

4 Appendix A: Form to accept the invitation to acquire TI "accredited" status

Team Acronym or Name : ABC-CERT

We hereby declare that we accept the invitation to acquire "accredited" status as laid out in the "Invitation Package for TI "accredited" Status" Version 1.1 – 31 October 2011 (in short: Invitation Package) as sent to us by the Trusted Introducer service provider (in short: TI), and that we support the criteria, procedures and timeline set out in the Invitation Package.

More specifically, we:

- declare that we are prepared to meet and maintain the „MUST“ criteria for "accredited" status laid out in Invitation Package Appendix C ;
- commit ourselves to file completed appendices B and C of the Invitation Package to the TI within two (2) months ;
- agree to the publication of various data, as specified in the Invitation Package, on the public and restricted TI web sites (note on privacy: personal data will not appear on the public web site) ;
- commit ourselves to pay a one-off amount of EUR 800 to TERENA to cover the cost of the application for "accredited" status (if your organisation is a TERENA member a discount arrangement may apply here) ;
- declare that we have taken note of, and intend to pay, the annual fee of EUR 1,056 that is due to TERENA if and when we obtain "accredited" status

City, Country, Date: _____

Representative: _____

Signature: _____

5 Appendix B : Information Template for “accredited” teams

The set of information a team needs to provide to acquire “accredited” 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 case instead of copying the relevant copy simply sending in the RFC 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 accredited teams.
- **TI INTERNAL** : this information will only be used to provide TI services. It is therefore not directly available to accredited teams (like SMS numbers for the alerting service), 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. Another set of information for which such considerations might apply is the IRT object, which contains e-mail addresses and telephone numbers. If in doubt, contact your primary introducer and discuss this with him.

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

This recommendation is not a MUST but highly recommended – also the TI will only sign keys corresponding with these minimum demands.

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 constituency: verbal description explaining the formal and informal constituencies and the exact relationship, especially if more than one type of constituency is listed above.
- 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, timezone)
- Emergency telephone number (country code, telephone number, timezone)
- Facsimile number (country code, telefax number, timezone)
- Other telecommunication facilities (if applicable)
- Postal address of team

- E-mail address of team
 - 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, timezone)
 - Mobil telephone number (country code, telephone number, timezone)
 - Facsimile number (country code, telefax number, timezone)
 - Other telecommunication facilities (if applicable)
 - Postal address if different from team
 - E-mail address
 - 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, timezone)
 - Mobil telephone number (country code, telephone number, timezone)
 - Facsimile number (country code, telefax number, timezone)
 - Other telecommunication facilities (if applicable)
 - Postal address if different from team
 - E-mail address
 - Associated GPG/PGP key, e-mail address MUST be present in a user-id of it

Policies SECURE

- Specify how incoming information is “tagged” or “classified” or “sorted” to differentiate between various information sources and priorities?
- 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?
- What considerations are adopted for the disclosure of information (“when what?”), especially incident related information passed on to other teams or to sites?
- Specify any special legal considerations to take into account with regards to the handling and disclosure of information.
- Specify any special legal considerations to take into account with regards to the use of cryptography (based on e.g. GPG/PGP or X.509) in the handling of information. This specification must include possible legal boundary conditions as key escrow or enforceability of weak cryptographic technologies.

RFC 2350 PUBLIC

- The information beyond is usually contained in the filled-out RFC 2350, in which case submitting this document will be enough to satisfy the need for this information.
- URL of the published RFC 2350
- Date of last update and version number (if applicable)
- Distribution mechanisms for notifications about updates

Membership of professional team / security organisations MIXED

- Does your team participate in TF-CSIRT and if yes, since what year? SECURE
- Is your team a member of FIRST and if yes, since what year? PUBLIC
- Is your team member of a national CERT cooperation or community and if yes, since what year? PUBLIC
- Specify other CERT or security organisations where your team (or it's host organisation) is a member of and if yes, since what year? SECURE

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!
- 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 a 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)

Tools and Expertise SECURE

- Specify your team’s Incident Management process tool (workflow, reporting interfaces, exchange formats, contact person).

Please note : This is about the IM process only. It can vary from software like AIRT or RTIR (the next question asks for the software details of that) and how they are used unto the simple use of logbooks, spreadsheets, and human written e-mail as well as exchange formats.
- Specify your team’s Incident Management related software (name, last update, version, URL, license, description, contact person)
- Specify (special/specific) expertise of your team on TCP/IP and/or other Networks
- Specify (special/specific) expertise of your team on System Platforms
- Specify (special/specific) expertise of your team on Operating Systems
- Specify (special/specific) expertise of your team on Specific Software Packages (e.g. SAP)

Team / Process Information SECURE

- Specify any relevant team or host organisation accreditations or certifications, like ISO 27001, ISO 9000, etcetera. Explain where needed.
- Specify relevant team projects (name, goal, time-period, partners, contact person) : **note** that the goal here is not to provide detail but to enable others teams to see what your team is up to – this serves as aid for more effective collaboration and sharing.

