SUMMARY REPORT
ON
ISO/IEC JTC1 SC27
Meeting

9 April 2016
Tampa, FL, USA

Prepared by:

Dr. Suresh Ramasamy,
Chairman of INS WG

On Behalf
MALAYSIAN TECHNICAL STANDARDS FORUM BHD

TABLE OF CONTENTS

Page

1. Abstract 1
2. List of Participants 1
3. Introduction /Background 1
4. Agendas/Topics 1
5. Findings 13
6. Conclusion 13
7. Acknowledgement 13

1. Abstract

The Information & Network Security Working group has been participating on the ISO/IEC JTC1 SC27 Working group meetings, contributing towards the development of the ISO 27000 family of standards on Information Security.

2. List of Participants

The participation for this event from MTSFB are as follows:

i. Dr. Suresh Ramasamy (INS WG Chairman)

3. Introduction /Background

ISO/IEC JTC1 SC27 is the International Standards Organization which is responsible in setting global standards, and SC27 specifically is responsible in the development of standards pertaining to Information Security family of standards, namely the ISO 27000 family. These standards have been adopted worldwide and is currently used as organizational benchmark towards Information Security readiness through audit and certification process.

INS WG, since its inception has been participating actively in ISO/IEC JTC1 SC27 meeting for the first time in Kuching, Sarawak. Through the leadership of the WG and support from MCMC, Dr. Suresh Ramasamy is actively involved in the SC27 working group. This results in Dr. Suresh Ramasamy nominated at the Co-Chair for the WG2 ISO 29192 Part 6 – Lightweight Algorithms – Message Authentication Code.

4. Agendas/Topics

The following were the discussions of SC27 WG2.

i. 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

ii. Entity authentication (9798)

Part 1: General *To be discussed by BCM (Systematic review)*

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

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:

Part 3: Mechanisms using digital signature techniques

[WG2 N1160] 3rd WD
[WG2 N1161] DoC on 2nd 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
[WG2 N1202] SoC
[WG2 N1233] draft DoC

Part 4: Mechanisms using cryptographic check function
To be discussed by BCM (Systematic review)

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

Part 5: Mechanisms using zero knowledge techniques
[SC27 N15207] confirmation

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

Part 6: Mechanisms using manual data transfer
To be discussed by BCM (Systematic review)

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

iii. Message authentication codes (MACs) (9797)

Part 1: Mechanisms using a block cipher

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

Part 2: Mechanisms using a dedicated hash-function
[SC27 N13965] confirmation

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

Part 3: Mechanisms using a universal hash-function
[SC27 N13966] confirmation

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

iv. Non-repudiation (13888)

Part 1: General

Project JTC 1.27.06.01 [SC27 N15208] confirmation
ISO/IEC 13888-1: 2009 (3rd Edition): confirmed in 2015

Corrigendum 1 to Part 1
To be discussed by BCM

Editor: Mr. Christoph Ruland
13888-1/DCOR1

Part 2: Mechanisms using symmetric techniques
To be discussed by BCM (Systematic review)

Project JTC 1.27.06.02
ISO/IEC 13888-2: 2010-12-15 (2nd Edition)
13888-2: 2010/COR1: 2012-12-15

Part 3: Mechanisms using asymmetric techniques

Project JTC 1.27.06.03 [SC27 N15209] confirmation
ISO/IEC 13888-3: 2009 (2nd Edition): confirmed in 2015

v. Digital signature schemes giving message recovery (9796)

Part 2: Integer factorization based mechanisms
To be discussed by BCM (Systematic review)

Project JTC 1.27.07.02
ISO/IEC 9796-2: 2010-12-15 (3rd Edition)

Part 3: Discrete logarithm based mechanisms

Project JTC 1.27.07.03 [SC27 N13967] confirmation
ISO/IEC 9796-3:2006 (2nd Edition), 2013-09-15(Corrected 2nd Ed.)

vi. Digital signatures with appendix (14888)

Part 1: General
To be discussed by BCM (Pre-review)

Project JTC 1.27.08.01
ISO/IEC 14888-1:2008 (2nd Edition) [SC27 N13266] confirmation

Part 2: Integer factorization based mechanisms
To be discussed by BCM (Pre-review)

Project JTC 1.27.08.02
ISO/IEC 14888-2:2008 (2nd Edition)
14888-2/COR1: 2015-10-01 (notice: SC27 N15534)

Part 3: Discrete logarithm based mechanisms
[WG2 N1225] KR defect report

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
ISO/IEC 14888-3: 2016-03-15 (3rd Edition) (notice: SC27 N16098)

