GFCE Triple-I Event Playbook

GFCE Triple-I is a GFCE initiative for enhancing justified trust in Internet connections and email exchanges through awareness raising on a number of state-of-the-art open internet security standards and instigating take up of those building on good practice experience.

This GFCE initiative is meant to "facilitate" awareness raising and capacity building events in different regions of the world in order to "enhance justified trust" in the using of Internet and/or email in those regions (specific priorities to be determined by stakeholders in the region). Local and regional actors are stimulated and supported in setting up and running local/regional events between regional stakeholders, bringing in local expertise, when useful. The initiative builds on the experience of two years of events (2018, 2019).

Preparation of Events

In order to build on previous Triple-I activities and to discuss further opportunities for awareness raising and instigating take up of open standards that enhance security of web- and email traffic, it is important to meet with the local stakeholders "in the regions".

In preparation of the events, GFCE Triple-I developed the following resources:

1- The GFCE Good Practices Document on Triple I;
2- A model agenda for the GFCE Triple-I Day (see annex I – model agenda)
3- A model "hold the date" message, indicating date, location and setup of the event, to pre-announce the event and invite subscription (see annex II – model invitations)

The expectation is that between 30 to 50 people from different stakeholder groups participate in the workshop discussions. This includes a limited number of global experts that join specifically to inspire with explanations about the mentioned standards, and/or to present good practices that may be relevant to inspire local practice.

In previous years, GFCE has supported these events with providing administrative support (e.g. publishing of the agenda, sending out invitations, registration of participants, publishing of the results, and with contributions to cover the logistical costs for organizing the events (e.g. costs of room and refreshments, lunch) and with limited support to travel costs for key organizers and presenters that require this.

Over the last year, as the COVID-19 pandemic resulted in drastically reduced ability to travel, many international events have shifted to a virtual mode: using tools like ZOOM, or WEBEX. In line with this, GFCE Triple-I events may also benefit from these tools and be set up as virtual events. This approach has both advantages and disadvantages, though the idea is to capitalize on the opportunities for reaching a wider audience and mitigating issues such as diminished social interaction by making knowledge and expertise available and accessible online.

Outline agenda for events

Aim of each meeting is to come to a common understanding amongst multiple stakeholders how to best progress implementation of selected open Internet standards, locally, in order to "enhance justified trust in the use of the Internet and email". For this we want to bring together policy makers from public and private sector and civil society organizations with practical and technical expertise.

Outline agenda for GFCE Triple-I meetings

The GFCE Triple-I events all followed the same model: whether they were full day events, or shorter events. Whereas we propose this modular agenda for your inspiration, this is not an obligation – it is up to you, as key organizer, to define together with your colleagues the way forward you feel would work best in your region. And work with other partners that are committed to help with bringing in expertise and documentation, as well as people to participate.

Module 1 – knowledge transfer. This module is intended to present the issues that can be addressed by the open standards selected. The presentation will highlight the advantages, and also the possible downsides, of relevance for the specific region. And it will highlight "what it takes" to implement these standards in the region.

- In a full day workshop, this first module typically took 2 to 3 hours;
- In a virtual setting, this first module would take 60 to 90 minutes.

The following standards will be discussed:

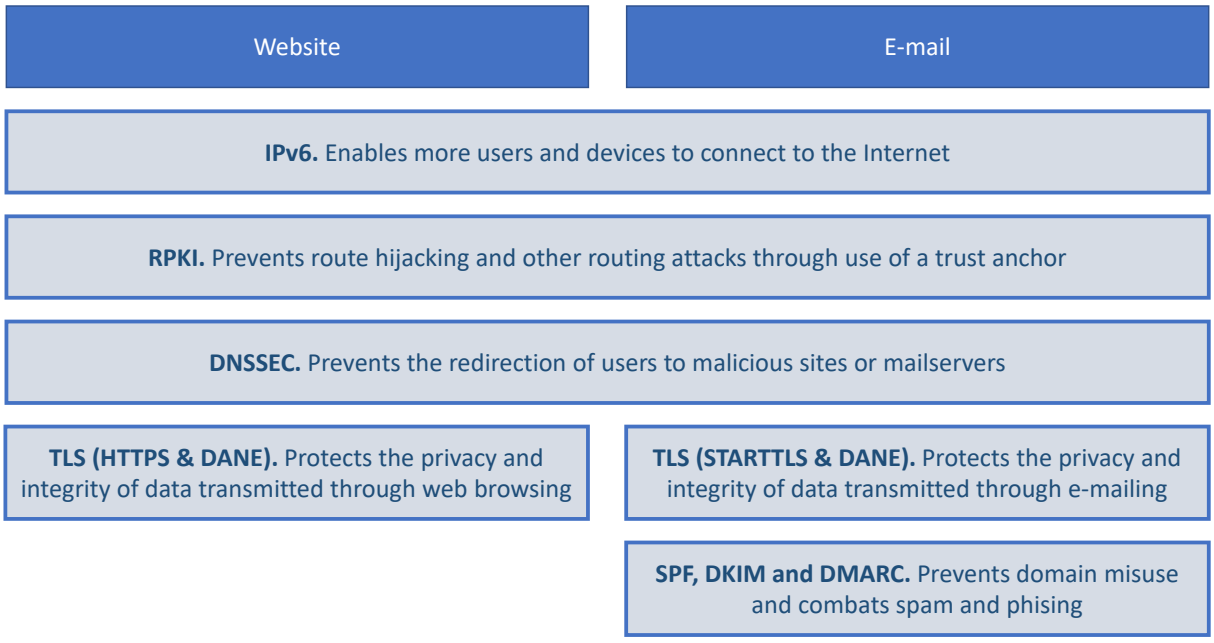

Fig. 1- Standards promoted by GFCE Triple-I

Please note that the website www.internet.nl helps you to check whether internet is up to date. The test tool Internet.nl is an initiative of the Dutch **Internet Standards Platform**. The aim of the platform is to jointly increase the use of modern Internet standards to make **the Internet more accessible, safer**

and more reliable for everyone. The platform is a collaboration between parties from the Dutch Internet community and the Dutch government, and is promoted for use, world-wide.

Module 2 – learning from practice. This module is intended to introduce new ideas that may be useful for the specific region, based on practice from other parts of the world, or to provide more attention to specific regional initiatives that are ongoing. There is no such thing as "best practice" that is the best solution, everywhere – yet much can be learned from successes and failures elsewhere. This module will be case-based and will include but not necessarily be limited to some of the good practice cases collected in the context of GFCE.

- In a full day workshop, this session typically took 2 to 3 hours;
- In a virtual setting, duration 60 to 90 minutes;

Examples of such inspirational practices that have been shared in earlier events include:

- DDOS Radar, which facilitates a Dutch proactive and collaborative DDoS mitigation strategy;
- Abuse mitigation through increasing transparency (e.g. Cybergreen, ICANN DAAR, M3AAWG, etc.);
- MANRS: a call by ISOC upon network operators to join the Routing Resilience Manifesto Initiative, and to agree to the Mutually Agreed Norms for Routing Security (MANRS) Principles;
- OTA IoT Trust Framework by ISOC as a guideline for safer IoT implementation;
- IDN, Universal Acceptance, and confusability practice by UASG;
- IX supporting secure/clean communications by implementing IRR as well as RPKI based filtering for their members.

Module 3 – action planning. The participants, with the help of the experts present, will work on possible actions and priorities, in a moderated session that, depending on the number of participants, will happen in break-out sessions organized in "Open Space" format. At the end of the session the moderator summarizes the findings, and participants commit to those actions they are willing to commit to. The results of this session will be published on the GFCE Triple-I pages by the GFCE Secretariat.

- In a full day session, duration is typically between 90 minutes and 2 hours;
- In a virtual setting, duration up to 60 minutes.

Examples of actions resulting from GFCE Triple-I events include:

- Awareness raising on relevant information to key stakeholders on standards and abuse practice;
- DDOS mitigation through collaboration inspired by Dutch practice;
- IoT Security enhancement based on the OTA Framework and IGF DC IoT good practice paper;
- Setup a RPKI deployment tracker, together;
- Explore ways to make the level of security more visible to end users when using websites;
- Plan for better ways to inform users about the risks related to [IoT] devices, and how to deal with this;
- Explore using the compliance testing tool in the region, and consider to set-up a regional version of www.internet.nl, that links to local priorities, local sources for support, and relates the "Hall of Fame" to the regional situation;
- More "Triple-I" capacity building workshops in the future.

