전자여권의 국제적 호환성 및 보안성을 확보하기 위한 PKI 체계 연구

전경화*°, 윤성근**
*LG CNS, **외교통상부

Electronic Passports PKI– the Interoperability and Security Aspects

Jun, Gyung Hwa°, Yun, Sung-geun
LG CNS, Ministry of Foreign Affairs and Trade
E-mail : ghjun@lgcns.com, sgyun06@mofat.go.kr

요 약

본 연구는 2008년 하반기 전면 시행예정인 전자여권의 기반을 구성하고 있는 전자여권 PKI의 개념과, 국내외 적용되어 있는 현황을 소개한다. 국제민간항공기구(ICAO)와 유럽연합을 중심으로 추진되고 있는 전자여권 PKI에 대한 표준화 동향을 소개하고, 전자여권 PKI체계와, GPKI, NPKI 등 타 PKI체계와의 차이를 분석한다. 현재 논의되고 있는 전자여권 PKI에 대한 기술적인 이슈를 살펴보고 이에 대한 방안을 논의한다. 끝으로 기 논의된 기술적인 이슈 등의 분석을 통한 향후 발전방안을 제시한다.

1. 서론

전자여권은 국제민간항공기구(ICAO)와 국제표준화기구(ISO)에서 정한 국제표준에 따라 이름, 여권번호와 같은 개인정보와 함께 얼굴, 지문과 같이 바이오 인식정보가 내장되어 있는 여권을 말한다. 전자여권의 겉모습은 기존 여권과 유사하나, 여권에 개인신원정보, 바이오인식정보, 보안요소 등이 포함된 전자칩이 내장되어 있다.

2005년 외교통상부 집계에 따르면 해외에서 분실되는 여권이 약 만건 정도이며, 중국에서만 약

1,900여 건이 분실되었고, 중국 내 외국인 여권분실건수의 80% 정도가 대한민국 여권이라고 한다. 중국 공안국은 이렇게 분실된 우리나라 여권의 70~80%가 위·변조되어 다시 불법행위에 사용되는 것으로 보고 있다.

또한 러시아에서는 인적사항이 일부 훼손된 여권을 소지한 우리나라 국민의 입국거부사태가 발생하였고, 위조된 우리나라 여권을 소지한 아시아인이 핀란드를 경유하여 EU회원국으로 불법이민 하려다 체포된 사례가 다수 발생하였다.

이와 같은 문제점 때문에 여권의 위·변조를 방지하여 여권에 대한 국제적 신뢰도를 제고하고 여행객들의 편의를 증진하기 위하여, 우리나라뿐만 아니라 세계 각국이 종이 여권으로부터 위·변조가 어려운 전자여권으로 전환하고 있다.

대한민국 정부는 2008년 3월에 관용여권과 외교관 여권에 대하여 전자여권을 시범 발급하고, 이후 2008년 하반기에는 일반인에게도 전자여권의 전면 발급을 계획하고 있다.

전세계적으로 현재 44개국이 전자여권을 발급하고 있으며, 이중 말레이시아를 제외한 43개국이 ICAO 표준을 따르고 있다. 또한 EU국가들은 2009년 6월에 지문도 함께 포함된 전자여권 발급을 전면 시행할 것을 계획하고 있다.[1]

국가명	도입시기	국가명	도입시기
말레이시아	98.03	리투아니아	06.08
벨기에	04.11	룩셈부르크	06.08
태국	05.08	슬로베니아	06.08
모나코	05.07	폴란드	06.08
스웨덴	05.10	헝가리	06.08
노르웨이	05.10	체코	06.09
호주	05.10	러시아연방	06.09
뉴질랜드	05.11	안도라	06.09
독일	05.11	스위스	06.09
영국	06.03	산마리노	06.10
일본	06.03	아일랜드	06.10
프랑스	06.04	리히텐슈타인	06.10
싱가포르	06.04	이태리	06.10
아이슬란드	06.05	소말리아	07.01
오스트리아	06.06	홍콩	07.02
포르투갈	06.07	마케도니아	07.04
미국	06.08	에스토니아	07.05
덴마크	06.08	몰디브	07.07
스페인	06.08	나이지리아	07.08
핀란드	06.08	베네수엘라	-
네덜란드	06.08	리트비아	07.11
그리스	06.08	슬로바키아	08.01

표1. 세계각국 전자여권 도입시기

ICAO 9303 표준은 비접촉식 스마트카드, 대칭 및 비대칭방식 암호기술과 바이오인식 등에 대한 기존의 기술표준을 채택하여 전자여권 요소기술을 규정하고 있다.[2]

구체적으로, 광학식(Optical) 판독기술과 ISO/IEC 14443 규격에 따르는 비접촉식 RF통신기술, ISO/IEC 7816의 스마트카드 기술, 그리고 ISO/IEC 19794-5의 얼굴인식과, ISO/IEC 19794-4의 지문인식, ISO/IEC 19785의 바이오정보 공통포맷 등을 준수한 바이오 인식기술에 기반하여 구현된다.