Amendment 1 to Part 3
[WG2 N1184] 1st WD [SC27 N15638] justification

Project JTC 1.27.08.03.01

Editor: Mr. Zhenfeng Zhang, Co-editor: Ms. Limin Liu
WD14888-3/Amd1: Review of comments
[WG2 N1203] SoC
[WG2 N1226] draft DoC

vii. Hash-functions (10118)

Part 1: General
To be discussed by BCM

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

Part 2: Hash-functions using an n-bit block cipher
To be discussed by BCM (Systematic review)

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

Corrigendum 2 to Part 2
To be discussed by BCM
[WG2 N1119] defect report, [SC27 N15610] justification

Project JTC 1.27.09.02
Editor: Liqun Chen
10118-2: 2010/DCOR2:

Part 3: Dedicated hash-functions
To be discussed by BCM
[WG2 N1162] DoC on 3rd WD

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
CD10118-3:

Part 4: Hash-functions using modular arithmetic
[SC27 N13968] confirmation

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

viii. Key management (11770)

Part 1: Framework
To be discussed by BCM (Systematic review)

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

Part 2: Mechanisms using symmetric techniques
To be discussed by BCM (Pre-review)

Project JTC 1.27.18.02

ISO/IEC 11770-2: 2008 (2nd Edition) [SC27 N13268] confirmation
11770-2:2008/COR1: 2009-09-15

[Cancelled] Corrigendum 2 to Part 2
[SC27 N15636] justification cancel

Editor: Mr. Chris Mitchell [WG2 N1118] Editor's report
11770-2/DCOR2

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)

Amendment 1 to Part 3 [WG2 N1172] 1st WD
[SC27 N15615] justification

Editor: Mr. Michael Ward
WD 11770-3/Amd1: Review of comments [WG2 N1204] SoC
[WG2 N1229] draft DoC

Corrigendum 1 to Part 3
To be discussed by BCM

Editor: Ms. Atsuko Miyaji
11770-3/DCOR1

Part 4: Mechanisms based on weak secrets
To be discussed by BCM
[WG2 N1163] DoC on 2nd 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
CD11770-4

Part 5: Group key management
[SC27 N13970] confirmation

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

Part 6: Key derivation
To be discussed by BCM

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

ix. Check character systems (7064)

Project JTC 1.27.23
ISO/IEC 7064: 2003 (1st Edition): stabilised in 2009

x. Cryptographic techniques based on elliptic curves (15946)

Part 1: General

To be discussed by BCM

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

Part 5: Elliptic curve generation
To be discussed by BCM [WG2 N1164] DoC on 1st WD

Project JTC1.27.26.05
(revision of 15946-5: 2009 (1st Edition) + 15946-5: 2009/COR1: 2012-12-01)
Editor: Ms. Atsuko Miyaji
CD15946-5:

xi. Time-stamping services (18014)

Part 1: Framework
[SC27 N14752] confirmation

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

Part 2: Mechanisms producing independent tokens
[SC27 N15210] confirmation

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

Corrigendum 1 to Part 2
To be discussed by BCM

Editor: Mr. Christoph Ruland
18014-2/DCOR1

Part 3: Mechanisms producing linked tokens
[SC27 N15211] confirmation

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

Part 4: Traceability of time sources

Project JTC1.27.27.04
ISO/IEC 18014-4: 2015-04-15 (1st Edition)

xii. Random bit generation (18031)
[SC27 N13423] press release
[SC27 N13971] confirmation

Project 1.27.31
ISO/IEC 18031: 2011-11-15 (2nd Edition)
18031: 2011/COR1: 2014-10-01

Amendment 1
To be discussed by BCM

Project1.27.31.01 (Amendment 1 to ISO/IEC 18031: 2011)

Editor: Mr. Pascal Paillier
18031/DAM1

xiii. Prime number generation (18032)

To be discussed by BCM

Project 1.27.32 (revision of 18032:2005 (1st Edition))
Editor:
CD 18032 (n.a.)

xiv. Encryption algorithms (18033)

Part 1: General

Project1.27.33.01
ISO/IEC 18033-1: 2015-08-01 (2nd Edition)

Part 2: Asymmetric ciphers
[SC27 N13972] confirmation

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

Amendment 1 to Part 2
[WG2 N1196] 1st WD

Project 1.27.33.02.01 [SC27 N15639] justification
Editor: Mr. Le Trieu Phong, Co-editor: Ms. Shiho Moriai
WD 18033-2/Amd1: Review of comments
[WG2 N1205] SoC
[WG2 N1228] draft DoC

