정 보 보 호 학 회 지
제 25 권 제 4 호, 2015. 8

SC27/WG2에서의 디지털서명과 실체 인증 표준 소개

이 필 중*

요 약

ISO/IEC JTC1/SC27/WG2 (Information technology — Security techniques — Cryptography & Security Mechanisms, 이하 줄여서 'SC27/WG2'로 표시)은 암호학을 중심으로 기술적인 정보보호 기법들을 표준화하는 기구이며, 그 역사 및 상세 소개는 같은 호에 송정환 교수가 할 것으로 알고, 본인은 SC27/WG2에서 다루는 디지털서명과 실체 인증에 관한 표준들에 대해 모든 내용을 구체적으로 소개하는 것 보다는 기법의 분류 및 찾아 볼 수 있도록 참고문헌을 소개하겠다.

Ⅰ. 디지털서명

디지털서명(digital signature, 이하 줄여서 '서명')은 서명자(signer)를 확인하고 서명자가 전자문서(이하 메시지, message)에 서명하였음을 나타나게 할 목적으로, 종이문서에 대한 도장이나 수(手)서명 하듯이, 메시지의 내용이나 그 요약(hash값)과 서명자만이 갖고 있는 서명키(signature key, 비공개키(private key)라고도 함)를 이용하여 만드는 디지털 정보이다.

'서명된 메시지(signed message)'란 서명과 해당 메시지(전부 또는 일부가 전달될 필요 없을 경우도 있음)을 붙인 것을 말한다.

검증자(verifier)는 서명된 메시지와 누구나 알 수 있는 서명자의 검증키(verification key, 공개키(public key)라고도 함)로 검증과정을 거쳐, 그 서명자가 그 메시지의 내용에 대한 서명했다는 (즉, 위조나 변조가 아니라는) 사실을 확인한다.

서명은 검증과정 도중에 서명으로부터 메시지 전체 혹은 일부를 복원하는 '메시지 복원형 서명(Digital signature schemes giving message recovery)'과 전혀 복원이 되지 않아 서명을 전체의 메시지에 첨부하는 형태로 보내야 하는 '메시지 부가형 서명(Digital signature with appendix)'로 나눌 수 있다.

전자의 경우의 서명된 메시지는 서명만으로 구성되거나 혹은 서명과 복구되지 않는 메시지로 구성되고 ISO/IEC (이하 줄여서 'IS') 9796으로 표준화되어 있고, 후자의 경우는 서명된 메시지는 서명과 메시지 전체로 구성되어 있고 IS 14888로 표준화되어 있다.

또한 어느 그룹(group)에 속해 있는 서명자가 자신의 서명키로 서명을 하되, 검증자는 그룹키(group key) 혹은 특정한 여러 개의 검증키 모두를 사용하여 검증함으로써, 누구인지는 모르나 그룹에 속해 있는 서명자이거나 여러 개의 검증키 중 하나에 해당하는 서명키를 갖고 있는 서명자가 서명했음을 확인할 수 있다. 이렇게 서명자 개인의 익명성은 보장될 수 있는 서명 방식을 '익명 서명(Anonymous digital signatures)'이라 하고, IS 20008로 표준화되어 있다. 검증자는 그 그룹에 속해 있는 서명자이거나, 특정한 여러 개의 공개키 중 어떤 하나에 관계된 서명키를 갖고 있는 서명자가 서명했음을 확인할 수 있다.

그리고 원하는 메시지에 대한 서명을 받기를 원하는 '요청자(requestor)'가 서명자를 지정해서 서명을 받되 서명자는 메시지의 내용을 알지 못하고 서명키를 사용하여 만드는 서명을 '은닉 서명(Blind digital signatures)이라고 하고, IS 18370로 표준화되고 있다. 서명된 메시지를 받은 검증자는 서명자의 검증키를 사용하여 서명자가 요청자에 의해 제공된 메시지에 서명했음을 확인할 수 있다. 전자투표나 전자화폐에서 이용될 수 있다.

본 연구는 미래창조과학부 및 정보통신기술진흥센터의 대학ICT연구센터육성 지원사업의 연구결과로 수행되었음" (IITP-2015-H8501-15-1003)
포항공과대학교 전자전기공학과 (pjl@postech.ac.kr)

<IS 9796> 메시지 복원형 서명 - 덧붙임을 이용한 기법 (Digital signature schemes giving message recovery – Part 1: Mechanisms using redundancy)

(내용) 메시지에 정해진 덧붙임(redundancy)을 추가해서 RSA 서명[RSA78]을 하는 기법을 표준화했다.

(역사) 초판(1st edition)의 편집자(editor)는 확인되지 않으나 1991-09-19에 발간되었다. 그 후 다른 부(part)들이 생기면서, L. Guillou(FR)가 편집자가 되어 IS 9796에서 IS 9796-1로 표준번호도 바꾸고 내용을 보강하려고 하던 중 심각한 공격방법[CNS99]이 발표됨에 따라 1999-10-06에 문서번호 IS JTC1/SC27 N2424로 (IS JTC1/SC27은 생략 하겠음) 본 표준을 철회(withdrawal)를 결정하고, 2000-07-27에 N2636으로 철회를 발표했다.

(현황) 철회된 상태

<IS 9796-2> 메시지 복원형 서명 - 2부: 정수 소인수분해의 어려움에 기반한 기법 (Digital signature schemes giving message recovery – Part 2: Integer factorization based methods)

(내용) 큰 정수의 소인수분해의 어려움에 기반한 3개의 메시지 복원형 서명 기법을 표준화했다. 그 중 2개는 결정론적인(deterministic, 즉 주어진 메시지에 대해 항상 동일한 서명을 주는) 기법이고, 다른 1개는 무작위적(randomized, 즉 같은 메시지라도 서명이 높은 확률로 거의 항상 변하는) 기법이며, 모두 완전(total) 메시지 복원을 줄 수도 있고, 부분(partial) 메시지 복원을 줄 수도 있다.

1. 기법 1 — IS 9796에 의해 이미 구현되어 사용되고 있는 제품들과의 역방향호환(backward compatibility)을 위해 표준화된 기법으로, 공격자가 선택한 메시지를 많이 얻을 수 있는 환경에서는 사용하지 말 것을 권고하고 있다.

2. 기법 2 — [P1363a]에서 IFSSR(Integer Factorization Signature Scheme with Recovery)라고 규정해 놓은 것과 호환(compatible)되는 무작위적인 기법이며, [BR96]에서 PSS-R(Probabilistic Signature Scheme - Recovery)을 수정한 것이다.

3. 기법 3 — 기법 2에서 무작위적 솔트(salt)의 자리에 서명자가 지정한 고정된 값을 넣는 결정론적인 기법이다.

(역사) 1997-08-28에 초판, 2002-10-01에 재판, 2010-12-15에 3판이 발간되었다. 초판은 M. Girault(FR)가, C. Mitchell(GB)이 재판과 3편의 편집자였다. 재판의 중간까지는 본 부의 제목이 해시함수를 이용한 기법(Mechanisms using a hash-function)이었으나 본 표준의 3부가 만들어지면서 본 부의 제목을 현재와 같이 수정하였다. 재판의 내용은 FDIS N3032에서, 3부는 FDIS N8979에서 확인할 수 있다. (각 편집자의 뒤에 2자는 ISO 3166-1 alpha-2의 국가코드이다.)

(현황) 지난 최종 정기검토는 2013년 이었고, 2013-04-26에 유지하기로 결정(N12710) 되었다. 2016년에 다음 검토가 계획되어 있다.

<IS 9796-3> 메시지 복원형 서명 - 이산 대수의 어려움에 기반한 기법 (Digital signature schemes giving message recovery – Part 3: Discrete logarithm based methods)

(내용) 1개의 정수에서 이산대수 문제가 어렵다는 것에 기반한 기법과, 5개의 타원곡선 상에서의 이산대수 문제가 어렵다는 것에 기반한 기법들을 표준화했다.