For 2018 and 2019, a specific GFCE Triple-I facilitator was assigned to ensure the first series of workshops took place and that all experiences were brought together for future use.

For a draft agenda, see Annex I. For draft invite, see Annex II.

Physical GFCE Triple-I events

By devoting a full day together, it becomes possible to better grow a common understanding of the technical challenges, as well as other challenges related to implementation of those standards, even if the group of participants is very diverse. Good practice experience (from the region itself, or from elsewhere) will help inspire finding new ways forward.

Experience shows that it is important to have a clear event owner, supported by the GFCE Secretariat, that works with a "regional committee" of active people to ensure the region-specific priorities are reflected in the agenda, and that the message to join for the workshop can go out to different mailing lists as to ensure a good mix of participants from the different mailing groups.

Virtual GFCE Triple-I events

Experience with online events over the last year has learned that for virtual events, the attention span is less, and rather than a full day of interaction, it is better to organize more focused sessions to tackle specific problems. The big advantage is that there is no travel time or travel costs involved.

Like with physical events, it is deemed to be important to have a clear event owner that works with a "regional committee". The GFCE Secretariat can support the event with providing zoom facilities, and the usual support for organizing events such as publishing of the agenda, sending out invitations, and taking care of registrations.

In addition the GFCE will make existing knowledge and expertise that it has gained and developed through this project available and accessible on its platform, leveraging its network to update this information regularly and providing stakeholders with further tools for conducting activities and organizing their own events related to raising awareness and instigating take up of open Internet standards.

Participants

For the workshops, we are looking at a mix of local stakeholders that would like to improve the Internet experience in the specific region. We encourage people to join and bring their colleagues they work with, upstream of downstream the Internet value chain, to work on these issues together. Participation is typically free. In order to ensure stakeholders are learning to appreciate each other, workshops would typically limited to 30 – 50 participants.

For physical events, in order to make best use of travel costs, organizers are encouraged to connect to events where key participants would typically participate in, as well. Examples where multiple stakeholder groups typically meet include the regional IGFs, regional Schools for Internet Governance, and other regional events organized by regional or global internet groups such as the RIRs.

For virtual events, organizers are encouraged to make use of a number of relevant mailing lists as to establish a good mix across stakeholders.

Committed parties

Improving justified trust in the Internet through adoption and implementation of Open Standards has the interest of the global Technical Community who are willing to work with the Global Forum on Cyber Expertise partners to help organize local workshops towards capacity building. During the first series of seven events, the following parties contributed: AfriNIC, AfricaCERT, AFNOG, APRICOT, APNIC, ICANN, Internet Society and several of its local/regional chapters, Indian School for Internet Governance (INSIG), LACIGF, LACTLD, LACNIC, LACAAWG, nic.br/cgi.br, RIPE NCC, WACREN, the Indian Ministry of Electronics and IT (MeitY), and the Dutch Ministry of Economic Affairs and Climate.

GFCE is committed to support these events at its best ability – support level to be agreed per event via a clear email exchange between the local organizer and the GFCE Secretariat. For more information on the GFCE Internet Infrastructure Initiative: https://thegfce.org/initiatives/internet-infrastructure-initiative/

Annex I – Model agenda GFCE Triple-I workshop

Please find below the model invite for both the physical event (full day) and virtual event (half day).

Physical workshop draft agenda

<date>

Starting time: 09:00 registration for a 09:30 start <may vary per location.

09:30 Opening by Host

Welcome and intent of the day

10:00 Block I: Better Use of Today's Open Internet Standards:

Moderated discussion about the use and usefulness of Open Internet Standards such as DNSSEC, TLS, DANE, RPKI, ROA, DMARC, DKIM, SPF and IPv6 (with invited experts [to be named] in the room to inform participants).

12:00 lunch

13:00 Block II: Inspiration from Good Practice Actions

(We foresee a number of other good practices from the region, and beyond, to be presented during this "Block II", with a mix of international and regional speakers. This information will be updated as soon as we know.)

