Re: Indian Delegation for JTC 1/SC 27 meeting March April 2024

From : gautham sekar <gautham.sekar@gmail.com> Wed, Apr 17, 2024 01:32 PM
Subject : Re: Indian Delegation for JTC 1/SC 27 meeting March April 2024
To : BIS Information Systems Security and Privacy Sectional Committee <litd17@bis.gov.in>
Cc : ska262001@yahoo.co.in, gargi@keenis.com, Jyoti Kushwaha <jkushwaha@bis.gov.in>, srinivasp@infosys.com, Sancindian@gmail.com, vkanhere@gmail.com, ns@lntenc.com, rakesht@cdac.in, abhik2 c <abhik2.c@tcs.com>, Govindarajulu Yuvaraj <Govindarajulu.Yuvaraj@in.bosch.com>, drshalinibhartiya@gmail.com, N Sathyan <N.Sathyan@larsentoubro.com>, Arvind Kumar <cca@cca.gov.in>, Arvind Kumar <akumar@meity.gov.in>

Dear Kshitij ji,

Here is my report:

I attended the WG2 and WG3 meetings virtually during 8-12 April, 2024. Initially, I attended WG2 meetings alone due to overlapping sessions with WG3. WG2 commenced with a discussion of the items in the agenda. The status of the documents, editorships and the results of voting were presented by Hirotaka Yoshida (JP). Of particular interest were ISO/IEC 18031, 29192, 18033, 11770 and 14888-4. The comments from 3 MBs (JP, DE and GB) on ISO/IEC 18031 were discussed. India's consolidated comments on ISO/IEC 29192-4 were discussed. I urged the experts to explore the possibility of a revision / amendment to include lightweight algorithms that can provide more than 80-bit security, while informing them that India was yet to discuss alternative algorithms that could be included. Tanja Lange (NL) supported India's comment on the need for a higher security level. Chris Mitchell (GB) requested India to suggest alternative lightweight algorithms providing more than 80-bit security. Akira Nagai (JP) suggested inclusion of NTRU with 128-bit or a higher level of security, which I provisionally accepted. Japan also wanted to include NTRU in ISO/IEC 18033-2 and presented the advantages of NTRU over Kyber. The other comments from India, except the one on ISO/IEC 29192-2 versus 18033-3, were agreed upon. Finally, WG2 recommended initiating a PWI to analyse the suitability of the inclusion of new lightweight asymmetric cryptographic techniques in the ISO/IEC JTC1/SC27 WG2 standards. The call for contributions shall
include questions to confirm with WG2 experts the new mechanisms and security levels to be included in ISO/IEC 29192-4. Yu Sasaki (JP) was proposed as the Editor and Koutarou Suzuki (JP) , Akira Nagai (JP) and myself were proposed as the Co-Editors. A detailed call for contribution is to be prepared by the proposed editors and circulated by the WG2 Secretariat. There were offline discussions with the Japanese delegation and I was unable to follow up on ISO/IEC 5891.2 (WG3), but participated in a session on ISO/IEC 15408.

Regards,
Gautham

On Sat, 13 Apr 2024 at 00:24, litd17 <litd17@bis.gov.in> wrote:

> Dear Sir/Madam,

In continuation to trailing mails, Indian Delegates are requested to provide their report of participation at the earliest. Please specifically inform the item which would be decided by JTC 1/SC 27 during 16th -18th April 2024.
Dr. Gargi Keeni would be attending plenary meeting in person at Berlin and she is HoD for the plenary meeting. Agenda of the SC 27 plenary meeting is enclosed for your reference.

Thanks & Regards
Kshitij Bathla
Scientist-C/Deputy Director
Electronics & IT Department
Bureau of Indian Standards
Manak Bhavan
9 Bahadur Shah Zafar Marg
New Delhi - 110002, INDIA
Tel:91-11-23230131/Extension 8450
91-11-23608450

From: "BIS Information Systems Security and Privacy Sectional Committee" <litd17@bis.gov.in>
To: "Sumitra Biswal" <Sumitra.Biswal@in.bosch.com>, "govindarajulu yuvaraj" <govindarajulu.yuvaraj@in.bosch.com>, balaji@cdac.in, rakesht@cdac.in, "Dr. RAHUL RASTOGI" <rahul.rastogi@eil.co.in>, "JASPREET SINGH BINDRA" <jaspreet.bindra@eil.co.in>, "VEDANT RAI" <vedant.rai@eil.co.in>, info@Excaliburancy.com, anilpr@ee.iitm.ac.in, srinivasp@infosys.com, "sarmistha neogy" <sarmistha.neogy@jadavpuruniversity.in>, vkanhere@gmail.com, "n sathyan" <n.sathyan@larsentoubro.com>, "gautham sekar" <gautham.sekar@gmail.com>, "Sushil KumarNehra" <snehra@meity.gov.in>, "Arvind Kumar" <cca@cca.gov.in>, "Somnath Chandra" <schandra@meity.gov.in>, kishor@narnix.com, null@null.co.in, neelu@null.co.in, valli@panaceamedical.com, "dhivya t" <dhivya.t@panaceamedical.com>, "deepareddy g" <deepareddy.g@panaceamedical.com>, "chetan anand" <chetan.anand@profinch.com>, "shree hegde" <shree.hegde@securemachines.in>, "Arvind KumarUpadhyaya" <akupadhyay@stqc.gov.in>, "VISHAL KUMAR JAISWAL" <vishal.jaiswal@stqc.gov.in>, "Suresh Chandra" <suresh@stqc.gov.in>, "abhik2 c" <abhik2.c@tcs.com>, pprabs06@yahoo.co.in, "jkm cse" <jkm.cse@gmail.com>, drshalinibhartiya@gmail.com, sancindian@gmail.com, gargi@keenis.com, agnidipta@gmail.com, "rajendra kathal" <rajendra.kathal@gmail.com>, parthachakravarty1@gmail.com, aswathytasok@gmail.com, mtq0306@yahoo.com, gg@infosec.clinic, "abhik chaudhuri" <abhik.chaudhuri@gmail.com>, jkmandal@klyuniv.ac.in, regulatory@panaceamedical.com, void@null.co.in, "Arvind Kumar" <akumar@meity.gov.in>, ns@lntenc.com, madrasfintech@gmail.com
Sent: Tuesday, March 26, 2024 10:39:44 AM
Subject: Re: Meeting of LITD 17 WG 1, WG 2, WG 3 , WG 4 and WG 5 20th March (10:30 AM to 12:30 PM)

Dear Sir/Madam,

In continuation to trailing mails, Minutes, duly approved by the Chairperson LITD 17, for the meeting held on 20th March (10:30 AM to 12:30 PM) are enclosed.

Last date of comments: 10 April 2024

Comments, if any, confined to the accuracy of recording, may please be sent to the undersigned at the earliest. If no reply is received by the above-mentioned date, we will presume your concurrence with the minutes as recorded.