情 報 保 護 學 會 誌
第 12 券 第 4 號, 2002. 8

ISO/IEC JTC1/SC27(정보기술보안) WG2 24차 베를린 회의 참가 보고

장 청 룡*, 천 동 현**, 강 경 희***, 차 재 현****

요 약

SC27의 WG2는 정보기술보안을 위한 관련 메커니즘들에 대한 표준을 만드는 Working Group이다. 본 고에서 소개하는 24차 베를린회의(2002. 4) 이전에 개최된 21차 동경회의(2000. 10)와 22차 오슬로회의(2001. 4)는 동 학회지 제11권 1호(2001년 2월)와 제11권 3호(2001년 6월)를 참고하면 본 고를 이해함에 있어 많은 도움이 될 것으로 사료된다. 한편 23차 서울회의에 대하여는 WG2 중 블록암호 표준화 동향에 대하여 기고한 제11권 6호(2001년 12월)를 참고로 하기 바란다. 본 고에서는 지난 2002. 4. 22(월)~26(금)에 걸쳐 독일 베를린의 DIN(Deutsches Institut für Normung)에서 개최된 24차 회의에 다녀와서 보안기술 표준화에 관한 최신 정보를 이 분야에 관심이 있는 전문가들에게 전파하고자 각 과제별로 진행사항과 회의결과 및 회의 중 특기 할만한 사항들을 정리하였다.

Ⅰ. 서 론

이번 SC27/WG2 베를린 회의에는 한국에서 본 고의 기고자 4명이 참여하였고, WG1에 2명, WG3에 2명 등 총 8명이 참석하였다. 작년 WG2 서울회의 때에는 미국 9. 11 테러 사건으로 인하여 미국과 유럽 등지로부터의 불참이 많았으나, 이번 회의에는 미국 3명, 영국 3명, 일본 8명, 독일 6명, 벨기에 4명, 그리고 캐나다, 에스토니아, 프랑스, 폴란드, 러시아, 스웨덴이 각각 1명씩의 대표가 참여하였다.

회의는 WG2 Convener인 M. DeSoete(벨기에)가 4월 18일자 개정 의제 문서인 SC 27 N3137rev2 (WG2 N471rev2) "Agenda for the 24th SC 27/WG2 meeting in Berlin, Germany"에 따라 진행되었고, 회의의 결의사항들은 4월 26일에 작성된 WG2/N472draft "Resolutions of the 24th SC 27/WG 2 meeting in Berlin, Germany"로 처리되었다. 본 고는 이러한 결의와 각 과제별 회의에서의 논의사항을 중심으로 정리하기로 한다.

본 고는 본문에서 자주 쓰일 약어를 Ⅱ절에서 설명하고, Ⅲ절에서 과제별로 진행사항을 정리하였다. 간혹 과제번호가 누락된 것이 있는데 이것은 다른 WG의 과제이거나 없어진 과제인 경우이며, 과제 18의 세부과제가 18.02부터 시작하는 것은 18.01은 WG1이 담당하고 있기 때문이다. Ⅳ절에서는 논의된 신규 과제에 대하여 정리하였고, Ⅴ절에서는 소감을 중심으로 결론을 정리하였다.

Ⅱ. 약어 풀이

과제(project) 이름에 대한 약칭은 과제별 진행사항의 (과제)번호 밑에 표기하였다. 다음은 본 고에서 자주 사용되는 약어이다.

CD	Committee Draft
CfC	Call for (National Body) Comments
DIS	Draft International Standard
DoC	Disposition of (National Body) Comments
FCD	Final Committee Draft

* 경동대학교 정보통신공학부(crjang@kyungdong.ac.kr)
** 한국정보보호진흥원 기술단 암호기술팀(dhcheon@kisa.or.kr)
*** 한국통신 멀티미디어연구소(puppycat@hanmir.com)
**** 산업자원부 기술표준원 (chajh@ats.go.kr)

FDIS	Final Draft International Standard
IS	International Standard(ISO/IEC 표준)
NB	National Body
NWI	New Work Item
SoC	Summary of (National Body) Comments
SoV	Summary of Voting
WD	Working Draft

Ⅲ. 과제별 진행사항

본 절에서는 다음과 같은 순서로 각 과제별 논의 및 진행 결과를 정리하였다.

- **번호 과제명**(실제는 'JTC 1.27.XX.YY'이나 본 고에서는 과제번호의 'JTC 1.27.'을 생략하고 'XX.YY'만으로 표기함)
- **과제약칭** (관련문서번호 및 주요 처리 내역)
- 논의사항 및 보고.

01 Modes of operation for a 64-bit block cipher algorithm

Mo64 IS 8372(1987-1st ed., 2nd confirmation in 1997, 3rd confirmation in 2000)가 2003년 재심 예정이므로 이번 회의에서 논의되지 않았음.

02 Modes of operation for an n-bit block cipher algorithm

MoN IS 10116 (1991-1st ed., 1997-2nd ed.)의 개정작업.

