

Laporan

Mesyuarat 23rd ISO/IEC JTC1/SC27 Working Group and Plenary di Seoul, Korea pada 15 hingga 24 Oktober 2001

1. Tujuan

Tujuan laporan ini adalah untuk memaklumkan hasil penyertaan delegasi Malaysia dalam mesyuarat **23rd ISO/IEC JTC1/SC27 Working Group and Plenary** yang telah diadakan di Seoul, Korea dari 15 hingga 24 Oktober 2001

2. Latarbelakang

2.1 **ISO/IEC JTC1/SC27** ialah subcommittee kepada Joint Technical Committee 1 yang bertanggung jawab menggubal standard keselamatan teknologi maklumat.

2.2 Malaysia baru saja menjadi *P (Participation) Member* mulai August 2001.

2.2 Dibawah **ISO/IEC JTC1/SC27** terdapat tiga (3) *Working Groups* yang dipertanggungjawabkan untuk mengkaji beberapa projek (*work items*) yang telah dipersetujui sepertimana di **Lampiran A**.

3. Kehadiran

Di dalam **23rd ISO/IEC JTC1/SC27 Plenary and Working Group Meeting**, Malaysia telah diwakili oleh pegawai berikut:

- i) Dr. Ahmad Zainal Abidin
Pengurus Besar
Pusat Kepintaran Buatan
SIRIM Bhd

Merangkap Pengerusi *Technical Committee – Information Security*

4. Mesyuarat Working Group 1

4.1 Mesyuarat *Working Group 1* atau *WG1* membincangkan projek (*Work Item*) seperti berikut:

Tarikh	Mesyuarat / Perbincangan
15 Okt 2001	<i>GMITS Part 1 and Part 2 Intrusion Detection Framework, Network security</i>
16 Okt 2001	<i>GMITS Part 1 and Part 2, GMITS Part 3 Intrusion Detection Framework, Network security</i>
17 Okt 2001	<i>ISO/IEC 17799 Intrusion Detection Framework, Network security Security incident management</i>
18 Okt 2001	<i>ISO/IEC 17799 Security incident management</i>
19 Okt 2001	<i>Plenary WG1</i>

4.2 Oleh kerana perkara yang dibincangkan agak meluas WG1 telah dibahagikan kepada beberapa kumpulan kecil mengikut tajuk-tajuk berkenaan. Setiap tajuk telah dipengerusikan oleh editor yang dilantik. Oleh kerana wakil dari Malaysia hanyalah seorang sahaja perbincangan yang diikuti adalah ditumpukan kepada GMITs dan ISO/IEC 17799 sahaja. Ini adalah selari dengan usaha-usaha JK Teknikal standard kebangsaan.

4.3 Resolusi *Plenary WG 1* adalah seperti di **Lampiran B**.

5. Mesyuarat 23rd Plenary ISO/IEC JTC1

5.1 Penyertaan

Mesyuarat 23rd *Plenary ISO/IEC JTC1* yang berlangsung selama dua hari ini telah dihadiri oleh lebih kurang 36 orang delegasi dari pelbagai negara ahli.

5.3 Laporan dari Working Group

Covenor dari setiap *Working Group* telah membentangkan kemajuan *Work Item* dan projek-projek yang di senaraikan. *Editing Committee* dan *Project Team* telah diminta untuk menyelaras semua komen-komen yang diterima dari negara-negara yang menjadi *P – Member* dan pertubuhan-pertubuhan yang menjadi *liaison member* kepada ISO/IEC JTC1.

5.4 Resolusi

Resolusi penuh dari mesyuarat 23rd *Plenary ISO/IEC JTC1* akan diperolehi daripada laman ISO/IEC di www.din.de.

6. Kesimpulan

6.1 Tindakan susulan

Malaysia menjadi ahli kepada sub-editorship bagi bahagian 2 dan 3 revised ISO/IEC 17799. Oleh yang demikian maklumbalas kepada editor yang dilantik perlu dikemukakan.

Perbincangan dan maklumbalas serta komen-komen dari Malaysia juga perlu dikemukakan keatas deraf-deraf International Standards yang akan dihantar dari masa kesemasa.