1. NR — Nyberg와 Rueppel의 [NR96]에서 가져온 것이다.

2. ECNR — NR기법을 타원곡선(elliptic curve)형태로 바꾼 것이다.

3. ECMR — Miyaji 의 [Miy97]에서 가져온 것이다.

4. ECAO — Abe와 Okamoto의 [AO99]에서 가져온 것이다.

5. ECPV — Pintsov와 Vanstone의 [PV00]에서 가져온 것이다.

6. ECKNR — ECKCDSA를 NR기법과 유사하게 변환시켜 것으로 [LL98]을 참고하여 만든 [YSL02]에서 가져온 것이다.

(역사) 1997년 K. Nyberg(FI)가 편집자가 되어 시작했고 NR기법만 포함하여2000-04-15에 초판(FDIS N2299)이 발간되었다. 처음에는 과제번호가 9796-4였다가, 1996년 L. Guillou(FR)가 편집자가 되어 시작했던 9796-3 확인함수를 이용한 기법(Mechanisms using a check function)이 N1622에서 지적된 약점으로 폐기됨에 따라, 과제번호를 9796-3로 바꿨다.

한편 당시 새로운 개념이었던 타원곡선 기반 암호 기술(Cryptographic techniques based on elliptic curves)

을 IS 15946로 표준화하자는 시도가 1998년 시작되었는데 1부 - 일반(General), 2부 – 서명(Digital Signatures), 3부 – 키 설립(Key establishment)으로 시작했다가, 2000년 추가로 4부 복원형 서명(Digital Signatures with Message Recovery)도 시작되어 A. Miyaji(JP)가 편집자가 되어 2004-10-01에 위의 5가지 EC기법을 규정하는 초판(N3743)이 발간되었다가, IS 9796-3의 재판이 출판되면서 2007-11-16에 폐기되었다.

IS 9796-3은 2003년 수정이 결정되어 A. Miyaji(JP)가 편집자가 되어 IS 9796-3의 초판과 IS 15946의 초판에 있는 기법들을 합쳐서 IS 9796-3의 재판(FDIS N5202)이 2006-09-15에 발간되었다.

(현황) 지난 최종 정기검토는 2014년 이었고, 2014-04-11에 유지하기로 결정(N13967) 되었다. 2017년에 다음 검토가 계획되어 있다.

<IS 14888-1> 부가형 서명 - 일반 (Digital signature with appendix – Part 1: General)

(내용) 부가형 서명의 일반 개념, 용어, 모델, 요구사항 등을 설명하고, 2부와 3부에서 다룰 내용에 대한 소개를 하였다.

(역사) 1995년 K. Nyberg(FI)가 편집자가 되어 시작했고(1995년 10월 서울회의에서는 본인이 acting editor를 맡았었음) 1998-12-20에 초판(N2027)이 발간되었다. 2부와 3부의 제목과 내용이 변경됨에 따라 2003년 A. Otsuka(JP)가 편집자가 되어 개정이 시작되었고, 2008-04-15에 재판(N5422)이 발간되었다.

(현황) 지난 최종 정기검토는 2013년 이었고, 2013-10-25에 유지하기로 결정(N13266) 되었다. 2016년에 다음 정기검토가 계획되어 있다.

<IS 14888-2> 부가형 서명 - 정수 소인수분해의 어려움에 기반한 기법 (Digital signature with appendix – Part 2: Integer factorization based mechanisms)

(내용) 큰 정수의 소인수분해의 어려움에 기반한 기법들을 표준화했다.

1. RSA, RW — RSA는 [RSA78]에서, RW는 [Rab79]과 [Wil84]에서 가져온 것이다.

2. GQ1 — Guillou & Quisquater의 [GQ88c]와 [GQ88e]에서 가져온 것이다.

3. GQ2 — Guillou, Ugon와 Quisquater의 [GUQ01]에서 가져온 것이다.

4. GPS1 — Girault [Gir92] 와 Poupard & Stern [PS98]에서 가져온 것이다.

5. GPS2 — Girault & Paillès [GP03]에서 가져온 것이다.

6. ESIGN — Fujioka, Okamoto and Miyaguchi [FOS92]에서 가져온 것이다.

(역사) 1995년 ID기반 기법(Identity-based mechanisms)이란 제목으로 K. Nyberg(FI)가 편집자가 되어 시작했으나 (1995년 10월 서울회의에서는 본인이 acting editor를 맡았었음) 곧 M. Chawrun으로 편집자가 바뀌어 1999-12-16에 2부의 초판(N2028)을 발간했다. 여기에는 GQ1과 그 변형, GPS1이 표준화되어 있었다. 2003년 개편이 결정되면서 제목과 내용에 대해 많은 토론 후 본 부의 제목을 현재와 같이 수정하였고, L. Guillou(FR)가 편집자가 되어 2008-04-15에 재판(N5424)을 발간했다. 여기에는 기법 1과 기법6은 IS 14888-3의 초판에서, 기법 2은 IS 14888-2의 초판에서, 그리고 나머지 3기법들은 새로 포함되었다.

(현황) 최종 정기검토는 2013년 이었고, 보안 요구사항이 바뀜에 따라 추천되는 비트의 길이도 길어져야 한다는 의견도 있었지만, 2013-10-25에 유지하기로 결정(N13267)되었다. 2016년에 다음 정기검토가 계획되어 있다. 비트길이가 길어져야 한다는 부분에 대해서는, K. Suzuki(JP)가 편집자가 되어 비트길이의 수정과 그 길이에 맞춘 GPS1의 수치예를 담은 수정본 COR1(N15205)을 만들어 곧 발간될 예정이다.

<IS 14888-3> 부가형 서명 - 이산대수의 어려움에 기반한 기법 (Digital signature with appendix – Part 3: Discrete logarithm based mechanisms)

(내용) 이산대수 문제가 어렵다는 것에 기반한 기법들을 표준화했다. 그 중 10개는 인증서(certificate)를 기반으로 하고 있고 (그 중 4개는 정수 상에서, 다른 6개는 타원곡선(EC) 상에서 구현), 다른 2개는 ID를 기반으로 하고 있다.

1. DSA — (US) Digital Signature Algorithm의 줄인 말이며, [DSS4]에서 가져온 것이다.

2. KCDSA — Korean Certificate-based DSA의 줄인 말이며, [KCDSA3]에서 가져온 것이다.

3. Pointcheval/Valdenay 기법 — Pointcheval와 Vaudenay의 [PV96] 에서 가져온 것이다.

4. SDSA — Schnorr의 [Sch90]에서 가져온 것이다.

5. EC-DSA — [DSS4]와 [ECDSA05] 에서 가져온 것이다.

6. EC-KCDSA — [EC-KCDSA2] 에서 가져온 것이다. 안전성 관련하여 [YL99]가 참조되었다

7. EC-GDSA — EC German DSA의 줄인 말이며, [EP05]에서 가져온 것이다.

8. EC-RDSA — EC Russian DSA의 줄인 말이며, [GOST10]에서 가져온 것이다.

9. EC-SDSA — EC Schnorr DSA의 줄인 말이며, [Sch91]에서 가져온 것이다.

10. EC-FSDSA — EC Full Schnorr DSA의 줄인 말이며, [Sch91]에서 가져온 것이다.

11. IBS-1 — Hess의 [Hes02] 에서 가져온 것이다.

12. BS-2 — Cha & Cheon의 [CC02] 에서 가져온 것이다.

(역사) 1995년 인증서 기반 기법(Certificate-based mechanisms)이란 제목으로 Morris(US)가 편집자가 되어 시작했으나 곧 D. Wallner(US)가 이어 받아 1998-12-20에 3부의 초판(N2030)을 발간했다. 여기의 본문에는 정수 소인수분해의 어려움에 기반한 기법과 이산대수의 어려움에 기반한 기법을 설명하고, 부기에 전자의 예로 RSA[RSA78] 와 ESIGN[FOS92]을, 후자의 예로 DSA[DSS0]를 들었다.