- Specify your team's reporting structure (type of reports, target audience(s), frequency).

Team / Staff Information

SECURE

- Specify the team members required or recommended relevant education levels (examples: TRANSITS, SANS, CERT/CC trainings for CERT/technical expertise)

Please note : You can also state your team's policy here in that regard like the goals that are set. That might be easier to maintain than any representation of an actual situation.

- Specify your team's headcount (normal and backup).

Please note : This is the number of people involved in the team operational business. "Normal" is the standard category – "backup" imply all people that are not part of your team's operation normally, but could be utilized e.g. in cases of emergency.

- Specify your team's work force in terms of FTE (full time equivalent) both for "normal" and "backup"

Please note : The number of FTE is smaller than or equal to the headcount by definition. A team might have a headcount of 7 (part time staff) with a budgeted or estimated workload of 2.5 FTE for instance.

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

IRT Object related information

PUBLIC

- If a IRT object shall be created, all information might be taken from the above set of fields about the team.
- In case specific information shall be used for the IRT object, this will need to be listed.

5.3 Service related fields used internally by the TI

Encrypted TI Accredited Teams Mailing List TI INTERNAL

- Designated e-mail address for subscription to mailing lists for TI accredited teams only, used for alerts, announcements and discussion
 - Associated GPG/PGP key, e-mail address MUST be present in a user-id of the GPG/PGP key.

Encrypted TI Accredited Team Reps Mailing List TI INTERNAL

- *Note: The information for this mailing list – encrypted and only for team representatives – is taken from the already provided data for the team representative.*

Outband Alerting System TI INTERNAL

- In time of a real Internet crisis an out-of-band – phone, not Internet based – alerting system is available. All registered contacts will receive an SMS and/or a telephone call in case of an alert. A PIN must be provided by the called person for authentication purposes.
- For each recipient you would like to register the following information must be provided:
 - number to send to / call
 - type of contact:
 - SMS: a SMS will be send to the given number
 - phone: a call will be made to it
 - mobil: both, SMS and phone, will be triggered
 - time zone information including DST
 - time period (from / to) in 24h notation (for example 09:00 for 9am and 15:00 for 3pm)
 - coverage: weekday (Mo-Fr) or all (Mo-Su)
- more than one point of contacts can be added

Billing Information TI INTERNAL

- Postal address for invoices (if different from team's postal address)

Please note : The billing address used will contain the name of the team representative, the short team name and the team address otherwise.
- Reference field for billing (if applicable)

Please note : The reference field is an additional line of information for the invoice and can contain e.g. an internal reference or purchase order number, or any other

codeword or personal name as required by your organisation. If no information is provided, this field will be left empty.

- VAT number of the legal organisation

Please note : If no VAT number is assigned (i.e. for Government agencies) please write “N/A”.



6 Appendix C: Criteria for “Accredited” Status

6.1 Explanation and Guidance

An “accredited” team **MUST** or **SHOULD** meet the below criteria.

- The **MUSTS** are criteria which have to be met to successfully pass the accreditation process and to acquire/maintain the “accredited” status.
- The **SHOULD**S are strong recommendations, not obligations.
- **MUST** and **SHOULD** are defined according to IETF standards, see Appendix D.

Describe in as few words as possible your support of the various accreditation criteria. Please be as concise as possible.

- If you support a **MUST** criterion, just put down “supported”.
- If you do **NOT** (yet) fully support a **MUST** criteria, put down : “not (fully) supported (yet)”, **and explain what you do not support (yet) and why, and when you plan to support it**. Support of the **MUST** criteria is obligatory to acquire “accredited” status, so any non-support of such criteria must be cleared as soon as possible between your team and the TI Personal Introducer.
- If you support a **SHOULD** criteria, put down “supported”.
- If you do not support a **SHOULD** criteria, put down “not supported”. Explain if needed or indicate planned support.

6.2 List of all Criteria

1. 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.

YOUR SUPPORT: ...

2. Teams **MUST** present at least their external services, if any, to the outside world as per RFC 2350,⁴ including a specification of quantitative values and ensure that these descriptions continue to match reality, including indicated service levels.