또한 칩에 저장되는 데이터에 대한 표준을 정의하고, 보안성을 확보하기 위하여 기존 PKI, 암호 알고리즘 및 보안 프로토콜에 대한 표준을 활용하여 전자여권 PKI체계를 정의하였다.[2,3,4,5]

이 논문에서는 전자여권의 국제적 호환성을 확보하기 위하여 우리나라와 세계 각국이 채택한 ICAO 및 EU 표준 전자여권 PKI 체계를 살펴보고, 이를 통해 전자여권 칩 내의 개인정보 및 바이오정보가 보호되는 메커니즘과 위·변조 방지, 복제방지 대책, 판독과정의 보안성 등에 대하여 살펴본다.

본 논문은 다음과 같이 구성된다. 2장에서, 전자여권 데이터 표준을 포함한 전자여권 PKI에 대한 전반적인 내용을 다룬다. 2.1절에서는 전자여권 PKI 표준화 동향을 간략히 소개하고, 2.2절에서는 전자여권 판독과정을 다룬다. 2.3절에서는 세계 각국의 PKI 적용 현황을 제시한다. 또한 2.4절에서는 GPKI 및 NPKI와의 차이를 분석하고, 2.5절에서는 국내외에서 논의되고 있는 전자여권 PKI에 대한 기술적인 이슈들을 소개한다. 마지막으로 3장에서는 기술적인 이슈 분석을 통한 향후 전자여권의 발전방향을 제시함으로써 마무리한다.

2. 본론

전자여권 칩 내에 저장되는 데이터는 ICAO에서 규정한 데이터 구조인 LDS[1] 형태로 저장된다.

전자여권 인쇄 면에 기록된 성명, 여권번호 등과 칩 고유의 정보인 지문 등의 바이오인식정보, 키 정보 등을 포함한다. LDS 데이터는 ASN.1 인코딩되어 저장되고, DG2~DG4는 CBEFF 인코딩을 사용한다.[6]

DG	내용	구성요소
DG1	MRZ[2]에 기록된 세부사항	여권 종류
		발행국 또는 발행기관
		영문 성명(소지자)
		여권 번호
		Check digit
		국적
		생년월일
		Check digit
		성별
		여권만료일
		Check digit
		추가내용
		추가내용 Check digit
		전체 Check digit
DG2	필수바이오정보	얼굴
DG3	추가바이오정보	지문
DG4		홍채
DG14	키 정보	CA 공개키 정보

[1] LDS, Logical Data Structure, The collection of Data Groups

[2] MRZ, Machine Readable Zone

DG15		AA 공개키 정보
DG16	기타	연락처
SOD	Security Object	LDS에 대한 서명값 DS인증서포함(선택)

표2. 전자여권 데이터 포맷(LDS) 발췌

2.1 전자여권 PKI 표준화 동향

전자여권 PKI는 ICAO 중심의 PKI 체계와 얼굴 이외의 지문 등 부가적인 바이오정보에 대한 접근제어(Extended Access Control, EAC)를 위한 독일과 싱가포르 중심의 PKI체계로 이원화되어 표준화 활동이 진행되고 있다.

ICAO는 전자여권 칩 내 저장되는 필수 바이오정보로서 얼굴을 채택하고 있고, 지문이나 홍채 등은 해당 국가의 선택에 맡겨 놓고 있다.

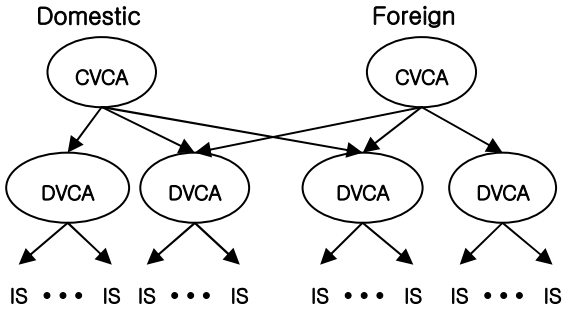
독일 BSI[3] 표준은 EU 표준으로서, 독일은 2007년 11월, 독일 이외의 EU 회원국은 2009년에 적용

될 예정이고, 싱가포르 방식은 현재 싱가포르 내에서 사용된다.