· 이번 과제 회의는 O. Jung(독일)의 주재로 진행되었으며 직접 참여를 못하여 WG 전체 회의 및 결의를 참고로 정리한다.

· 현 표준 개정안에 대한 각국의 편집 의견을 수용하여 이의 수정 결과를 5월 20일까지 editor를 경유 사무국에 송부토록 함. 또한 editor로 하여금 현행 표준(2차 개정) 대비 신규 개정판에서의 알고리즘에 대한 기술적 변경 사항을 정리하여 편집 부기(editorial annex)로 추가시키도록 함(베를린 회의 결의 1(WG2 N472 Draft)).

· Statistical Self-Synchronization 부분에 대한 상세 평가 결과를 얻을 수 있도록 2차 CD 투표 요청 문서에 명기하기로 함(베를린 회의 결의 6(WG2 N472 Draft)).

· 독일 측으로부터 상세 평가 결과를 준비하여 제출하기로 함.

03.01 Entity authentication Part 1 : General model

EA1 IS 9798-1 (1991-1st ed., 1997-2nd ed., 1st confirmation in 2000)은 2004년 재심 예정이므로 이번 회의에서는 논의되지 않았음.

03.02 Entity authentication Part 2 : Mechanisms using symmetric encipherment algorithm.

EA2 IS 9798-2 (1994-1st ed., 1999-2nd ed.)는 2002년 재심으로 금번 회의에서 acting editor인 영국 런던대학의 Chris Mitchell에 의해 주재되었음.

가) 검토 문서

· SC27 N3095(CfC for the periodic review of ISO/IEC 9798 Part 2 and Part 5)

· SC27 N3157(SoC/tables of replies for the periodic review of ISO/IEC 9798 Part 2 and Part 5)

· SC27 N3172(Additional UK expert comments in response to N3095)

나) 주요 토의 사항

· 본 표준의 개정 심의에 대한 각 회원국들의 검토 의견에 대한 투표결과로 현 표준의 유지에 찬성 7개국, 개정 1개국(한국)이었으나, 개정 의견에 대한 우리나라의 투표 결과가 투표 처리 과정에서 표현상의 오류임을 인식하여 이를 현 표준의 유지로 찬성하는 것으로 변경함으로써 모두 현 표준을 그대로 유지하는 것으로 투표 결과를 얻음. 또한 전문가의 의견도 접수되지 않아 이번 회의에서 본 표준을 그대로 개정 없이 그대로 유지하기로 함을 권고하기로 함.

다) 문서의 조치: 회원국들의 기고를 9월 15일까지 요청하기로 함(베를린 회의 결의 9(WG2 N472 Draft)).

03.03 Entity authentication Part 3 : Mechanisms using digital signature techniques.

EA3 지난 회의에서 reconfirm된 IS 9798-3 (1993-1st ed., 1998-2nd ed. 1st confirmation

in 2001)는 2004년 재심 예정이므로 이번 회의에서는 논의되지 않았음.

03.04 Entity authentication Part 4 : Mechanisms using a cryptographic check function

EA4 IS 9798-4 (1995-1st ed., 2000-2nd ed.)는 2003년 재심 예정이므로 이번 회의에서는 논의되지 않았음.

03.05 Entity authentication Part 5 : Mechanisms using zero knowledge techniques

EA5 IS 9798-5 (1999-1st ed.)는 2002년 재심으로 금번 회의에서 acting editor인 영국 런던대학의 Chris Mitchell에 의해 주재되었음.

가) 검토 문서 : 과제번호 03.02(IS 9798-2)와 동일

나) 주요 토의 사항

· 본 표준의 개정 심의에 대한 각 회원국들의 검토 의견에 대한 투표결과로 현 표준의 유지에 찬성 5개국, 개정에 3개국(프랑스, 한국, 영국)이었으나, 개정 의견에 대한 우리나라의 투표 처리는 과제번호 03.02(IS 9798-2)와 동일하게 찬성으로 정정 처리함으로써 개정에 대한 투표 결과는 2개국이며 이에 대한 다음과 같은 의견을 반영하여 본 표준을 개정할 것을 권고(SC27 N3226)하기로 함.

- 기 표준 수용 메커니즘 보다 구현상의 장점을 갖는 새로운 소인수 분해 문제-기반 메커니즘인 GQ2를 추가하는 것이 바람직한 것으로 논의됨.
- 7절에 있는 기존 메커니즘들에 상호인증 기능을 추가하는 것이 바람직한 것으로 논의됨.
- 5절에 있는 알고리즘중 본 표준의 발간시부터 철회되었던 ISO/IEC 9796에 종속하는 일부 알고리즘의 수정이 필요한 것으로 논의됨.

다) 문서의 조치: 과제 회의의 권고(SC27 N3226)를 승인하고 이에 따라 문서를 수정 보완하여 본 표준의 개정안을 다음회의에서 논의하도록 함(베를린 회의 결의 10 및 13(WG2 N472 Draft)).

