



Regional Asia Information Security Standards Forum Proceedings

AUSTRALIA CHINESE TAIPEI JAPAN MALAYSIA NEW ZEALAND SINGAPORE SOUTH KOREA THAILAND



SINGAPORE

ABSTRACT

This paper provides an update on the focus and priorities of Singapore's IT security standards technical committee for the current fiscal year (FY 2006),¹ and discusses some of the priorities and focus in view of recent security and technology developments that the technical committee has observed.

1. Introduction

In the inaugural RAISS Forum meeting held in Tokyo in November 2004, Kin-Chong Chan [1] had discussed the background and motivations leading to the formation of the IT Security and Privacy Standards Technical Committee (SPSTC) in Singapore. Chan has also provided an elaborated discussion and shared the experience gained by the technical committee and individuals on the organization, structure, developmental work items, and completed standards published by the SPSTC over the years. In the past three meetings, Chan [2-4] has continued to provide greater insights into more specific Working Groups, and other related standards technical committees, and shared more information and experience in the various aspects of standards development and promotion in Singapore.

The purpose of this paper is to revisit the status of development and progress of SPSTC at the technical committee level since November 2004, review some of the work items and priorities in current fiscal year (FY 2006), and discuss the priorities and focus based on observations made in the security and technology risk landscape in the recent years.

2. Organization Structure

Since the previous update [1], the SPSTC organization structure has remained intact, as shown in Figure 1. Each working group (WG) is also aligned to one or more working groups in ISO/IEC JTC 1/SC 27. Projects to be initiated in the two new working groups in SC 27, i.e., WG 4 and WG 5, have also been aligned to two separate working groups in SPSTC. The alignments ensure focus and follow-up by relevant standards experts in SPSTC for each related project undertaken in SC 27.

¹ For SPSTC, fiscal year 2006 is from 1 April 2006 to 31 March 2007.

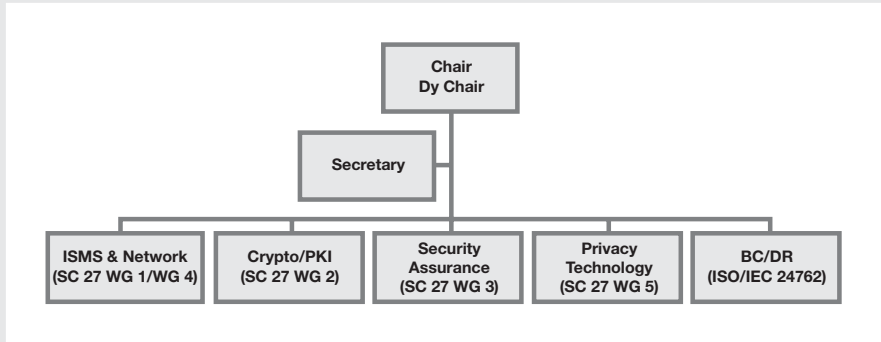


Figure 1: Organization Structure of the Singapore IT Security & Privacy Standards Technical Committee (SPSTC)

3. FY06 Activities and Focus

At the immediate front following the completion of this RAISS Forum meeting was the SC 27 WG 1 and WG 4 Joint Meeting (on 31 October 2006) and a Cybersecurity seminar (on 1 November 2006) held in Singapore. The SPSTC organized the two events, and lined up the security standards experts from the participating SC 27 national bodies for a full day agenda in the Cybersecurity seminar.

The purpose of the WG 1-WG 4 Joint Meeting was to complete the handover of relevant standards development projects from WG 1, and assist WG 4 in identifying the priorities and roadmap for discussion in the coming SC 27 Working Groups meeting in South Africa.

Besides leveraging the security standards experts from the SC 27 national bodies participating in the WG 1-WG 4 Joint Meeting in Singapore to share information on security standards and trends in the international arena with the local practitioners, the purpose of the Cybersecurity seminar was also to invite contributions from participants to the WG 4 work item on Cybersecurity standards development.

To continue its standards promotion effort, the SPSTC has also scheduled additional security seminars to be held in early 2007.

In the area of standards development, the working groups in SPSTC are currently focused on developments relating directly to the work items in SC 27 WG 1 and WG 4, in particular, the development of ISO/IEC 24762 on ICT Disaster Recovery Services, and new work items on application security, Cybersecurity, and ICT Readiness for Business Continuity.

In relation to the work of the RAISS Forum, SPSTC has contributed to the development of the “Security Standards Toolkit” project, and is currently developing the first draft of the “Application Security Standards” project.

Besides SC 27 and RAISS Forum participation, SPSTC is also supporting two projects undertaken in Question 6 of Study Group 17 in ITU-T, on Cybersecurity. They are:

- Guidelines for Prevention of Spyware and Other Deceptive Software; and
- Guidelines on Vulnerability Life-cycle Management

Both projects have been accepted by SG17 and targeted to be published as ITU-T Recommendations upon completion.