한편 IS 9796-3에서 설명했듯이 IS 15946-2 타원곡선 기반 암호 기술 - 서명(Cryptographic techniques based on elliptic curves - Digital Signatures)가 1998년 시작되었는데 R. Horne(GB)가 편집자가 되어 기법들 5, 6, 7을 포함하여 2002-12-01에 초판(N2555)이 발간되었다가, IS 14777-3의 재판이 출판되면서 2008-01-25에 폐기되었다. 여기에는 [LL98]과 [YL99]가 참조되었다.

2003년 개편이 결정되면서 제목과 내용에 대해 많은 토론 후 본 부의 제목을 현재와 같이 수정하였고, 본인과 L. Chen(GB)가 편집자가 되어 기법들1, 2, 3, 5, 6, 7, 10, 11을 포함하여 2006-11-15에 재판(N5060)을 발간했다.

그 후 사소한 오류들에 본인이 편집자가 되어 2007-09-01에 COR1(N5906)과 2009-02-15 COR2(N6690)를 발간했다.

2007년 RU의 요청으로 A. Chmora(RU)와 A. Lunin(RU)가 편집자가 되어 기법 8을 넣기로 하고 수정(Amendment)을 시작했는데 추후 Schnorr 기법들을 추가하자는 요청이 있어 기법들 4, 9, 10을 포함시켜 2010-06-15에 AMD1(N8181)을 발간했다.

또한 GB가 EC Schnorr 서명에서 y축을 생략해도 안전상의 문제가 없으니 그 option도 넣자고 해서 M. Ward(GB)가 편집자가 되어 2012-07-01에 AMD2(N10693)을 발간했다.

(현황) 2013년 정기검토에서 GB가 IBS에서 R 값이 정수인데 비트열을 내는 해시코드를 직접 사용하는 것이 문제가 있음을 지적하며 관련 수정사항들이 여러 곳 있다는 결함보고(defect report)를 N12260로 냈고, COR도 2개, AMD도 2개이고, 또한 80-비트 이상의 보안강도로 되어 있고, 수치예들도 80-bit security example들이 대부분인데 더 높은 보안강도를 갖는 수치예들을 넣어야 한다고 본인이 의견을 냈다. 그래서 재개정을 하기로 하고 본인과 L. Chen(GB)가 편집자가 되어 1stWD N12561, 2ndWD N13204, 3rdWD N13975, 1stCD가 N14756이어, 2015-07-29에 DIS가 N15419로 나와 투표결과를 기다리는 중이다.

그런데 지난 4월 회의에서 중국은 키-교체(KS, Key Substitution)공격([BM99], [MS04], [BRS06])의 중요성을 강조하며 기존의 기법 중 4개(EC-DSA, EC-GDSA, EC-RDSA and EC-FSDSA)는 KS 공격에 취약점이 있고, 서명에 사용된 Public Key를 메시지에 포함시키면 해결될 수 있다는 점은 본문에 주석으로 추가하기로 했음. (KCDSA와 EC-KCDSA에서는 설계 당시부터 이미 KS 공격이 불가능하도록 검증키를 메시지 앞에 넣어 해시를 하는 방식을 표준으로 했음.) 그리고 자국에서 표준으로 사용되고 있는 SM2와 새로 개발된 IBS를 본 표준에 포함시키자는 의견은 해결이 쉽지 않아서 L. Liu(CN)를 조사위원(rapporteur)으로 하여 이들을 IS 14888-3에 추가할 것인지를 연구하는 기간을 갖기로 했음.

<IS 20008-1> 익명 서명 - 일반 (Anonymous digital signatures – Part 1: General)

(내용) 익명성을 보장하는 서명의 일반 개념, 용어, 모델, 요구사항 등을 설명하였다.

(역사) 2009년 시작된 과제로 L. Chen(GB)가 편집자가 되어 시작했고, 2013-12-15에 초판(N12582)이 발간되었다.

(현황) 2016년에 다음 정기검토가 계획되어 있다.

<IS 20008-2> 익명 서명 - 그룹공개키를 사용하여 검증하는 기법 (Anonymous digital signatures - Part 2: Mechanisms using a group public key)

(내용) 익명성을 보장하기 위해 그룹공개키를 사용하여 검증하는 기법의 보다 상세한 모델과 요구사항을 설명하며, 연결성을 제공하는 기법들(Mechanisms with linking capability) 1 ~ 4, 공개성을 제공하는 기법들(Mechanisms with opening capability) 5& 6, 공개성과 연결성을 모두 제공하는 기법(Mechanisms with both opening and linking capabilities) 7이 규정되어 있다.

1. 기법 1 — List signature scheme로 Canard, Schoenmakers, Stam와 Traoré의 [CSST06] 에서 가져온 것이다.

2. 기법 2 — DAA(직접 익명 입증, Direct Anonymous Attestation)의 기본. Brickell, Camenisch와 Chen의 [BCC05t]와 [BCC05a]에서 가져온 것이다.

3. 기법 3 — DAA에 pairing을 이용 효율을 높인 기법. Brickell와 Li의 [BL10]에서

4. 기법 4 — 보다 효율적으로 DAA. Chen, Page와 Smart의 [CPS10] 에서 가져온 것이다.

5. 기법 5 — Furukawa와 Imai의 [FI06] 에서 가져온 것이다.

6. 기법 6 — Isshiki, Mori, Sako와Teranishi의 [IMSTY06] 에서 가져온 것이다.

7. 기법 7 — Hwang, Lee, Chung, Cho와Nyang의 [HLCCN11]와 [HLCCN13] 에서 가져온 것이다.

(역사) 2009년 시작된 과제로 K. Sako(JP)와 J. Li(US)가 편집자가 되어 시작했고, 2013-11-15에 초판(N12582)이 발간되었다.

(현황) 2016년에 다음 정기검토가 계획되어 있다.

<IS 18370-1> 은닉 서명 - 일반 (Blind digital signatures - Part 1: General)

(내용) 은닉 서명에 대한 일반 개념, 용어, 모델, 요구사항 등을 설명하였다.

(역사) 2010년 J. Traoré(FR)을 조사위원(rapporteur)으로 하여 '은닉 서명'이란 제목의 연구기간(study period)을 갖다가, 2012년 정식으로 시작된 과제로, D. Turner(US)와 J. Traoré(FR)가 편집자가 되어 1stWD N11195, 2ndWD N11824, 3rdWD N12586, 1stCD N14010, 2ndCD N14774를 냈다.

(현황) 2015-06-30에 DIS N15196가 나와 투표 절차를 거치고 있는 중이다.

<IS 18370-3> 은닉 서명 - 이산대수의 어려움에 기반한 기법 (Blind digital signatures - Part 3: Discrete logarithm based mechanisms)

(내용) 익명성을 보장하기 위해 그룹공개키를 사용하여 검증하는 기법의 보다 상세한 모델과 요구사항을 설명하며, 연결성을 제공하는 기법들(Mechanisms with linking capability) 1 ~ 4, 공개성을 제공하는 기법들(Mechanisms with opening capability) 5 & 6, 공개성과 연결성을 모두 제공하는 기법(Mechanisms with both opening and linking capabilities) 7이 규정되어 있다.

1. 기법 1 — 기본적인 은닉서명으로 Okamoto의 [Oka92]에서 가져온 것이다.

2. 기법 2 — 부분 노출이 있는 은닉서명(with partial disclosure)으로 Abe 와 Okamoto 의 [AO00] 에서 가져온 것이다.

3. 기법 3 — 보다 효율적인 부분 노출이 있는 은닉서명으로 Canard, Malville 와 Traoré 의 [CMT08] 에서 가져온 것이다.

4. 기법 4 — 선택적 노출이 있는(with selective disclosure) 은닉서명으로 Brands 의 [Bra00] 에서 가져온 것이다.

5. 기법 5 — 추적이 가능한(traceable) 은닉서명으로 Gaud 와 Traoré 의 [GT03] 에서 가져온 것이다.