04.01 Message authentication codes Part 1 : Mechanisms using a block cipher

Mac1 IS 9797-1 (1989-1st ed., 1994-2nd ed., 2000-3rd ed.)는 2003년 재심 예정으로 이번 회의에서 논의되지 않음.

04.02 Message authentication codes Part 2 : Mechanisms using a hash-function

Mac2 IS 9797-2 표준발간을 준비중에 있어 이번 회의에서 논의되지 않음.

06.01 Non-repudiation Part 1 : General

NR1 IS 13888-1 (1997-1st ed.) 개정.

· 현 표준 개정안에 대한 각국의 편집 의견을 수용하여 이의 수정 결과를 5월 20일까지 editor를 경유 사무국에 송부토록 함. 또한 editor로 하여금 현행 표준(2차 개정) 대비 신규 개정판에서의 알고리즘에 대한 기술적 변경 사항을 정리하여 편집 부기(editorial annex)로 추가시키도록 함(베를린 회의 결의 1(WG2 N472 Draft)).

06.02 Non-repudiation Part 2 : Mechanisms using symmetric techniques

NR2 IS 13888-2 (1998-1st ed., 1st confirmation in 2000)는 2003년 재심 예정으로 이번 회의에서는 논의되지 않음.

06.03 Non-repudiation Part 3 : Mechanisms using asymmetric techniques

NR3 IS 13888-3 (1997-1st ed., 1st confirmation in 2000)는 2003년 재심 예정으로 이번 회의에서는 논의되지 않음.

07.01 Digital signature schemes giving message recovery Part 1 : Mechanisms using redundancy

DSM1 이 표준은 철회된 상태라 이번 회의에서 논의되지 않음.

07.02 Digital signature schemes giving message recovery Part 2 : Integer factorization based methods

DSM2 IS 9796-2(1997-1st ed.) 개정

· 현 표준의 2차 개정안에 대한 최종 DIS 투표에 대한 의견 접수가 없어 이번 회의에서 논의되지 않음.

07.03 Digital signature schemes giving message recovery Part 4 : Discrete logarithm based mechanisms

DSM3 *IS 9796-3 (2000-1st ed.)*는 2003년 재심 예정으로 이번 회의에서는 논의되지 않음.

08.01 Digital signature with appendix - Part 1: General

DSA1 IS 14888-1 (1998-1st ed., 2000-corrected)은 2003년 재심 예정으로 이번 회의에서는 논의되지 않음.

08.02 Digital signature with appendix - Part 2: Identity-based mechanisms

DSA2 IS 14888-2 (2000-1st ed.)는 2003년 재심 예정으로 이번 회의에서는 논의되지 않음.

08.03 Digital signature with appendix - Part 3: Certificate-based mechanisms

DSA3 IS 14888-3(1998- 1st ed., 2000-corrected)는 2003년 재심 예정으로 이번 회의에서 논의되지 않음.

09.01 Hash-functions Part 1: General

HF1 IS 10118-1 (1994-1st ed., 2000-2nd ed.)는 2003년 재심 예정으로 이번 회의에서 논의되지 않음.

09.02 Hash-functions Part2 : Hash-functions using an n-bit block cipher algorithm

HF2 IS 10118-2 (1994-1st ed., 2000-2nd ed.)는 2003년 재심 예정으로 이번 회의에서 논의되지 않음.

09.03 *Hash-functions Part 3 : Dedicated* hash-functions

HF3 IS 10118-3 (1998-1st ed.)개정.

· 현 표준의 2차 개정안(SC27 N3034)에 대한 이번 회의에서 논의된 각국 편집 의견을 수용하여 이의 수정 결과 문서를 5월 20일까지 editor를 경유 사무국에 송부토록 함(베를린 회의 결의 1(WG2 N472 Draft)).

· 수정된 표준 개정안 문서(SC27 N3193)를 최종 CD로 등록후 투표를 위한 회람을 각 회원국에 송부하기로 함(베를린 회의 결의 7(WG2 N472 Draft)).

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

HF4 IS 10118-4 : (1999-1st ed.) 개정.

· 현 표준의 개정 검토에서 현재의 표준을 그대로 유지 찬성에 4개국, 개정에 2개국(프랑스, 한국(개정 의견에 대한 우리나라의 투표 결과가 투표 처리 과정에서 표현상의 오류임을 인식하여 이를 현 표준의 유지로 찬성하는 것으로 변경함)), 철회 1개국(캐나다)으로 WG2 결의에는 특별한 내용이 없음.

18.02 Key management Part 2 : Mechanisms using symmetric cryptographic techniques

KM2 IS 11770-2 (1996-1st ed., 1st reconfirmation in 1999)는 2002년 재심으로 금번 회의에서 acting editor인 영국 런던대학의 Chris Mitchell에 의해 주재되었음.

