



TF-CSIRT
Trusted Introducer

INVITATION PACKAGE
FOR
TI “LISTED” STATUS



INDEX

<u>1</u>	<u>ESSENTIALS</u>	<u>3</u>
1.1	WHAT IS TI LISTING ALL ABOUT?	3
1.2	THE FURTHER STEPS INTO OUR COMMUNITY.....	5
1.3	STARTING THE TI LISTING PROCESS	6
1.4	MOVE ON TOWARDS TI "LISTED" STATUS.....	6
1.5	BEING AN "LISTED" TEAM!	7
<u>2</u>	<u>LISTING CANDIDATE STATUS</u>	<u>8</u>
<u>3</u>	<u>LISTED STATUS</u>	<u>9</u>
<u>4</u>	<u>APPENDIX A: FORM TO ACCEPT THE INVITATION</u>	<u>11</u>
<u>5</u>	<u>APPENDIX B: INFORMATION TEMPLATE FOR "LISTED" TEAMS</u>	<u>12</u>
5.1	MANDATORY FIELDS DESCRIBING THE TEAM	13
5.2	OPTIONAL FIELDS DESCRIBING THE TEAM	17
5.3	SERVICE RELATED FIELDS USED INTERNALLY BY THE TI.....	17
<u>6</u>	<u>APPENDIX C: CRITERIA FOR "LISTED" STATUS</u>	<u>18</u>
6.1	EXPLANATION AND GUIDANCE	18
6.2	LIST OF ALL MUST CRITERIA	18
6.3	LIST OF ALL SHOULD CRITERIA	19
<u>7</u>	<u>APPENDIX D: STANDARD DEFINITIONS TAKEN FROM THE IETF APPROACH [RFC2119]</u>	<u>20</u>
<u>8</u>	<u>APPENDIX E: TI BACKGROUND</u>	<u>21</u>
8.1	TI ENTITIES	21
8.2	TI STATUS: "LISTING CANDIDATE", "LISTED", "RE-LISTING CANDIDATE" AND "RE-LISTING PENDING"	22
8.3	VALIDATION OF INFORMATION.....	23

1 ESSENTIALS

Your team is invited to join the TI (=Trusted Introducer) Framework as "TI Listed" team. This is the "entry" level, and therefore your team will receive some services for free (which are financed with the membership fees of TI Accredited and TI Certified).

This document describes all what you as candidate team need to know to acquire the "listed" status, i.e. passing the voting 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 will oversee your listing process from beginning to end and assist you when you meet with problems.

1.1 What is TI Listing all about?

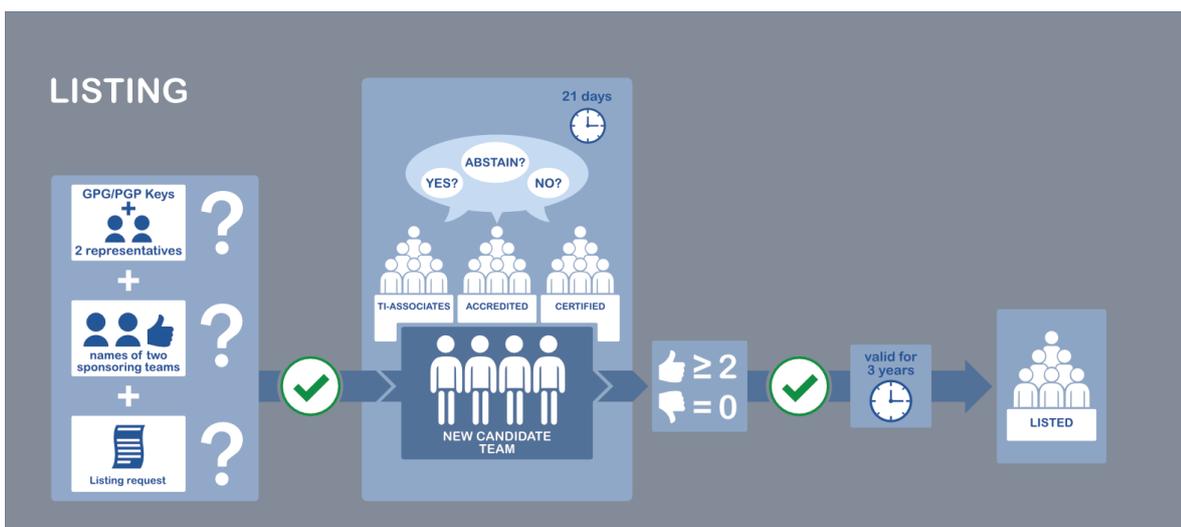
The TI Framework has been created based on an initiative of the European security and incident response team community in 2000. Such teams (or functions) within an organisation deal with all kind of computer and network security incidents including providing services to whole nations or business sectors. 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 or being asked for help.