6.2 Manfaat

Dengan menghantar delegasi ke mesyuarat *Working Group dan Plenary ISO/IEC JTC1*, Malaysia telah mula menempah nama sebagai suatu negara mengambil bahagian dan menceburkan diri secara terus kepada penetapan dan penyediaan beberapa dokumen standard bagi keselamatan ICT.

Pengalaman berbincang dan berkenalan dengan pakar-pakar dalam berbagai aspek keselamatan ICT memberi peluang kepada Malaysia berada dalam teknologi terkini.

Sebagai ahli P, delegasi Malaysia yang dilantik oleh SIRIM Bhd. dapat memberi komen, bantahan, sokongan serta undian melalui mesyuarat Plenary, Working Group, Editing Committee ataupun Project Team demi manfaat negara ini di masa akan datang.

6.3 Pembiayaan menghadiri Mesyuarat Plenary dan Working Group ISO/IEC JTC1 di masa akan datang

Sebagaimana yang dapat diperhatikan bidang ICT yang dibincangkan dalam merumus standard-standard adalah teknikal dan mendalam. Contohnya bidang cryptography dan common criteria. Oleh yang demikian adalah diharapkan pihak-pihak lain seperti industri dan akademia akan dapat sama-sama mengambil bahagian membiayai wakil ke mesyuarat ini.

December 2001

Working group 1

Convenor: Ted Humprey

Projects and work items:

Reference	Description	ISO/IEC #
JTC 1.27.10	Review of IS 9979: 1991, Procedures for the registration of cryptographic algorithms (review in 2002)	N 3024
JTC 1.27.13 (15816): IS 15816	Security information objects for access control (awaiting publication)	
JTC 1.27.14 (13335)	Guidelines for the Management of IT Security	
TR 13335-1:1996	Concepts and models for IT Security (revision in 2000)	N 2865, N 2865r, N 2866, N 2967
TR 13335-2:1997	Managing and planning IT Security (revision in 2000)	N 2866, N 2867
TR 13335-3:1998	Techniques for the management of IT Security (review in 2001)	
TR 13335-4:2000	Selection of safeguards (review in 2003)	
TR 13335-5	Management guidance on network security (awaiting publication)	N 2868
JTC 1.27.18 (IS 11770)	Key management (review in 2002)	
IS 11770-1:1996	Framework	
JTC 1.27.19 (TR 14516)	Guidelines on the use and management of Trusted Third Party services (awaiting publication)	
JTC 1.27.24 (IS 15945)	Specification of TTP services to support the application of digital signatures (awaiting publication)	
JTC 1.27.25 (DTR 15947)	IT intrusion detection framework	N 2993c, N 2993, N

		29931, N 2992, N 29933, N 3011, N 3012
JTC 1.27.28 (WD 18028)	IT network security	N 2871, N 2992, N 3014
JTC 1.27.34(NP 18043)	Guidelines for the implementation, operations and management of Intrusion Detection Systems (IDSs)	N 2968, N 3015, N 3016
JTC 1.27.35(NP 18044)	Information security incident management	N 2969r, N 3018
JTC 1.27.37(IS17799)	Code of practice for information security management (revision)	N 2957, N 2958, N 2986 rev1, N 2988, N 3003 r1, N 3019, N 3020

Working group 2

Convenor: Marijke De Soete

Projects and work items:

Reference	Description	ISO/IEC #
JTC 1.27.01(8372)	Status of IS 8372:1987 (2 nd confirmation) (review in 2000) Modes of operation for a 64-bit block cipher algorithm	N 2531, N 3071,
JTC 1.27.02(10116)	Status of IS 10116:1997 (2 nd edition) (review in 2000) Modes of operation for an n-bit block cipher algorithm	N 2972,
JTC 1.27.03 (9798)	Entity authentication	
IS 9798-1:1997 (2 nd edition)	General (confirmed in 2000)	
IS 9798-2:1999 (2 nd edition)	Mechanisms using symmetric encipherment algorithms (review in 2002)	
IS 9798-3:1998 (2 nd edition)	Mechanisms using digital signature techniques (review in 2001)	N 3029