가) 검토 문서

- SC27 N3097(CfC for the periodic review of ISO/IEC 11770 Parts 1, 2 and 3)
- SC27 N3159(SoC/tables of replies for the periodic review of ISO/IEC 11770 Parts 1, 2 and 3)
- SC27 N3171(Additional UK expert comments in response to N3097)

나) 주요 토의 사항

· 본 표준의 개정 심의에 대한 각 회원국들의 검토 의견에 대한 투표결과로 현 표준의 유지에 찬성 3개국, 개정 4개국(캐나다, 프랑스, 독일, 한국)이었으나, 개정 의견에 대한 우리나라의 투표 결과가 투표 처리 과정에서 표현상의 오류임을 인식하여 이를 현 표준의 유지로 찬성하는 것으로 변경함으로 현 표준을 그대로 유지하는 것의 찬성은 4개국으로 됨.

· 본 표준의 개정을 위한 다음과 같은 캐나다의 의견에 대하여 본 과제의 회의에서는 개정 사유가 불분명하여 상세한 개정사유들이 각 회원국들로부터 제시될 경우 다음회의에서 논의하기로 함.

- 현 표준에서 어떤 측면이 구체적으로 규정됨이 바람직함에도 특정 메커니즘들이 여러 가지의 프로토콜의 범주에 포함되도록 설계되어 정확

한 메시지 포맷을 규정하기가 불가능하다. 표준은 광범위한 범주의 응용 프로토콜 개발자들에게 사용될 수 있도록 하여야 한다.

- 회의를 통하여 특정 메커니즘이 안전하지 못함이 알려지든지 혹은 의심이 감이 밝혀지면 그 메커니즘은 반드시 삭제되어야 한다.

다) 문서의 조치: 회원국들의 기고를 9월 15일까지 요청하기로 함(베를린 회의 결의 9(WG2 N472 Draft)).

18.03 Key management Part 3 : Mechanisms using asymmetric techniques

KM3 IS 11770-3 (1999-1st ed.)는 2002년 재심으로 금번 회의에서 acting editor인 영국 런던대학의 Chris Mitchell에 의해 주재되었음.

가) 검토 문서 : 과제번호 18.02(IS 11770-2)와 동일.

나) 주요 토의 사항

· 본 표준의 개정 심의에 대한 각 회원국들의 검토 의견에 대한 투표결과로 현 표준의 유지에 찬성 2개국, 개정에 5개국(캐나다, 프랑스, 독일, 한국, 영국)이었으나, 개정 의견에 대한 우리나라의 투표처리는 과제번호 18.02(IS 11770-2)와 동일하게 찬성으로 정정 처리함으로써 현 표준을 그대로 유지하는 것으로의 찬성 투표는 3개국으로 됨.

· 본 표준의 개정에 대한 각 국의 의견은 다음과 같음.

- 프로토콜 설계 시 최근의 개발 결과를 반영할 수 있는 메커니즘의 추가(예, IPsec/IKE, SSL/TSL, ...).
- (ISO/IEC 15946-4에 기 표준화된 메커니즘에 기반하는) 두 가지 새로운 메커니즘 추가.
- 기존의 표준화된 메커니즘에 대한 보다 이론적인 두 가지 공격법의 취급.
- 메커니즘의 속성에 대한 좀 더 많은 지침의 제공.
- "informative" 자료의 "normative"화와 메커니즘의 어떤 측면을 좀 더 구체화시킬 것.

· 본 과제 회의에서는 개정 사유가 불분명하여 상세한 개정사유들이 각 회원국들로부터 제시될 경우 다음회의에서 논의하기로 함.

다) 문서의 조치: 회원국들의 기고를 9월 15일까지 요청하기로 함(베를린 회의 결의 9(WG2 N472 Draft)).

23 Data processing check character systems

CCS ISO/IEC 7064 2차 개정 표준의 발간을 준비중에 있어 이번 회의에서 논의되지 않음.

26.01 Cryptographic techniques based on elliptic curves Part 1 : General

EC1 ISO/IEC 15946-1 제정 표준의 발간을 준비중에 있어 이번 회의에서 논의되지 않음.

26.02 Cryptographic techniques based on elliptic curves Part 2 : Digital Signatures

EC2 ISO/IEC 15946-2 제정 표준의 발간을 준비중에 있어 이번 회의에서 논의되지 않음.

26.03 Cryptographic techniques based on elliptic curves Part 3 : Key establishment

EC3 ISO/IEC 15946-3 제정 표준의 발간을 준비중에 있어 이번 회의에서 논의되지 않음.

26.04 Cryptographic techniques based on elliptic curves Part4: Digital Signatures with Message Recovery

EC4

· 현 CD 표준안(SC27 N3036)에 대한 각국의 편집 의견을 수용하여 이의 수정 결과 문서를 5월 20일까지 editor를 경유 사무국에 송부토록 함(베를린 회의 결의 1(WG2 N472 Draft)).