Part 3: Block ciphers
To be discussed by BCM (Systematic review)

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

Part 4: Stream ciphers
[SC27 N13973] confirmation

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

Part 5: Identity-based ciphers

Project1.27.33.05
Editor: Mr. Kai Sui Liu, Co-editor: Mr. Toshihiko Matsuo
ISO/IEC 18033-5: 2015-12-01 (notice: SC27 N15871)

Part 6: Homomorphic encryption
[WG2 N1165] 2nd WD
[WG2N1166] DoC on 1st WD

Project1.27.33.06 [WG2N1181] call for contri
Editor: Mr. Pascal Paillier, Co-editor: Ms. Atsuko Miyaji
WD 18033-6: Review of comments on WD [WG2 N1206, 1207] SoC, SoContri
[WG2 N1218] PRACTICE comm

[WG2 N1232, 1231] draft DoC, draft revised text

xv. Authenticated encryption (19772)
[SC27 N14753] confirmation

Project 1.27.38
ISO/IEC 19772: 2009 (1st Edition)
19772: 2009/COR1: 2014-09-01

xvi. Signcryption (29150)
[SC27 N13974] confirmation

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

xvii. Lightweight cryptography (29192)

Part 1: General [SC27 N15212] confirmation

Project 1.27.82.01
ISO/IEC 29192-1: 2012-06-01 (1st Edition): confirmed in 2015

Part 2: Block ciphers [SC27 N15213] confirmation

Project 1.27.82.02
ISO/IEC 29192-2: 2012-01-15 (1st Edition): confirmed in 2015

Amendment 1 to Part 2 [WG2N1185] 1st WD
[WG2N1194] DoC on prelim WD

Project 1.27.82.02.01 [SC27 N15640] justification
Editor: Mr. Louis Wingers, Co-editor: Mr. Doug Shors [WG2N1187] call for contri
WD 29192-5/Amd1: Review of comments on WD [WG2N1208, 1209] SoC, SoContri
[WG2N1217] additional comm

Part 3: Stream ciphers
[SC27 N15214] confirmation

Project 1.27.82.03
ISO/IEC 29192-3: 2012-10-01 (1st Edition): confirmed in 2015

Part 4: Mechanisms using asymmetric techniques
To be discussed by BCM

Project 1.27.82.04 *(Pre-review)*
ISO/IEC 29192-4: 2013-06-01 (1st Edition)

Amendment 1 to Part 4

Project1.27.82.04.01
Editor: Mr. Erwin Hess
ISO/IEC 29192-4/AMD1: 2016-02-15 (notice: SC27 N15980)

Part 5: Hash-functions
To be discussed by BCM

Project 1.27.82.05

Editors: Mr. Axel Poschmann, Ms. Shiho Moriai
FDIS 29192-5

Part 6: Message authentication codes (MACs)
[WG2 N1186] 1st WD
[WG2 N1195] DoC on prelim WD

Project 1.27.82.06 [SC27 N15637] justification
Editor: Mr. Hirotaka Yoshida, Co-editor: Suresh Ramasamy [WG2 N1188] call for contri
WD 29192-6: Review of comments on WD [WG2 N1210] SoC

xviii. Anonymous entity authentication (20009)

Part 1: General
To be discussed by BCM (Pre-review)

Project 1.27.83.01
ISO/IEC 20009-1: 2013-08-01 (1st Edition)

Part 2: Mechanisms based on signatures using a group public key
To be discussed by BCM

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

Part 3: Mechanisms based on blind signatures
To be discussed by BCM

Project 1.27.83.03
Editor:
Project cancelled

Part 4: Mechanisms based on weak secrets
To be discussed by BCM

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

xix. Anonymous digital signatures (20008)

Part 1: General
To be discussed by BCM (Pre-review)

Project 1.27.84.01
ISO/IEC 20008-1: 2013-12-15 (1st Edition)

Part 2: Mechanisms using a group public key
To be discussed by BCM (Pre-review)

Project 1.27.84.02
ISO/IEC 20008-2: 2013-11-15 (1st Edition)

xx. Blind digital signatures (18370)

Part 1: General *To be discussed by BCM*

Project 1.27.100.01

Editor: Mr. Jacques Traoré, Co-editor: Mr. David Turner
DIS 18370-1

Part 2: Discrete logarithm based mechanisms
To be discussed by BCM

Project 1.27.100.02
Editor: Mr. Jacques Traoré, Co-editor: Mr. David Turner
FDIS 18370-2

xxi. Secret sharing (19592)

