# SUMMARY REPORT
# ON
# SC27 JAIPUR

## 26 - 30 October 2015

## Marriott, Jaipur, INDIA


**Prepared by:**

**Dr. Suresh Ramasamy**
**Azleyna Ariffin**
**INS WG Chairman & Secretary**

**On Behalf**
**MALAYSIAN TECHNICAL STANDARDS FORUM BHD**

# TABLE OF CONTENTS

**Page**

## 1. Abstract

This report outlines the attendance of selected participants from MTSFB and the Information/Network Security Working Group.

## 2. List of Participants

With the assistance from MTSFB and SKMM, these are the participants participating in this event.

i. Dr. Suresh Ramasamy (INS Chairman)
**ii.** Azleyna Ariffin (INS Secretary)

## 3. Introduction /Background

The SC27 meeting that is held in Jaipur, India is to hold the ISO/IEC JTC/SC27 Working Group, Study Group and Plenary Meetings. The SC27 is responsible for managing and maintaining the standards responsible for Information Security Management System.

The Information/Network Security Working Group is a working group under the Malaysian Technical Standards Forum, which is tasked to produce the technical papers regarding Information/Network Security, using the ISO/IEC 27000 series standards.

## 4. Agendas/Topics

### i. WG participation

Participation on WG gives clear understanding into the current documents being discussed. The document discussion involved in includes the change proposal for ISO 27011 – guidelines for telecommunications industry and ISO 27021 – a new ISO standard for competence. This also includes emergence of ISO 31000, which is to standardize the risk management approach and request to align existing 27000 series to that document. Participation on WG2 reveals the details and changes on the ISO 29192 for addition of new ciphers as well as submission of new hash algorithms for ISO 14888 and ISO 10118.

This meeting will be a follow up from the earlier participation of ISO/IEC JTC1 SC27 from Kuching, Sarawak. This includes deliberation on WG2 on draft proposals for cipher/hash algorithms, including proposal from different countries to include their respective national level algorithms into the standards.

## 5. Findings

Based on the participation on the SC27 meetings, the delegates were exposed and become aware of the following processes and way of work –

i. Understanding of standards process
ii. Involvement of National Bodies and Organizations in Standards
iii. Evolution of standards and WG over time
**iv.** Latest happenings in the standards world and drafts being proposed

This also includes implementation of the standard, which is coming into enforcement (ISO 27001:2013).

**5.0.1 Modes of operation for an n-bit block cipher algorithm (10116)** *To be discussed by BCM*

Project JTC 1.27.02 (revision of 10116: 2006 (3rd Edition)) Editor: Mr. Michael Ward, Co-Editor: Mr. Atsushi Waseda
DIS 10116

**5.0.2 Entity authentication (9798)**

**5.0.2.1 Part 1: General**

Project JTC 1.27.03.01 ISO/IEC 9798-1: 2010-07-01 (3rd Edition)

**5.0.2.2 Part 2: Mechanisms using symmetric encipherment algorithms**

[WG2 N1002 (n.a.)] 1st WD [SC27 N13962] recommendation, [SC27 N14336] endorsement of revision

Project JTC 1.27.03.02 (revision of 9798-2:2008 (3rd Edition)+9798-2:2008/COR3:2013-02-15) Editor: Mr. Jens Hermans WD 9798-2:

**5.0.2.3 Part 3: Mechanisms using digital signature techniques** [WG2 N1082] 2nd WD

[WG2 N1083] DoC on 1st WD

Project JTC 1.27.03.03 (revision of 9798-3:1998 (2nd Edition) +9798-3:1998/COR1:2009-09-15+9798-3:1998/AMD1:2010-06-01 +9798-3:1998/COR2:2012-03-15+9798-3:2008/COR3:2013-02-15)
Editor: Mr. Jens Hermans, Co-Editor: Mr. Zhiqiang Du WD 9798-3: Review of comments on WD

**5.0.2.4 Part 4: Mechanisms using cryptographic check function**

Project JTC 1.27.03.04 ISO/IEC 9798-4: 1999 (2nd Edition) 9798-4: 1999/COR1: 2009-09-15 9798-4: 1999/COR2: 2012-07-15

**5.0.2.5 Part 5: Mechanisms using zero knowledge techniques**

Project JTC 1.27.03.05 ISO/IEC 9798-5: 2009 (3rd Edition): confirmed in 2015

**5.0.2.6 Part 6: Mechanisms using manual data transfer**

Project JTC 1.27.03.06 ISO/IEC 9798-6: 2010-12-01 (2nd Edition)