· 수정된 표준안 문서(SC27 N3195)를 최종 CD로 등록 후 투표를 위한 회람을 각 회원국에 송부하기로 함(베를린 회의 결의 7(WG2 N472 Draft)).

27.01 Time Stamping Services - Part 1 : Framework

TSS1 (SC27 N3038 FDIS 18014-1) 해당 Part에 대한 회의는 최종 DIS투표 추진으로 개최되지 않았음.

27.02 Time Stamping Services - Part 2 : Mechanisms producing independent tokens

TSS2

가) 검토 문서

- SC27 N3196 (Text for FDIS 18014-2)
- SC27 N3147rev1 (Disposition of comments report on 18014-2)

나) 주요 토의 사항

· 본 회의에서는 Final CD에 대한 voting 요청에 대한 comment 문서를 가지고 회의가 진행되었음.

· 본 문서에 대해 comment를 보낸 NB는 Canada, Germany, Japan, Poland, Switzerland, UK, US의 7개 comment가 있었으며, 폴란드의 comment를 제외한 모든 comment들은 평이한 comment였음.

다) 문서의 조치

· Editor는 5월 20일까지 해당 문서를 업데이트하기로 함(베를린 회의 결의 1(WG2 N472 Draft)).

· WG2에서는 part 2 문서를 FDIS로 진행시키는 것을 승인하였으며, 그에 따른 투표절차의 진행을 위해 해당 문서를 ITTF에 제출할 것을 Secretariat에게 요청함(베를린 회의 결의 8(WG2 N472 Draft)).

27.03 Time Stamping Services - Part 3 : Mechanisms producing linked tokens

TSS3

가) 검토 문서

- SC27 N3042 (Text for 1st CD 18014-3)
- SC27 N3148 (NB Comment on the text for 1st CD18014-3)
- SC27 N3173 (NB comment on the text for CD 18014-3)
- SC27 N3106 (Expert comment on the text for CD 18014-3)

나) 주요 토의 사항

· Part 3에 대한 회의는 한국을 비롯한 Japan, Netherlands, UK 및 Estonia가 comment를 제출하였음.

· Japan와 UK의 comment는 모두 editorial로 채택되었으며, Netherlands comment는 NB가 참석하지 않은 채로 진행되었으며 1개를 제외한 모든 comment가 거절되었음.

· 한국의 comment는 technical comment4와 5를 제외한 나머지는 accept 됨. Technical comment 1의 경우에는 기존 데이터 항목의 정의를 정확하게 표현할 수 있도록 수정하자는 내용이었으며, 이에 대해 에스토니아 NB의 반대도 있었으나, 사전에 작성한 구조체들간의 연관표와 관련 구문 지적으로 채택되었음. Technical comment2와 3의 경우에는 현재 해당 구조체에 대한 ASN.1 OID가 정의되지 않았기 때문에 이에 대한 정의가 이루어지면 해당 구조체에 반영키로 함. 그리고, technical comment 7번은 IETF spec과 관련하여 해당 필드 값의 의미1개를 수정하자는 내용이었는데, 본 문서가 Part 3이고 Part 1에서 일반적인 사항을 기술하고 있기 때문에 해당 내용을 Part 1의 annex에서 반영한 후에 Part 3에서 해당 부분을 인용하여 쓰기로 함. 현재 Part 1은 Final DIS이기는 하나 해당 내용이 단순한 comment이기 때문에 표준문서의 진척상황에는 지장이 없을 것으로 판단됨.

· 본 회의에서 문제가 된 comment는 에스토니아 comment이다. 그 중에서 특히 전자서명된 타임스탬프 토큰이 aggregation 서비스를 사용하는 경우 이에 대해 클라이어트가 어떻게 검증할 수 있느냐, 이를 위해 aggregation 서비스를 검증할 수 있도록 새로운 구조체 정의 및 프로세스를 제안 (결국 별도의 프로토콜 제안)하였음. 그러나, 이에 대해 editor의 반대 의견이 상대적으로 강하였음. 대부분의 표면상의 이유는 표준의 진행 상태와 에스토니아가 제안하는 부분은 Part 1에서 기술되어야 하는데, Part 1 문서의 상태가 FDIS이기 때문에 반영하기 어렵다는 editor의 의견이었고, 해당 부분의 논의 시간이 상대적으로 길고 Part 2에 대한 회의를 해야 했기 때문에 Part 1editor의 중재로 에스토니아 comment를 포함한 수정된 Part 3 문서를 회의 참석자들에게 e-mail로 보내어 각국의 의사표현을 하도록 함.

다) 문서의 추진

· Editor는 5월 20일까지 해당 문서를 업데이트를 하기로 함(베를린 회의 결의 1(WG2 N472 Draft)).