The teams of our TI community cooperate worldwide to combat attacks on IT systems and infrastructures or other IT related crime. Starting as a task force founded by European NREN (national research and education network) teams the forum for such cooperation is called TF-CSIRT. To be able to cooperate efficiently and swiftly when security incidents occur or sharing of sensitive cyber threat intelligence is needed, 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 supporting services, allowing such sharing as well as providing communication mechanisms enabling effective coordination, need to be made available and maintained in a reliable manner.

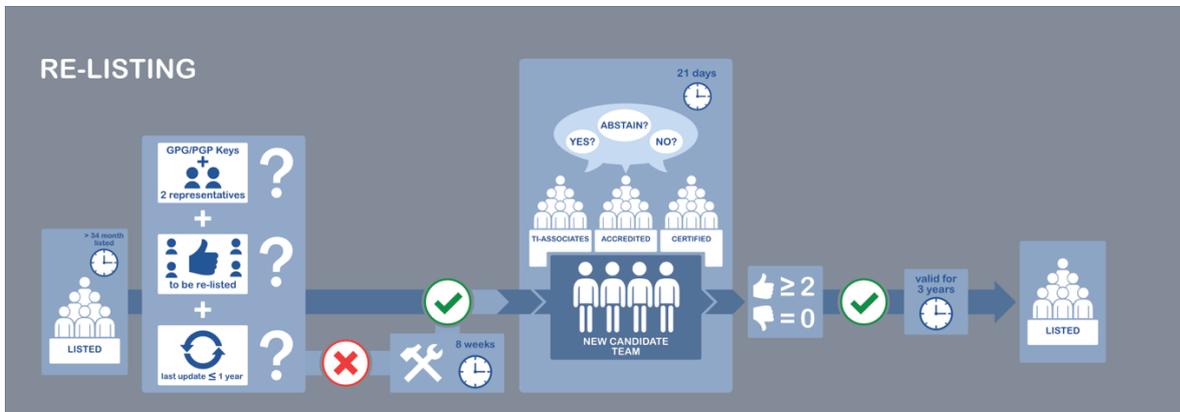
The TI "Listing" service is meant as the first step into our TI community: to help establishing trust by indicating to all other teams that the own team is ready to accept its responsibility and assist not only their local constituency but also other teams and in exchange receiving the support of those teams should the need arise. The requirements for any TI "Listed" team are not as strict as for more mature teams that proceed to the next level: TI "Accreditation".

Please note, that the TI "Listing" is free of cost for the teams. The TI "Accredited" and "Certified" teams had decided in the beginning and confirmed this decision from time to time, that they see value of an extensive directory of trusted contacts, regardless whether such teams would be prepared to pay an annual fee or more formally would like to demonstrate their maturity. But even if no fee is charged, TI "Listed" teams need to adhere to the established rules, which are only set by the TI "Accredited" and "Certified" teams.

The overview illustrates the successful listing process, which we will describe in the following sections in more detail.