**5.0.3. Message authentication codes (MACs) (9797)**

**5.0.3.1 Part 1: Mechanisms using a block cipher**

Project JTC 1.27.04.01 ISO/IEC 9797-1: 2011-03-01 (2nd Edition)

**5.0.3.2 Part 2: Mechanisms using a dedicated hash-function**

[SC27 N13965] confirmation ISO/IEC 9797-2: 2011-05-01 (2nd Edition), 2011-06-15 (Corrected 2nd Ed.)
Project JTC 1.27.04.02

**5.0.3.3 Part 3: Mechanisms using a universal hash-function**

Project JTC 1.27.04.03 ISO/IEC 9797-3: 2011-11-15 (1st Edition)

**5.0.4. Non-repudiation (13888) 11.1 Part 1: General Project JTC**

**1.27.06.01 ISO/IEC 13888-1: 2009 (3rd Edition): confirmed in 2015**
**11.1.1 Corrigendum 1 to Part 1 Editor: Mr. Christoph Ruland 13888-1/DCOR1 11.2 Part 2: Mechanisms using symmetric techniques**

**Project JTC 1.27.06.02 ISO/IEC 13888-2: 2010-12-15 (2nd Edition) 13888-2: 2010/COR1: 2012-12-15 11.3 Part 3: Mechanisms using asymmetric techniques Project JTC 1.27.06.03 ISO/IEC 13888-3: 2009 (2nd Edition): confirmed in 2015**

**5.0.5 Digital signature schemes giving message recovery (9796) 12.1 Part 2: Integer factorization based mechanisms Project JTC**

**1.27.07.02 ISO/IEC 9796-2: 2010-12-15 (3rd Edition) 12.2 Part 3: Discrete logarithm based mechanisms [SC27 N13967] confirmation ISO/IEC 9796-3:2006 (2nd Edition), 2013-09-15(Corrected 2nd Ed.)**

Project JTC 1.27.07.03

**5.0.6. Digital signatures with appendix (14888)**

**5.0.6.1 Part 1: General**

Project JTC 1.27.08.01 ISO/IEC 14888-1:2008 (2nd Edition)

**5.0.6.2 Part 2: Integer factorization based mechanisms**

Project JTC 1.27.08.02 ISO/IEC 14888-2:2008 (2nd Edition)

**5.0.6.2.1 Corrigendum 1 to Part 2**

Editor: Mr. Koutarou Suzuki 14888-2/COR1: 2015-10-01 (notice: SC27 N15534)

**5.0.6.3 Part 3: Discrete logarithm based mechanisms**

Project JTC 1.27.08.03 (revision of 14888-3:2006 (2nd Edition) + 14888-3/Amd1:2010-06-15 + 14888-3/Amd2: 2012-07-01 + 14888-3/Cor1: 2007 + 14888-3/Cor2:2009)
Editors: Ms. Liqun Chen, Mr. Pil Joong Lee DIS 14888-3

**5.0.7. Hash-functions (10118)**

**5.0.7.1 Part 1: General** *To be discussed by BCM* [WG2 N1114, 1117] Preliminary revised text, SoC

Project JTC 1.27.09.01 (revision of 10118-1:2000 (2nd Edition)) Editor: Mr. Vasily Shishkin, Co-Editor: Mr. Alexey Urivskiy CD 10118-1

**5.0.7.2 Part 2: Hash-functions using an n-bit block cipher**

Project JTC 1.27.09.02 ISO/IEC 10118-2: 2010-10-15 (3rd Edition) 10118-2: 2010/COR1: 2011-12-01

**5.0.7.3 Part 3: Dedicated hash-functions**

Project JTC 1.27.09.03 (revision of 10118-3:2004 (3rd Edition) +10118-3:2004/AMD1:2006-02-15+10118-3:2004/COR1:2011-12-01)
Editor: Mr. Vasily Shishkin, Co-editor: Ms. Lily Chen, Mr. Ivan Lavrikov
WD10118-3: Review of comments on WD

**5.0.7.4 Part 4: Hash-functions using modular arithmetic**

Project JTC 1.27.09.04 ISO/IEC 10118-4:1998 (1st Edition) 10118-4: 1998/COR1: 2014-07-15 10118-4: 1988/AMD1: 2014-11-15

**5.0.8. Key management (11770)**

**5.0.8.1 Part 1: Framework**

Project JTC 1.27.18.01 ISO/IEC 11770-1: 2010-12-01 (2nd Edition)

**5.0.8.2 Part 2: Mechanisms using symmetric techniques**

Project JTC 1.27.18.02 ISO/IEC 11770-2: 2008 (2nd Edition) 11770-2:2008/COR1: 2009-09-15