(역사) 1부와 같이 시작했고 같은 편집자들이 1stWD N11196, 2ndWD N11826, 3rdWD N12588, 1stCD N14012, DIS-by-editors N14776에 이어 DIS-by-ITTF가 2015-02-19에 N14958로 나왔다.

(현황) 투표 결과가 SoV_DIS N14961로 2015-06-01 나왔는데 반대한 국가는 없었고, JP와 GB만이 의견을 냈고, 다음 10월 IN회의에서 논의될 계획이다.

Ⅱ. 실체 인증 소개

실체 인증(entity authentication, 개체인증이라고 번역되기도 함)은 어떤 실체가 주장하는 신원(identity)을 확인하는 과정을 말한다. 일반적으로 식별 '요구자(requestor)'가 제시하는 증거를 '검증자(verifier)'가 확인하는 데, 그 증거로 그 실체만이 알고 있는 지식이나, 실체만이 갖고 소유물, 실체만의 신체적/행위적 특성을 사용한다.

SC27/WG2에서 표준화하고 있는 실체 인증은 IS 9798에서 다루고 있는데, 주로 실체만이 알고 있는 지식(비밀키(secret key) 혹은 비공개키(private key))를 확인하는 것이고, 가끔 그 실체만이 갖고 있는 소유물(물리적인 토큰)을 확인하는 경우도 있지만, 실체만의 신체적/행위적 특성을 사용하는 경우는 없다.

한편 실체의 신원까지는 필요 없지만, 어떤 그룹에 속해 있는지, 어떤 자격을 갖고 있는지 만을 확인하면 충분한 경우에는, 그렇게 확인하면서 받아들이거나 관련된 서비스를 제공할 수 있다. 이러한 인증을 익명성이 있는 실체 인증(Anonymous Entity authentication, 줄여서 '익명인증')이라고 하고, IS 20009로 표준화되어 있다.

<IS 9798-1> 실체 인증 - 일반 모델 (Entity authentication – Part 1: General model)

(내용) 실체 인증의 일반 개념, 용어, 모델, 요구사항 등을 설명하고, 다음 이어지는 부(part)들에서 다룰 내용에 대한 소개를 하였다.

(역사) 1991-08-29에 초판이 발간되었다. 4부와 5부가 추가됨에 따라 1995년 개정을 결정하였고 L. Nilson(NO)가 편집자가 되어 1997-07-31에 재판을 발간하였다. 2008년 정기검토 시 5부가 추가됨과 그 사이 변화된 참조문서들을 갱신해야 한다는 주장에 개정을 결정(N6664)하고 R. Domingues(ZA) 가 편집자가 되어 2010-07-01에 3판을 발간하였다.

(현황) 최종 정기검토는 2013년 이었고, 2013-04-26에 유지하기로 결정(N12626) 되었다. 2016년에 다음 검토가 계획되어 있다.

<IS 9798-2> 실체 인증 - 대칭형 암호 알고리즘을 이용한 기법 (Entity authentication – Part 2: Mechanisms using symmetric encipherment algorithm)

(내용) 대칭형 암호의 비밀키를 다른 사람을 모르고 요구자와 검증자만 알고 있다고 가정하고, 대칭형 암호 기법을 사용하여 인증하는 방식을 규정했다.

1. 일방인증 - 1회전송 (Unilateral authentication – One pass) — 타임스탬프나 일련번호 사용.

2. 일방인증 - 2회전송 (Unilateral authentication – Two pass) — 난수 사용.

3. 쌍방인증 - 2회전송 (Mutual authentication - Two pass) — 타임스탬프나 일련번호 사용.

4. 쌍방인증 - 3회전송 (Mutual authentication - Three pass) — 난수 사용.

5. TTP포함 기법 - 4회전송 (Mechanism involving a trusted third party - Four pass) — 타임스탬프나 일련번호 사용. ISO/IEC 11770-2(1996)의 기법 8와 같다.

6. TTP포함 기법 - 5회전송 (Mechanism involving a trusted third party - Five pass) — 난수 사용. ISO/IEC 11770-2(1996)의 기법 9와 같다.

(역사) 1994-12-15에 초판이 발간되었다. 1998년 다른 부와 조화를 위해 개정이 결정되어 C. Mitchell(GB)가 편집자가 되어 1999-07-22에 재판(N2145)을 발간하였다. 2005년 정기검토 시 OID가 빠진 것, 참조문헌이 바뀐 것 등에 대한 지적에 2005-04-19에 개정이 결정되어(N4569) T. Tatsuta(JP)가 편집자가 되어 2008-12-15에 3판(N6952)을 발간하였다.

2008년 N7066으로 GB가 제기한 문장 구문 분석의 모호함을 해결하고자 수정본을 내기로 결정(N7303)하였고, C. Mitchell(GB)가 편집자가 되어 2010-02-15에 COR1(N8289)을 냈다. 또 JP가 2011년 Basin과 Cremers가 role-mixup attacks과 type-flaw attacks에 9798-2, 9798-3, 9798-4 가 모두 공격당한다는 CRYPTREC 보고서에 냈던 논문을 N9651로 제출하면서 수정 요청을 해 수정을 결의(N9848)하고, S. Matsuo (JP)가 편집자가 되어 2012-03-15에 COR2(N10040)를 냈다.

한편 GB는 2012년 N10861로 Basin, Cremers & Meier의 [BCM12]를 언급하며 사소한 수정이 필요하다고 보고했음. 필요한 수정과 Cor1 & Cor2의 내용을 함께 모아 Cor3을 만들기로 결정하고 S. Matsuo(JP)와 C.

Mitchell(GB)가 편집자가 되어 2013-03-21에 COR3(N11802)를 냈다.

(현황) 2011년 정기검토에서는 유지하기로 결정(N9782)되었다. 그러나 2014년 COR이 너무 가독성이 없다고 수정하자는 FR의 요청으로 개정을 결정(N13962) 하였고, R. Domingues(ZA)와 J. Hermans(BE)가 편집자가 되어 작업을 하기로 했으나, 그 후 아직 아무 문서가 나온 것이 없어서 지난 회의에서 독촉을 했고, 1stWD를 기다리는 중이다.

<IS 9798-3> 실체 인증 - 서명 기법 이용한 기법 (Entity authentication – Part 3: Mechanisms using digital signature techniques)

(내용) 서명을 하는 비공개 서명키를 다른 사람을 모르되, 거기에 해당하는 공개 검증키로 누구나 검증할 수 있다는 것에 착안하여 요구자를 인증하는 방식을 규정했다.

1. 일방인증 - 1회전송 (Unilateral authentication – One pass) — 타임스탬프나 일련번호 사용.

2. 일방인증 - 2회전송 (Unilateral authentication – Two pass) — 난수 사용.

3. 쌍방인증 - 2회전송 (Mutual authentication - Two pass) — 타임스탬프나 일련번호 사용.

4. 쌍방인증 - 3회전송 (Mutual authentication - Three pass) — 난수 사용.

5. 쌍방인증 - 2회병렬전송 (Mutual authentication - Two pass parallel authentication) — 타임스탬프나 일련번호 사용.

6. TTP포함 기법 - 5회전송1 (Mechanism involving an on-line trusted third party - Five pass 1) — 난수 사용, 요구자 시작.

7. TTP포함 기법 - 5회전송2 (Mechanism involving an on-line trusted third party - Five pass 2) — 난수 사용, 검증자 시작.

(역사) 1993-11-18에 초판이 발간되었다. 여기에는 위의 5가지의 기법만이 포함되어 있었다. B. Preneel(BE)이 편집자가 되어 1998-10-15에 재판(N1868)을 발간하였다.

2007년 뒤의 2개를 추가하기 위해 개정(N6211)이 결정되었고 X. Lai(EH)가 편집자가 되어 2010-07-16에 AMD1(N8394)을 냈다.

2008년 N7066으로 GB가 제기한 문장 구문 분석의 모호함을 해결하고자 수정본을 내기로 결정(N7303)하였고, C. Mitchell(GB)가 편집자가 되어 2009-09-16에 COR1(N7150)을 냈다. 또 9798-2에서와 같이 N9651에 대해 수정을 결의(N9848)하고 A. Otsuka(JP)가 편집자가 되어 2012-03-15에 COR2(N10041)를 냈다.

