TF-CSIRT
TRUSTED INTRODUCER

INVITATION PACKAGE
FOR
TI "CERTIFIED" STATUS

Version 3.1 – 1 July 2025

INDEX

1 ESSENTIALS

Your team is invited to join the TI (=Trusted Introducer) Framework as "TI Certified" team. This document describes all what you as invited team need to know to acquire the "certified" status, i.e. passing the certification process for your team. If you have any questions during the process, please direct them to:

E-mail address: ti@trusted-introducer.org

If you send e-mail to us, please make sure to include the ticket number send to you as part of the subject of our e-mail to you with your invitation. That way we can keep track of the progress and ensure a consistent view of your process.

To send confidential data encrypted to us use the following public key, available through the TI web site as https://www.trusted-introducer.org/pgp-ticket-system.asc:

```
User ID:       Trusted Introducer (TI) ** TICKET SYSTEM ** key
               <ti@trusted-introducer.org>
Key ID:        0xA778F9E1
Key type/size: DSA and Elgamal / 1024D/4096Elg
Fingerprint:   C5BB A470 AAD6 7013 2917  F1BF A648 80D2 A778 F9E1
```

The TI team has assigned two of its members—called "Primary" and "Secondary SIM3 Auditor" – to oversee your process from beginning to end and assist you when you meet with problems. You reach both through the above service e-mail address – please do not use personal e-mail addresses for reasons of contingency for all official steps.

1.1 What is TI Certification all about?

The TI Framework has been created based on an initiative of the European security and incident response team community in 2000. Such teams (or functions) within an organisation deal with all kinds of computer and network security incidents. They strive to prevent incidents from happening, help detecting attacks, support the mitigation of as well as the recovery from incidents, and coordinate all activities including the contact to external teams when they do occur.

The teams of our community cooperate worldwide to combat attacks on IT systems and infrastructures or other IT related crime. Starting from Europe the forum for such cooperation is called TF-CSIRT. To cooperate efficiently and swiftly when security incidents occur, a certain level of mutual trust is needed between teams. An important pre-requisite for mutual trust is shared operational knowledge about one another. But also some services, supporting such sharing as well as the coordination needs to be made available.

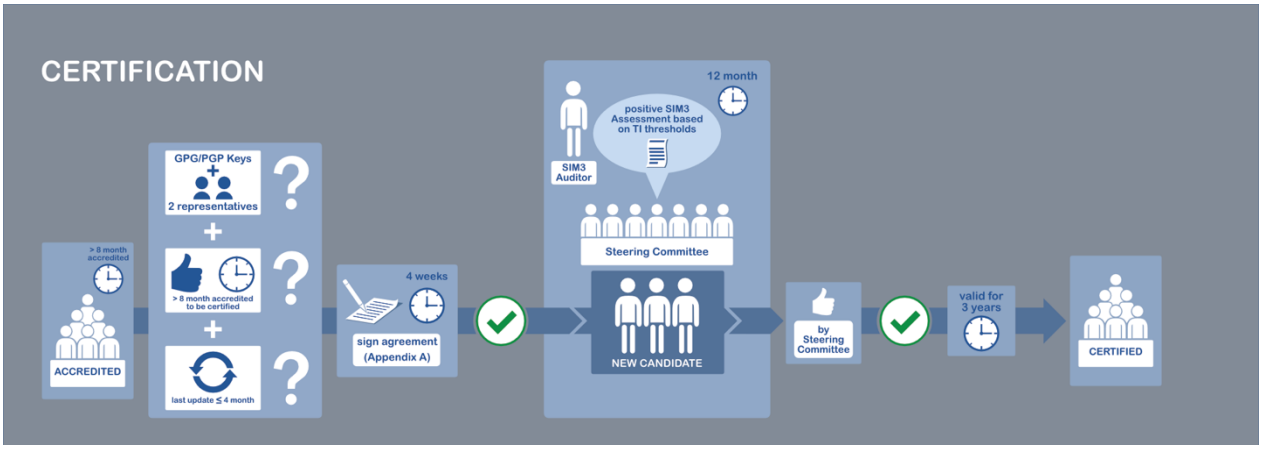
The TI accreditation service is meant to do just that: facilitate trust by formally accrediting teams that are ready to take that step. For a team to proceed from the status

of "listed" to the status of "accredited" its organisation needs to go through a formalised accreditation scheme – but you know all this as you have become "accredited" before.