**5.0.8.2.1 Corrigendum 2 to Part 2**

Editor: Mr. Chris Mitchell 11770-2/DCOR2

**5.0.8.3 Part 3: Mechanisms using asymmetric techniques**

Project JTC 1.27.18.03 (revision of 11770-3: 2008 (2nd Edition)) Editor: Ms. Atsuko Miyaji, Co-editor: Ms. Thyla van der Merwe ISO/IEC 11770-3: 2015-08-01 (notice: SC27 N15462)

**5.0.8.3.1 Corrigendum 1 to Part 3**

Editor: Ms. Atsuko Miyaji 11770-3/DCOR1 (n.a.)
[WG2 N1139] SoC [WG2 N1153] draft DoC
[SC27 N13968] confirmation
-4-
[WG2 N1119] defect report

[WG2 N1084] 3rd WD [WG2 N1085] DoC on 2nd WD
[SC27 N13268] confirmation
[WG2 N1118] Editor's report

**5.0.8.4 Part 4: Mechanisms based on weak secrets** [WG2 N1086] 2nd WD

[WG2 N1087] DoC on 1st WD

Project JTC 1.27.18.04 (revision of 11770-4: 2006 (1st Edition) + 11770-4:2006/COR1: 2009-09-15)
Editor: Mr. Feng Hao, Co-editor: Mr. SeongHan Shin WD11770-4: Review of comments on WD

**5.0.8.5 Part 5: Group key management**

Project JTC 1.27.18.05 ISO/IEC 11770-5: 2011-12-15 (1st Edition)

**5.0.8.6 Part 6: Key derivation**

Project JTC 1.27.18.06 Editor: Mr. Rich Davis DIS 11770-6

**11. Check character systems (7064) Project JTC 1.27.23 ISO/IEC 7064: 2003 (1st Edition): stabilised in 2009**

**12. Cryptographic techniques based on elliptic curves (15946) 17.1 Part 1: General**

Project JTC1.27.26.01 (revision of 15946-1:2008 (2nd Edition)+15946-1:2008/COR2: 2014-04-01) Editor: Ms. Atsuko Miyaji DIS 15946-1

**5.0.9.2 Part 5: Elliptic curve generation** [WG2 N1088] 1st WD [SC27 N15200] revision Project JTC1.27.26.05 [SC27 N15478] limit date

(revision of 15946-5: 2009 (1st Edition) + 15946-5: 2009/COR1: 2012-12-01)
Editor: Ms. Atsuko Miyaji WD15946-5: Review of comments on WD

**5.0.10. Time-stamping services (18014) 18.1 Part 1: Framework**

Project JTC1.27.27.01 ISO/IEC 18014-1: 2008 (2nd Edition)

**5.0.10.2 Part 2: Mechanisms producing independent tokens**

Project JTC1.27.27.02 ISO/IEC 18014-2: 2009 (2nd Edition): confirmed in 2015

**5.0.10.2.1 Corrigendum 1 to Part 2**

Editor: Mr. Christoph Ruland 18014-2/DCOR1
-5-
[WG2 N1125, 1143] SoC, late comm [WG 2 N1145] draft DoC
[SC27 N13970] confirmation
[WG2 N1126] SoC [WG2 N1152, 1151] draft DoC, draft revised text
[SC27 N14752] confirmation [SC27 N15210] confirmation

**5.0.10.3 Part 3: Mechanisms producing linked tokens**

Project JTC1.27.27.03 ISO/IEC 18014-3: 2009 (2nd Edition): confirmed in 2015

**5.0.10.4 Part 4: Traceability of time sources**

Project JTC1.27.27.04 Editor: Mr. Masakazu Uehata ISO/IEC 18014-4: 2015-04-15

(notice: SC27 N15174)

**19. Random bit generation (18031) Project 1.27.31 ISO/IEC 18031: 2011-11-15 (2nd Edition) 18031: 2011/COR1: 2014-10-01 19.1 Amendment 1 Project1.27.31.01 (Amendment 1 to ISO/IEC 18031: 2011) Editor: Mr. Pascal Paillier 18031/DAM1**

**20. Prime number generation (18032) Project 1.27.32 (revision of 18032:2005 (1st Edition)) Editor: CD 18032 (n.a.)**

**21. Encryption algorithms (18033) 21.1 Part 1: General**

[SC27 N15211] confirmation

Project1.27.33.01 Editor: Mr. Riaal Domingues, Co-editor: Ms. Atsuko Miyaji ISO/IEC 18033-1: 2015-08-01 (2nd Edition) (notice: SC27 N15426)