(현황) 2011년 정기검토에서는 유지하기로 결정(N9784)되었다. 그러나 2014년 정기검토에서는 AMD1과 2개의 COR은 너무 지저분하며, 기법들 간의 비교표를 추가하는 것이 좋겠다는 의견에 개정을 결의(2014-05-16) 하였고, J. Hermans(BE)와 Z. Du(CN)가 편집자가 되어 1stWD 2N1050로 나왔고, 2015-07-17에 2ndWD가 2N1082로 나와 전문가들의 의견을 기다리고 있는 중이다.

<IS 9798-4> 실체 인증 - 암호학적 검토함수를 이용한 기법 (Entity authentication – Part 4: Mechanisms using a cryptographic check function)

(내용) 암호학적 검토함수 즉 메시지인증코드(MAC, message authentication code)에 사용되는 대칭형 비밀키를 다른 사람을 모르고 요구자와 검증자만 알고 있다고 가정하고, MAC을 사용하여 인증하는 방식을 규정했다.

1. 일방인증 - 1회전송 (Unilateral authentication – One pass) — 타임스탬프나 일련번호 사용.

2. 일방인증 - 2회전송 (Unilateral authentication – Two pass) — 난수 사용.

3. 쌍방인증 - 2회전송 (Mutual authentication - Two pass) — 타임스탬프나 일련번호 사용.

4. 쌍방인증 - 3회전송 (Mutual authentication - Three pass) — 난수 사용.

(역사) 1995-03-02에 초판이 발간되었다. 개정이 결정되어 C. Mitchell(GB)가 편집자가 되어 1998-12-15에 재판(N2289)을 발간하였다.

2008년 N7066으로 GB가 제기한 문장 구문 분석의 모호함을 해결하고자 수정본을 내기로 결정(N7303) 하였고, C. Mitchell(GB)가 편집자가 되어 2009-09-16에 COR1(N7151)을 냈다. 또 9798-2에서와 같이 N9651에 대해 수정을 결의(N9848)하고 S. Matsuo(JP)와 A. Otsuka(JP)가 편집자가 되어 2012-07-15에 COR2(N10042)를 냈다.

(현황) 최종 정기검토는 2013년 이었고, 2013-04-26에 유지하기로 결정(N12627) 되었다. 2016년에 다음 검토가 계획되어 있다.

<IS 9798-5> 실체 인증 - 영지식증명기술을 이용한 기법 (Entity authentication – Part 5: Mechanisms using zero knowledge techniques)

(내용) 어떤 비밀을 알고 있다는 사실은 증명하면서도 비밀 자체는 알려주지 않는 기법을 이용해서 요구자를 인증하는 방식을 규정했다.

1. ID기반 기법 Fiat-Shamir, GQ1 (Mechanisms based on identities) — A. Fiat 와 Shamir 의 [FS87]과, Guillou & Quisquater 의 [GUQ01] 에서 가져온 것이다.

2. 정수 인수분해 기반 기법 GQ2 (Mechanisms based on integer factorization) — Guillou, Ugon & Quisquater 의 [GUQ01] 에서 가져온 것이다.

3. 소수에서 이산대수 기반 기법 Schnorr (Mechanisms based on discrete logarithms with respect to prime numbers) — Schnorr 의 [Sch90] 에서 가져온 것이다.

4. 합성수에서 이산대수 기반 기법 GPS1, GPS2 (Mechanisms based on discrete logarithms with respect to composite numbers) — GPS1은Girault 의 [Gir92] 와 Poupard & Stern 의 [PS98] 에서, GPS2는 Girault & Paillès 의 [GP03] 에서 가져온 것이다.

5. 비대칭형 암호시스템 기반 기법 Brandt-Damgard, Mitchell-Yuen (Mechanisms based on asymmetric encryption systems) — Brandt-Damgard 는 Brandt, Damgård, Landrock & Pedersen 의 [BDLP90] 에서, Mitchell-Yuen은 Mitchell & Yeun 의 [MY98](IS 11770-3의 키전달기법 6과도 같음)에서 가져온 것이다.

6. 타원곡선에서 이산대수 기반 기법 EC-GPS (Mechanisms based on discrete logarithms with respect to elliptic curves) — Girault, Poupard & Stern 의 [GPS06]을 Girault, Juniot & Robshaw [MJR07]의 기법으로 타원곡선에서 구현하게 한 것으로, [GL04]의 LHW변형에서도 적용 가능하다.

(역사) 같은 표준의 다른 부보다 늦게 1995년에 시작한 과제로 M. King(GB)가 편집자가 되어 1999-03-25에 초판(N2266)이 발간되었다. 5가지의 기법들을 포함시키고자 2002년 개정이 결의(N3411)되었고 L. Guillou(FR)가 편집자가 되어 2004-12-01에 재판(N3959)을 발간하였다. 6번째 종류의 기법을 포함시키고자 2007년 개정이 결의(N5823)되었고 J. Misarsky(RU) & M. Ward(GB)가 편집자가 되어 2009-12-15에 3판(N7904)을 발간하였다.

(현황) 2015년 정기검토에서는 유지하기로 결정(N15207)되었다. 2018년에 다음 정기검토가 계획되어 있다.

<IS 9798-6> 실체 인증 - 손으로 데이터를 전단하는 기법 (Entity authentication – Part Part 6: Mechanisms using manual data transfer)

(내용) 요구자만이 작은 토큰 같은 것에 데이터를 담아 갖고 사실과, 어떤 비밀을 알고 있다는 사실을 함께 이용하여 요구자를 인증하는 방식을 규정했다.

1. 기법 1 — 한 토큰은 간단한 입력만, 다른 토큰은 간단한 출력만 사용하고, 짧은 확인값을 사용하는 기법 (Mechanisms using a short check-value – One device with simple input, one device with simple output)

2. 기법 2 — 쌍방 모두 간단한 입력만 가능한 토큰을 사용하고, 짧은 확인값을 사용하는 기법 (Mechanisms using a short check-value – Devices with simple input capabilities

3. 기법 3 — 한 토큰은 간단한 입력만, 다른 토큰은 간단한 출력만 사용하고, 짧은 확인값이나 짧은 키를 직접 전달하는 기법 (Mechanisms using a manual transfer of a short digest-value or a short key – One device with simple input, one device with simple output

4. 기법 4 — 한 토큰은 간단한 입력만, 다른 토큰은 간단한 출력만 사용하고, 짧은 확인값이나 짧은 키를 직접 전달하는 기법 (Mechanisms using a manual transfer of a short digest-value or a short key – One device with simple input, one device with simple output

5. 기법 5 — 쌍방 모두 간단한 입력만 가능한 토큰을 사용하고, 짧은 확인값이나 짧은 키를 직접 전달하는 기법 (Mechanisms using a manual transfer of a short

digest-value or a short key – Devices with simple input capabilities)

6. 기법 6 — – 쌍방 모두 간단한 입력만 가능한 토큰을 사용하고, 짧은 확인값이나 짧은 키를 직접 전달하는 기법 (Mechanisms using a manual transfer of a short digest-value or a short key – Devices with simple input capabilities)

7. 기법 7 — 쌍방 모두 간단한 출력만 가능한 토큰을 사용하고, MAC을 사용하는 기법 (Mechanisms using a MAC – Mechanisms using a MAC – Devices with simple out capabilities)

8. 기법 8 — 한 토큰은 간단한 입력만, 다른 토큰은 간단한 출력만 사용하고, MAC을 사용하는 기법 (Mechanisms using a MAC – One device with simple input, one device with simple output)

(역사) 같은 표준의 마지막으로 2003년에 시작한 과제로 C. Mitchell(GB)이 편집자가 되어 2005-08-01에 초판(N4365)이 발간되었다. 2008년 정기검토에서 GB가 새 기법들(기법 3 ~ 기법 6, [LR11]에 정리되어있음)을 추가하는 개정을 하자고 하여 받아들였고 (N7130) L. Nguyen(GB)가 편집자가 되어 2010-12-01에 재판(N8949)을 발간하였다.