YOUR SUPPORT: ...

⁴ <http://www.ietf.org/rfc/rfc2350.txt>

3. Teams **MUST** cooperate with the publication of all delivered data on the TI **members-only** website. Access is restricted to “accredited” teams (including all certified teams), TI Associates, the TI team and the TI Review Board.

YOUR SUPPORT: ...

4. 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/>).

YOUR SUPPORT: ...

5. 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.

YOUR SUPPORT: ...

6. 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.

YOUR SUPPORT: ...

7. Teams **MUST** support (not financially) a site visit if the TI team or the TI Review Board 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.

YOUR SUPPORT: ...

8. 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. Teams **MUST** describe their policy in that respect and are urgently advised in this regard to establish a secure communications scheme based on GPG/PGP and/or X.509.

YOUR SUPPORT: ...

9. Teams **MUST** recognise and support the “Information Sharing Traffic Light Protocol”⁵ as ratified by the TI Accredited Teams.

YOUR SUPPORT: ...

10. Teams **SHOULD** actively support the signing of their team and representatives GPG/PGP keys, during TI/TF-CSIRT meetings and other occasions, by the TI team.

YOUR SUPPORT: ...

11. Teams **SHOULD** comply with the “CSIRT Code of Practice”⁶ as ratified by the TI Accredited Teams.

YOUR SUPPORT: ...

12. Teams **MUST** comply with the “CSIRT Code of Practice” **if and only if** they support compliance here. If your team does not support the Code of practice, the statement is **NOT APPLICABLE**.

YOUR SUPPORT: ...

13. Teams **SHOULD** regularly attend TI and TF-CSIRT meetings.

YOUR SUPPORT: ...

14. Teams **SHOULD** use the “SIM3 Maturity Model”⁷ as a starting point for self-assessments or audits of their services.

YOUR SUPPORT: ...

15. Teams **MUST** pay the fees established for acquiring and maintaining “accredited” status as set by TERENA.

YOUR SUPPORT: ...

⁵ <https://www.trusted-introducer.org/links/ISTLP-v1.1-approved.pdf>

⁶ <https://www.trusted-introducer.org/links/CCoP-v2.1-approved.pdf>

⁷ <https://www.trusted-introducer.org/links/SIM3-mkXV-TI.pdf>

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, TI Review Board 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/>), 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.
- **TI Review Board:** The Review Board 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 Review Board 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
 - Advise TERENA on the continuity of the service, its fee structure and contractual issues with regards to the TI team.
 - Handle specific inquiries about the functioning of the TI service, which are related to the strategical perspective represented by the Review Board.
 - Decide about any issues that are outside existing TI policies, like making exceptions to the defined rules for status change (towards "accredited" status, or

fallback to "listed" status), deciding on a site visit to clarify issues that could not be handled otherwise, etcetera.

The Board 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 Review Board and to enable an overall review of the TI service.

The Board has 5 members, of which:

- One (1) is appointed by TERENA to act on it's behalf, as the party that legally holds the contract with the TI operator (member *ex officio*) ;
- One (1) is the chair of TF-CERT (member *ex officio*) ;
- Three (3) are elected out of the ranks of accredited teams. These elected Review Board members will serve a three (3) year term each, which is devised such that each year in September ONE AND ONLY ONE member's term expires, thus ensuring continuity within the Review Board.

The Review Board members will appoint a chair from their midst, following the election of a new member, every year.

- **TERENA:** The "Trusted Introducer" service originated in September 2000 from cooperation activities between CERTs and security teams in ope that were organized by TERENA (<http://www.terena.nl/>). TERENA continues to act as the financial and legal focal point for the TI service:
 - as the party contracting the TI operator ;
 - invoicing the “accreditation candidates” and “accredited” teams ;
 - supporting the TI Review Board.

One of TERENA's task forces, TF-CSIRT, focusses on the cooperation among vendors, CERTs, security teams as well as security experts. Therefore many of the TF-CSIRT members are listed or accredited teams.

- **TI Operator:** PRESECURE GmbH, Germany, with support of other well-known experts of the field operates the TI service since September 2010, having been involved since its conception back in 2000.

8.2 TI Status: “listed”, “accreditation candidate” and “accredited”

As you received this invitation, your team already has acquired the “listed” status, meaning it's 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 it's 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.

8.3 Validation of Information

To acquire “accredited” status a team has to 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 it's 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 to recognized here:

- **Authenticity** : This means that the TI team can be sure that the statement came from the team and/or it's 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 ensure⁸ 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:

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.

- 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-date. 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.