전자여권 PKI는 ICAO 표준이 규정하는 CSCA[4], DS[5], PKD[6] 와, EU 표준이 규정하는 CVCA[7], DVCA[8], IS[9] 등으로 구성된다.[7,8]

CSCA는 최상위 인증기관으로서, LDS에 대하여 서명을 생성할 때 사용하는 DS인증서를 발급하는 주체이다. 또한 PKD는 전자여권 발급국가의 DS인증서와 CRL을 보관하고 제공하는 기능을 수행한다.

CVCA는 EAC 계층 구조의 최상위 인증기관으로서, DVCA인증서를 발급하고, DVCA는 전자여권에서 지문이나 홍채 등의 바이오정보를 접근하는 최하위 IS의 인증서를 발급한다.



외국 출입국에서 우리나라 전자여권 내 사진 이외의 바이오정보에 접근하기 위해서는, 바이오정보에 대한 양 국가간 협약이 체결된 후, 우리나라 CVCA가 해당국에 대하여 DVCA인증서를 발급하고, 그 DVCA로부터 인증서를 발급받은 판독시스템만이 우리나라 전자여권의 지문이나 홍채 등의 부가적인 바이오정보에 접근할 수있다.

ICAO가 권고하는 암호 알고리즘은 CSCA인증서는 RSA 3072비트 이상, DSA 3072비트, 256비트 이상, ECDSA 256비트 이상이며, DS인증서는
RSA 2048비트 이상, DSA 2048비트 이상, 224비트
이상, ECDSA 224비트 이상이다.

EU표준에서 규정하는 암호 알고리즘은 RSA 1024비트, 1280비트, 1536비트, 2048비트, 또는 3072 비트고, ECDSA 160비트, 192비트, 224비트, 256비트다. ECDSA의 경우, Base Curve는 Brainpool Curve를 사용한다.[9]

전자여권 PKI 인증서의 유효기간은 전자여권의 유효기간, 개인키 유효기간, 배포기간을 고려하여 다음과 같이 규정하고 있다.

인증서 종류	유효기간
CSCA인증서	13년 3개월 ~ 15년 3개월
DS인증서	10년 1개월 ~ 10년 3개월
CVCA인증서	6개월 ~ 3년
DV인증서	0.5개월 ~ 3개월
IS인증서	1일 ~ 1개월

표3. 전자여권 PKI 인증서 유효기간

2.2 전자여권 판독

전자여권 판독을 위하여 ICAO 9303에서 규정하는 보안 메커니즘은 Passive Authentication(PA), Active Authentication(AA), Basic Access Control(BAC)이다.[2]

구분	기능	기술	구현
PA	Authenticity	Digital Signature	Mandatory
AA	Originality	Challenge-Response	Optional
BAC	Confidentiality	Authentication & Secure Channels	Optional

표4. ICAO 보안메커니즘

PA 과정은 다음과 같다. ①전자여권 칩에서 SOD를 읽는다. ②SOD 내부 또는 판독시스템에서 DS인증서를 찾고, 상위 CSCA인증서를 찾아낸다. ③DS인증서를 검증하고, DS인증서로 SOD서명을 검증한다. ④LDS의 DG에 대한 해쉬값을 계산하여 SOD로부터 추출한 해쉬값과 비교한다. 일치하면 PA성공이다.[2,8]

AA 과정은 ①판독시스템이 DG15로부터 AA 공개키를 획득하고, ② 랜덤하게 생성한 메시지를 전자여권에 전달한다. ③전자여권이 랜덤

[3] BSI, Bundesamt für Sicherheit in der Informationstechnik, 독일 정보보호 관련 기관
[4] CSCA, Country Signing Certificate Authority
[5] DS, Document Signer
[6] PKD, Public Key Directory, DS인증서 및 CRL보관
[7] CVCA, Country Verifying Certificate Authority
[8] DVCA, Document Verifying Certificate Authority
[9] IS, Inspection System, 판독시스템

메시지에 전자서명 하여 전달하면, ④판독시스템은 서명을 검증한다. 검증이 성공하면 AA를 통과한다.