4. Evolving Priorities and Focus

In the coming years, the SPSTC will continue to participate and contribute to the agenda and developments of ISO/IEC JTC 1/SC 27. In terms of the topics of interest, in line with Singapore’s national developmental needs and priorities, and the technical committee’s views on evolving risk in the technology and information security landscape, the technical committee has identified five areas of focus and development (not in sequence of priority):

- 1) Business continuity and disaster recovery - this is in view of Singapore’s strategic advantage in providing related ICT services and infrastructure, from a geographical perspective, and the experience that the economy had gained over the past years in successfully responding and managing various related incidents. Going forward, SPSTC has identified ICT readiness as the next area of focus in order to further improve

competencies, and enhance responsiveness of services and infrastructures to the multitudes of disastrous situations where ICT will play a significant role.

- 2) Privacy technology - the proliferation of the Internet and related technology has resulted in an increasing concern over the use and safeguard of personal identifiable information. Information security technology and related standards play a significant role in providing the safeguard, and assisting proper use (in compliant with related privacy policy). In this regard, SPSTC is reviewing the standards requirements, and tracking the work of SC 27/WG 5 to determine possible development and contributions.
- 3) Application security - the recent security trend has shown that attacks on the Internet are continuing to move “up the stack”, i.e., towards exploiting weaknesses at the application layer. At the same time, the practice of secure application development has also been found to be lacking. One of the issues identified is the lack of standards in such area of development. The initial work that SPSTC has initiated in the RAISS Forum in application security standardization has further confirmed the needs for such standards. In this regard, continue focus and priority will be important in developing application security related standards to help narrow if not close the related security gap.
- 4) Cybersecurity - the open, seamlessly interconnected, and highly interactive architecture of the Internet is increasingly being exploited by cyber criminals, rogue individuals, and businesses for financial gains, and pursuant of other adversarial agendas, through the use of various forms of malicious software, SPAM, Phishing techniques on computing systems and social engineering on end-users. The implications of such exploitations and related cyber incidents are immense, from undermining user’s confidence and trust of computing systems and the Internet, to severe retardation of social and economical progress and development. In many cases, hefty financial and reputation losses had been incurred. As such, developing countermeasures, including the use of security standards, is critical to protect and respond against such a risk. SPSTC is therefore also supporting and placing priority and focus in this area of standardization.

- 5) Information security management (ISM) - this is fundamental to providing and ensuring information security in organizations. The recent development and publication of various ISM-related standards in the ISO/IEC 27000 series have provided a useful set of baseline to strengthen this fundamental in organizational information security environment. In addition to the continuing contributions for further development of ISM-related standards, SPSTC is also promoting awareness and adoption of these standards as part of its ongoing plan and activities.

5. Conclusion

While the SPSTC has achieved several significant milestones over the past eight years, the ICT environment that it had based upon to establish its plans and activities had changed significantly, especially in the past few years. We have been responsive to those changes, and new priorities and focus have been developed to align to the risks assessed. This paper has shared our insights on those risks that we have observed and assessed that are significant in the current context, and our strategy in addressing them.

6. References

- [1] Chan, K.-C. Singapore Standards Development - The Singapore Experience. in RAISS Forum. 2004. Tokyo, Japan: RAISS Forum.
- [2] Chan, K.-C. Standards Updates from Singapore including Development of a New Business Continuity and Disaster Recovery Standard. in RAISS Forum. 2005. Singapore: RAISS Forum.
- [3] Chan, K.-C. Guidelines for Information and Communications Technology Disaster Recovery Services Standard. in RAISS Forum. 2005. Kuala Lumpur, Malaysia: RAISS Forum.

- [4] Chan, K.-C. Updates from Singapore: Introduction to Biometric Technical Committee and Singapore Standard for Identification. in RAISS Forum. 2006. Jeju, South Korea: RAISS Forum.
- [5] Flood, R.L., Rethinking the Fifth Discipline - Learning within the unknowable. 1999: Routledge. 213.

Note: The biography of the author is available at the preface on page 05.



Regional Asia Information Security Standards Forum Proceedings

AUSTRALIA CHINESE TAIPEI JAPAN MALAYSIA NEW ZEALAND SINGAPORE SOUTH KOREA THAILAND



SOUTH KOREA

ABSTRACT

This paper provides an overview of the current status of standardization activities in the information security field in South Korea, focusing on the activity of Telecommunication Technology Association (TTA). Standards on information security that are in place and currently being developed in TTA are also highlighted.