15:00 Block III: Planning for a More Trusted Internet: Marketplace for Action

(Facilitated brainstorming)

16:30 Conclusions and Closing Remarks

17:00 Ends

Virtual workshop draft agenda

<date>

<starting time>

00:00 Opening by Host

Welcome and intent of the day

00:10 Block I: Better Use of Today's Open Internet Standards:

Moderated discussion about the use and usefulness of Open Internet Standards such as DNSSEC, TLS, DANE, RPKI, ROA, DMARC, DKIM, SPF and IPv6 (with invited experts [to be named] in the room to inform participants).

01:30 Block II: Inspiration from Good Practice Actions

(We foresee a number of other good practices from the region, and beyond, to be presented during this "Block II", with a mix of international and regional speakers. This information will be updated as soon as we know.)

03:00 Block III: Planning for a More Trusted Internet: Marketplace for Action

(Facilitated brainstorming)

03:50 Conclusions and Closing Remarks

04:00 Ends

Annex II – Model "save the date"

Please find below the model invite for both the physical event (full day) and virtual event (half day).

Physical workshop

+++Save the date+++Save the date+++Save the date+++Save the date+++Save the date+++

Triple I Capacity Building Day | The Internet Infrastructure Security Day

Creating a more Trusted Internet experience, together

Following workshops in 2018 and 2019, GFCE Triple-I will be back with its capacity building workshop in [location event, possible association with other event]. On [date], GFCE Triple-I will work with [supporting organizations] to host The GFCE Triple-I Internet Infrastructure Security Day.

This will be a workshop in which participants from different stakeholder groups together:

- learn more about Open Internet Standards such as DNSSEC, TLS, DANE, RPKI, ROA, DMARC, DKIM, SPF, and IPv6, in support of more trusted communications;
- be inspired by Good Practice experience that helped improve reliability of the Internet and collaborative security. Good practice examples will be presented from the region, and from elsewhere that may be of interest in the region;
- with a collaborative foundation, work to develop and commit to specific actions that will help improve the region's Internet economy. For this we will work according the *Open Space* methodology which means that the participants set the agenda, together.

Participants are sought across regional Internet stakeholder groups, including government, business and technical community. Collaborative security is how we build trust in the Internet's infrastructure. You are called to join this workshop in order to improve the trusted Internet experience in the region. You may want to stimulate people you would need to work with as well to register for this workshop. Participation is upon confirmed registration, only, and limited in numbers.

This workshop is initiated by the Global Forum for Cyber Expertise (http://www.thegfce.com), and is supported by [to be filled in].

The workshop will stretch over 4 * 90 minute blocks during the day. A link for registration and a more detailed agenda and speakers' list will be presented closer towards the date. For more information about previous events, please see [GFCE website location].

Virtual workshop

+++Save the date+++Save the date+++Save the date+++Save the date+++Save the date+++

GFCE Triple I Capacity Building | The Internet Infrastructure Security virtual workshop

Creating a more Trusted Internet experience, together

Following workshops in 2018 and 2019, GFCE Triple-I will be back with a virtual capacity building workshop in [location event, possible association with other event]. On [date], GFCE Triple-I will work with [supporting organizations] to host The GFCE Triple-I Internet Infrastructure Security workshop.

This will be a virtual workshop in which participants from different stakeholder groups together:

- learn more about Open Internet Standards such as DNSSEC, TLS, DANE, RPKI, ROA, DMARC, DKIM, SPF, and IPv6, in support of more trusted communications;
- be inspired by Good Practice experience that helped improve reliability of the Internet and collaborative security. Good practice examples will be presented from the region, and from elsewhere that may be of interest in the region;
- with a collaborative foundation, work to develop and commit to specific actions that will help improve the region's Internet economy. For this we will work according the *Open Space* methodology which means that the participants set the agenda, together.

Participants are sought across regional Internet stakeholder groups, including government, business and technical community. Collaborative security is how we build trust in the Internet's infrastructure. You are called to join this workshop in order to improve the trusted Internet experience in the region. You may want to stimulate people you would need to work with as well to register for this workshop. Participation is upon confirmed registration, only, and limited in numbers.

This workshop is initiated by the Global Forum for Cyber Expertise (http://www.thegfce.org), and is supported by [to be filled in].

The workshop will stretch over 3 * 60 minute blocks during the [morning/afternoon]. A link for registration and a more detailed agenda and speakers' list will be presented closer towards the date. For more information about previous events, please see [GFCE website location].