(현황) 최종 정기검토는 2013년 이었고, 2013-04-26에 유지하기로 결정(N12628)되었다. 2016년에 다음 검토가 계획되어 있다.

<IS 20009-1> 익명 인증 – 일반 (Anonymous entity authentication – Part 1: General)

(내용) 익명성을 보장하는 실체 인증의 일반 개념, 용어, 모델, 요구사항 등을 설명하고, 다음 이어지는 부(part)들에서 다룰 내용에 대한 소개를 하였다.

(역사) 2009년 시작된 과제로 C. Mitchell(GB)이 편집자가 되어 시작했고, 2013-08-01에 초판(N12578)이 발간되었다.

(현황) 2016년에 다음 정기검토가 계획되어 있다.

<IS 20009-2> 익명 인증 – 그룹공개키를 사용하여 검증하는 서명 기반 기법 (Anonymous entity authentication – Part 2: Mechanisms based on signatures using a group public key)

(내용) IS 20008-2에서 개발된 익명 서명을 사용하여 익명 인증을 하는 기법으로 IS 9798-3 '실체 인증 – 서명 기법 이용한 기법'을 기반으로 개발되었다.

1. 기법 1: 1회전송, 일방익명인증 (One-pass unilateral anonymous authentication) — IS 9798-3의 '일방인증 - 1회 전송' 기법을 변형. 타임스탬프나 일련번호 사용

2. 기법 2: 2회 전송, 일방익명인증 (Two-pass unilateral anonymous authentication) — IS 9798-3의 '일방인증 - 2회 전송' 기법을 변형. 난수 사용

3. 기법 3: 2회 전송, 쌍방익명인증 (Two-pass mutual anonymous authentication) — IS 9798-3의 '쌍방인증 - 2회 전송' 기법을 변형. 타임스탬프나 일련번호 사용

4. 기법 4: 3회 전송, 쌍방익명인증 (Three-pass mutual anonymous authentication) — IS 9798-3의 '쌍방인증 - 3회 전송' 기법을 변형. 난수 사용

5. 기법 5: 2회병렬전송, 쌍방익명인증 (Two-pass parallel mutual anonymous authentication) — IS 9798-3의 '쌍방인증 - 2회병렬전송' 기법을 변형. 타임스탬프나 일련번호 사용

6. 기법 6: 2회전송, 일방익명 쌍방인증 (Two-pass unilateral-anonymous mutual authentication) — 기법 3과 유사하나 1명은 익명 다른 1명은 실명 인증

7. 기법 7: 3회전송, 일방익명 쌍방인증 (Three-pass unilateral-anonymous mutual authentication) — 기법 4와 유사하나 1명은 익명 다른 1명은 실명 인증

8. 기법 8: 2회 병렬전송, 일방익명 쌍방인증 (Two-pass parallel unilateral-anonymous mutual authentication) — 기법 5와 유사하나 1명은 익명 다른 1명은 실명 인증

9. 기법 9: 3회 전송, 후-서명, 쌍방익명인증 (Three-pass sign-later mutual anonymous authentication) — 기법 4와 유사하나 묶임성(binding-property), 즉 전송되는 메시지 사이에 묶임을 확인할 수 있는 성질을 나중 메시지에 한 서명을 통해서 확인.

10. 기법 10: 3회 전송, 선-서명, 쌍방익명인증 (Three-pass sign-first mutual anonymous authentication) — 기법 4와 유사하나 묶임성을 먼저 메시지에 한 서명을 통해서 확인

11. 기법 11: 2회 병렬 전송, 후-서명, 쌍방익명인

증 (Two-pass parallel sign-later mutual anonymous authentication) — 기법 5와 유사하나 묶임성을 나중 메시지에 한 서명을 통해서 확인

12. 기법 12: 2회 병렬 전송, 선-서명, 쌍방익명인증 (Two-pass parallel sign-first mutual anonymous authentication) — 기법 5와 유사하나 묶임성을 먼저 메시지에 한 서명을 통해서 확인

13. 기법 13: 3회 전송, 후-서명, 일방익명 쌍방인증 (Three-pass sign-later unilateral- anonymous mutual authentication) — 기법 7과 유사하나 나중 메시지에 한 서명을 통해서 확인

14. 기법 14: 3회 전송, 선-서명, 일방익명 쌍방인증 (Three-pass sign-first unilateral -anonymous mutual authentication) — 기법 7과 유사하나 묶임성을 먼저 메시지에 한 서명을 통해서 확인

15. 기법 15: 2회병렬전송, 선-서명, 일방익명 쌍방인증 (Two-pass parallel sign-later unilateral-anonymous mutual authentication) — 기법 8과 유사하나 묶임성을 나중 메시지에 한 서명을 통해서 확인

16. 기법 16: 2회병렬전송, 선-서명, 일방익명 쌍방인증 (Two-pass parallel sign-first unilateral-anonymous mutual authentication) — 기법 8과 유사하나 묶임성을 먼저 메시지에 한 서명을 통해서 확인

17. 기법 17: 요구자 시작, 4회전송, 일방익명인증 (Four-pass unilateral anonymous authentication(initiated by A) — 기법 19에서 1회전송을 줄여 일방인증으로 변형

18. 기법 18: 검증자 시작, 4회전송, 일방익명인증 (Four-pass unilateral anonymous authentication(initiated by B) — 기법 20에서 1회전송을 줄여 일방인증으로 변형

19. 기법 19: 요구자 시작, 5회전송, 쌍방익명인증 (Five-pass mutual anonymous authentication(initiated by A) — IS 9798-3의 'TTP포함 기법 - 5회전송1' 기법을 변형. 난수 사용.

20. 기법 20: 검증자 시작, 5회전송, 쌍방익명인증 (Five-pass mutual anonymous authentication(initiated by B) — IS 9798-3의 'TTP포함 기법 - 5회전송2' 기법을 변형. 난수 사용

21. 기법 21: 익명인 요구자 시작, 5회전송, 일방익명 쌍방인증 (Five-pass unilateral-anonymous mutual authentication initiated by A who is anonymous) — 기법 19을 변형하여 익명인 요구자 시작하고, 실명인 검증자와 쌍방인증

22. 기법 22: 요구자 시작(검증자는 익명) 시작, 5회전송, 일방익명 쌍방인증 (Five-pass unilateral-anonymous mutual authentication initiated by A and B is anonymous) — 기법 19을 변형하여 실명인 요구자 시작하고, 익명인 검증자와 쌍방인증

23. 기법 23: 검증자 시작(요구자는 익명), 5회전송, 일방익명 쌍방인증 (Five-pass unilateral-anonymous mutual authentication initiated by B and A is anonymous) — 기법 20을 변형하여 실명인 검증자가 시작하고, 익명인 요구자와 쌍방인증

24. 기법 24: 익명인 검증자 시작, 5회전송, 일방익명 쌍방인증 (Five-pass unilateral-anonymous mutual authentication initiated by B who is anonymous) — 기법 20을 변형하여 익명인 검증자가 시작하고, 실명인 요구자와 쌍방인증

여기서 난수를 이용하여 쌍방인증을 하는 기법들 4, 5, 7, 8은 잘못 묶임을 이용한 공격(misbinding attack)에 취약할 수 있음이 Walker & Li의 [WL10]에서 밝혀졌고, 그들은 후-서명을 통해 그 공격의 위협에서 벗어나는 방법을 보여주었고 이를 이용한 기법들 9, 11, 13, 15를 만들었다. 한편 선-서명을 통해 강한 묶임성을 확인하는 기법들 10, 12, 14, 16은 Hwang, Eom, Chang, Lee & Nyang의 [HECLN12]에서 가져온 것이다.