1. The Standardization System in South Korea

TTA is one of the South Korean standardization bodies in the information and communication field, responsible for developing standards in information and telecommunications area. Two major international standardization bodies that TTA has established a close relationship and hence supporting their standardization activities are the International Telecommunication Union (ITU) and the Joint Technical Committee 1 (JTC 1) of ISO/IEC. TTA, a non-profit organization under the supervision of the Ministry of Information and Communication (MIC), is responsible for developing the domestic standards and supporting ITU-T standardization activities, while the Agency for Technology and Standards (ATS) which comes under the purview of the Ministry of Commerce, Industry and Energy (MOCIE) is responsible for supporting ISO/IEC JTC 1 activities. Figure 1 shows how TTA's relate to both domestic and international standardization organizations.

Although MOCIE supports the standardization activities of ISO/IEC JTC 1, its scope goes beyond the information technologies (IT) and communications area as it also covers the mechanics, since MIC is only focusing on IT and communications standardization. The main role of the Agency for Technology and Standards (ATS) is to adopt ISO/IEC standard as Korean Standard (KS), and it has the privilege to develop Korean Standards for domestic use. Therefore, ATS can adopt the Information Security Management Systems (ISMS) series standards to become Korean standards. TTA develops the domestic standards and at the same time adopts ISO/IEC and ITU-T standards. Organizations such as network providers, service providers, and various manufacturers and experts can submit standards proposals to TTA for development into domestic standards. Some of the TTA standards will be selected and submitted to MIC to be developed into a national standard. MIC publishes qualified

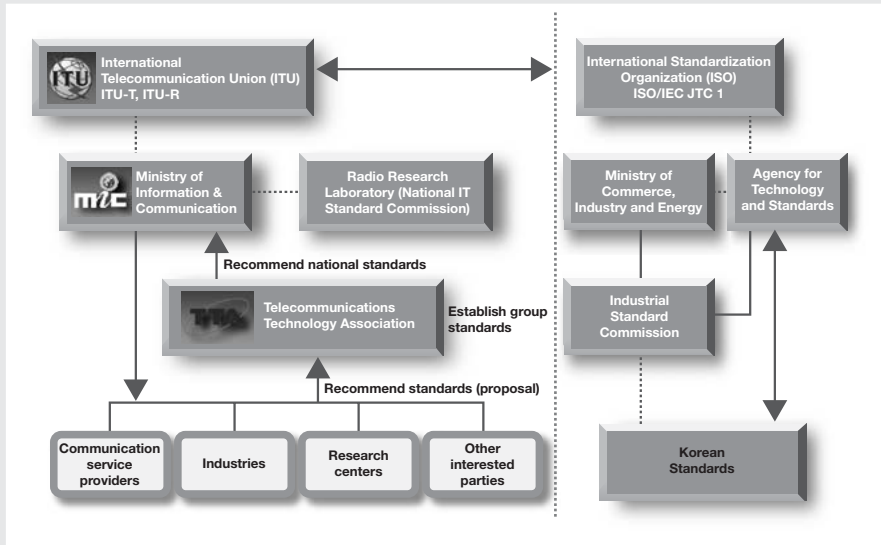


Figure 1: The Standardization System in South Korea

standards as national standards, which are known as the Korean Information and Communication Standard (KICS). Hence, there are two types of national standards in South Korea, namely KS published by ATS and KICS published by MIC.

There are a number of international standardization organizations, such as ITU-T, IETF, IEEE, 3GPP2, 3GPP, etc, which are related to the activities of TTA. Some of the standards will be adopted by TTA, and at the same time, TTA will submit contributions to develop international or forum standards. An example is in the area of portable wireless Internet, known as Wibro¹, TTA has submitted its standards to IEEE, and IEEE has adopted a TTA's contribution.

¹ Wibro (Wireless Broadband) : The Wibro is a portable Internet service that provides a high-speed Internet connection anytime, anywhere for both mobile and stationary connectivity.

MIC has initiated the IT839 strategy to promote Korean's Information, Communication, and Telecommunication (ICT) industries since 2003. The IT839 strategy comprises eight new services, three infrastructures, and nine new growth engines. The eight new services are: Wibro, DMB², Home Network, Telematics, RFID³ Application, W-CDMA⁴, Terrestrial DTV⁵ and VoIP⁶ whilst the three infrastructures are Broadband Convergence Network, U-Sensor Network⁷ and IPv6⁸. The nine new growth engines comprise Next Generation Mobile Communication, Digital TV, Home Network, IT SoC⁹, Next Generation PC, Embedded Software, Digital Contents, Telematics and Intelligent Robot. New growth engines for ICT could generate wealth by launching new IT services using the three infrastructures. The strategies are to promote South Korean IT services and the South Korean industries. 37 key standardization target technologies in IT839 have been selected by MIC for standardization. The standardization on those target technologies are carried out via 52 standardization committees known as Project Groups in TTA.

2. TTA Standardization Committees in South Korea

TTA standardization activities are open to all organizations and individuals. Every member of TTA enjoys the benefits of being able to participate in any of the 52 standardization committee activities, receive information service on a complimentary or discounted basis, and participate in seminars and educational events. Every member of TTA could be classified according to participation type or business type. By participation type, every member could

² DMB (Digital Multimedia Broadcasting) : The concept of DMB was introduced to satisfy the consumer need for a mobile multimedia broadcasting service that provides quality audio and video services anytime, anywhere.

