TRUSTED NETWORKS POLICY, *Beta-version vs0.7, November 24, 2014*

This document describes the qualification rules to which a network should comply to be qualified as a Trusted Network.

0. Definitions:

Rules: *this Trusted Networks Policy*
Trusted Networks Initiative (TNI) *the group of members and observers jointly responsible for managing the Trusted Networks project*
TNI Member: *a participant of this group having signed the Agreement between participants, and as such having voting rights.*
TNI Observer: *a participant of this group not having signed the Agreement, however invited by the members to participate, though without voting rights*
Trusted Network (TN): *a network being qualified as being compliant with the Rules of TNI*
Trusted Routing (TR): *the method of routing between Trusted Networks*
IXP: *an IXP with who TNI has an agreement to facilitate Trusted Routing*

1. PRELIMINARY PROVISIONS

1.1. These Rules set out the conditions for compliance with the policy of the 'Trusted Networks Initiative' (hereinafter "TNI") and as such become a qualified 'Trusted Network'.

1.2. TNI serves as a means of permanent or emergency communication, 'Trusted Routing' (hereinafter "TR"), for the members/customers of IXPs, providing a high level of confidence and security in the event of a major attack on the internet infrastructure.

1.3. TNI was created with the aim of providing at minimum a "last resort" interconnection to other Trusted Networks in case a Trusted Network infrastructure should become the target of an attack.

1.4. Networks can be qualified as Trusted Network by TNI, there may be costs for being qualified, periodically to be determined.

1.5. Any party can apply for a qualification as Trusted Network. The basis for this is the ASN(s) of the party, with which he requires to be qualified as Trusted Network

1.6 The party should apply for qualification as Trusted Network by issuing a statement in writing to TNI that party commits to comply with the Rules, as in Addendum I.
TNI will react to this request in writing, within 10 workingdays, with a decission if party is qualified as Trusted Network, or with further questions.

2. CONDITIONS FOR NETWORKS TO BE QUALIFIED AS 'TRUSTED NETWORK'

2.1. In order to become qualified, a Trusted Network should have the intention to connect to at least one of the participating IXPs.

2.2. A candidate for being qualified as Trusted Network must declare in writing that they shall adhere to the present Rules, to be judged by TNI, as in Addendum I.

2.3. Duration of the validity of the qualification will be determined by TNI.
If Rules significantly change, TNI may require a Trusted Network to be qualified again, or may solely link a qualification to a certain version of the Rules.

2.4. A network may submit a valid Trusted Network qualification request provided that they:

2.4.1. have in the past not repeatedly or seriously violated the Rules;

2.4.2. secure that their Network Operations Center (NOC) functions 24-hours a day, 7 days a week, with an email contact and at least two telephone numbers (of which at least one must be technically independent of the IP protocol) available and listed on the hidden TNI website. The engineer-on-duty should start dealing with reported events within 0,5 hour. Other Trusted Networks may use this contact info to address security-related issues to other Trusted Networks;

2.4.3. use source address filtering (to prevent IP spoofing) in the sense of either BCP-38 or SAC004;

2.4.4. have a system for detecting and eliminating sources of attacks similar to and including DNS amplification (banning unmanaged open resolvers, implementing response rate limiting);

2.4.5. monitor traffic on their network, at least in terms of flows and packets; this monitoring must be able to actively detect and signal an irregularity in the monitored values;

2.4.6. do not advertise other prefixes than those they are allowed to advertise;

2.4.7. do not send traffic from prefixes on its network that it does not advertise;

2.4.8. protect their routers in compliance with the RFC6192 (control plane policy) recommendations;

2.4.9. operate a capable CERT (Computer Emergency Response Team) / CSIRT (Computer Security Incident Response Team), or similar;

2.4.10. have implemented internal incident resolution procedures;

2.4.11. intervene to remove/limit a security incident as quickly as possible;

2.4.12. monitor security messages from the suppliers of network components and react to them as appropriate;

2.4.13. cooperate with authorities to trace the cause and suspects of the incident.