또한 공개하는 절차 및 연결성을 확인하는 절차도 Brickell & Li의 [BL10] 과 Hwang, Lee, Chung, Cho & Nyang의 [HLCCN11]에서 가져온 방법을 포함시켰다.

(역사) 2009년 시작된 과제로 본인과 S. Matsuo(JP)가 편집자가 되어 시작했고, 2013-12-01에 초판(N12842)이 발간되었다. 처음에는 제목이 익명서명에 기반한 기법(Mechanisms based on anonymous digital signature schemes)이었으나 익명서명의 범위가 너무 넓다고 판단되어 본인의 주장으로 현재의 제목으로 수정했다.

(현황) 2016년에 다음 정기검토가 계획되어 있다.

<IS 20009-3> 익명 인증 - 은닉 서명 기반 기법 (Anonymous entity authentication - Part 3: Mechanisms based on blind signatures)

(내용) 1stWD에는 단 한 개의 기법만이 규정되어 있다. 더 많은 기법들이 포함될 것을 예상한다.

1. 기법 1: 2회전송, 일방익명인증 (Two-pass unilateral anonymous authentication) — IS 9798-3의 '일방인증 - 2회전송' 기법을 변형. 난수 사용

(역사) 2011년 성립(N10059)된 과제로 J. Traoré(FR)가 편집자가 되었었으나, 은닉 서명 표준인 IS 18370이 먼저 표준화되어야 한다고 미루고 있다가, D. Turner(US)로 편집자가 바뀐 후 1stWD가 N13236로 나왔다. D. Turner(US)도 편집자를 사임하여 더 이상 진척이 없다.

(현황) 새 편집자가 나와 2ndWD를 만들기를 기다리는 중이다.

<IS 20009-4> 익명 인증 - 약한 비밀 기반 기법 (Anonymous entity authentication - Part 4: Mechanisms based on weak secrets)

(내용) 패스워드만 사용하는 PAEA(패스워드 기반 익명인증) 2 기법과 패스워드 이외에 저장매체도 사용하는 PAEA 2 기법을 규정하고 있다.

1. SKI 기법 — Shin, Kobara & Imai의 [SKI10]에서 가져온 기법이다.

2. YZ 기법 — Yang & Zhang 의 [YZ08] 에서 가져온 기법이다.

3. YZW 기법 — Yang, Zhou, Wong & Bao 의 [YZWB10] 에서 가져온 기법이다.

4. QGZ 기법 — Qian, Gong & Zhou의 [QGZ12] 에서 가져온 기법이다.

(역사) 2011년 Y. YANG(SG)을 조사위원(rapporteur)으로 하여 '패스워드 기반 익명인증' 이란 제목의 연구기간(study period)을 갖다가, 2013년 본 부를 현재의 제목으로 시작하기로 결정(N12718)해 Y. YANG(SG)과 K. Kobara(JP)가 편집자가 되어, 1stWD N12604, 2ndWD N13224, 3rdWD N14008, 1stCD N14759에 이어 2015-06-29에 2ndCD N15194를 냈다.

(현황) 2015-09-01이 마감인 2ndCD에 대한 투표결과를 기다리는 중이다.

Ⅲ. 결 론

이상으로 SC27/WG2에서 표준화되고 있는 디지털서명과 실체 인증에 대해 정리해 보았다. 두 분야의 국제표준화에 대한 이해에 도움이 되었으면 한다.

참 고 문 헌

[1] M. Abe & T. Okamoto, "Provably Secure Partially Blind Signatures," *Crypto 2000*, LNCS 1880, pp.271-286, 2000.

[2] M. Abe & T. Okamoto, "A signature scheme with message recovery as secure as discrete logarithm," *Asiacrypt 1999*, LNCS 1716, pp.378-389, 1999.

[3] E. Brickell, J. Camenisch, L. Chen, "Direct anonymous attestation," *11th ACM Conference on Computer & Communications Security*, pp.132-145, 2005.

[4] E. Brickell, J. Camenisch, L. Chen, "The DAA scheme in context," *Trusted Computing*, The Institute of Electrical Engineers, 2005.

[5] D. Basin, C. Cremers & S. Meier, "Provably repairing the ISO/IEC 9798 standard for entity authentication", *POST 2012*, LNCS 7215, pp.129-148, 2012.

[6] J. Brandt, I. Damgård, P. Landrock & T. Pedersen, "Zero-knowledge authentication scheme with secret key exchange," *Crypto 1988*, LNCS 403, pp.583-588, 1990.

[7] E. Brickell & J. Li, "A pairing-based DAA scheme further reducing TPM resources," *TRUST 2010*, LNCS 6101, pp.181-195, 2010.

[8] S. Blake-Wilson & A. Menezes, "Unknown key-share attacks on the station-to-station(STS) protocol," *PKC 1999*, LNCS 1560, pp. 154-170, 1999.

[9] M. Bellare & P. Rogaway, "The exact security of digital signatures: How to sign with RSA & Rabin," *Eurocrypt 1996*, LNCS 1070, pp.399-416, 1996.

[10] S. Brands, "Rethinking Public Key

Infrastructures & Digital Certificates," *The MIT Press*, August 2000.

[11] J. Bohli, S. Rohrich & R. Steinwandt, "Key substitution attacks revisited: Taking into account malicious signers", *International Journal of Information Security 5*, pp.30-36, 2006.

[12] J. Cha & J. Cheon, "An identity-based signature from gap Diffie-Hellman groups," *PKC 2002*, LNCS 2567, pp.18-30, 2002.

[13] S. Canard, E. Malville & J. Traoré, "Identity federation & privacy: one step beyond," t*he 4th ACM workshop on Digital identity management*, pp.25-32, 2008.

[14] J. Coron, D. Naccache & J. Stern, "On the security of RSA Padding," *Crypto 1999*, LNCS 1666, pp.1-18, 1999.

[15] L. Chen, D. Page & N. Smart, "On the design & implementation of an efficient DAA scheme," *the 9th Smart Card Research & Advanced Application IFIP Conference*, pp.223-237, 2010.

[16] S. Canard, B. Schoenmakers, M. Stam & J. Traoré, "List signature schemes," *Discrete Applied Mathematics*, 154(2), pp.189-201, 2006.

[17] FIPS PUB 186, "Digital Signature Standard," U.S. National Institute of Standards & Technology, Gaithersburg, Maryland, 1994.

[18] FIPS PUB 186-4, "Digital Signature Standard(DSS)," *U.S. National Institute of Standards & Technology*, Gaithersburg, Maryland, 2013.

[19] American National Standards Institute, "Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm(ECDSA)," *ANSI X9.62-2005*, 2005.

[20] Telecommunications Technology Association, "Digital Signature Mechanism with Appendix - Part 3: Korean Certificate-based Digital Signature Algorithm using Elliptic Curves EC-KCDSA," *TTAK.KO-12.0015/R2*, 2014. (In Korean)

[21] H. Erwin, & S. Pascale, "Digital Signature Scheme EC-GDSA," German Federal Office for Information Security, December 2005.

[22] J. Furukawa & H. Imai, "An efficient group signature scheme from bilinear maps," *IEICE Transactions*, 89-A(5), pp.1328-1338, 2006.

[23] A. Fujioka, T. Okamoto & S. Miyaguchi, "ESIGN, an efficient digital signature implementation for smart cards," *Eurocrypt 1991*, LNCS 547, pp.446-457, 1992.

[24] A. Fiat & A. Shamir, "How to prove yourself: Practical solutions to identification & signature problems," *Crypto 1986*, LNCS 263, pp.186-194, 1987.

[25] M. Girault, "Self-certified public keys," *Eurocrypt 1991*, LNCS 547, pp.490-497, 1992.

[26] M. Girault & D. Lefranc, "Public key authentication with one(online) single addition," *CHES 2004*, pp.413-427, 2004

[27] GOST R 34.10-2012, State Standard of the Russian Federation, "Information technology. Cryptographic data security. Signature & verification processes of[electronic] digital signature." *State Committee of the Russian Federation on Standards & Metrology*, 2012.(In Russian)

[28] M. Girault & J. Paillès, "On-line / off-line RSA-like," *Workshop on Cryptography & Coding* 2003, 2003

[29] M. Girault, G. Poupard, & J. Stern, "On the fly authentication & signature schemes based on groups of unknown order," *J. Cryptology*, 19(4), pp.463-487, 2006.