³ RFID (Radio Frequency Identification) : The RFID is a sensor technology that identifies information on the product with an RFID tag and gathers information from surrounding environments.

⁴ W-CDMA (Wideband CDMA) : The W-CDMA is an IMT-2000 service that provides voice, video and high-speed data services in the 2GHz band.

⁵ Terrestrial Digital TV : This service is to provide a high definition and stereophonic sound on a large-sized screen.

⁶ VoIP (Internet Telephony) : The VoIP converts voice signals into packet data to provide a phone service over the Internet.

⁷ USN (Ubiquitous Sensor Network) : The USN recognizes and manages information over the Internet through an RFID tag attached to a product.

⁸ IPv6 (Next-Generation Internet Protocol) : Since the Internet address resource in use today (IPv4) will be depleted starting from 2006, we need to find a fundamental solution to the problem. Our aim is to become an Internet powerhouse by promoting IPv6.

⁹ SoC (System on Chip) : The SoC refers to a non-memory integrated circuit which is not only a growth engine itself for the next-generation but also a key that determines the success of IT products.

be classified into full member, associate member, observer, and special member. There are 184 full members, 29 associate members, 12 observers and seven special members. By business type, there are 202 general businesses, 13 cooperative association members, nine communication service providers, four broadcasting stations and four research centers.

As mentioned earlier, TTA is also responsible for developing Korean domestic standards in the area of ICT. There are four technical committees (TCs) namely TC1, TC2, TC3, TC4. TC1 is the committee on common infrastructure technologies, comprises nine project groups (PGs), and three of them are involved in the standardization activities of information security. There are three PGs under TC1, i.e., PG101, PG102 and PG103, that are developing information security standards. Before 2005, there was one PG on Integrated Circuit (IC) card. However, this PG was merged into Biometric PG in 2005.

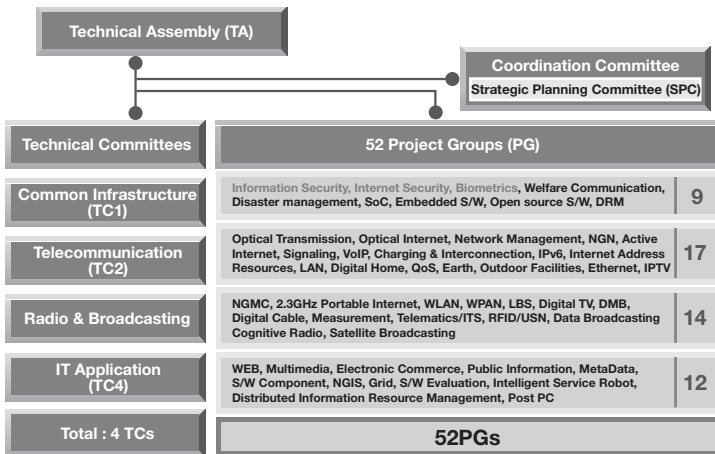


Figure 2: TTA's Standards Committees

There are a number of domestic standardization fora within South Korea which actively participate in the development of standards. In particular, there are two fora in the area of information security, namely: the Internet Security Technology Forum (ISTF) and the Korea Biometric Association (KBA). The former is responsible for developing Internet security related standards while the latter is responsible for developing biometric related standards.

2.1 Information Security Infrastructure PG (PG101)

PG101 deals with standardization on information security infrastructure, which includes basic information security technologies such as ISMS, Common criteria, Public-key infrastructure (PKI), and cryptographic algorithms. The terms of reference (ToR) covers the activities on ISMS and security guideline for administrators and users, certification and evaluation of information security system, secure operating system (OS), PKI, cipher algorithm and key management. The members of PG101 are 35 experts from 16 industries. The Chair of PG101 is Dr Seok-Lae Lee of Korea Information Security Agency (KISA), and the Vice-Chair is Dr Seung-Hun Jin of the Electronics & Telecommunications Research Institute (ETRI).

There are a number of domestic standards which have been developed by PG101 between 2004 and 2005, as shown in Table 1. Among them, a 128-bit block cipher algorithm, known as SEED, which is a Korean standard block encryption algorithm, has been revised in 2005. The current draft standards under development by PG101 are shown in Table 2.