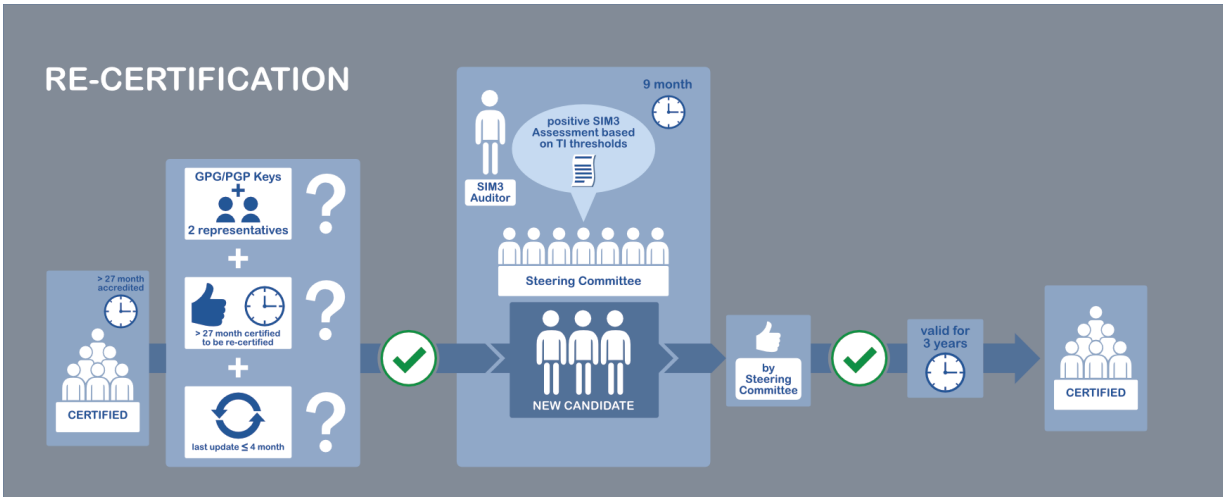
"Certified" teams stay "accredited" (and "listed") within the speak of the TI, which means "certified" teams share the same rights but also obligations as "accredited" teams! So what is "certification" all about?

A crucial benefit that is part of the TI certification framework is maturity based on capacity (you have staff to carry out the activities) and capability (your staff is trained to carry out the activities). Maturity without both cannot exist, but even if both exist your staff might have not a long-term expertise or experience. Or important processes have been documented but are not formally endorsed or enforced. This will lead to an uncertain quality of the services offered towards the clients and constituents.

In a maximum amount of 12 month including a one day on-site workshop the auditors will find out, how to rate your team regarding the Security Incident Management Maturity Model (abbreviated, known as: SIM3) model. The SIM3 model was adopted in 2010 as baseline for the parameters that are observed and assessed during the certification candidate phase. The following figure visualizes the process from being an "accredited" team to become a "certified" team successfully.



And those parameters that have been confirmed during the "certification candidate" phase will be observed again three years after the certification as part of the re-certification to confirm, that the team – despite whatever might have happened to the team in terms of changed mandates, budgets, constituency or internal re-organizations – is still able to provide the called-for capabilities with sufficient capacity and the right level of maturity. Another figure on the next page visualizes this process, which will start not earlier than 27 months after the date of the last successful (re-) certification and should end 36 months after that date.



The following sections will provide more details on the certification process itself. More background on TI and its set-up can be found in Appendix B. As the "certified" teams still have the same obligations in terms of managing their data and provide timely updates, as "accredited" teams, those details have been omitted.