If a TI "Listed" team has not acquired the TI "Accredited" Status within three years a new vote of confidence is required. This implies that the team's data is up-to-date and actively maintained. Once this has been clarified the team will be marked as TI "Re-Listing" Candidate team and a new vote is started with the same requirements, namely that the team receives the support of at least two TI "Accredited" or "Certified" teams or "Associates" (individuals that have been recognized as trusted but are no longer part of a team). The successful re-listing process will be described later, the figure explains the steps involved:



1.2 The further Steps into our Community

For a team to proceed from the status of TI "Listed" to the status of TI "Accredited" its organisation needs to go through a formalised accreditation scheme as documented on the TI public web site.¹ Once "accredited" the team gains access to the "members-only" TI information: there they find the details about their fellow accredited teams but also all listed teams. In addition, tailored value-added services towards the needs of cooperating teams are accessible: readily downloadable contact databases and GPG/PGP keyrings, access to secure discussion fora, registration of RIPE Database IRT objects, etc.

A crucial benefit that is part of the TI framework is maintenance: in a four-monthly cycle the actuality of data is verified with the accredited teams to prevent the information from going out-of-date and ensure, necessary updates are made in time. For TI "Listed" teams the verification is required at least every twelve months.

The TI framework is being further developed, as information and IT security plays an increasingly important role in today's networks, and indeed the world at large, and more severe demands are placed on teams involved worldwide. While FIRST, the global meeting place of CERTs, had adopted part of the TI framework for their membership procedures back in 2006, the TI teams added a TI "Certified" status² as important scheme to improve the maturity – the quality and ability to perform the functions these teams provide towards their constituencies – and demonstrate this based on the objective assessment of TI Auditors. The certification framework chosen in 2011 by the TI community is based on the Security Incident Management Maturity Model (SIM3).³

¹ <https://www.trusted-introducer.org/processes/accreditation.html>

² <https://www.trusted-introducer.org/processes/certification.html>

³ SIM3 is maintained by the OpenCSIRT Foundation, see <https://opencsirt.org>



1.3 Starting the TI Listing Process

The first step is to move your team from “known” to “listing candidate” status. Moving to “listing candidate” status is simple:

1. Please inform us about your wish to join the TI community by filling out the small form on the TI web site:
https://www.trusted-introducer.org/list_v40.txt
2. We will send you an Appendix A, which defines some minimum requirements, that you will need to accept, to get it signed and send it back to us. This proves your team's approval and acceptance of the requirements as well as the governing principles as laid out in this invitation.
3. Once we have both – the form and the signed Appendix A – we will register your team as “known”. Via a one-time-link you will receive by email you can submit your team data using an online web application.
4. We will check all data submitted and once complete we will change your team status as “listing candidate” and inform the TI Accredited and TI Certified teams to vote upon your request. To speed up this phase you are requested to identify two potential sponsors already in step 3.

Your signed Appendix A should be e-mailed to

ti@trusted-introducer.org

You will be asked again at the time of the re-listing – unless you have become TI Accredited in the meantime – to sign up again to start the TI Re-Listing Process! Our request, if you want to continue will come approx. three months before the three year period ends.

PLEASE NOTE:

If there should be any problem with the filled-out Appendix A or the data provided the TI team will contact you to sort out any such issue. Once a properly signed Appendix A is available, the TI team will inform you and acknowledge your progress in the process. We will also contact you during the voting time, if there is not enough support yet. So you will have enough time to contact your sponsors before the voting period ends.

1.4 Move on towards TI “Listed” Status

Moving to TI “Listed” status depends on your team's ability to provide the required set of information (see Appendix B) as well as responding to a number of requirements (see Appendix C). It is vital for the TI framework that all listed teams understand, appreciate, and fulfil those requirements.

To make it easier for everyone you need to provide all data and statements using an online form (from step 3). Access is protected by a unique URL for your application. All data is saved, if you have completed the data entry including providing PGP keys and two



persons that are authorized to speak for the team, the data set needs to be submitted by you – there is a specific button to do that.

Once the applying team makes all data available, the TI team will review all information your team has provided and then discuss any issues arising out of this review. Once all issues have been satisfactorily met, you can update your team data until the voting started, the application will be approved and made available on both the public and restricted TI web site. Then the TI community is informed about your application and a vote is started. Within three weeks the representatives eligible to vote can express their support, their objection or abstain from voting.