TTA standard		Source	Issued date	Equivalent to	
Number	Title				
1	TTAS.KO-12.0003/R1	Digital Signature with appendix - Part 1 : General Architecture and Model	KISA	2005.12	ISO/IEC 14888-1
2	TTAS.KO-12.0004/R1	128-bit Block Cipher Algorithm (SEED)	KISA	2005.12	RFC 4009
3	TTAS.KO-12.0011/R1	Hash Function Standard - Part 2 : HAS-160	KISA	2005.12	ISO/IEC 10118-1, 3
4	TTAS.KO-12.0028	Path processing algorithm for Digital Signature Certification	KISA	2005.12	RFC 3280
5	TTAS.KO-12.0029	Subscriber Identification based on VID	KISA	2005.12	X.509, RFC 3280
6	TTAS.KO-12.0030	User Authentication mechanisms for home network using home server	ETRI	2005.12	X.homesec-3
7	TTAS.IF-RFC3217	Triple DES and RC2 key wrapping	ISTF	2005.12	RFC 3217
8	TTAS.IF-RFC3370	Cryptographic Message Syntax (CMS) Algorithm	ISTF	2005.12	RFC 3370
9	TTAS.IF-RFC3394	Advance Encryption Standard (AES) key wrap algorithm	ISTF	2005.12	RFC 3394
10	TTAS.IF-RFC3267	Framework for Certification Policy and Certification Practice Statement	KISA	2004.12	RFC 3267
11	TTAS.KO-12.0018/R1	Wireless certification request message format protocol	ISTF	2004.12	WAP-217-WPKI
12	TTAS.KO-12.0027	Guideline for key management and certification on encryption key distribution	KISA	2004.12	-
13	TTAS.OT-12.0001	Wireless Certification Management Protocol	ISTF	2004.12	WAP-217-WPKI
14	TTAS.OT-12.0002	PKCS#11 Conformance Profile for Cryptographic Token	ISTF	2004.12	PKCS11

Table 1: PG101 Standards, 2004-2005

PG101 draft		Source	Milestone	Equivalent to	
Number	Title				
1	2006-478	Digital Signature with Anonymity	KISA	2007.06	-
2	2006-477	The Verification Information for Duplicable Join using Alternative Method of National ID Number Specification	KISA	2006.12	-
3	2006-476	Home Network Security Policy Description Language	ETRI	2006.12	Proposal to SG17
4	2006-370	Addition of SEED Cipher Suites to Transport Layer Security (TLS)	KISA	2006.12	RFC 4162
5	2006-369	The SEED Cipher Algorithm and Its Use with IPsec	KISA	2006.12	RFC 4196
6	2006-368	Security Assertion Markup Language v2.0	ETRI	2006.12	X.1141
7	2006-002	Digital Signature Certificate Profile	KISA	2006.12	RFC 3280
8	2006-001	Open System Interconnection - Security Framework in Open Systems - Part 4 : Non-Repudiation	KISA	2006.12	ISO/IEC 10181-4
9	2005-839	The Criteria for Information Security Management System	KISA	2006.12	X.1051-rev1
10	2005-677	Framework for security technologies for home network	SCH Univ.	2006.12	X.homesec-1
11	2004-002, 003	Use of the Additional Algorithm in Cryptographic Message Syntax (CMS) : SEED, AES	ISTF	2005.12	RFC 3394, 3565

Table 2: PG101 Draft Standards, 2006

2.2 Internet Security PG (PG102)

PG102 deals with the standardization on Internet security which includes S/MIME, Wireless, E-commerce, and VPN. The members of PG102 are 35 experts from 16 industries. The Chair of PG102 is Dr Yoo-Jae Won of KISA, and the Vice-Chair is Dr Sung-Kyong Un of ETRI. There are a number of domestic standards developed by PG102 during the period from 2004 to 2005, as shown in Table 3. The current draft standards under development by PG102 are shown in Table 4.

TTA standard		Source	Issued date	Equivalent to	
Number	Title				
1	TTAS.KO-12.0031	Secure use guide for wireless LAN	KISA	2005.12	IEEE 801.11b, x, I
2	TTAS.KO-12.0032	IPv6 IPsec AH/ESP Conformance Test	ISTF	2005.12	RFC 2406
3	TTAS.KO-12.0033	IPv6 IPsec IKE Conformance Test	ISTF	2005.12	RFC 2409
4	TTAE.IF-RFC2401	Security Architecture for the Internet Protocol	ETRI	2005.12	RFC 2401
5	TTAE.IF-RFC2402	IP Authentication Header	ETRI	2005.12	RFC 2402
6	TTAE.IF-RFC2406	IP Encapsulating Security Payload (ESP)	ETRI	2005.12	RFC 2406
7	TTAE.IF-RFC2716	PPP EAP TLS Authentication Protocol	ETRI	2005.12	RFC 2716
8	TTAE.IF-RFC3588	Diameter Base Protocol for Authentication, Authorization and Accounting	ETRI	2005.12	RFC 3588
9	TTAE.IF-RFC3748	Extensible Authentication Protocol (EAP)	ETRI	2005.12	RFC 3748
10	TTAS.KO-10.0162	Integrity Service Component Interface	ISTF	2004.12	-
11	TTAS.KO-10.0163	Confidentiality Service Component Interface	ISTF	2004.12	-
12	TTAS.OT-12.0003	Advanced Security Conformance Test Method of Information Security System	KISA	2004.12	ISO/IEC 9646, 9126
13	TTAS.IF-RFC3075	XML - Signature Syntax and Processing	ETRI	2004.12	RFC 3075
14	TTAS.IF-RFC3076	Canonical XML Version 1.0	ETRI	2004.12	RFC 3076
15	TTAS.IF-RFC3741	Exclusive XML Canonicalization Version 1.0	ETRI	2004.12	RFC 3741