3. OPERATIONAL PREREQUISITES FOR BEING QUALIFIED AS TRUSTED NETWORKS

3.1. A Trusted Network should monitor the communication on the special Trusted Routing mailing tech-lists.

3.2. A Trusted Network can only advertise a prefix where he can guarantee that the Rules will be reasonably applied.

4. MONITORING RULE COMPLIANCE

4.1. Adherence to these Rules may be monitored by TNI, who is authorized to carry out audits to ensure compliance (and to this aim are authorized to violate these Rules). Identified violations may be announced to TNI members. The Trusted Network concerned is allowed to comment on the findings; other networks can demand clarification or additional information.

4.2. Upon the violation of these Rules, including cases where a Trusted Network no longer complies with the conditions outlined in the Rules, TNI can decide to :

- suspend qualification for upto 3 months and have the network temporary disconnected from Trusted Routing at the IXP
- expel the network from being qualified and have the network permanently disconnected from Trusted Routing at the IXP

Reentering as qualified Trusted Network is to be decided by TNI.

4.3 Dispute Procedure:
A Trusted Network being accused of violating the Rules, and for that reason has been suspended or expelled as Trusted Network, may dispute this decision. Both the accused

party as the accusing party should within 20 workingdays hand-over arguments to TNI, whereby TNI will decide within 10 workingdays.

5. RULE CHANGES AND OTHER DECISIONS; COMMUNICATION

5.1. All TNI-related communication between Trusted Networks happens via the special mailing tech-list. Communication important or relevant for more parties, may occur via this mailinglist. Communication intended for 1-to-1, should exchange bilateral.

5.2. Each Trusted Network has the obligation to provide other Trusted Networks with information about significant security incidents that TNI is supposed to prevent.

5.3. Each Trusted Network is obliged to maintain confidentiality regarding the facts they have learned as Trusted Network, including and especially: all information exchanged through communication; information about security incidents detected on other Trusted Networks; information regarding the compliance or violation of the prerequisites set out by these Rules; information about rejected applications for Trusted Network in TNI.

5.4. In the case of a dispute about the interpretation of any of these Rules, especially when deciding whether or not one of the provisions in these Rules has been violated, the final decision rests with TNI.

5.5. A Trusted Network should provide all the contact-details to TNI as relevant subject to clause 2.4.2

6. PUBLICITY

6.1. Each Trusted Network has the right to use the special Trusted Network logo and name in the form approved by TNI.

6.2. On its website, TNI publishes a list of Trusted Networks. Trusted Networks allow TNI to publish these lists, unless otherwise agreed.

7. OPTIONAL REQUIREMENTS

The following is strongly advised, however not mandatory:

7.1. The Trusted Network' domains, which it uses to communicate with customers/business partners (including company websites and product websites), are preferably signed by DNSSEC technology, unless such signing is prevented by serious technical issues, and the validation on their resolvers has been turned on;

7.2. Participating Trusted Networks will support a Black Hole community such that if one Trusted Network advertises a route with a BGP community tag consisting of it's own AS number, with ':666' behind it (eg: 12345:666), parties will accept the route even if it is more specific then a /24 (upto a /32) and will drop outgoing traffic destined toward that IP address.

7.3. Within the TNI, BGP sessions are protected against session hijacking, for example using TCP MD5 signatures (RFC2385).

7.4 The Trusted Network is aware of the valid global Routing Manifesto policy on Collective Responsibility and Collaboration for Routing Resilience and Security:
"Mutually Agreed Norms for Routing Security (MANRS)"
(https://www.routingmanifesto.org/manrs/)

8. THE TRUSTED NETWORKS INITIATIVE STATEMENT OF ANTITRUST POLICY

It is the policy of the Trusted Networks Initiative that its members comply fully with all applicable competition and antitrust laws and trade regulations of the Netherlands when engaged in activities of the Trusted Networks Initiative. Each company is likely to have their own anti-trust policies in place and all members should familiarize themselves with these. Where possible you should also discuss any questions that you may have with your own legal advisers.
This Policy has to be accepted by all participants of the Trusted Networks Initiative meetings and entails that each of the participants to these meetings expresses its agreement with this Policy and the accompanying behaviour resulting from this policy.
Competition and antitrust laws prohibit many types of agreements and concerted practices among competitors with respect to the terms or conditions on which they compete. An (verbal) exchange of sensitive information may be in itself in breach of competition rules even if the parties participating in such exchange do not take part in anticompetitive agreements or collusive practices.
Because a court or government administrative agency might conclude (correctly or not) that persons who have talked about a subject have explicitly or implicitly reached an agreement with respect to it, or may be seen as conducting a concerted practice, representatives of members should in any way not discuss (or exchange information regarding) any of the following topics with their competitors absent advice from counsel that the particular discussion is appropriate under the circumstances:

- information or arrangements about prices, price components, rebates, pricing strategy and calculation, and intended changes in prices,

- terms and conditions for supply and payment, relating to contracts with third parties,
- information about business strategies, future market conduct and new product launches or roll-outs,
- detailed information about profits, profit margin, market shares, capacity and intended investments, as far as this information is not publicly available,
- commercially sensitive information about specific research and development projects,
- coordination of bidding towards third parties, regional or personal division of markets, customers or sources, express or tacit agreement about boycotting certain companies or cutting-off the supply or purchase against a certain company,
- coordination of dividing the market in whatever form.

In order to ensure that the meeting will take and have taken place in accordance with the guidelines included above, the Trusted Networks Initiative shall organise that each meeting will be governed by an agenda send to all participants prior to the meeting and that minutes will be made of such meetings. Minutes, prepared and distributed as soon as practically possible after the meeting, should (briefly) summarise all matters discussed and conclusions, if any, reached and who was (not) present during that discussion in case participants enter or leave during the meeting.

Members should understand that these guidelines apply not only to discussions at formal meetings, but to all informal discussions as well outside the formal meetings. You should be aware that there is no such thing as an "off the record discussion" when it relates to competition and antitrust law.

It is important to realise that competition and antitrust law investigations, proceedings, indictments and civil lawsuits have arisen from informal conversations at industry meetings or in social settings.

If a representative of a member ever has any questions as to the legality of any proposed course of action, the matter should immediately be referred to the (in-house or outside) legal department of your own company to assure full compliance with applicable competition and antitrust laws.

Statement to be read out before each meeting and to be included in TNI meeting agendas and minutes:

QUOTE

"This meeting will be conducted in accordance with the Trusted Networks Initiative compliance policy set forth in the Trusted Networks Initiative Statement Of Antitrust.

It is the policy of the the Trusted Networks Initiative that its members comply fully with all applicable competition and antitrust laws and trade regulations when engaged in activities of the Trusted Networks Initiative.

Each Party present at this meeting accept the Trusted Networks Initiative Antitrust policy and will ensure that none of topics will be discussed which are considered inappropriate according to competition law and the Antitrust policy".

UNQUOTE

ADDENDUM I: QUALIFICATION REQUEST

Parties interested in being qualified as Trusted Network may issue a request to the chairman of the Trusted Networks Initiative by e-mail. The e-mail should contain a signed and scanned letter with company logo and letterhead with at least the text and signatures as indicated below. Please copy this form, fill in the blanks, sign and scan the form and send it by e-mail to trustednetworksinitiative@thehaguesecuritydelta.com

==========

Herewith we state that our company

_____ *(Company-name)*
_____ *(Postal Address of Company)*
_____ *(Postal Address of Company)*
_____ *(Chief Security Officer name)*
_____ *(Statutory/senior management name)*

will comply per _____ *(date)*
to Trusted Networks Policy <Beta-version vs0.7, November 24, 2014>

with respect to our AS number(s):
_____ *(Participating AS number(s))*

Our contact details for this purpose are:
_____ *(NOC-email)* _____ *(Peering-email)*
_____ *(telephone primary office-hours)*
_____ *(telephone secondary/escalation/24-7)*

We accept being invoiced as follows:
X *We accept being charged for Euro 0 /yr*) upfront for* ***qualification*** *as Trusted Network*
□ *We also request to become a* ***member*** ***) of Trusted Networks Initiative at a premium of Euro 0 /yr *) upfront*

You can invoice us at:
_____ *(Company-name)*
_____ *(Postal Address of Company)*
_____ *(Postal Address of Company)*

As stated, date: _____

_____ *(Chief Security Officer signature)*

_____ *(Statutory/senior management signature)*

**): No first-year charges are applied if request is issued before April 1, 2015*

***): For the membership requirements and agreement see www.trustednetworksinitiative.nl*

==========