To become accepted as TI "Listed" team no objections are allowed and at least two positive votes supporting the applications need to be recorded. Once the outcome has determined, the applying team will receive a formal "TI Listing Vote Acknowledgement" explaining the outcome.

Your team will then also receive TI specific cryptographic credentials (X.509 user certificates) required to log into the TI Self-Service and maintain all data provided by the team at: <https://up.trusted-introducer.org>

1.5 Being an "Listed" Team!

From the moment of your team's listing, you can enjoy the value-added services that come with the "accredited" status. Most namely:

- Access to the public part of the TI web site, featuring an overview of operational data of all teams within the TI directory;
- Access to simple information available about all teams within the TI directory either as JSON and/or CSV export or via a web-based interface which also supports searches;
- Access to the TI mailing lists open to listed teams only, e.g., meant for discussion of open security issues within a low-level trusted environment;
- Access to the TI chat server open to all listed / accredited / certified teams with channels for various topics and private communication means;
- Access to open TF-CSIRT meetings and TRANSITS trainings.

To keep your team's information current and actual, every twelve (12) month you will be prompted to update the information. If there are no changes, your team's representative will still need to acknowledge that fact. This is part of the TI processes called "Maintenance".



2 LISTING CANDIDATE STATUS

From the moment on that your team – because of a correctly filed Appendix A – has received a formal “TI Listing Candidate Status Acknowledgement”, the team is considered as “listing candidate”. The only goal of that status is to move to “listing” status, as follows:

- The change to “listing candidate” status is reflected on the TI public website.
- Within three (3) weeks from the Acknowledgement date, your team has to provide the information as described in Appendix B and to meet the further criteria as defined in Appendix C. All materials are collected via the online form, no further data is requested by email or other media! How to meet those criteria is described below.
- In addition, relevant public keys need to be submitted also, i.e. your team’s GPG/PGP key and those of your team’s representatives.
- Your team will need to meet all **MUST** criteria as laid out in Appendix C. The TI team strongly advocates taking into consideration the **SHOULD** criteria at the same time. To document the status, your team needs to fill out Appendix C, which is meant to summarize your position with regards to all criteria.
- The TI team will gauge the material you sent in. Once all requirements are met, your team will receive a notice once the voting period of three (3) weeks is started.
- The “listing candidate” status of your team provides the TI team with the right to publish the information it receives from your team on its restricted TI web site, which is only open to accredited teams as well as the TI Associates, TI team and the TF-CSIRT SC and a sub-set of it on the open public TI web site.
- If TI “Listed” status has not been reached after the voting, the team’s entry will be removed from the restricted and public TI web sites. But the information submitted will be stored by the TI team to maintain a record of activities and to be able to check future registrations of the same team.



3 LISTED STATUS

From the moment that your team has properly documented that it meets the listing criteria – by means of correctly filed Appendices B and C – and has received the formal results after a successful vote of the TI community, the team is publicly considered as being TI "Listed". The following then applies:

- The change to TI "Listed" status is reflected on the TI web sites together with the supporting teams on the TI restricted web site.
- The TI "Listed" status of your team provides the TI team with the right to update the information about your team:
 - The information about your team contained in Appendix B and C marked for PUBLIC release will be provided on the public TI web site.
 - Other information contained will be provided only on the restricted TI web site.
- Your team will receive information about how to access the TI Self-Service.
- The designated e-mail address provided by your team will be subscribed to a restricted mailing list of all listed teams.
- Your team will be reminded of the necessary maintenance if needed. Maintenance of the information about your team is essential. If your team fails to uphold that maintenance, it will lose its "listed" status, because the maintenance is one of the MUST criteria for all teams. More in detail the following rules apply with regards to maintenance activities:
 - Your team MUST inform the TI team about any change that relates to contact or public key information or changes that impact its establishment (like constituency or fundamental organisational changes) within two (2) weeks and provide the appropriate corrections to the Appendix B form and/or RFC 2350.
 - All other changes to the information provided by means of Appendices B and C MUST be passed on to the TI within four (4) months – preferably sooner. This includes information about new GPG/PGP keys. Changes are to be submitted by the TI Self-Service.
 - Your team MUST reply to requests by the TI team regarding the status of the information your team has provided.
- At least every twelve (12) months the information available about listed teams MUST be verified. The success of this practice depends on the joint effort of your team and the TI. If no status updates are received by the TI for twelve consecutive months, the TI will send out a message requesting an acknowledgement, that the