Table 3: PG102 Standards, 2004-2005

PG102 draft			Source	Milestone	Equivalent to
Number	Title				
1	2006-487	Requirement of IDS policy for IPv6 network	ETRI	2006.12	-
2	2006-486	IDS functional requirements for IPv6 network	ETRI	2006.12	-
3	2006-485	Framework for cipher Key Management	ETRI	2006.12	Draft-ietf-eap-keying-14.txt
4	2005-787	Framework for IT System Security Level Management	Korea DSC	2007.06	DoD Directive 5200.40
5	2005-682	An Extension to Http - Digest Access Authentication	KISA	2006.12	RFC 2617
6	2005-623	A Guideline for Internet Security Management	ETRI	2006.12	ISO/IEC TR 13335

Table 4: PG102 Draft Standards, 2006

2.3 Biometrics PG (PG103)

PG103 is known as Biometrics PG, responsible for standards relating to terminology, testing, and privacy protection of biometric system. Its ToR includes the activities on terminology and privacy protection for biometric systems, interoperability, testing and technologies for biometrics systems, personal identity and electronic IC card. PG103 comprises 20 members from 14 industries. The Chair of PG103 is Dr Jason Kim of KISA, and the Vice-Chair is Dr Yoon-Su Jung of ETRI. There are a number of domestic standards developed by PG103 during 2004-2005, as indicated in Table 5. The draft standards currently under development are shown in Table 6.

TTA standard		Source	Issued date	Equivalent to	
Number	Title				
1	TTAS.KO-12.0034	A guideline for telebiometric protection	KISA	2005.12	X.ttp-11
2	TTAS.OT-10.0001	Conformance Testing Method and Procedure for BioAPI(K-CTS)	KISA	2004.12	ANSI BioAPI v1.1, X.bip

Table 5: PG103 Standards, 2004-2005

PG103 draft			Source	Milestone	Equivalent to
Number	Title				
1	2006-003	Digital Signature Key Generation Mechanism based on Biometric Data	HShin Univ.	2006.12	Proposal to SG17
2	2005-840	Guideline for Protection of Multi-modal Biometric Data in the Wire/Wireless Network Environment	ETRI	2006.12	X.ttp-2
3	2005-789	Test and Certification Procedure on Biometrics	KISA	2007.12	-
4	2005-788	Performance Test Criteria of Biometric System	KISA	2007.12	-
5	2005-005	Methods and Procedures for Performance Test of Face Recognition System	KISA	2007.12	-
6	2004-585	Standard Interface of Fingerprint Sensors for the on-line Authentication	Hyundai Security	2006.12	-
7	2004-584	Standards of Metrics for Fingerprint Image Quality	Inha Univ.	2006.12	-
8	2003-845	Multi-Modal Biometric Framework Standard	ETRI	2007.12	-

Table 6: PG103 Draft Standards, 2006

3. TTA's Standards on Information Security

This section introduces the various standards on information security that have been developed by PG101, PG102 and PG103.

3.1 SEED, 128-bit Block Cipher Algorithm

This standard specifies the 128-bit symmetric block cipher, SEED, that is, a Korean standard for a symmetric key encryption algorithm that transforms a fixed-length block of plaintext to/from encrypted text. SEED has been adopted by ISO/IEC and IETFs as international standard. The SEED algorithm is used as symmetric cryptographic algorithm in IETF Request For Comment (RFC) 4009 in 2005. RFC 4009 specifies the details of SEED algorithm as shown Figure 3. In ISO/IEC, SEED is published as an international standard ISO/IEC 18033- 3 in 2005.

