CTI-TC
Interoperability Subcommittee

Meeting Date:  Wednesday, June 8, 2016, 2016
Time:  18:00 UTC - 02:00pm to 03:00pm EDT
Purpose:  Monthly Meeting

Proposed Agenda:

- Preamble: Register Attendance through OASIS Portal (Kavi)
- Nomination Nicole Gong CTI TC Interoperability SC Secretary
- Brief Updates:
  - RSA 2017 Interop WG
  - Conformance and Interoperability Test Framework– Patrick Maroney
  - CTI Supporters Registration and Data – Patrick Maroney
- Briefing on ETSI, NISD, TC CYBER – Tony Rutkowski
  - Tony Rutkowski is the designated rapporteur in ETSI TC CYBER for a work item technical report on cyber security information sharing specifications, as well as part of an ENISA Experts Group on the NISD implementation. The next meeting of TC CYBER is at ETSI’s Sophia Antipolis, France, headquarters, 15-17 June. Tony’s presentation will be the primary agenda item for this month’s Interoperability SC meeting.

Meeting Notes:

Moderator: Patrick Maroney
Co-Chair: David Eilken
Recorder: Nicole Gong

Nomination & Motions:

- Announcement that Jane Ginn has stepped up to serve as a Secretary of the CTI Technical Committee,
- The CTI TC Interoperability sub-committee greatly appreciates Jane’s dedication, hard work, positive attitude, and the contributions she continues to make in all aspects of the CTI TC efforts.
- Nomination for Nicole Gong as Secretary for the CTI TC Interoperability sub-committee
- Approved
- Brief Introduction of Nicole Gong

https://www.oasis-open.org/apps/org/workgroup/cti-interoperability/
RSA Demo working group update:

- **Basically two meetings occurred, a kick off meeting and then June 8th morning’s bi-weekly meeting**
  - **Issues:** the participation has been lacking, there should be 12 participants, but only 9 have seen responded. Out of those 9 people, today there are only 5 attended. One dropped out without participating.
  - **Comment:** please participant and be active. The reality is that if you don’t participant, the decisions will be made by the active members.
  - **Summary:** so that’s where we are right now, we have not decided the next meeting, but we just need active participation, so that is my pled to the group.

- **Documentation Review:** there is a working document to share. We are working through this document that describes the user scenarios, the products support in those demonstration show case. So again, if you are a vendor, plan to participating in these show case, please participant, because if you don’t, then your product specifics, opinions or scenarios may not be described.

- **Discussions on participation:** DHS participants requested a copy, and invitations for the other meeting. vendors who pay the money and other participants. How and who should be included?
  - **Discussion on type of participation:**
    - **Type 1:** Vendors who signed up for show case
    - **Type 2:** The other ones don’t do show case but are interested to participating in helping develop use scenarios and testing.
  - **Who should participant?** The vendors who’ve committed funds and resources to showcase their products and interoperability wish to limit participation in the RSA 2017 WG. They welcome people to observe. Once they’ve defined their use cases, scenarios, and data sets they will consider sharing outside of the core group.

**Interoperability Showcase and Plug-fest Working Group**

- **Should we start an inclusive Interoperability Showcase and Plug-fest working group?**
  - Co-chair Patrick Maroney opened the question of starting a working group to focus on the development and execution of both OASIS member Interoperability Showcases and Plug-fests that are open publicly to any in the open community wishing to participate.
  - While the RSA 2017 showcase is exclusive to paid participants there are also Interoperability Showcases and Plug-fests. Anyone in the TC, can join those type demo, to show their implementation of the interoperability.
  - So the key away of this suggestion is that we need another WG to develop the use case scenarios that we can all use and share across the TC. Make this as a shared effort.

Co-Chair David Eilken suggested we start with baby steps for the testing process: Get some criteria, categories of implementation out there on the supporter’s page. Keep it up-to-date.
Whatever the criteria may be, we can talk about it. We can provide outputs and deliverables for the demos and show cases and post them back to the member’s supporter’s pages, so we know specifically who is doing what.