1.2 What is the first Step in the TI Certified Process?

The first step is to move your team from "accredited" to "certification candidate" status. Your team already has acquired "accredited" status because that is a pre-requisite for being invited to the certification process. Moving to "certification candidate" status is simple: just print out Appendix A that you got with your invite, have it properly filled and signed (this proofs your team's approval and acceptance of the fee structure as well as the governing principles as laid out in this invitation), and send the original version to the TI service provider. Please either use fax or e-mail, but also send it by normal post, registered post is not needed.

Send your agreement by e-mail to **ti@trusted-introducer.org** , but only PGP-signed!

We appreciate the original by postal mail to:

Trusted Introducer
c/o DFN-CERT Services GmbH
Sachsenstraße 5
20097 Hamburg / Germany

PLEASE NOTE:

This step must be completed within 28 days after receiving the invitation.[1]

If there should be any problem with the filled-out Appendix A the TI team will contact you to sort out any such issue. Once a properly signed Appendix A is available, the TI team sends out a formal "TI Certification Candidate Status Acknowledgement" by signed e-mail: that means your team is an "certification candidate" as of the date specified within the acknowledgement.

1.3 Move on towards TI "Certified" Status

Moving to "certified" status depends on your team's ability to provide and demonstrate the required capability, capacity and maturity as defined by the vision and mission of your team.

The criteria and in some cases minimum requirements are defined in two documents that are available from the TI restricted web site:

- **SIM3 Reference Model (authoritative)**
  https://tiw.trusted-introducer.org/SIM3-mkXVIII-TI.pdf

- **SIM3 TI Certification Standard (authoritative)**
  https://tiw.trusted-introducer.org/SIM3-mkIV-TI-Standard.pdf

As the SIM3 parameters cover a very large context of organisational, human, process and tool related issues, no information is handled via the TI Self-Service. Many of the documents and processes are at least sensitive and shall not be published to the whole TI Community. Instead, a so-called "SIM3 Auditor" will work with the "certification candidate" to assess the appropriate level within the rules and guidelines of the SIM3 model as defined by the OpenCSIRT Foundation. While the assessment could be purely be based on a paper review a full-day workshop (at the time of the re-certification every three years a half-day workshop is anticipated) will be organized on-site. During this workshop the approach and details will be shortly introduced. Most of the workshop is used to discuss open issues and the levels of all SIM3 parameters. Based on this preliminary assessment a list of open issues or To-Dos will be defined by the SIM3 Auditor. The team will thereafter focus on the open issues and To-Dos to submit relevant material that show the issues have been addressed to the SIM3 Auditor. Questions etc. will be answered by the SIM3 Auditor, who also act as a coach during this process to help the team finishing their task assignments successful.

[1] Please note also: as a rule, an invitation package will be sent out to any team no more than twice every twelve (12) months.

Once all materials are sufficiently stable and meet the demands as defined by the TI Certification Standard the SIM3 Auditor will put his findings into writing, submitting the final assessment report after consideration by the team itself to the TF-CSIRT Steering Committee. The SC will take a vote and might ask more questions not sufficiently addressed by the assessment report.

The date of the final assessment report should be within twelve plus one (12+1) months of the "TI Certification Candidate Status Acknowledgement" date, unless the delay is caused by the TI due to additional checks or discussions. [2] After the vote of the SC has been taken a "TI Certification Status Acknowledgement" will be send, outlining the outcome of the vote. If the vote was positive, the team status will be changed to "certified" for three years. Usually within the three years the team must be re-certified if the team wants to retain the "certified" status for another three years.