BAC는 MRZ을 통해 추출한 암호화 및 MAC 세션키, K_{ENC}, K_{MAC}을 사용하여 세션 암호화(Secure Messaging)를 수행한다.

EU표준에서는 EAC를 위하여 추가적으로, Chip Authentication과 Terminal Authentication을 규정하고 있다. CA와 TA는 전자여권 판독 시 바이오정보에 접근을 허용하기 위해 정의된 프로토콜이다.

CA는 칩의 복제여부 확인과 세션 암호화를 동시에 수행한다. CA의 복제확인 기능이 AA의 기능과 유사한데, AA는 Challenge-Response 형태로, 판독기가 원하면 언제든지 개인정보를 수집할 수 있는 프라이버시 이슈[10]가 있다.

한편, CA는 BAC보다 키 엔트로피가 2배 이상인 Strong Session Key를 사용함으로써, 세션의 보안성을 강화한다. 이렇게 Challenge Semantics을 극복하고, 세션키 강도를 높이는 이유로 CA가 AA의 대안으로 간주된다.

TA는 전자여권의 지문정보에 접근할 때 판독시스템의 적합성을 판단하기 위한 용도로, 칩이 판독시스템의 인증서 체인(DVCA, IS 인증서) 검증과 판독시스템이 제공하는 전자서명 검증을 수행한다. CA 및 TA가 성공해야만 판독시스템이 지문정보를 읽을 수 있다.

EAC용 전자여권은 전자여권 칩과 판독시스템이 EAC 요건을 모두 만족할 경우, 아래와 같은 순서에 의하여 판독을 진행한다. BAC, CA, PA가 성공하면 DG1, DG2까지 데이터를 판독하여 칩 내 MRZ 정보와 사진정보를 판독시스템 화면상으로 확인할 수 있고, 이후 TA가 성공하면 칩의

지문을 읽어, Live Capture한 지문과 대조하여 본인임을 한번 더 확인 할 수 있다.

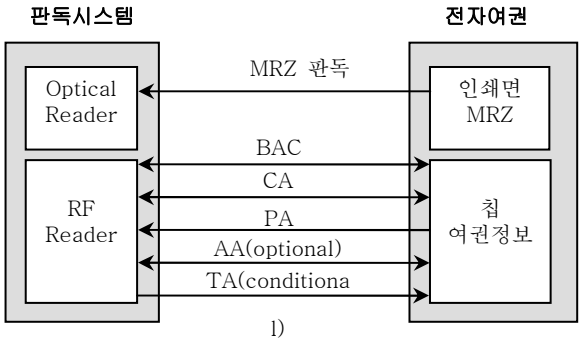


그림1. Advanced Inspection Procedure

[10] 이와 같은 AA의 단점을 Challenge Semantics라 함

2.3 세계 각국의 적용현황

[표1] 세계각국 전자여권 도입시기에서 보듯이, 미국의 비자 면제 프로그램의 요구에 따라 2005년과 2006년에 전자여권이 본격적으로 시행되기 시작하였다. 집계에 따르면, 44개국 중에서 36개국이 PA를 구현한 것으로 확인되었고, 그 중 태국과 소말리아는 BAC를 지원하지 않는다.

현재 전자여권에 지문을 넣은 국가는 말레이시아[11], 태국, 몰디브, 독일, 싱가포르이며, 상기한 바와 같이 EU 회원국들은 EAC를 적용하는 2009년에 지문을 추가할 것으로 예상된다.

AA를 지원하는 국가는 전자여권을 도입한 44개국 중 11개국에 불과하며, 그 중 9개국은 EU 회원국으로 EU Regulation에 의해 2009년 중반에 EU EAC 도입하여 CA로써 AA를 대체할 수 있다.[1]

2.4 GPKI/NPKI와의 차이

전자여권 PKI는 개인을 대상으로 인증서를 발급하지 않는다는 것이 GPKI/NPKI와 가장 구별되는 점이다. 여권 내에 저장되는 인증서는 DS인증서와 CVCA인증서 정보인데, 이들은 각각 SOD 검증과 바이오정보 판독에 사용된다.

GPKI/NPKI가 발급하는 인증서는 G2B, G2C,

B2B, B2C간의 정보전송의 무결성을 제공하기 위한 용도로 사용되며, 현재 배포된 공인인증서가 2007년 12월 현재 1,715만개로 광범위한 영역에서 범용적으로 사용되고 있다.