[30] L. Guillou & J. Quisquater, "A paradoxical identity-based signature scheme resulting from zero knowledge," *Crypto 1988*, LNCS 403, pp.216-231, 1988.

[31] L. Guillou & J. Quisquater, "A practical zero-knowledge protocol fitted to security microprocessor minimizing both transmission & memory," *Eurocrypt 1988*, LNCS 330, pp.123-128, 1988.

[32] M. Gaud & J. Traoré, "On the Anonymity of Fair Offline E-cash Systems," *Financial*

Cryptography 2003, LNCS 2742, pp.34-50. 2003.

[33] L. Guillou, M. Ugon & J. Quisquater, "Cryptographic authentication protocols for smart cards," *Computer Networks Magazine*, Vol. 36, pp.437-451, 2001.

[34] J.Hwang, S.Eom, K.Chang, P. Lee & D. Nyang, "Anonymity-based authenticated key agreement with binding properties," *WISA 2012*, pp.177-191, 2012.

[35] F. Hess, "Efficient identity based signature schemes based on pairings," *SAC 2002*, 2002.

[36] J. Hwang, S. Lee, B. Chung, H. Cho & D. Nyang, "Short group signatures with controllable linkability," *the 2011 Workshop on Lightweight Security & Privacy: Devices, Protocols, & Applications*, pp.44-52, 2011.

[37] J. Hwang, S. Lee, B. Chung, H. Cho & D. Nyang, "Group signatures with controllable linkability for dynamic membership," *Information Sciences*, vol. 222, pp.761-778, 2013.

[38] T. Isshiki, K. Mori, K. Sako, I. Teranishi & S. Yonezawa, "Using group signatures for identity management & its implementation," *the 2006 Workshop on Digital Identity Management*, pp.73-78, 2006.

[39] Telecommunications Technology Association, "Digital Signature Mechanism with Appendix - Part 2: Korean Certificate-based Digital Signature Algorithm KCDSA," *TTAK.KO-12.0001/R3*, 2014. (In Korean)

[40] C. Lim & P. Lee, "A key recovery attack on discrete log based schemes using a prime order subgroup," *Crypto 1997*, LNCS 1294, pp.249-263, 1997.

[41] C. Lim & P. Lee, "A study on the proposed Korean digital signature algorithm," *Asiacrypt 1998*, LNCS 1514, pp.175-186, 1998.

[42] L. Nguyen & A. Roscoe, "Authentication protocols based on low-bandwidth unspoofable channels: a comparative survey," *Journal of Computer Security*, 19-1, pp.139-201, 2011

[43] A. Miyaji, "Another Countermeasure to Forgeries over Message Recovery Signature," *IEICE Trans*., Fundamentals, vol. E80-A, No.11, pp.2192-2200, 1997.

[44] M. Girault, L. Juniot & M. Robshaw, "The feasibility of on-the-tag public key cryptography." *RFIDSEC 2007*, July 2007.

[45] A. Menezes, P. van Oorschot & S. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1997.

[46] A. Menezes & N. Smart, "Security of signature schemes in a multi-user setting," *Designs, Codes and Cryptography 33*, pp.261-274, 2004.

[47] C. Mitchell & C. Yeun, "Fixing a problem in the Helsinki protocol," *ACM Operating Systems Review*, Vol. 32-4, pp.21-24, October 1998.

[48] K. Nyberg & R. Rueppel, "Message recovery for signature schemes based on the discrete logarithm problem," *Designs, Codes & Cryptography 7*, pp.61-81, 1996.

[49] T. Okamoto, "Provably Secure & Practical Identification Schemes & Corresponding Signature Schemes," *Crypto 1992*, pp.31-53, 1992.

[50] IEEE Standard P1363a, "Standard specifications for public key cryptography ― Amendment 1: Additional techniques," 2004.

[51] G. Poupard & J. Stern, "Security analysis of a practical 'on the fly' authentication & signature generation," *Eurocrypt 1998*, LNCS 1403, pp.422-436, 1998.

[52] L. Pintsov & S. Vanstone, "Postal Revenue Collection in the Digital Age," *the Fourth International Financial Cryptography Conference*, 2000.

[53] D. Pointcheval & S. Vaudenay, "On provable security for digital signature algorithms," Technical Report LIENS-96-17, LIENS, 1996.

[54] H. Qian, J. Gong, Y. Zhou, "Anonymous Password-based Key Exchange with Low Resources Consumption & Better User-friendliness," *Security & Communication Networks*,

Vol. 5, pp.1379-1393, February, 2012.

[55] M. Rabin, “Digital signatures & public-key functions as intractable as factorization,” *Technical Report MIT/LCS/TR-212*, MIT Laboratory for Computer Science, January 1979.

[56] R. Rivest, A. Shamir & L. Adleman, “A Method for Obtaining Digital Signatures & Public-Key Cryptosystems,” *Communications of the ACM*, Vol. 21(2), pp.120─126, 1978.

[57] C. P. Schnorr “Efficient identification & signature for smart cards,” *Crypto 1989*, LNCS 435, pp.239-252, 1990.

[58] C. P. Schnorr “Efficient signature generation for smart cards,” *Journal of Cryptology*, vol. 4, pp.161-174, 1991.

[59] S. Shin, K. Kobara & H. Imai, "Anonymous Password-Authenticated Key Exchange: New Construction & Its Extensions, " *IEICE Transactions on Fundamentals of Electronics*, Communications & Computer Sciences, Vol. E93-A, No. 1, pp.102-115, January 2010.

[60] H. Williams, “Some public-key crypto-functions as intractable as factorization,” *Crypto 1984*, LNCS 196, pp.66-70, 1985.

[61] J. Walker & J. Li, “Key Exchange with Anonymous Authentication using DAA-SIGMA Protocol,” *2nd International Conference on Trusted Systems*, LNCS 6802, pp.108-127, 2010.

[62] D. Yum & P. Lee, “Security Proof for KCDSA under the Random Oracle Model,” *the 9th Conference on Information Security & Cryptology 1999*, pp.173-180, 1999.

[63] D. YUM, S. SIM & P. LEE, “New Signature Schemes Giving Message Recovery Based on EC-KCDSA,” *the 12th Conference on Information Security & Cryptology 2002*, pp.595-597, 2002.

[64] J. Yang & Z. Zhang, “A New Anonymous Password Based Authenticated Key Exchange Protocol,” *Indocrypt 2008*, LNCS. Volume 5305, pp.200-212, 2008.

[65] Y. Yang, J. Zhou, J. W. Wong & F. Bao, "Towards Practical Anonymous Password Authentication,” *Proc. 26th Annual Computer Security Applications Conference*, pp.59-68, ACM, 2010.

〈저자소개〉

이 필 중 (Pil Joong Lee)
종신회원

1974년 2월 : 서울대학교 전자공 학과 학사
1977년 3월 : 한국대학교 전자공 학과 석사
1982년 6월 : U.C.L.A System Science. Engineer
1985년 6월 : U.C.L.A Electrical Engineering. Ph.D
1980년 3월~1985년 8월 : Jet Propulsion Laboratory. Senior Engineer
1985년 8월~1990년 2월 : Bell Communication Research. M.T.S
1990년 2월~현재 : 포항공과대학교 전자전기공학과 교수
2000년 9월~2003년 8월 : 포항공대 정보통신대학원 원장 (정보통신연구소 소장 겸임)
2004년 1월~2004년 12월 : 한국정보보호학회 회장
2003년 12월~현재 : 한국IT리더스포럼 회원
2005년 1월~현재 : 한국정보보호학회 명예회장
2007년 1월~현재 : 한국공학한림원 정회원
관심분야 : 암호학을 주로 한 정보보호 전반