Part 1: General
To be discussed by BCM

Project 1.27.110.01
Editors: Mr. Dan Bogdanov, Mr. Shin'ichiro Matsuo
CD19592-1

Part 2: Fundamental mechanisms
To be discussed by BCM

Project 1.27.110.02
Editors: Mr. Koutarou Suzuki, Mr. Dan Bogdanov
CD 19592-2

xxii. [WG 3] Test and analysis methods for random bit generators within ISO/IEC 19790 and ISO/IEC 15408 (20543)

[SC27 N15533] DE prop of joint project between WG 2/3
[WG2 N1219 (=WG3 N1229)] WD

Project 1.27.117
Editors:
WD 20543: Review of comments [WG2 N1220 (=WG3 N1286)] SoC

xxiii. WG 2 Study Preiods

30.1 [terminated] Review of UK proposal for a new mechanism in ISO/IEC 11770-3
[WG2 N1173] meeting report
Rapporteur: Mr. Michael Ward

30.2 [terminated] Amendment to ISO/IEC 29192-2
[WG2 N1174] meeting report
Rapporteurs: Mr. Louis Wingers, Mr. Doug Shors

xxiii.3 [terminated] Lightweight MACs (title changed from "MACs to include Chaskey")
[WG2 N1175] meeting report
Rapporteurs: Mr. Hirotaka Yoshida

30.4 Inclusion of Chinese IBS scheme in ISO/IEC 14888-3 (title changed from "Inclusion of Chinese SM2 and IBS schemes in ISO/IEC 14888-3")
[WG2 N1176] meeting report
Rapporteurs: Ms. Limin Liu, Mr. Zhenfeng Zhang [WG2N1193] call for contri
Review of contributions [WG2 N1211] SoContri
[WG2 N1227] draft DoContri

30.5 Quantum computing resistant cryptography
[WG2N1177] meeting report, [WG2 N1190] call for contri
Rapporteur: Ms. Lily Chen
Review of contributions [WG2 N1212] SoContri, [SC27 N15866] PQCRYPTO LS

30.6 [terminated] Inclusion of SM3 in ISO/IEC 10118-3
[WG2 N1178] meeting report
Rapporteurs: Ms. Xiaoyun Wang, Ms. Limin Liu

xxiii.7 [terminated] Inclusion of FACE in ISO/IEC 18033-2
[WG2 N1179] meeting report
Rapporteurs: Mr. Le Trieu Phong, Ms. Shiho Moriai

xxiii.8 Mechanisms and properties for ISO/IEC 9798 and ISO/IEC 11770
[WG2 N1180] meeting report
Rapporteur: Mr. Jens Hermans
Review of contributions

xxiii.9 Inclusion of new mechanisms in ISO/IEC 9798-3 [WG2N1192] proposal init
[WG2 N1182] call for contri
Rapporteurs: Mr. Hu Yanan, Mr. Li Qin
Review of contributions

xxiii.10 [terminated] [joint SP with WG 5] A privacy-respecting identity management scheme using attribute-based credentials
Rapporteur: Mr. Pascal Paillier (from WG 2)

30.11 [proposed] Lightweight broadcasting protocols

[WG2 N1230] BE expert proposal

xxiv. WG 2 standing documents

SD1 (WG 2 Roadmap) [WG2 N1167]
[WG2 N1168] DoC on previous vsersion
Editor: WG 2 Convenor

SD2 (WG 2 OID List) [WG2 N1169]
Rapporteur: Mr. Kenji Naemura

SD3 (WG2 Harmonized Vocabulary)
Editor:

SD4 (Analysis and status of cryptographic algorithms) [SC27 N14908] 1st Edition
Editors: Mr. Shin'ichiro Matsuo
Co-editor: Ms. Liqun Chen, Mr. Grigory Marshalko

SD5 (Process for inclusion and deletion of cryptographic mechanisms)
[SC27 N14020] 1st Edition
Editor: Mr. Riaal Domingues, Ms. Atsuko Miyaji

SD6 (Guidelines for effective communication on security mechanism issues)
[WG2 N1024] DoC on previous text, [WG2 N1023] revised text
Editors: Mr. David Grawrock, Mr. Art Manion, Mr. Damir Rajnovic, Mr. Grigory Marshalko

SD7 (Conversion functions) [WG2 N1170] 2nd text
[WG2 N1171] DoC on 1st text
Editors: Mr. Chris Mitchell, Ms. Liqun Chen [WG2 N1213] SoC