Your team will from then on be invoiced on an annual basis for maintenance of the "certified" status by the OpenCSIRT Foundation (The Netherlands, the host of TF-CSIRT since 2022) in addition to the "accredited" fee. The annual fees of EUR 800 (VAT might apply) are applicable for all teams. But based on the location different set-up fees will be charged in addition to cover the workshop costs:

- **for teams within Europe, Middle East and Mediterranean Africa:**
  - set-up certification: EUR 1000 (VAT might apply)
  - set-up re-certification: no fee
- **for teams from other geographic areas:**
  - set-up certification: EUR 2200 (VAT might apply)
  - set-up re-certification: EUR 1600 (VAT might apply)

1.4 Being an "Certified" Team!

From the moment of your team's certification, you can enjoy the new status. But you retain the same obligations and rights as before as "accredited" team. So, in case your team fails to update its data accordingly, you might by a vote of the Steering Committee become "suspended". This also applies to "certified" teams without difference.

The certification is seen as a benefit for the team which can be communicated. In the future specific TI services for "certified" teams only might be developed and offered.

[2] Please note: non-compliance to this deadline will be discussed based on your reasons and justifications, as well as the assessment of the TI team by the TF-CSIRT Steering Committee. Based on their decision the deadline will be extended, or not. In case no extension is granted, this causes an immediate fall back of your team to "accredited" status, the invitation counting as a failed invitation.

2 APPENDIX A: FORM TO ACCEPT THE INVITATION

The form required will be send to any applying team by email!

3 APPENDIX B: TI BACKGROUND

This background information about the TI service and its processes is offered as additional information. There is no formal requirement to read this appendix, but it might be useful, if you are not yet familiar with the TI services and its framework.

3.1 TI Entities

The following entities are of interest within the TI framework:

- **TI Community:** Formally the group of TI Accredited and Certified teams including its individual members and TI Associates, TF-CSIRT SC members as well as the TI team. Informally all security and incident response teams and its members in operation.
- **TI Associates:** Individuals whose experience and/or skills can be of clear benefit to the TI Community, but who are not member of an TI Accredited team (anymore) and thus cannot contribute through their team.
- **(the) TI** or **TI Team:** The group of people operating the TI process, maintaining the TI web site (https://www.trusted-introducer.org/contact.html), and offering the provided services.
- **Primary and Secondary Introducer:** A member of the TI team who guards your accreditation process from beginning to end and assists you with your questions. The "Secondary" is acting as backup. While routine tasks like answering basic e-mail questions or handling acknowledgements are handled in shifts by TI team members, the "Personal" introducers provides you with continuity and a personal touch.
- **GÉANT (formerly TERENA):** The "Trusted Introducer" service originated in September 2000 from cooperation activities between CERTs and security teams that were organized by TERENA (http://www.terena.org/). GÉANT (formerly TERENA) continued to act as the financial and legal focal point for the TI service until August 2022. Since then, the OpenCSIRT Foundation is the host of TF-CSIRT activities including the TI services.
- **OpenCSIRT Foundation:** Since September 2022 the foundation is the legal host of the TF-CSIRT activities including TF-CSIRT Meetings, TRANSITS trainings, and the TI Service. RIPE NCC and GÉANT have agreed as founding fathers of the foundation to support those activities in the long-term. In addition to support the TF-CSIRT activities the foundation will continue to maintain, promote and further develop the SIM3 standard for all kind of cyber security teams.

In support of the TF-CSIRT the foundation provides logistical and administrative functions like:

- sub-contracting to service providers;
- organizing the SIM3 auditors to oversee TI Certifications;
- invoicing for "re-/certification candidates" and "certified" teams;
- supporting the TF-CSIRT SC.

- **TF-CSIRT Steering Committee (TF-CSIRT SC):** The TF-CSIRT SC reviews the operation of the TI team and addresses all special issues that might result from its operation as well as any question that is not addressed by the operational framework. In particular, the TF-CSIRT SC performs the following tasks:
  - Support and foster the acceptance and recognition of the TI service.
  - Oversee and change policies and framework, in close cooperation with the community of accredited teams and the TI team.
  - Review the TI service, including the review of tri-annual reports issued by the TI team, and an annual overall service review
  - Handle specific inquiries about the functioning of the TI service, which are related to the strategical perspective represented by the TF-CSIRT SC.
  - Decide about any issues that are outside existing TI policies, like making exceptions to the defined rules for status change (towards "accredited" status, or fall-back to "listed" status), deciding on a site visit to clarify issues that could not be handled otherwise, etcetera.