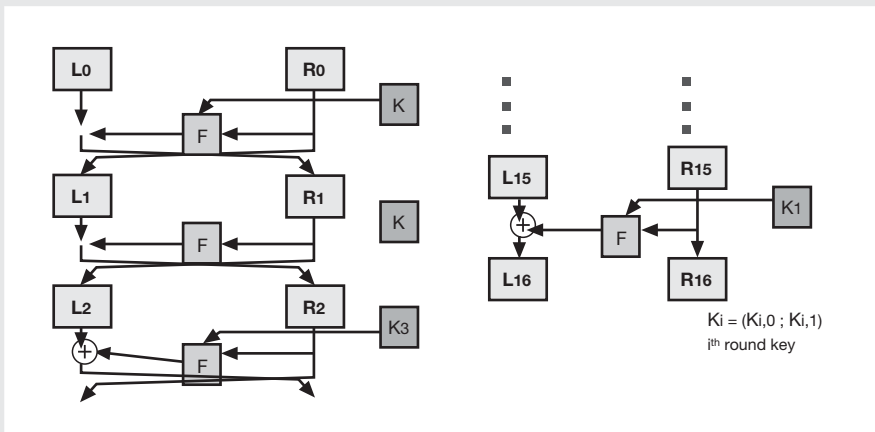


Figure 3: 128-bit Block Cipher Algorithm (SEED)

3.2 Framework of Security Technologies for Home Network

This standard describes the security threats in home network environments and the related security requirements, from the perspective of home users and remote users. It excludes the security requirements from the service providers' perspective. In addition, this standard categorizes security technologies by a) security functions that satisfy the home users and remote users security requirements, and b) the location to which the security technologies are applied in the model of the home network. The security function required for each entity in the network and possible implementation layer for security function are also presented

in the standard. This standard was consented as ITU-T Candidate Recommendation X.homesec-1(ITU-T X.1111) during ITU-T SG17 meeting held from 6-15 December 2006. Figure 4 shows the general model of the home network for security.

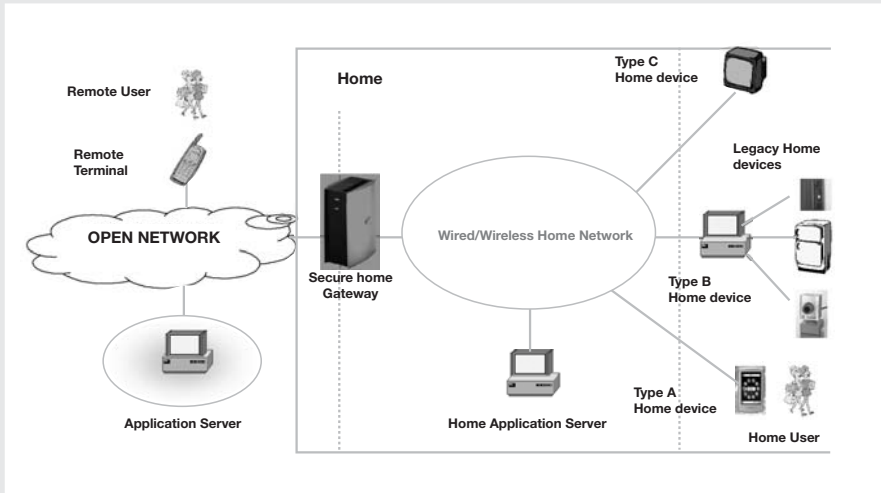


Figure 4: General Model of the Home Network for Security

3.3 User Authentication Mechanisms for Home Network using Home Server

This standard describes the user authentication techniques that enable home user to choose various authentication means for secure home network services and user convenience. This standard is now being developed by the ITU-T SG17 Q.9, which covers Secure Communication Services, as X.homesec-3: "User authentication mechanisms for home network service". This standard specifies a user authentication model for home network as shown in Figure 5.

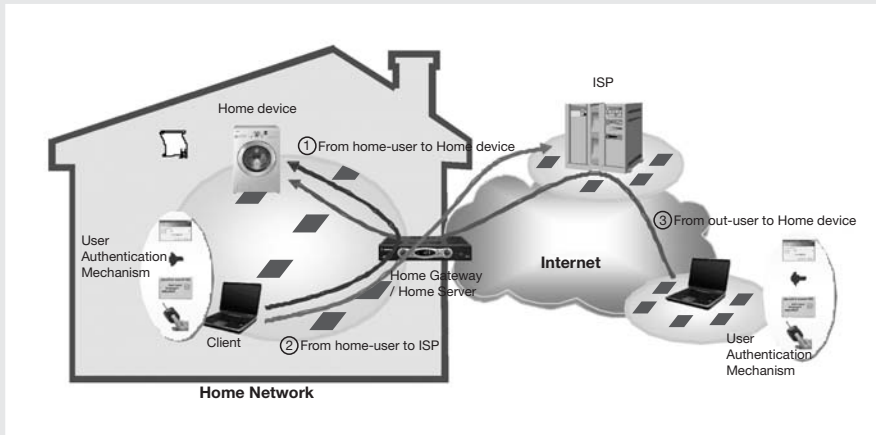


Figure 5: A Model for User Authentication in Home Network Environment

3.4 Secure Use Guide for Wireless LAN

This standard specifies characteristics of vulnerabilities and intrusion methods of wireless LAN and provides guidelines for wireless LAN managers and users. The standard categorizes the attacks on a wireless LAN into three types of attacks, namely physical attack, system attack and network attack. The physical attacks comprise wireless Access Point (AP) breakdown and theft, wireless LAN security equipments breakdown and theft, and wireless terminal breakdown and theft. The system attacks include wireless AP authority, hacking, etc. The network attacks include wireless signal interruption, various forms of network traffic attack, distributed denial of service (DDoS) attack, unauthorized access, etc. This standard incorporates references to IEEE 802.11b(1999), 802.1x(2001) and 802.11i(2004).