Although the proposed **Interoperability Showcase and Plug-fest working group** have merit, it may be better to start later, for easy activity sync. Focus should be on developing use cases, scenarios, and testing frameworks for now. When those are defined, the **Interoperability Showcase and Plug-fest working group** can split off then. The overall focus of the Interoperability SC should be on developing the interoperability criteria for the broader TC. The **RSA 2017 Interoperability Demonstration, Interoperability Showcases and Plug-fests** should be a secondary goal and activities.

Discussion on this topic was tabled in order to cover the other agenda items for the meeting.

**Re-statement of the OASIS CTI TC Interoperability Subcommittee Charter:**

The Interoperability SC will help guide adherence to CTI TC-promulgated standards and interoperability between CTI TC standards-based implementations, while encouraging standards maturity throughout the industry.

The SC will develop parameters and processes to allow CTI TC members to test/ validate, and where possible measure the maturity of another organization’s implementation. Testing parameters and processes should be straight-forward and objective to provide clear confirmation that minimum standards' requirements have been achieved. Initially, in regard to maturity measurement efforts, the SC will develop guidelines to support a more qualitative review of an implementation.

In addition, the SC will identify opportunities and approaches to promoting interoperability with externally-defined cyber threat intelligence standards and frameworks.

**Deliverables**

Documents addressing guidelines, parameters and processes for testing, validating and measuring implementations' adherence to CTI standards

Proposals for promoting interoperability with other, externally-defined cyber threat intelligence standards and frameworks”
Conformance and Interoperability Test Framework Update:

- The sub-committee evaluated other OASIS TC Interoperability frameworks.
- Research validates assumptions that a non-trivial amount of effort is required. For example, the KMIP TC Interoperability SC have invested 1,000s of hours over many years to reach current level of capability maturity.
- After researching various options, we engaged with the University of New Hampshire Interoperability Labs Interoperability Labs (UNH-IOL) to discuss partnership and published a draft proposal for this option.
- OASIS advised that the OASIS TAB published a white paper on Self-Certification. This will be posted and share with everyone for review by the Interoperability SC.
- Key take away is that we are evaluating various frameworks and processes to see how we can best establish an Interoperability Testing Framework for the OASIS CTI TC.

CTI Supporters Registration and Data

- The legacy and new registration data have been reconciled.
- A process is established to take the CTI Supporters Registration data and publish it on the OASIS CTI TC Interoperability SC Wiki Pages.
- This data is now online and available for review and comment
- Any Questions on CTI registration data?

Tony’s Briefing on ETSI, NISD, TC CYBER Initiatives – Tony Rutkowski

The work of OASIS TCI occurs against a backdrop of cyber security legislative activity in the U.S. and Europe that frequently shapes similar actions worldwide. Basically this part reiterates the abstract. Tony did deconstruction of the U.S. Cybersecurity ACT for the January meeting. Most countries worldwide now have national cybersecurity strategies. On 18 December 2015, the U.S. passed the Cybersecurity Act of 2015 which was immediately signed into law. The same date, the European Parliament reached legislative agreement on a Security of Networks and Information Systems Directive (NISD).
Work product is always the construct of the CTI. Related to that European commission is EISI is the equivalent of U.S. Cert. Recommending OASIS CTI work closely to align with the constructs and requirements of the two instruments, or else capable of being adapted. Toward that end, an integrated presentation will be given at the upcoming Interoperability Subcommittee that treats the structure, models, derived interfaces, information structures contained in their provisions. Also identified are steps the seam necessary to harmonize the differences between the respective instruments, tasks left unanswered, and the how the OASIS TCI and its platforms can facilitate these ends.

Included in the presentation is treatment of actions that can be takes by OASIS and ETSI together toward the above ends. A cooperative agreement exists not only between the two organizations, but also explicitly concerning their CTI and CYBER Technical Committees. ETSI has a special standards status under European law - which may allow ETSI to designate CTI specifications as normative for EU purposes.

Open the Floor to Discussion
   No further issues brought up

Meeting Terminated