  The TF-CSIRT SC has the right to review the archive maintained by the TI team at any time to clarify any inquiries concerning the TI service directed to the TF-CSIRT SC and to enable an overall review of the TI service.

  The chair of the TF-CSIRT SC is elected by the TI accredited / certified teams.
- **TI Operator / Service Provider:** The OpenCSIRT Foundation operates the TI service based on a mixture of external service providers and own staff members.

3.2 TI Status: "Listed", "Accreditation Candidate" and "Accredited"

As you received this invitation, your team already has acquired the "listed" status, meaning its general information is already present on the public TI web site (https://www.trusted-introducer.org/). This invitation is aimed at your reaching out for "accredited" status, thereby passing the intermediate "accreditation candidate" status.

The various statuses are characterised as follows:

- **Listed:** Information about the team is available indicating that the team's service or operation is within the scope of the TI framework. This information is preferably provided by the team itself but can also be harvested from other sources (news spread within the community, public directories).
- **Accreditation Candidate:** Temporary intermediate phase for teams acquiring "accredited" status, with only two possible outcomes: formal accreditation if the team formally meets the defined criteria within the specified period, or fall back to "listed" status when it does not.
- **Accredited:** Detailed operational information about the team is available, obtained from individuals representing its organisation, thus ensuring authenticity and correctness. The team participates in the international community of CERTs and security teams and maintains the actuality of the information it had provided.

3.3 Validation of Information

To acquire "accredited" status a team must provide a useful, but limited, amount of operational information. The TI accreditation process focuses primarily on the team's statements on those criteria that the TI will use to gauge its operational status and standing. Statements can be provided in various forms, as filled-out form, as answers to additional questions, etcetera. Any such statement has three properties the TI framework depends on and needs to be recognized here:

- **Authenticity:** This means that the TI team can be sure that the statement came from the team and/or its parent organisation. This includes the integrity of the information of course: if the integrity is not assured then it is not authentic in any case.
- **Actuality:** The statement reflects the current state of affairs, and not one of a past no longer applicable. Actuality can only be achieved when statements are maintained: *maintenance* and *actuality* are two sides of the same coin.
- **Correctness:** This requires that the statements are more than just authentic and actual: they are met by reality. This can only be checked by – essentially – performance or quality measurements of a team's ability and performance. Within the certification available to accredited teams correctness of information is of critical importance.

The TI accreditation process concentrates on the *authenticity* and *actuality* properties of team statements alone: to check *correctness* is now part of the certification processes within the TI framework, for which you might apply once being accredited.

To ensure[3] the *authenticity* of information coming from "accredited" teams or "accreditation candidates", verification of the source of information is essential. One of the following two procedures is considered necessary and sufficient as verification method of the TI process:

- Direct (eye) contact is established with an individual from the team and/or its parent organisation who can prove the facts about the team and its operation. At least the personal ID is checked, and the individual can prove his/her right to represent the team and/or its parent organisation.
- Indirect (cyber) contact is established with an individual from the team and/or its parent organisation who can prove the facts about the team. Such contacts are secured with strong cryptography, and the identity of the individual must be linked to a cryptographic key that has been certified including a check of the personal ID. The individual can prove his/her right to represent the team and/or its parent organisation.

To ensure the *actuality* of information, the "accredited" teams are expected to keep the information they provided up-to-data. To help them meet that goal, the TI team entertains a four (4) monthly maintenance cycle, prompting all accredited teams about changes in their information set. Also, any changes that the TI team happens to notice by itself, are fed back to the related teams for validation, thus again prompting an update to the information set.

[3] „Ensuring" is to be understood as in statistics, i.e. if something is ensured, there is a high probability – definition of „high" deducible from the context – that it is in fact true: in matters of security there is no such thing as absolute certainty.