3.5 A Guideline on Telebiometrics Protection

This standard defines the weakness and threats in the telebiometric system and proposes a general set of security countermeasures guidance covering both technical and managerial requirements for establishing a safe environment of using telebiometric systems and protect individual privacy. From the technical point of view, this standard defines several countermeasures to ensure data integrity, mutual authentication, and confidentiality.

From the managerial perspective, this standard describes countermeasures that enable protection of biometric devices relating to their installation, removal, and delivery. Also, this standard outlines measures for protection of the biometric information as related to its generation, transmission, storage, and disposal. This standard is also supporting the development of the ITU-T SG17 Q.8 (Telebiometrics) as X.tpp-1: “Telebiometric Protection Procedure - Part 1”. In addition, it specifies a biometric verification process model as shown in Figure 6.

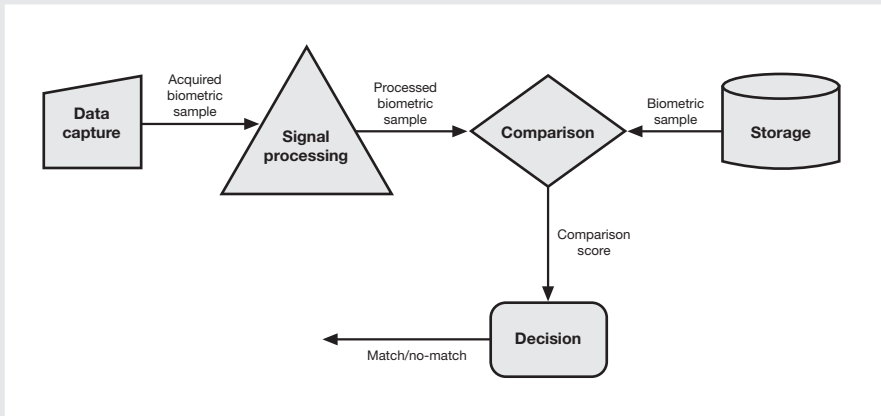


Figure 6: Biometric Verification Process Model

4. Conclusion

This paper introduces the overall standardization system and status of information security standards activities in South Korea. The role of TTA has been specifically emphasized, as it plays a key role in the development and promulgation of domestic standards, including responsibility for Korea’s active participation in the standard activities in ITU-T. TTA supports various projects to encourage numerous standardization experts to develop national standards supporting the MIC’s IT839 strategies. In addition, this paper introduces the common standards on information security produced by or being produced in TTA in the information security area.

Mr Heung-Ryong Oh

*Manager, Information & Communication Team
Standardization Department
Telecommunication Technology Association
South Korea*



Heung-Ryong Oh has been working for the Telecommunication Technology Association as a Manager, since 2004.

He has been involved in the research and development on standards related to information security. Also he is currently the TTA secretariat for PG101, PG102 and PG103 and serves as an associate editor of X.homesec-1 for ITU-T Study Group 17.

He received his Master degree of Information Security from Soonchunhyang University in 2004.

Prof Heung-Youl Youm

*Project Manager of Information Security, IT Policy Advisory Group
Ministry of Information and Communication
Republic of Korea*

*Professor, Department of Information Security
Soonchunhyang University
Republic of Korea*

Rapporteur, Q.9/SG17, ITU-T



Prof Heung-Youl Youm has been working for Soonchunhyang University as a Professor since 1990. Since joining Soonchunhyang University, he has taught thousands of students or technical experts on how information or network security works, and has published more than 60 technical papers in information security journals or conferences. He is the Author or Co-Author of ten books on information security, including Internet Security Technology, published in 2003 by Sangreung Publishing Company, Korea.

He had worked for ETRI as senior member of technical staff for more than eight years since 1982, and had been involved in research and development on various types of transmission systems, including NAS-CEPT conversion system, for telecommunication network.

He has been involved in ITU-T and TTA activities for many years. He is currently one of the members of TC1 technical committee of Telecommunication Technology Association, Korea, and also serves as the Rapporteur for Question 9 of SG17, ITU-T.

Prof Youm has served as a Board Member or a Chairman of a number of government-related committees from Ministry of Information and Communication, Korea Information Security Agency, and National Information Service. He is now serving as the Project Manager of information security, MIC, Korea, since November, 2006. His role covers planning and managing the MIC-sponsored projects in the information security area, and supporting the development of Information Security Policy for MIC, South Korea.

He received his PhD degree of information security from Hanyang University in Korea in 1990.