33.01 Encryption algorithms Part 1 : General

Encl

가) 검토 문서

- SC27 N3046(Text of 3rd WD 18033-1)

- SC27 N3129(SoC on 3rd WD 18033-1)
- SC27 N3133 (Late NB contributions on 3rd WD 18033-1)

나) 주요 토의 사항

Editor 인 영국 런던대학의 Chris Mitchell 에 의해 제안된 "Agenda for Berlin WG2 meeting on WD 18033-1"을 중심으로 논의하였음. 이의 주요 토의 결과로는,

· 본 표준의 Annex A(informative)에 대한 캐나다 측의 normative로의 변경 주장에 대하여 현재의 상태(informative)로도 적절하다는 각 회원국들의 입장으로 이에 대한 캐나다의 의견을 철회하고 캐나다의 입장을 반영하는 수정안을 제시하면 다음회의(바르샤바 회의)에서 논의하기로 함.

· 용어의 정의에서 지금까지 사용해 온 asymmetric (혹은 symmetric) encryption algorithm 과 *encryption algorithm*을 삭제하고 그 대신 encipherment(혹은 decipherment) system을 암·복호화의 기본 정의로 하고 이의 대안적 정의로 encryption(혹은 decryption) algorithm과 encipherment(혹은 decipherment) system을 사용하여 하기로 함. 또한 표준안 본문의 모든 곳에서 'encryption algorithm'과 'encipherment algorithm'을 모두 'cipher'로 변경하기로 함.

다) 문서의 추진 : 1st CD(베를린 회의 결의 5 (WG2 N472 Draft)).

33.02 Encryption algorithms Part 2 : Asymmetric ciphers

Enc2

가) 검토 문서

- SC27 N3048(Text of 2nd WD 18033-2)
- SC27 N3104(Expert contribution on 2nd WD 18033-2)
- SC27 N3105(Belgian NB comments on 2nd WD 18033-2)
- SC27 N3154(NB comments on 2nd WD 18033-2)
- SC27 N3155(Expert contribution on HIME(R) for 2nd WD 18033-2)

나) 주요 토의 사항

Editor인 스위스 IBM의 Victor Shoup에 의해 제안된 "ISO/IEC WD 18033-2 Berlin Meeting"을 중심으로 논의하였음. 이의 주요 토의 결과로는,

· 영국측에서 용어의 사용에 대한 통일된 기준마련이 필요함을 제안. 현재의 검토문서(N3048)에는 기존의 SC27 표준문서에서 사용하지 않는 용어를 사용하고 있음. 이에 대한 논의 결과 비대칭 암호와 관련이 있는 문서들인 ISO/IEC 14888-1, ISO/IEC 14888-2, ISO/IEC 14888-3, ISO/IEC 11770-3, ISO/IEC 9798-3을 검토하여 용어의 사용을 통일하기로 함.

· 영국과 벨기에측에서 표준문서에 사용된 용어에 대한 정의를 더욱 명확히 할 필요성이 있음을 지적함. 특히 영국은 필요성을 제안하면서 용어에 대한 정의까지 제안. 이에 대한 논의결과 영국에서 제안한 대부분의 정의를 수용하기로 함.

다) 문서의 추진 : 4th WD(베를린 회의 결의 5(WG2 N472 Draft)).

33.03 Encryption algorithms Part 3 : Block ciphers

Enc3

가) 검토 문서

- SC27 N3050(Text of 3rd WD 18033-3)
- SC27 N3123(Late Canadian NB contribution)
- SC27 N3156(SoC on 3rd WD 18033-3)

나) 주요 토의 사항

Editor인 일본 미쓰비시의 Takeshi Chikazawa 에 의해 제안된 "ISO/IEC WD 18033-3 Berlin Meeting"을 중심으로 논의하였음. 이의 주요 토의 결과로는,

· 독일측에서 각 블록 크기에 대하여 한 개의 알고리즘만을 표준안에 수용하기로 하자는 의견에 대하여, 지난 서울회의(2001. 10)에서 18033-1의 부기에 있는 기준을 만족하는 제안 알고리즘을 모두 수용하기로 함을 고지함.

· 캐나다측에서 본 표준안에 수용된 제안 알고리즘들에 대한 특성 테이블을 만들어 이를 이용하는 사용자들의 편의를 도모하자는 의견에 대하여 이를 editor가 준비하기로 함. 또한, CAST-128을 본 표준안에 수용해 줄 것을 요구하였으나 공인 평가 결과의 부족, 여러 형태(버전)의 규격 등으로 인하여 현재 표준안에의 수용이 어렵고 다음회의까지 이에 대한 평가 결과와 명확한 규격의 제안이 있을 경우 논의하기로 함.

· SEED에 대한 벨기에와 독일측에서의 공인

평가 결과의 불만족으로 현 표준안에서의 배제하자는 의견에 대하여 한국측에서 이를 위한 증거로서 자기 평가인 SC27 N2656r1(n2656_3.zip(ATT. 3= Korean contribution))을 동경회의 기고로서 기 제출하였으며 3자 평가로서 CRYPTREC으로부터 실시한 평가결과가 접근가능함을 제시함. 아울러 이 결과를 SC27 N3213(Third Party Evaluation on SEED by CRYPTREC, 2002-04-23)을 회의 현장에서 제출함.

