CERT-SE profile

Established according to RFC-2350.

1. Document Information

1.1. Date of Last Update

This is version 2.0 of 2015-05-06.

1.2. Distribution List for Notifications

This profile is kept up-to-date on the location specified in 1.3 .
E-mail notification of updates are sent to:

- The Trusted Introducer for CERTs in Europe (see https://www.trusted-introducer.org/)

Any questions about updates please address to the trusted-introducer@cert.se e-mail address.

1.3. Locations where this Document May Be Found

The current version of this profile is always available on https://www.cert.se/rapporter/RFC_2350_CERT-SE.pdf.

2. Contact Information

2.1. Name of the Team

Full name: CERT-SE
Short name: CERT-SE
CERT-SE is the national and governmental CERT of Sweden.

2.2. Address

Postal Address:
CERT-SE
MSB
651 81 KARLSTAD
SWEDEN

2.3. Time Zone

GMT+1 (GMT+2 with DST or Summer Time, which starts on the last Sunday in March and ends on the last Sunday in October)

2.4. Telephone Number

+46 8 678 57 99

2.5. Facsimile Number

+46 736 44 55 45
Note: this is not a secure fax.

2.6. Other Telecommunication

Not available.

2.7. Electronic Mail Address
cert@cert.se

This address can be used to report all security incidents to which relate to the CERT-SE constituency.

2.8. Public Keys and Encryption Information
PGP/GnuPG is supported for secure communication.
The current CERT-SE team-key can be found on **https://www.cert.se/cert_at_cert.se.asc.**

Please use this key when you want/need to encrypt messages that you send to CERT-SE. When due, CERT-SE will sign messages using the same key.

When due, sign your messages using your own key please - it helps when that key is verifiable using the public keyservers.

2.9. Team Members
Information is not provided about the CERT-SE team members on the website. Please use our team-key when you contact us. The current CERT-SE team-key can be found on:
https://www.cert.se/cert_at_cert.se.asc.

2.10. Other Information
- See the CERT-SE webpages https://**www.cert.se**
- CERT-SE is accredited by the Trusted Introducer for CERTs in Europe, see https://www.trusted-introducer.org/teams/country_AS.html .
- CERT-SE is described in the RIPE whois database by means of an IRT-object, see http://www.db.ripe.net/whois and search for "-B IRT-CERT-SE"
- CERT-SE is a full member of FIRST, see http://www.first.org/members/teams/cert-se

2.11. Points of Customer Contact
Regular cases: use CERT-SE e-mail address.
Regular response hours: Monday-Friday, 09:00-17:00 (except public holidays in Sweden).
Phonenumber: +46 8 678 57 99

3. Charter

3.1. Mission statement
The mission of CERT-SE is stated in Ordinance (2008:1002) with Instructions for the Swedish Civil Contingencies Agency (MSB). In brief the Ordinance states that CERT-SE shall:

1. respond promptly when IT incidents occur by spreading information, and where needed work with the coordination of measures, and partake in work to remedy or mitigate the incident's consequences,
2. cooperate with authorities that have specific tasks in the field of information security, and
3. act as Sweden's point of contact for equivalent services in other countries, and develop cooperation and information exchanges with them.

3.2. Constituency

CERT-SE is the National CERT of Sweden, and the constituency consists of the Swedish society, including but not limited to, Governmental authorities, Regional authorities, Municipalities, Enterprises and Companies. In addition, CERT-SE is also the Governmental CERT of Sweden and have additional responsibilities within the Governmental body.

3.3. Sponsorship and/or Affiliation

CERT-SE is part of MSB – The Swedish Civil Contingencies Agency, which is a Swedish governmental agency. CERT-SE is fully financed by MSB.

3.4. Authority

CERT-SE coordinates security incidents on behalf of its constituency and has no authority reaching further than that. CERT-SE is however expected to make operational recommendations regarding vulnerabilities and mitigation of incidents and/or incident handling. Such recommendations can include but are not limited to blocking addresses or networks. The implementation of such recommendations is not a responsibility of CERT-SE, but solely of those to whom such recommendations are made.

4. Policies

4.1. Types of Incidents and Level of Support

All incidents are considered normal priority. CERT-SE itself is the authority that can set and reset the EMERGENCY label. An incident can be reported to CERT-SE as EMERGENCY, but it is up to CERT-SE to decide whether or not to uphold that status.

4.2. Co-operation, Interaction and Disclosure of Information

ALL incoming information related to incidents is handled confidentially by CERT-SE, regardless of its priority.

Information that is evidently sensitive in nature is only communicated and stored in a secure environment, if necessary using encryption technologies. When reporting an incident of sensitive nature, please state so explicitly, e.g. by using the label SENSITIVE in the subject field of e-mail, and if possible using encryption as well.

CERT-SE supports the Information Sharing Traffic Light Protocol (ISTLP – see https://www.trusted-introducer.org/links/ISTLP-v1.1-approved.pdf) - information that comes in with the tags WHITE, GREEN, AMBER or RED will be handled appropriately.

CERT-SE will use the information you provide to help solve security incidents, as all CERTs do. This means that by default the information will be distributed further to the appropriate parties – but only on a need-to-know base, and preferably in an anonymized fashion.

If you object to this default behavior of CERT-SE, please make explicit what CERT-SE can do with the information you provide. CERT-SE will adhere to your policy, but will also point out to you if that means

that CERT-SE cannot act on the information provided.

CERT-SE does not report incidents to law enforcement, unless national law requires so. Likewise, CERT-SE only cooperates with law enforcement EITHER in the course of an official investigation – meaning that a court order is present – OR in the case where a constituent requests that CERT-SE cooperates in an investigation. When a court order is absent, CERT-SE will only provide information on a need-to-know base.

4.3. Communication and Authentication

See 2.8 above. Usage of PGP/GnuPG, or other pre-approved cryptographical means, in all cases where sensitive information is involved is highly recommended.
In cases where there is doubt about the authenticity of information or its source, CERT-SE reserves the right to authenticate this by any (legal) means.

5. services

5.1. Incident Response (Triage, Coordination and Resolution)

CERT-SE is responsible for the coordination of security incidents somehow involving their constituency (as defined in 3.2). CERT-SE therefore handles both the triage and coordination aspects. Incident resolution is left at the discretion of the involved constituents – however CERT-SE will offer support and advice on request.

An overview of the Incident Handling Process that is used internally by CERT-SE can be found at https://www.cert.se/incidenthantering (Swedish only).

5.2. Proactive Activities

CERT-SE pro-actively advises their constituency in regard to recent vulnerabilities and on matters of computer and network security.
CERT-SE is not responsible for implementation, that is always left at the discretion of the constituents.

6. Incident reporting Forms

Not available. Preferably report in plain text using e-mail - or use the phone.

7. Disclaimers

None.