IS 9798-4:1999 (2 nd edition)	Mechanisms using a cryptographic check function (review in 2002)	
IS 9798-5:1999 (2 nd edition)	Mechanisms using zero knowledge techniques (review in 2002)	
JTC 1.27.04 (9797)	Review of IS 9797: 1994 Message authentication Codes (MACs)	
IS 9797-1:1999	Mechanism using a block cipher (review in 2003)	
IS 9797-02	Mechanisms using a hash-function (awaiting publication)	
JTC 1.27.06(13888)	Non-repudiation	
IS 13888-1:1997	General (review in 2000)	
IS 13888-2:1998	Mechanisms using symmetric techniques (confirmed in 2000, review in 2003)	
IS 13888-3:1997	Mechanisms using asymmetric techniques (confirmed in 2000, review in 2003)	
JTC 1.27.07(9796)	Digital signature schemes giving message recovery	
IS 9796-2:1996	Integer factorization based mechanisms (revision in 2000)	
9796-3:2000	Discrete logarithm based mechanisms (review in 2003)	
JTC 1.27.08(14888)	Digital signatures with appendix	
IS 14888-1:1999	General (review in 2003)	
IS 14888-2:1999	Identity-based mechanisms (review in 2003)	
IS 14888-3:1999	Certificate based mechanisms (review in 2003)	
JTC 1.27.09 (10118)	Hash-functions	
IS 10118-1:2000	General	
IS 10118-2:2000	Hash-functions using an n-bit block algorithm (review in 2003)	
IS 10118-3:1997	Dedicated hash-functions (review in 2001)	N 2926, N 2973
IS 10118-4:1998	Hash-functions using modular arithmetic	

	(review in 2002)	
JTC 1.27.18(11770)	Key management	
IS 11770-2:1996	Mechanism using symmetric techniques (confirmed in 1999, review in 2002)	
IS 11770-3: 1999	Mechanisms using asymmetric techniques (review in 2002)	
JTC 1.27.23 (7064)	Data processing- Check character systems (revision)	
JTC 1.27.26(15946)	Cryptographic techniques based on elliptic curves	
FDIS 15946-1	General	N 2713
FDIS 15946-2	Digital signatures	N 2555
FDIS 15946-3	Key establishment	N 2708
WD 15946-4	Digital signatures with message recovery	N 2974 rev 1 N 3035,
JTC1.27.27(18014)	Time stamping services and protocols	
FCD 18014-1	Framework	N 2977, N 3037, N 3038
CD 18014-2	Mechanisms producing independent tokens	N 2964,
WD 18014-3	Mechanisms producing linked tokens	N 2979
JTC 1.27.31 (NP 18031)	Random number generation	N 2905, N 2906
JTC 1.27.32 (NP 18032)	Prime number generation	N 2907, N 2908
JTV 1.27.33 (NP18033)	Encryption algorithms	
WD 18033-1	General	N 2971
WD 18033	Asymmetric ciphers	N 2990, N 2991, N 3006, N 3007, N 3008
WD 18033	Block ciphers	N 2975 rev1, N 2980, N 2989
WD 18033	Stream ciphers	N 2921, N

		2922, N 3073
--	--	--------------

Working group 3

Convenor: Mats Ohlin

Projects and work items:

Reference	Description	ISO/IEC #
JTC 1.27.16 (15408)	Evaluation criteria for IT security	
15408-1	Introduction and general model (review in 2002)	
15408-2	Security functional requirements (review in 2002)	
15408-3	Security assurance requirements (review in 2002)	
JTC1.27.20(15292)	Protection profile registration procedures	
JTC1.27.21 (15443)	A framework for IT security assurance	
WD 15443-1	Overview and framework	N 2886, N 2927
WD 15443-2	Assurance methods	N 2740, N 2886
WD 15443-3	Analysis of assurance methods	N 2740
JTC 1.27.22(WD15446)	Guide for protection of protection profiles and security targets	N 2994, N 3064
JTC1.27.36(NP18045)	Methodology for IT security evaluation	N 2729r, N 2924, N 2959, N 2960, N 2998