**5.0.11.2 Part 2: Asymmetric ciphers**

Project 1.27.33.02 ISO/IEC 18033-2: 2006 (1st Edition)

**5.0.11.3 Part 3: Block ciphers**

Project 1.27.33.03 ISO/IEC 18033-3: 2010-12-15 (2nd Edition)

**5.0.11.4 Part 4: Stream ciphers**

Project1.27.33.04 ISO/IEC 18033-4: 2011-12-15 (2nd Edition)

**5.0.11.5 Part 5: Identity-based ciphers**

Project1.27.33.05 Editor: Mr. Kai Sui Liu, Co-editor: Mr. Toshihiko Matsuo ISO/IEC 18033-5: Editorial final corrections

[SC27 N13972] confirmation

[SC27 N13973] confirmation



[SC27 N13423] press release [SC27 N13971] confirmation

*To be discussed by BCM*

*To be discussed by BCM*

[WG2 N1109] Call for Editor

**5.0.11.6 Part 6: Homomorphic encryption**

Project1.27.33.06 Editor: Mr. Pascal Paillier, Co-editor: Ms. Atsuko Miyaji WD 18033-6: Review of comments on WD

**5.0.12. Authenticated encryption (19772) Project 1.27.38 ISO/IEC 19772: 2009 (1st Edition) 19772: 2009/COR1: 2014-09-01**

**5.0.13 Signcryption (29150) Project 1.27.67 ISO/IEC 29150: 2011-12-15 (1st Edition) 29150: 2011/COR1: 2014-03-15**

**5.0.14 Lightweight cryptography (29192) 24.1 Part 1: General Project 1.27.82.01 ISO/IEC 29192-1: 2012-06-01 (1st Edition): confirmed in 2015 24.2 Part 2: Block ciphers Project 1.27.82.02 ISO/IEC 29192-2: 2012-01-15 (1st Edition): confirmed in 2015 24.3 Part 3: Stream ciphers Project 1.27.82.03 ISO/IEC 29192-3: 2012-10-01 (1st Edition): confirmed in 2015 24.4 Part 4: Mechanisms using asymmetric techniques Project 1.27.82.04 ISO/IEC 29192-4: 2013-06-01 (1st Edition) 24.4.1 Amendment 1 to Part 4 Project1.27.82.04.01 Editor: Mr. Erwin Hess Final text for publication 24.5 Part 5: Hash-functions Project 1.27.82.05 Editors: Mr. Axel Poschmann, Ms. Shiho Moriai DIS 29192-5**

**6 Anonymous entity authentication (20009) 25.1 Part 1: General Project 1.27.83.01 ISO/IEC 20009-1: 2013-08-01 (1st Edition)**

[WG2 N1025] 1at WD

[WG2 N1124] SoC [SC27 N14753] confirmation
[SC27 N13974] confirmation
[SC27 N15212] confirmation
[SC27 N15213] confirmation
[SC27 N15214] confirmation

**5.0.15.2 Part 2: Mechanisms based on signatures using a group public key**

Project 1.27.83.02 ISO/IEC 20009-2: 2013-12-01 (1st Edition)

**5.0.15.3 Part 3: Mechanisms based on blind signatures**

Project 1.27.83.03 Editor: WD 20009-3: Review of comments contributions on WD

**5.0.15.4 Part 4: Mechanisms based on weak secrets**

Project 1.27.83.04 Editor: Mr. Yanjiang Yang, Co-editor: Mr. Kazukuni Kobara CD 20009-4

**5.0.16 Anonymous digital signatures (20008) 26.1 Part 1: General Project 1.27.84.01 ISO/IEC 20008-1: 2013-12-15 (1st Edition) 26.2 Part 2: Mechanisms using a group public key Project 1.27.84.02 ISO/IEC 20008-2: 2013-11-15 (1st Edition)**

**5.0.17 Blind digital signatures (18370) 27.1 Part 1: General Project 1.27.100.01 Editor: Mr. Jacques Traoré, Co-editor: Mr. David Turner DIS 18370-1 27.2 Part 2: Discrete logarithm based mechanisms Project 1.27.100.02 Editor: Mr. Jacques Traoré, Co-editor: Mr. David Turner DIS 18370-2:**

**5.0.18 Secret sharing (19592) 28.1 Part 1: General Project 1.27.110.01 Editors: Mr. Dan Bogdanov, Mr. Shin'ichiro Matsuo CD19592-1 28.2 Part 2: Fundamental mechanisms Project 1.27.110.02 Editors: Mr. Koutarou Suzuki, Mr. Dan Bogdanov CD 19592-2**

[WG2 N1010 (n.a.)] 2nd WD [WG 2 N1110] call for editor *To be discussed by BCM*

## 5.1 WG2 Participation

Dr. Suresh Ramasamy was nominated to be the co-editor for the **Study Period paper on Lightweight MAC together with Mr Hirotaka Yoshida [WG2 N1099]**. The nomination is pending approval by DSM Malaysia, as it requires travel expense commitment from MTSFB.