한편 전자여권 PKI 인증서는 공항 출입국 등의 특정 지역에 위치한 판독시스템이, 전자여권 칩 정보의 무결성을 검증하거나, 바이오 정보에 대하여 접근 허용 여부를 판단할 때 사용하는 등 범용적이기 보다는 특수 목적 용도의 인증서이다.

2.5 기술적인 이슈들

전자여권에 대한 호환성 이슈와 프라이버시 이슈를 식별하고, 이러한 위협에 대하여 가능한 대책을 살펴본다.

첫째, 호환성 이슈로서 AA 전자서명 프로토콜 표준에 관한 것이다. ICAO에서 규정하는 AA는 RSA 1024 비트 이상, DSA 1024 비트, 160 비트 이상, ECDSA 160 비트 이상을 사용할 것을 권장하고 있다. 그러나, AA를 위한 전자서명 프로토콜로서, "ISO 9796-2, RSA 기반 메시지 복원형 전자서명 프로토콜"만 명확하게 정의하고 있고, DSA 나 ECDSA 기반의 표준 프로토콜은 규정하지 않았다. 따라서, DSA 나

ECDSA 를 기준으로 AA 를 구현하는 경우, 상호호환성 확보가 가능하지 않다.[2]

둘째, ICAO 가 참조하는 DSA 표준의 최신화가 필요하다. ICAO 는 DSA 에 대하여 FIPS 186-2 를 따르게 되어 있다. 그러나, FIPS 186-2 에서는 512 비트 이상 1024 비트 이하만 정의하고 있어서, ICAO 가 권고하는 기준에 부합하도록 DS 인증서와 CSCA 인증서를 구현을 하더라도, 근거가 되는 표준이 없는 상황이다.

2006 년 3 월에 발표된 FIPS 186-3 Draft 는 3072 비트까지 지원하고 있으나, 현재 최종 완료되지 않고 있다. 따라서, DSA 를 사용하는 데에 있어서도 역시 호환성 확보의 문제점이 있다.

다행히, ICAO 표준을 따르는 43개국 중에서 DSA를 사용하여 CSCA인증서를 발급하는 나

라는 없으므로, 실제 환경에서 문제 발생가능성은 희박한 것으로 보여진다.

셋째, EU EAC 표준에서 정의하는 ECDSA 기반 인증서의 공개키와 개인키에서 호환성 문제가 발견된다. EAC 인증서 프로파일은 X.509 와 다르고, TLV형태로 정의된다. TLV 포맷이 ASN.1 과 다르다. ASN.1에서 정의하는 INTEGER는 "signed integer"를 의미하지만, EAC 표준에서 INTEGER는 "unsigned integer"를 의미한다. 또한 ECDSA 개인키의 Domain Parameter 포함여부가 명확하지 않아 판독과정에서 혼란이 야기될 수 있다.[8]

Data Object	Tag	Type	Certificate
Object Identifier	0x06	OID	mandatory
Prime modulus p	0x81	INTEGER	optional
First coefficient a	0x82	INTEGER	optional
Second coefficient b	0x83	INTEGER	optional
Base point G	0x84	Elliptic Curve Point	optional
Order of the base point r	0x85	INTEGER	optional
Public Point Y	0x86	Elliptic Curve Point	mandatory
Cofactor f	0x87	INTEGER	optional

표5. EAC ECDSA 공개키 포맷

또한, [표5]에서 정의하는 ECDSA 공개키 정보 중 optional 필드에 대한 명확한 기준이 없다.

같은 맥락에서 판독시스템에 대한 표준과 평가 기준이 현재 마련되지 않아, 각국에서 구축하는 판독시스템의 호환성의 확보가 불투명한 상황이다. 이와 같이, 전자여권 PKI의 호환성 측면에서 현재 좀더 명확하게 정의하여야 할 여지가 있다.

다음은 전자여권 관련 프라이버시 이슈와 그에 대한 대응책을 살펴본다. 여권 소지자가 인식하지 못하는 가운데 전자여권이 작동하여 정보가 노출되는 것을 Skimming이라 하고, 전자여권 칩과 판독기 간의 정상적인 통신을 원격에서 수신하는 경우를 Eavesdropping이라고 한다.

Skimming을 막기 위하여, 전자여권 표지에 RF신호 차단이 가능한 차폐막(Faraday Cage)을 적용할 수 있다. 간편하게는 차폐막 대신 쿠킹 호일로 전자여권을 감싸고, 사용 시에만 오픈 하여, 불필요한 외부의 RF신호를 차단하고 Skimming을 막을 수 있다. 차폐막이 적용된 여권은 판독시스템 구조에 적합하지 않아 판독과정의 불편함을 초래하고, 판독시간이 더 오래 소요되어, 실효성 면에서 부정적인 의견이 많으며 대다수 나라에서 채택되고 있지 않다.