- 이에 대하여 논의 결과 4th WD(SC27 N3210)에 계속 수용토록 함. 그러나, WG2 전체 회의 결의에서 각 회원국의 작업문서에 대한 의견 회람시 "including a note on the cover sheet of the ballot requesting National Bodies to conduct a detailed evaluation on the SEED algorithm"을 포함하여 처리하기로 함. (베를린 회의 결의 4(WG2 N472 Draft))
- SEED에 대한 그 밖의 각국 편집 의견을 수용하여 이의 수정 결과를 5월 20일까지 editor를 경유 사무국에 송부토록 함.(베를린 회의 결의 1(WG2 N472 Draft))

· RC6에 대하여는 현 작업문서에는 가변 블록으로 제안이 되어 이의 처리를 별도로 할 것인가에 대한 논의 결과 일단 128비트로 처리(현재 NESSIE에의 제안에는 128비트로 제안)하기로 함.

· Khazad(64비트, 벨기에와 브라질이 공동 개발하여 벨기에 제안)에 대한 벨기에로부터 현 작업문서에의 수용 의견에 대하여 NESSIE의 결과를 가을 회의까지 확인될 수 있으므로 다음회의에서 논의하기로 함.

· 현재 작업문서에 수용된 블록 알고리즘(TDEA, MYSTY(이상 64비트), AES, Camellia, SEED, RC6(이상 128비트))과 비대칭 알고리즘에 대하여 NESSIE와 CRYPTREC에 평가 결과의 요약보고서를 2002년 9월말까지 받고 이를 다음 바르샤바 회의에서 발표토록 의뢰함.(베를린 회의 결의 9(WG2 N472 Draft))

다) 문서의 추진 : 4th WD(베를린 회의 결의 5(WG2 N472 Draft)).

33.04 Encryption algorithms Part 4 : Stream ciphers

Enc4

가) 검토 문서

- SC27 N3053(Text of 2nd WD 18033-4)
- Attachment of SC27 N3053(Editor's report on Revision history for WD 18033-4(from 1st WD N2922 to 2nd WD N3053)
- SC27 N2922(Text of 1st WD 18033-4)
- SC27 N3086(CfC for project 1.27.33.04(18033-4)-Encryption algorithm-Part 4 : Stream cipher)
- SC27 N3044(CD 18031 Random bit generation)
- SC27 N3127(SoC to 18031)

나) 주요 토의 사항

Editor인 일본 구주대학의 Kouichi Sakurai에 의해 제의된 "Agenda for WG2-meeting @ Berlin on WD 18033-4 Stream ciphers"에 의해 논의된 주요 토의결과로,

· 독일 측에서 제안하여 CD 10116에 수용된 Statistical Self-Synchronous Model에 대한 평가 결과가 아직 없어 이를 현재의 작업문서에 바로 수용이 어려우며(벨지움 측) 평가 기관 또는 평가 결과에 의해 계속 검토하기로 함. 또한 독일 측의 이의 검토 결과를 제출하여 차기 회의에서 검토하기로 함(베를린 회의 결의 6(WG2 N472 Draft)과 연계됨).

· 지금까지 키 스트림 생성을 위한 전용 알고리즘으로 제안된 것이 없음. NESSIE에 key-stream generator로 제안된 BMGL을 현 작업문서에의 수용을 검토한 바, 이는 AES에 비하여 16배정도 느린 것으로 보고됨(NESSIE deliverable 참조). 일단, 제안국인 스웨덴측에서 좀더 보완하여 제안하기로 함.

· Panama : CRYPTREC의 평가 결과 안전성에 문제는 없음. 3rd WD에 계속 수용 유지.

다) 문서의 조치 : 3rd WD로 차기 회의에서 검토하기로 함(베를린 회의 결의 4(WG2 N472 Draft)).

Ⅳ 신규과제에 대한 논의

- 영국 BSI에서 Key Establish mechanism based on weak secrets(password based

key management)에 대한 신규과제를 제안(SC27 N3135)하여 향후 투표로 결정.
- 신규과제로의 채택시 Key Management Part-4로 추진 예정.

- Germany에서 Data encapsualation mechanisms에 대한 신규 과제 제안 (SC27 N3160, 2002-04-09).

- SC27 N3154(NB comments on 2nd WD 18033-2(SC27 N3048) Encryption algorithms-Part 2: Asymmetric cipher)의 논의 중 US comments 중 AES key wrapping algorithm에 대한 신규과제를 미국측으로부터 제안 예정.

- 생체 인식에 대한 과제는 새로운 WG에서 할지 혹은 일반 과제로 할 것인지에 대하여 계속 논의.