[WG2 N1223, 1224] draft DoC, draft revised text

xxv. Standing document on Assessment of cryptographic techniques & key lengths (SC27 SD12)
[SC27 N13432]
Co-editors: Mr. Riaal Domingues, Mr. Hans von Sommerfeld [SC27 N15892] call for contri
[SC27 N16052] SoContri, [SC27 N16095] MasterCard LS

xxvi. [FYI] SC27 standing documents

SD1 (Meeting Calendar) [SC27 N15227] Jul 2015
SD2 (Mailing List) [SC27 N15952] Apr 2016
SD3 (List of Officers) [SC27 N15953] Apr 2016
SD4 (Program of Work) [SC27 N15954] Jan 2016
SD5 (Management Guideline) [SC27 N13525] Dec 2013
SD6 (Glossary) [SC27 N15456] Oct 2015
SD7 (Catalog of Projects and Standards) [SC27 N15457] Oct 2015
SD8 (Patent Information) Withdrawn
SD9 (Help for electronic distribution of documents using World Wide Web) Withdrawn
SD10 (Management of OID & ASN.1 Syntax) [SC27 N8218] Feb 2010
SD11 (Marketing Report) [SC27 N15560] Sep 2015
SD12 (Cryptographic algorithms and key lengths) See 32.
SD13 (Best practices guide for use of WG Livelink) [SC27 N15439] Aug 2015
SD14 (Transversal Item handling) [SWG-T N32 (draft)]
SD15 (Scope alignment on SC 27 transversal projects) [SWG-T N31 (draft)]
SD16 (Information security library (ISL))
SD17 (SC 27 Guide for editors) [SC27 N15802 (preliminary draft)]
SD18 (SC 27 Structure and scopes of its Working Groups and Special Working Groups)
[SC27 N15398 (draft)] Aug 2015
SD27 (Benefits and requirements for hosting SC 27 meetings)[SC27 N15490 (draft)] Sep 2015

xxvii. Other business

Improvement of WG2 activities

JTC 1 Directives ISO/IEC Directives Part 1 & Part 2: 2016 (to be published in May 2016)
[JTC1 N12972] revised consolidated JTC1 Supplement 2016
[SC27 N14915] Consolidated JTC1 Supplement 2015
[SC27 N15429] Guidelines for pilot of voting of remote participants
[SC27 N15497] Recomm from JTC 1/SWG 2 Directives
[JTC1 N15559] Presentation by SWG-Directives
[SC27 N16121] approved recomm Mar 2016 JAG

Others

SC27 Business Plan [SC27 N15445] Sep 2015
Eicher Award [SC27 N15515]
TMB Communiqu [SC27 N16096]
Next meeting (Fall 2016) [SC27 N16040] UAE

Recommendations

Closure of the meeting at no later than 1600 hrs on April 15th, 2016

5. Findings

The meeting through WG2 and other WG had highlighted some issues with current standards.

i. ISO 27005 – Risk management in relation to ISMS. Due to competing standards of ISO 31000 which has the risk assessment and management methodologies standardized, the ISO 27005 is no longer current and requires revision. However, due to lack of consensus, this paper has been terminated and fresh call for contributions shall ensue.
ii. ISO 29192 – Lightweight Cipher algorithms – proposal from US NB to include Simon & Speck. The standards were proposed by NSA US to be included into the standards, however met heavy resistance. This is due to earlier incident with NSA weakening an existing cipher – Dual ECDRBG and subsequent was highlighted through the Snowden revelations that NSA has been working against secure cryptography. Malaysia has voted for the study period to be extended as the consensus of further cryptanalysis is required in order for the algorithm to be considered.
iii. ISO 29192 – Lightweight algorithms – Part 6 MAC (under the co-chairperson of Dr. Suresh Ramasamy) – the Call for Contributions was done to identify possible candidates for the inclusion of algorithms and was discussed in length. Co-chairperson has been tasked to edit and provide the initial draft based on the discussed algorithm and a further call for contributions for Experts/NB to propose actual algorithms based on discussion in Tampa, FL.

6. Conclusion

Issue 5.ii highlights key importance of INS participation in ISO, in ensuring national security agenda for MY. Inclusion of a weak cipher adopted as international standards will cause systemic security failure as commercial products used by Government and private organizations fall to compromise.

It is recommended that INS WG continues to participate on the regional ISO/IEC SC27 regional meetings to further assist global community through the existing work in WG2 and participation in other WG within SC27 as well as expert participation in ensuring national interest are at helm.

The next ISO/IEC JTC1 SC27 meeting is slated to be held in Abu Dhabi, UAE in October 2016

7. Acknowledgement

The WG would like to express its gratitude to MTSFB and SKMM for graciously sponsoring the participation of the WG in ISO.

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