Eavesdropping은 공항 등에서 판독하는 과정의 합법적인 통신을 할 때 발생하는데, 이것은 차폐막으로도 막기 힘들다. 따라서, 암호화 통신을 적용해야 한다.

Eavesdropping을 막기 위하여 BAC를 적용하는데, 세션키 엔트로피가 낮은 점이 문제점으로 지적되고 있다. BAC 세션키는 여권번호, 생년월일, 유효기간을 초기값으로 하여 생성되고, 9자리 여권번호, 10년 유효기간의 여권인 경우, 세션키의 엔트로피는 최대 56비트이다.[2]

네덜란드의 보안전문가는 체크디지트 고정 한자리와 순차 증가하는 여권번호 8자리를 사용하는 네덜란드 여권에 대하여, 일일 여권 발급량을 기반으로 특정기간의 여권번호를 추측하여, 실제 키 엔트로피를 35비트 정도까지 낮출 수 있었고, 그 결과 보통의 개인용 컴퓨터로 2시간 내에 깨질 수 있음을 증명하였다.[10]

따라서, 이러한 키 엔트로피 공격에 대하여, 여권번호의 추측가능성을 최소화할 수 있도록 여권번호를 랜덤하게 생성해야 한다.

또한 EAC용 여권의 경우 BAC 직후 CA를 수행하는데, CA를 수행함으로써 새로운 보안채널을 형성하고, 이때 사용하는 세션키 엔트로피는 112비트(ECDH 224 비트를 사용할 경우)이다. 따라서, CA를 적용함으로써 Eavesdropping 및 키 엔트로피 공격을 막을 수 있다.

3. 결론

지금까지 살펴본 바와 같이 전자여권 PKI 체계에 대한 호환성 확보를 위해서 EAC 표준에 대한 좀 더 명확한 정의가 필요하며, 판독시스템에 대한 표준 및 평가기준이 준비되어야 한다.

또한 프라이버시 이슈에 대한 적절한 대응책으로서, BAC 및 CA를 적용하여야 한다. 또한 BAC를 통한 보안채널 형성 시 seed로 사용하는 여권

[11] 말레이시아는 ICAO 표준을 따르지 않음

번호의 추측가능성을 최소화하기 위하여 여권번호 랜덤화가 구현되어야 한다.

공항 등 전자여권을 판독하는 공간에 허가되지 않은 판독장치에 대한 원천적인 차단이 가능하도록 물리적인 보안을 강화하여야 한다.

전자여권의 도입은 거부할 수 없는 전세계적인 흐름이며, 향후 몇 년 내에 범용적으로 사용될 신분확인 매체임에 틀림없다. 전자여권은 사진부착식/사진전사식 여권에 비하여, PKI를 포함한 다양한 안전장치를 가지고 있어 국제범죄예방에 기여하고, 연간 1,300만 해외여행객에 편의성 제공을 통해 국가간 인적 교류 증진의 핵심수단이 될 것이다.

[참고문헌]

[1] Worldwide Overview Introduction e-passports, Introduction dates and technical specifications, IF4TD, January, 2008

[2] ICAO 9303 specification 6th Edition, ICAO, 2006

[3] RFC 3280, R. Housley, W. Polk, W. Ford, D. Solo, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List(CRL) Profile", April, 2002

[3] FIPS 180-2, Federal Information Processing Standards Publication (FIPS PUB), 180-2, Secure Hash Standard, August, 2002

[4] X9.62, "Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)", January 7, 1999

[5] ISO/IEC 9796-2, Information Technology – Security Techniques – Digital Signature Schemes giving message recovery – Part 2: Integer factorization based mechanisms, 2002

[6] ICAO Technical Report, Development of a logical data structure, ICAO, May, 2004

[7] ICAO Technical Report, PKI for Machine Readable Travel Documents offering ICC Read-Only Access Version - 1.1, October, 2004

[8] BSI Technical Guideline TR-03110, Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Version 1.01, 2006

[9] BSI Technical Guideline: Elliptic Curve Cryptography(ECC) based on ISO 15946, Version 1.0. TR-03111, 2007

[10] Attacks on digital passports. In What the Hack, Liempde, near Den Bosch, The Netherlands. Marc Witteman.