current set of available information is still correct. Two (2) more reminders of this will be sent, if no answer follows, within two (2) months of the first reminder.

- If your team does verifiable not comply with the above rules the TI team will give your team formal notice (by signed e-mail and written letter) that your TI "listed" status will be revoked within two (2) months. If your team still fails to comply within this time period, your TI "listed" status will be removed.
- If an urgent situation, not covered by any of the above rules, occurs that could impact the TI "listed" status of your team, the TF-CSIRT Steering Committee (SC) can take actions like making enquiries or direct the TI team to interact with your team, if necessary also by conducting a site visit. The TF-CSIRT SC can take appropriate actions including the revocation of the accredited status, based on their assessment of the overall situation.



4 APPENDIX A: FORM TO ACCEPT THE INVITATION

A PDF file for this Appendix your team will be made available to your team ONLY AFTER you have formally requested the listing!

THIS IS NOT VALID FOR SUBMISSION – IT IS JUST TO SHOW YOU WHAT TO EXPECT!

We hereby declare that we accept the invitation to acquire "listed" status as laid out in the "Invitation Package for TI "LISTED" Status" Version 3.0 – 1 September 2022 (in short: Invitation Package) as available from the public Trusted Introducer (in short: TI) web page, and that we support the criteria, procedures and timeline set out in the Invitation Package.

More specifically, we:

- *declare that **we** are compliant in regard to the "MUST" criteria for "listed" status as laid out in Invitation Package Appendix C;*
- *commit **ourselves** to complement available information about the team according to the appendices B and C of the Invitation Package to the TI within two (2) months using the TI self-service;*
- *agree to the publication of various data about **our team**, as specified in the Invitation Package, on the public and restricted TI web sites (note on privacy: personal data will appear on the public web site if not marked as "restricted", however personal data will appear on the restricted web site);*
- *declare that **we** are aware of the need to become sponsored again after three years (re-listing) unless we are becoming TI Accredited within that time period;*
- *declare that **we** understand that the team will be removed after three years, if the re-listing fails and the team is not supported by the TI community as defined by the rules;*
- *declare that **we** have taken note of the need to terminate the listing explicitly in writing by sending email to ti@trusted-introducer.org.*

5 APPENDIX B: INFORMATION TEMPLATE FOR "LISTED" TEAMS

The set of information a team needs to provide via the online form to acquire TI "listed" status – and that it needs to maintain after that – consists of three parts:

1. **Mandatory** fields describing the team;
2. **Optional** fields describing the team; and
3. **Service-related** fields used internally by the TI team.

In case the team has already a filled-out RFC 2350 many requested information might be already available. In such cases using the relevant texts is usually sufficient.

The complete set of information of part 1 and 2 will be published on the *members-only* TI web site. A subset of both parts will be published on the *public* web site. The following labels are used to make that explicit:

- PUBLIC:** this information will be published on the *public* TI web site. The whole world can potentially access and read this.
- SECURE:** this information will only be published on the *members-only* TI web site. It is therefore only available to TI "Accredited" and "Certified" teams.
- TI INTERNAL:** this information will only be used to provide TI services. It is therefore not directly available to other teams but might become visible indirectly (like bounces caused by mailer problems).
- MIXED:** Indicates that the corresponding section contains both PUBLIC as well as SECURE or TI INTERNAL fields as indicated.

In case you don't want a sensitive piece of information (for example an emergency contact number) to be published on the *public* TI web site, you might indicate this accordingly. Also if you would like to have different information published on the *public* and the *members-only* TI web site, you might indicate this for the applicable fields.