## 5.2 WG1 Participation

Azleyna has attended most of the WG1 sub-meetings especially the sub-meeting in which inputs that have been put forward by DSM Malaysia – for the ISO/IEC 27005, ISO/IEC 27007 and ISO/IEC 27008.

General message that have been conveyed by the Convenor during the Plenary meetings are as follows:

1. As of the date, there are still 20 Working Draft (WD) Text and 30 project which at the level of Committee Draft (CD) Text under the responsibilities of ISO/IEC JTC 1/SC 27 Information Technology Security Techniques.

2. Few documents are not going to be discussed during Jaipur's meeting due to the followings:
    a. ISO/IEC 27012 is already in the Final Draft International Standard (FDIS)
    b. ISO/IEC 27006 published in September 2015
    c. ISO/IEC 27017 and ISO/IEC 27023 are in the final process for the publishing.
    d. Three (3) projects have also been delayed, in which may requires attention from the WG
        i. ISO/IEC 27003 – 3 months
        ii. ISO/IEC 27004 – 6 months
        iii. ISO/IEC 27005 – 12 months

3. The Convenor has also stressed and reminds the WG regarding the standard for the development of ISO documents that need to be adhere to by WGs. This is to avoid any delays in completing the documents since approval and registered. Head of Malaysia Delegation – En Thaib has suggested for the document to be registered as one ISO Standard – that can be use as one of the reference for ISO Standard development. Malaysia's experts agreed to be the Editor. The Convenor accepted the suggestion and motion will be further discussed.

4. All nominated Information Technology Security Techniques experts are now to ensure their registration with the Global Directory – to attend the meetings. This is to avoid dissemination of the confidential documents.

5. The followings table depicted updates related to WG1 – which discussed and agreed upon during the meeting in Jaipur.

| **Bil** | **Item** | **Updates** |
|---|---|---|
| 1 | Review of ISO/IEC 27005 Comments | Documents approved as 4th WD ISO/IEC 27005 which will be further discussed in the next meeting in Florida. |
| 2 | ISO/IEC 27005 Document for CD | Discussed and pending SC27 approval |
| 3 | Documents for Study and Comment | The followings documents have been approved to be circulate to experts for study and comments:<br>• 2nd WD ISO/IEC 27007 Guidelines for Information security management systems auditing |

| | | |
|---|---|---|
| | | • 2nd WD ISO/IEC 27008 – Guidelines for auditors on information security controls<br>• 1st WD ISO/IEC 27019 – Information security mgmt. guidelines based on ISO/IEC 27002<br>• 2nd WD ISO/IEC 27021 – Competence requirements for information security mgmt. systems professionals<br>• 4th WD ISO/IEC 27005 – Information security risk management |
| 4 | Project Title Changed | Change of title for Guidelines for the assessment of information security controls approved by the WG1 Convenor. |
| 5 | Change of Scope | Change of scope approved for the Guidelines for the assessment of information security controls. |

## 6. Conclusion

The ISO/IEC JTC1 SC27 meeting that was held in Jaipur, India was a testament to Malaysia's commitment to global standards. SKMM's role was pivotal, together with Standards Malaysia & SIRIM helped to create conducive environment for development and propagation of standards. Participation of the INS Working Group and MTSFB representative not only shows Malaysia's alignment and commitment to global standards, but also presents avenue for learning, understanding and peer networking which gives long term benefits for the drafting of industry technical code under MTSFB. It is highly recommended that INS Working Group continues to be part of SC27 to keep abreast with the developments of the standards, as well as supplement the WG ability to contribute locally and globally to place Malaysia at the forefront of nations.

## 7. Acknowledgement

The participants would like to thank MCMC & MTSFB for organising and funding the participants to attend and carry forward the knowledge. The participants also thank SIRIM/DSM for providing assistance and support throughout the engagement.


## THE MALAYSIAN TECHNICAL STANDARDS FORUM BHD

4805-2-2, Block 4805,
Persiaran Flora, CBD Perdana 2,
Cyber 12,
63000 Cyberjaya
Selangor Darul Ehsan
Malaysia
Tel: (+603) 8322 1441
Fax: (+603) 8322 0115
Website: www.mtsfb.org.my