V. 소감 및 결론

이번 회의에서 우리나라는 128비트 블록 암호 알고리즘의 국제 표준화를 위하여 제안한 SEED에 대하여 회의 당시 문서는 3차 작업문서에 포함된 미국의 AES, 일본의 Camellia, 스웨덴의 RC6에 대한 논의 결과 우리의 제안 알고리즘에 대한 인식이 그 동안 회의 참여가 소홀했던 독일과 벨기에측으로부터 평가 결과에 대한 자료 불충분을 제기하였다. 이에 대한 우리의 대응으로 자기 평가인 SC27 N2656r1(n2656_3.zip(ATT. 3= Korean contribution))을 동경회의 기고로서 기 제출하였으며 제3자 공인 평가로서 CRYPTREC으로부터 평가결과인 SC27 N3213(Third Party Evaluation on SEED by CRYPTREC, 2002-04-23)을 회의 현장에서 제출하여 회의에 참여한 독일측 대표의 이해를 구하였다.

그리고, 이에 대한 논의 결과 4차 작업문서(4th WD, SC27 N3210)에 SEED를 계속 수용하기로 하였다. 그러나, WG2 전체 회의 결의에서 각 회원국의 작업문서에 대한 의견 회람시 "including a note on the cover sheet of the ballot requesting National Bodies to conduct a detailed evaluation on the SEED algorithm"을 포함하여 처리하기로 하였다.

결과적으로, 이번 회의에서는 SEED에 대한 유럽의 관심을 불러 일으켰으며 유럽을 비롯한 회원국들의 평가결과가 차기 바르샤바회의에서 본격적으로 논의될 것으로 예상되며, 이를 위하여 현재 한국정보보호진흥원에서 관리하고 있는 SEED 홈페이지의 자료를 모두 영문화하여 현행화 시켜 운영하고 있다.

또한, 신규 과제와 관련하여 영국에서 제안한 패스워드 기반의 키설정 프로토콜에 관한 것을 IEEE 및 국내 암호학자들이 많은 관심을 갖고 있어 이의 국제 표준화에 대한 준비가 필요할 것으로 사료된다. 이를 위하여 먼저 이에 대한 국내 표준화에 대한 논의를 조기에 마무리하고 이를 산업표준화는 물론 국가 표준화 수준으로 조속히 정리하여 이것도 국제 표준화의 후보 알고리즘으로 제안함이 바람직할 것으로 생각된다.

한편, 이번 회의에서의 표준 개정 문서처리(실체 인증, 키관리)의 착오에 따른 번복 등의 해프닝이 있어 향후 이와 같은 상황의 재연이 없었으면 한다. 이를 방지하기 위하여 국내의 문서 창구부서에서는 해당 국제 표준의 문서 처리 과정 중 특히, 4년 주기의 표준 개정에 대한 심의 결과를 해당 사무국으로 회신을 보낼 경우 Confirmation(표준 문서를 그대로 유지), Revision(표준 문서의 개정, 이 경우 사유 의견 반드시 첨부), Withdrawal(해당 표준 문서의 폐기, 이 경우 사유 의견 반드시 첨부) 그리고 Abstain(기권) 중 하나를 정하여 우리나라의 의견을 회신하여야 한다.

마지막으로 이번 출장을 배려하여 주신 산업자원부와 한국표준협회 관계자 여러분들에게 감사를 드리고 이번 회의에 동참하여 많은 조언과 도움을 주신 산업표준원 이경석 박사에게 감사를 드립니다.

〈著者紹介〉

장 청 룡 (Chung-ryong Jang)
종신회원
1980년 2월 : 성균관대학교 전자공학과 졸업
1986년 8월 : 연세대학교 대학원 전자공학과 석사
1994년 2월 : 성균관대학교 대학원 정보공학과 박사
1979년 12월~1983년 12월 : 한국전자통신기술연구소, 연구원

1984년 1월~1997년 1월 : 한국통신 연구개발본부 선임연구원
1997년 3월~현재 : 경동대학교 정보보통신공학부 부교수
관심분야 : 보안제품 시험, 통신망 보호, 블록암호

천 동 현 (Donghyeon Cheon)
1995년 2월 : 고려대학교 수학과 이학사
1997년 8월 : 고려대학교 대학원 수학과 이학석사
2001년 2월 : 고려대학교 대학원 수학과 이학박사
1999년 9월~2001년 8월 : 고려대학교 기초과학연구소 연구원
2001년 9월~현재 : 한국정보보호진흥원 암호기술팀 선임연구원
관심분야 : 암호학, 정보보호

강 경 희 (Kang Kyung Hee)
1991년 2월 : 한국외국어대학교 경영정보학과
1993년 2월 : 한국외국어대학교 경영정보학과 석사
1993년 3월~현재 : 한국통신 멀티미디어 연구소 선임연구원
관심분야 : PKI기반의 응용서비스 개발

차 재 현 (Jae-hyeon Cha)
1985년 2월 : 한양대학교 전자계산학과 석사
2002년 2월 : 숭실대학교 컴퓨터학과 공학박사
1982년~현재 : 산업자원부 기술표준원 보안기술담당관