Note on GPG/PGP and X.509: anywhere where a GPG key is requested, this of course can also be a PGP key as GPG is functionally equivalent to PGP. It can not be an X.509 certificate for now. X.509 is wholly different from GPG/PGP and is not used much yet by teams for external communication. For internal use within organisations and teams, X.509 is well suited, but not at this moment for inter-team communication as the installed base simply is not sufficient for that.

Regarding the standards for using GPG/PGP keys, the TI highly recommends the following:

- Crypto algorithm: RSA, Elgamal or DH/DSS



- Key length: at least 2048 bits

In all cases make sure that a team's or team member's "from" e-mail address is contained in either the primary user id of the corresponding GPG/PGP key, or in an additional user id (which can be added afterwards as well). This is for example needed to get subscribed on the TI's encrypted mailing list. Also the GPG/PGP key must be at least self-signed.

5.1 Mandatory Fields describing the Team

Name of the Team PUBLIC

- Short team name or acronym used
- Official team name
- Host organisation of which the team is a part of
- Country the team is located in (list multiple countries if needed)
- Date of establishment

Constituency PUBLIC

- Type of constituency: [CHOOSE ONE OR MORE OF] research-or-educational / government / military / national / financial-organisation / other-commercial-organisation / non-commercial-organisation / ISP-customers / commercial-customers / OTHER (EXPLAIN).
- Description of formal constituency: verbal description explaining the formal constituencies and the exact relationship, especially if more than one type of constituency is listed above.
- Description of informal constituency: verbal description explaining the informal constituencies which receive some sort of best-effort services.
- Internet domain, AS numbers and/or IP (and IPv6 if applicable) address information defining the constituency and its networks.
- All countries in which constituency members are located in

Contact Information PUBLIC

- Regular telephone number (country code, telephone number, time zone)
- Emergency telephone number (country code, telephone number, time zone)
- Facsimile number (country code, telefax number, time zone - if applicable)



- Other telecommunication facilities (if applicable)
- Postal address of team
- E-mail address of team and associated GPG/PGP key, e-mail address **MUST** be present in a user-id of it
- Public web page(s) if available

Business Hours MIXED

- Description of business hours PUBLIC
- Procedure for contacting the team outside business hours SECURE

Team Representative(s) SECURE

Please note: Two representatives can be registered – however also all team members **SHOULD** be registered to get access to the services and to complement the information about your team (see 5.2 Optional Fields).

- Name of primary person representing the team (mandatory)
 - Regular telephone number (country code, telephone number, time zone)
 - Mobile telephone number (country code, telephone number, time zone)
 - Facsimile number (country code, telefax number, time zone - if applicable)
 - Other telecommunication facilities (if applicable)
 - Postal address if different from team
 - E-mail address and associated GPG/PGP key, e-mail address **MUST** be present in a user-id of it
- Name of secondary person representing team (optional, but recommended)
 - Regular telephone number (country code, telephone number, time zone)
 - Mobile telephone number (country code, telephone number, time zone)
 - Facsimile number (country code, telefax number, time zone - if applicable)
 - Other telecommunication facilities (if applicable)
 - Postal address if different from team
 - E-mail address and associated GPG/PGP key, e-mail address **MUST** be present in a user-id of it



Policies SECURE

- Specify how information is handled, especially with regards to restricting access and protecting its confidentiality once received by your team? Are there legal considerations to take into account with regards to the information handling?

RFC 2350 PUBLIC

- URL of the published RFC 2350
- Date of last update and version number (if applicable)
- Distribution mechanisms for notifications about updates

SIM3 SECURE

- URL of the actual SIM3 self-check (on sim3-check.opencsirt.org)
- Date of last update

Membership of Professional Team / Security Organisations PUBLIC

- Is your team a member of FIRST and if yes, since what year?
- Is your team member of a national CERT cooperation or community and if yes, since what year?
- Specify other CERT or security communities in which your team (or your host organisation) is a member of and if yes, since what year?

