISP's and domain owners. The level of support depends on the type and severity of the incident or issue, and on the impact on Estonian critical infrastructure.

Information System Authority coordinates wide level incidents on State level. Communication methods are in place to inform the owners of critical infrastructure, and for escalation up to the government level. As a general rule no end-user support is offered.

CERT-EE primary constituents are:

- State institutions and local authorities of Estonia;
- Operators of Essential Services and Digital Service Providers in the context of NIS directive;
- Critical IT infrastructure of Estonia

CERT-EE secondary constituents are:

- private sector using IP addresses of Estonia and resources with TLD .ee;
- citizens using IP addresses of Estonia and resources with TLD .ee.

4.2. Co-operation, Interaction and Disclosure of Information

CERT-EE works in tight cooperation with State Institutions, Law Enforcement Organisations (LEO) and with professionals in the field. Standard privacy laws apply. In case of a potential criminal incident we recommend the proper LEO assessment. Rules and good practice are in place to avoid dissemination of private and company data. Cases and examples are disseminated in professional circles in an anonymised form.

4.3. Communication and Authentication

For international communications ordinary precautions apply – like communicating to/via previously trusted and listed teams (TI) and using PGP. CERT-EE tries to adhere to LEO standards where key persons know each other personally before any significant cooperation.

5. Services

5.1. Incident Response

CERT-EE will define, assess and prioritise all types of ICT incidents. Time for response is 2 working days. In particular, it will provide assistance or advice with respect to the following aspects of incident management:

5.1.1. Incident Triage

- Investigating whether indeed an incident occurred.
- Determining the extent of the incident.

5.1.2. Incident Coordination

- Determining and contacting the involved organisations.
- Facilitating contact with other parties including law enforcement, if needed.
- Asking for reports and/or composing reports, depending on the involved organisations, incident type and severity.
- Communicating with media, if necessary.

5.1.3. Incident Resolution

- Advising the involved organisation(s) on appropriate measures.
- Following up the incident solution process.
- Collecting evidence and interpreting data, if applicable.

5.2. Proactive Activities

- Providing relevant information on threats, trends and remedies to their constituency (and/or media, if necessary) to raise security awareness and competence.
- Collecting contact information of local security teams.
- Providing fora for community building and information exchange within the constituency.

6. Incident Reporting Forms

https://ria.ee/en/cyber-security/handling-cyber-incidents-cert-ee/reporting-cyber-incident – CERT-EE expects the reporter to be able to answer 3–5 standard questions (Where? When? What? How? Who?) and provide the assumptions according to the logs. It is also possible to submit the incident report form online at https://raport.cert.ee.

7. Disclaimers

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