Services provided to the Constituency SECURE

If you provide services not listed below – or if you believe, that the terms chosen do not fit clearly to your services – please describe those services in free text format!

These services are not yet aligned with the CSIRT Services Framework currently developed by experts within the FIRST context. We will start supporting this framework v 2.1 version later in 2020!

- Specify available reactive services, using the following list (or adding to it):
 - alerts and warnings
 - artifact analysis
 - artifact response
 - artifact response coordination
 - forensic analysis



- incident analysis
- incident response
- incident response support
- incident response on-site
- incident response coordination
- vulnerability analysis
- vulnerability response
- vulnerability response coordination
- Specify available proactive services, using the following list (or adding to it):
 - announcements
 - configuration and maintenance of security tools, applications and infrastructures
 - development of security tools
 - intrusion detection services
 - security audits or assessments
 - security-related information dissemination
 - technology watch
 - Trend and neighbourhood watch
- Specify security quality management services, using the following list (or adding to it):
 - awareness building
 - business continuity and disaster recovery planning
 - education/training
 - product evaluation or certification
 - risk analysis
 - security consulting



5.2 Optional Fields describing the Team

Contact Persons for Constituency SECURE

- Person representing the Constituency
 - Organisation
 - E-mail address

Contact Persons for Host Organisation SECURE

- Person representing the Host Organisation
 - Organisation
 - E-mail address

Team Members SECURE

- For each member of your team that shall receive an X.509 user certificate for accessing TI services, please provide
 - Full name
 - E-mail address
 - If applicable provide associated GPG/PGP keys as well. (e-mail address **MUST** be present in a user-id of the individual keys)

Information Resources SECURE

- If your team provide additional information resources (for example AnonFTP servers, specific web pages with tools) that are accessible for TI Accredited and Certified teams, please add:
 - URL of the service
 - Description
 - Process to get access

5.3 Service related Fields used internally by the TI

TI Listed Teams Mailing List TI INTERNAL

- Designated e-mail address for subscription to mailing lists for TI listed teams only, used for alerts, announcements and discussion

6 APPENDIX C: CRITERIA FOR “LISTED” STATUS

6.1 Explanation and Guidance

An “listed” team **MUST** or **SHOULD** meet the below criteria in section 6.2 and 6.3.

- The **MUSTS** are criteria which have to be met to successfully pass the accreditation process and to acquire/maintain the “listed” status.
- The **SHOULD**S are strong recommendations, not obligations.
- MUST** and **SHOULD** are defined according to IETF standards, see Appendix D.
- If you do **NOT** (yet) fully support a **MUST** criteria: Support of the **MUST** criteria is obligatory to acquire “listed” status, so any non-support of such criteria must be cleared as soon as possible with the TI Team.
- If you do not support a **SHOULD** criteria, put down “not supported”. It would be helpful if you explain what is missing or needed. Indicate planned support.

6.2 List of all MUST Criteria

- Teams **MUST** be described by qualitative and a minimum number of quantitative values as per Appendix B and ensure that these descriptions continue to match reality.
- Teams **MUST** cooperate with the publication of all delivered data on the TI members-only website. Access is restricted to TI “accredited” and TI “certified” teams (including all certified teams), TI Associates, the TI team and the TF-CSIRT SC.
- Teams **MUST** cooperate with the publication of the essentials of their contact information – meaning all items marked **PUBLIC** in Appendix B – on the TI public website (<https://www.trusted-introducer.org/>).
- Teams **MUST** register two team representatives.
- Teams **MUST** actively support the TI requirement to keep the information provided to the TI team up-to-date, that is to ensure its actuality and usability.
- Teams **MUST** support question-and-answer sessions per e-mail or on the phone with the TI team to discuss issues or questions arising with regards to the provided information, its authenticity or its actuality.
- Teams **MUST** support (not financially) a site visit if the TI team or the TF-CSIRT SC concludes that a site visit is necessary. Site visits are last-resort possibilities if question-and-answer sessions fail or when other pressing reasons exist – but a



site visit can also be invited. Observations made during the site visit bearing a relation to the criteria described here, will be objectively logged by the TI team member conducting the site visit.

- Teams **MUST** recognise and support the "Traffic Light Protocol"⁴ as ratified by the TI "Accredited" and "Certified" teams.
- Teams **MUST** handle all sensitive or private information sent to them – including all incident related information – in a secure and protective way (subject to local law), internally but also when sending it out again.

6.3 List of all SHOULD Criteria

- Teams **SHOULD** present at least their external services, if any, to the outside world as per RFC 2350,⁵ including a specification of quantitative values and ensure that these descriptions continue to match reality, including indicated service levels if applicable. (Especially in the beginning starting teams may not have already answers or procedures to fill it out completely, in such case it is important to update it frequently while your team progresses.)
- Teams **SHOULD** regularly attend TF-CSIRT meetings.
- Teams **SHOULD** comply with the "CSIRT Code of Practice"⁶ as ratified by the TI Accredited Teams.
- Teams **SHOULD** use the "SIM3 Maturity Model"⁷ as a starting point for self-assessments or audits of their services. (Especially for a starting team SIM3 might not be the most interesting self-check to run, but it will also provide for a useful list of issues to consider adding to the roadmap of your team's development.)
- Teams **SHOULD** respond to TI reaction tests to demonstrate that they can be reached via their official contacts.

⁴ <https://www.trusted-introducer.org/ISTLP.pdf>

⁵ <https://www.ietf.org/rfc/rfc2350.txt>

⁶ <https://www.trusted-introducer.org/CCoPv21.pdf>

⁷ SIM3 is maintained by the OpenCSIRT Foundation:
<https://www.trusted-introducer.org/SIM3-Reference-Model.pdf> (Standard)
<https://sim3-check.opencsirt.org/> (Self-Check)



7 APPENDIX D: STANDARD DEFINITIONS TAKEN FROM THE IETF APPROACH [RFC2119]

MUST

This word, or the terms "REQUIRED" or "SHALL", mean that the definition is an absolute requirement of the specification.

SHOULD

This word, or the adjective "RECOMMENDED", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.



8 APPENDIX E: 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.

8.1 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 provide 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 "accredited" 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. 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.

8.2 TI Status: "Listing Candidate", "Listed", "Re-Listing Candidate" and "Re-Listing Pending"

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 "listed" status, thereby passing the intermediate "listing candidate" status.



The various statuses are characterised as follows:

- **Listing Candidate:** Temporary intermediate phase for teams acquiring "listed" status, with only two possible outcomes: formal listing if the team formally meets the defined criteria within the specified period and is supported by the TI community, or removal from the directory when it does not.
- **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.
- **Re-Listing Pending:** After three years as TI "listed" team the status is changed to "pending" to indicate, that it is time for the formal "re-listing" process. The team will be asked if it wishes to stay in the TI community: if the team still meets the defined criteria, the team will become a TI "Re-Listing" candidate. If not, the team will be removed from the TI directory.
- **Re-Listing Candidate:** Temporary intermediate phase for teams acquiring "listed" status after having been listed for three years before, with only two possible outcomes: formal listing for another three years if the team formally meets the defined criteria within the specified period and is supported by the TI community, or removal if it is not supported by the community.

Instead of the need to become re-listed a TI "Listed" team can apply to become TI "Accredited" any time once listed.

8.3 Validation of Information

To acquire TI "Listed" status a team has to provide a useful, but limited, amount of operational information. The TI listing 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 listing (as well as the 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 ensure⁸ the *authenticity* of information coming from "listed" teams or "listing 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. Indirect (cyber) contact is currently supported for e-mail protected by GPG/PGP signatures or by the TI Self-Service which supports HTTPS and authenticates authorized users via X.509 user certificates.

To ensure the *actuality* of information, the "listed" teams are expected to keep the information they provided up-to-date. To help them meet that goal, the TI team entertains a twelve (12) monthly maintenance cycle, prompting all TI "Listed" 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.

⁸ „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.